A Comparative Study for New Aspects to Quantum Key Distribution

Prof. Dr. Siddeeq Y. Ameen
Computers and IT Eng. Department
University of Technology, Baghdad, Iraq

Asst. Lect. Salih H. Ali
Computers and IT Eng. Department
University of Technology, Baghdad, Iraq

Abstract

Quantum cryptography is anew branch of physics and cryptography which exploit quantum mechanical phenomena to guarantee the secrecy of cryptographic keys.

This paper introduces the basic concepts, problems and methods of quantum key distribution. It introduces some basic knowledge of quantum mechanics and explains how these physical laws can be used in cryptography.

The basic protocols of quantum cryptographic used for key distribution based on entangled polarization photons pair are also presented and assessed. The well known concepts based on entangled pairs of photons (Ekert) schemes are presented. In these schemes Alice and Bob perform measurements on each photon along one of two, three or four directions given by unit vectors α_i ***and*** β_j ***(i, j = 1, 2, 3,4) respectively. Therefore the combinations are used from Alice and Bob is four, nine, or sixteen with respect to number of measurement directions (i = 2, 3 or 4) respectively. The analysis and comparative study between these versions are presented.***

الخلاصـــــة

يعتبر التشفير الكمي فرعاً جديداً سواء بالنسبة للفيزياء أو لعلم التشفير والذي يعتمد على استخدام بروتوكولات مصممه للاستفادة من ظواهر الميكانيك الكمي لأجل ضمان سريه توزيع مفاتيح التشفير.

تناول هذا البحث المفاهيم والمشاكل والطرق المستخدمة في توزيع المفتاح الكمي وتم تناول بعض المعرفة في الميكانيك الكمي وتوضيح استخدام قوانين الفيزياء في التشفير.

تم دراسة وتحليل بروتوكولات التشفير الكمي الذي تعتمد على توزيع المفتاح الكمي باستخدام أزواج الفوتونات المتعاقدة من أهم البروتوكولات التي تعتمد على أزواج الفوتونات المتعاقدة هي بروتوكول (Ekert) وفي هذا البروتوكول (Bob, Alice) يستخدمون عدة اتجاهات (اثنان،ثلاثة،أو أربعة) اتجاهات لكشف الفوتونات وعلى هذا الأساس يكون عدد (المجاميع المؤتلفة) بين (Bob, Alice) أربعة، تسعة، ستة عشر مجموعه تبعاً لعدد الاتجاهات. تضمن البحث دراسة مقارنة وتحليل لبروتوكولات (Ekert) التي تعتمد على أزواج الفوتونات المتعاقدة.

1. Introduction

Classically, key distribution can be practically secure by some wise cryptographic systems, including symmetric cryptographic algorithm, Public Key Cryptography (PKC), etc.

Practically secure mean that, the required computational time and resources of breaking the key are simply beyond the human's capability and means. However, almost all the most cryptographic schemes can not be proven to be secure, that means those schemes may be broken theoretically. In 1994, Shor described a polynomial time quantum for factoring integers, which can be applied to break the public key cryptography, although the algorithm could not be implemented unless the quantum computer is invented [1]. Agrawal claimed an algorithm to distinguish prime number from composite numbers in polynomial time, which may lead to an efficient factoring method later to break the public key cryptography [2].

Quantum cryptography ensures perfect security based on accepted nature laws of quantum mechanics, while these wisest systems of classical cryptography can only assure unproven practical security. Thus quantum cryptography brings a new hope and will change aspects about cryptography and security.

Quantum cryptography offers several advantages over conventional key distribution schemes, these include:

i. It avoids the insider threat because key material does not exist before the quantum transmission takes place.

ii. It avoids the cumbersome physical security aspects of conventional key distribution methods.

2. Quantum Mechanics and Message Expression

Two aspects of knowledge of quantum mechanics need to be explored. One is the quantum state, which will be used to represent messages transferred in quantum channel. The other is how to apply quantum mechanics to ensure security in communication. Both of them are talking about the fundamental problems in quantum cryptographic key distribution.

Classically, analog/digital signals are used to represent each bit of the message, high voltage for 1, and low voltage for 0. However, in the case of quantum mechanics, other forms (Photon Polarization with orthogonal states), are used. To describe a photon, its property, such as polarization can be used. The experiment of photon polarization can be done only with a light source, a projection screen, and some polarization filters.

Suppose now we have two filters A and B. Filter A is polarized horizontally and filter B is polarized vertically, A and B have orthogonal direction of polarization. By inserting filter A between the light source and the screen (assume photons of incoming light are polarized randomly), the intensity of the outgoing light decrease to half of the incoming light while all the outgoing photons become horizontals polarized, which is the same direction of filter A as shown in **Fig.(1)**.

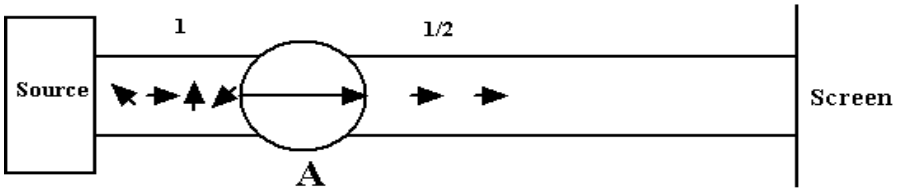


Figure (1) Photon polarization with horizontal state by using filter A

If filter A replaced by filter B then the outgoing photons become vertically polarized. Finally, by inserting filter B between filter A and the screen, the intensity of output drops to zero, which implies no photon from filter A would pass through filter B as shown in the **Fig.(2)**.

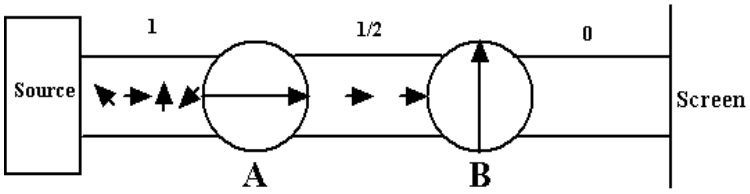


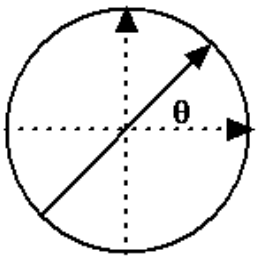
Figure (2) Photon polarization using two orthogonal filters

From the above experiments, the following can be summarized:

1. A polarized filter will absorb the photon with orthogonal direction of polarization;
2. A polarized filter will let the photon with the same direction of polarization pass through.
3. A photon, randomly polarized, will either annihilated by the filter, or pass through the filter with the same direction of the polarization as the filter.

Based on these facts, two photons with orthogonal direction of polarization can be distinguished, and represent the bits of messages by these orthogonal quantum states. A quantum state can be represented as a linear combination of the base states. For example, let $|\rightarrow\rangle$ **and** $|\uparrow\rangle$ denote the two base states of polarized photon. When filter A rotated at an angle θ to the position A', the polarization of photons passing through A would shift the same angle θ. Such a state can be represented as:

$$|\nearrow\rangle = \cos\theta\,|\rightarrow\rangle + \sin\theta\,|\uparrow\rangle \quad \text{..... (1)}$$



Thus any quantum state can be represented in the combination of base states. Moreover, the quantum states can be represented by polarization, positions, energies, spins, momentums, and so on, in terms of vectors and matrices or in the more compact bra/ket notation developed by Dirac [3].

The state of the Hilbert space H will be called kets. $|\mathbf{lable}\rangle$, where *lable* denotes some lable.

Suppose the base state of H is $\{|0\rangle,|1\rangle\}$, then the state $|S\rangle|$ in H can represent as:

$$|S\rangle = a\ |0\rangle + b\ |1\rangle$$

where:

a and b are two complex number and ($a^2 + b^2 = 1.$)

The two orthogonal states $|\rightarrow\rangle$ *and* $|\uparrow\rangle$ can be regarded as two base states $|0\rangle$ *and* $|1\rangle$ in the quantum system. The matching bra, denoted as $\langle lable|$, represents the conjugate transpose of $|lable\rangle$, combining $\langle x|$ *and* $|y\rangle$ as written as $\langle x|y\rangle$ *and* $|x\rangle\langle y|$ are the inner product and outer product of the two vectors, respectively.

Since $|0\rangle$, $|1\rangle$ are unit vectors i.e:

$\langle 0|0\rangle = 1$ (inner product of $|0\rangle$ *and* $|0\rangle$)

$\langle 0|1\rangle = \vec{0}$ (inner product of two orthogonal states $|0\rangle$ *and* $|1\rangle$

$|0\rangle\langle 0|$ is mapping from $|0\rangle$ *to* $|0\rangle$ and from $|1\rangle$ *to* $\vec{0}$.

$(|0\rangle\langle 0|)\ |0\rangle = |0\rangle\ (\langle 0|0\rangle) = |0\rangle$

$(|0\rangle\langle 0|)\ |1\rangle = |0\rangle\ (\langle 0|1\ \rangle) = \vec{0}$

The bra ($|0\rangle\langle 0|$) can be used to represent the filter A, and the bra ($|1\rangle\langle 1|$) to represent the filter B, i.e:

$(|1\rangle\langle 1|)\ |0\rangle = |1\rangle\ (\langle 1|0\rangle) = \vec{0}$

$(|1\rangle\langle 1|)\ |1\rangle = |1\rangle\ (\langle 1|1\ \rangle) = |1\rangle$

Furthermore, for any state $|\mathbf{S}\rangle = \mathbf{a}\ |\mathbf{0}\rangle + \mathbf{b}\ |\mathbf{1}\rangle$, the state after operation by $|0\rangle\langle 0|$ becomes:

$$|0\rangle\langle 0| \ |S\rangle = |0\rangle\langle 0| \ (a|0\rangle + b|1\rangle)$$

$$= |0\rangle\langle 0| \ (a|0\rangle) + |0\rangle\langle 0| \ (b|1\rangle)$$

$$= a(|0\rangle\langle 0| \ |0\rangle) + b(|0\rangle\langle 0| \ |1\rangle)$$

$$= a|0\rangle + \vec{0}$$

$$= a|0\rangle$$

Suppose $|0\rangle$, $|1\rangle$ are two basic orthogonal states in quantum system H, then state $|0\rangle$, $|1\rangle$ can be used to represent the classical bit values 0 and 1 respectively. Thus the message M with L bits can be represented by L quantum states, in the form of $|\mathbf{x_0}\rangle \ |\mathbf{x_1}\rangle \ldots\ldots\ldots |\mathbf{x_{n-1}}\rangle$. When sending M, the sender can use the operator $|\mathbf{0}\rangle\langle\mathbf{0}|$ and $|\mathbf{1}\rangle\langle\mathbf{1}|$ to generate states $|0\rangle$ *and* $|1\rangle$, respectively. The receiver can use $|\mathbf{0}\rangle\langle\mathbf{0}|$ or $|\mathbf{1}\rangle\langle\mathbf{1}|$ to distinguish each bit of M. **Figure (3)** represents the message expression and its transfer in a noiseless quantum channel.

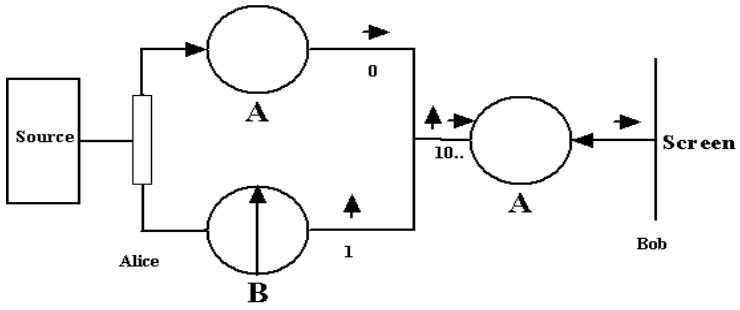


Figure (3) Message expression and its transfer in a noiseless channel

3. Communication Security

The classical way of security is unproven to be absolute secure, and more over, it is even difficult to detect whether or not the message has been accessed by eavesdropper without authority. This kind of eavesdropping detection can be achieved in the way of quantum mechanics. The non orthogonal quantum states can be used instead of orthogonal ones to express the transferring messages. This may introduce uncertainty into measurements, which can force Eve to leave disturbance for being detected. In practical experiment shown in **Fig.(2)**, two filters with orthogonal polarizations were used. Now filter C will be used, which is polarized at 45°. Thus C is neither orthogonal to A nor to B. After placing C between filter A and B, a small amount of light on the screen can be observed, exactly 1/8 of the original amount of light. This result is different from the result of practical experiment shown in **Fig.(2)** in which nothing is observed on the screen.

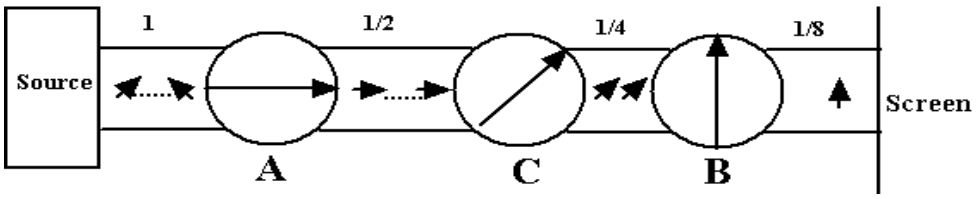


Figure (4) Message transfer expression by non orthogonal states

3.1 Probability Amplitude and Measurement

Suppose $\{ |0\rangle, |1\rangle \}$ is the base state then $|S\rangle = a|0\rangle + b|1\rangle$ (Linear combination of base states).

In fact the quantum mechanics claims that the probability of transforming $|S\rangle$ **to** $|0\rangle$ **by** $|0\rangle\langle 0|$ **is** a^2 observing that:

$$\langle 0|S\rangle = \langle 0| \ (a|0\rangle)$$

$$= a$$

This probability actually equals to $\|\langle 0|S\rangle\|^2$ while the probability of $|1\rangle$ to be the final state is $\|\langle 1|S\rangle\|^2$.

3.2 Eavesdropping Detection

In quantum system the eavesdropper can be detected because any measurement of quantum state in the channel will transform state and lead disturbance with a special probability. Based on this fact, the message transferred in quantum channel can be protected. In **Figure (5)**, Alice sends a message M with L bits to Bob. Alice and Bob can choose one of the two orthogonal states, $\{|\uparrow\rangle, |\rightarrow\rangle\}$ **and** $\{|\nearrow\rangle, |\nwarrow\rangle\}$, to represent the messages. Suppose they choose $\{|\uparrow\rangle, |\rightarrow\rangle\}$ securely, then for each bit valued '0', Alice sends photons through the filter A, while for '1' through filter B. Bob still places a filter A before screen to see whether light can be observed. If light is observed on the screen, Bob will know that '0' is received; otherwise '1' is received. This time, Eve tries to eavesdrop by measuring photons before its arrival at Bob's filter.

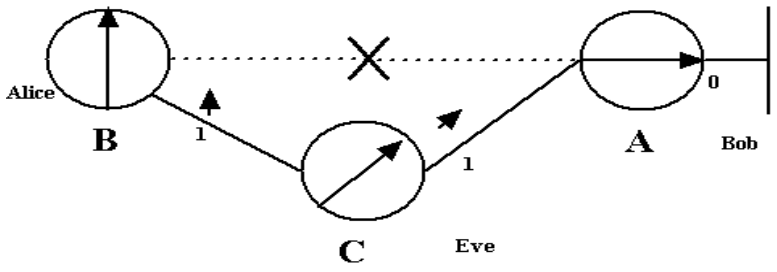


Figure (5) The disturbance that introduced from Eavesdropping

Now a simple situation, can be considered in which Eve does not know which orthogonal states Alice and Bob's chose to represent the messages. Thus, Eve have to guess which filter should be used. To measure $\{|\uparrow\rangle,|\rightarrow\rangle\}$, Eve should choose filter A; whereas to measure $\{|\nearrow\rangle,|\nwarrow\rangle\}$ Eve should choose filter C. Suppose for each bit, Eve choose one of the two filters in the same probability. Thus, if Eve chooses filter A, the state of photon will be observed without any disturbance because Eve's filter is the same Bob's filter. However if Eve chooses the wrong filter, i.e. C, then Eve will disturb the observation of Bob. Suppose Alice use filter A to send a photon P with state $|\uparrow\rangle$ for transferring bit valued '1', and Eve uses a filter C. The filter C can be represented as the projection operator $|\nearrow\rangle\langle\nwarrow|$ Thus P can pass through Eve's filter C with probability 1/2. Afterward, P will be transformed to the state $|\nearrow\rangle$, and can pass through Bob's filter A with probability 1/2 too. Thus the probability that the photon can not arrive at Bob's screen is 3/4, this will make Bob's think to receive '0', while Alice sending '1'. For a similar reason, when Alice sending '0', 1/4 photons will arrive at Bob's screen, then Bob will think to receive '1'. Thus, in the case of Eve choosing a filter C for measurements, if Alice send '0' and '1' with the same probability, the average error rate between Alice and Bob will become (3/4 + 1/4)*1/2=1/2. Since Eve choose the two filters, A and C, will the same possibility, the average error rate between Alice and Bob will be 1/4, unlike in the case without eavesdropping, where the error rate is always zero.

Based on this fact, Alice and Bob can detect eavesdropping by checking a set of their bits, if they find a number of errors, they should not trust their message as secure, because eavesdropping may be happened with high probability. Thus the security is ensured. However, the following three assumptions of the above scheme may not be reasonable in real case.

i. Alice and Bob can securely determine the base state they used.
ii. Eavesdropping is restricted to use simple measurement to steal the information;
iii. There is no noise in the channel such that Bob can receive the photon Alice sends exactly.

4. Analysis of Quantum Key Distribution Based Entangled Photons

Quantum cryptography can be classified into two major categories: QC based on single photons and QC based on photon pairs. The well-known concept for quantum key distribution based on single photon is the BB84 scheme. The BB84 scheme [4] uses single photons transmitted from Alice to Bob, who are prepared at random in four partly orthogonal polarization states: 0°, 45°, 90°, and 135°. If Eve tries to extract information about the polarization of the photons she will inevitably introduce errors, which Alice and Bob can detect by comparing a random subset of the generated keys.

The other well-known concept for quantum key distribution that is based on entangled pairs of photons is the Ekert scheme [5]. In this scheme the channel consists of a source that emits pairs of spin 1/2 particles, in a single state. The particles fly apart along the z axis, towards the two legitimate users of the channel, say Alice and Bob. After the particles have

separated, Alice and Bob perform measurements on spin components along one of three directions given by unit vectors α_i and β_j (i,j=1,2,3) , respectively. For simplicity, both α_i and β_j vectors lie in the x-y plane, perpendicular to the trajectory of the particles, and are characterized by azimuthally angles : $\alpha_1=0^\circ$, $\alpha_2=45^\circ$, $\alpha_3=90^\circ$ and $\beta_1=45^\circ$, $\beta_2=90^\circ$, $\beta_3=135^\circ$. The angles are measured from the vertical x-axis. Alice and Bob choose the orientation of the analyzers randomly and independently for each pair of incoming particles. Each measurement, in 1/2 h unit, can yield two results, +1 (spin up) and -1 (spin down), and can potentially reveal one bit of information. The quantity is the correlation coefficient of the measurements performed by Alice along α_i and by Bob along β_j.

$$\mathbf{E(\alpha_i,\beta_j) = P_{++}(\alpha_i,\beta_j) + P_{--}(\alpha_i,\beta_j) - P_{-+}(\alpha_i,\beta_j) - P_{+-}(\alpha_i,\beta_j)} \quad \text{..... (2)}$$

Here $P_{\pm\mp}(\alpha_i,\beta_j)$ denotes the probability that the result ±1 has been obtained along α_i and ±1 along β_j. For the two pairs of analyzers of the same orientation (α_2, β_1 and α_3, β_2) quantum mechanics predicts total anti correlation of the results obtained by Alice and Bob, i.e.

$$\mathbf{E(\alpha_2,\beta_1) = E(\alpha_3,\beta_2) = -1} \quad \text{..... (3)}$$

Which then constitute the quantum cryptographic key. As indicated in **Table (1)**, the result of other combinations (different orientation) are revealed and used in test of Bell inequalities, to check the presence of the eavesdropper ("Eve").

$$\mathbf{S = E(\alpha_1,\beta_1) - E(\alpha_1,\beta_3) + E(\alpha_3,\beta_1) + E(\alpha_3,\beta_3)} \quad \text{..... (4)}$$

Again, quantum mechanics requires $S = -2\sqrt{2}$

Table (1) Distribution of data dependent on Alice's and Bob's respective phase setting α_i and β_j

		Alice		
		$\alpha_1 = 0$	$\alpha_2 = \frac{\pi}{4}$	$\alpha_3 = \frac{\pi}{2}$
Bob	$\beta_1 = \frac{\pi}{4}$	S	Key	S
	$\beta_2 = \frac{\pi}{2}$	--------	--------	Key
	$\beta_3 = \frac{3\pi}{4}$	S	--------	S

As seen in **Table (1)**, only 2/9 of the data actually contribute to the row cryptographic key; 4/9 of the data used to test Bell's inequalities; and 3/9 are not used at all. The eavesdropper cannot elicit any information from the particles while in transit from the source to the legitimate users, simply because there is no information encoded there. The information "comes into being" only after the legitimate users perform measurements and communicate in public after words.

P.G. Kwiat investigates other version of the Ekert protocol [6]. In this protocol "Alice and Bob each receive one photon of a polarization-entangled pair in the state $|\phi^+\rangle = (|H_1H_2\rangle + |V_1V_2\rangle)/\sqrt{2}$, where H (V) represents horizontal (vertical) polarization. Each, respectively, measures the polarization of there photons in the bases $(|H_1\rangle + e^{i\alpha}|V_1\rangle$ **and** $(|H_2\rangle + e^{i\beta}|V_2\rangle)$, where α and β randomly take on the values: $\alpha_1 = \frac{\pi}{4}, \alpha_2 = \frac{\pi}{2}, \alpha_3 = \frac{3\pi}{4}, \alpha_4 = \pi$; $\beta_1 = 0, \beta_2 = \frac{\pi}{4}, \beta_3 = \frac{\pi}{2}, \beta_4 = \frac{3\pi}{4}$. they then disclose by public discussion which bases used are disclosed by public discussion, but not the measurement results. For the state $|\phi^+\rangle$, the probabilities for a coincidence between Alice's detector 1 (or 1', which detects the orthogonally polarized photons) and Bob's detector 2(2') are given by [6],

$$P_{12}(\alpha,\beta) = P_{1'2'}(\alpha,\beta) = [1+\cos(\alpha+\beta)]/4$$
$$P_{12'}(\alpha,\beta) = P_{1'2}(\alpha,\beta) = [1-\cos(\alpha+\beta)]/4 \quad \text{..... (5)}$$

When $\alpha + \beta = \pi$, a completely correlated results will be available, which then constitute the quantum cryptographic key. As indicated in **Table (2)**, the results from other combinations are revealed and used in two independent tests of Bell's inequalities, to check the presence of eavesdropper ("Eve").

Table (2) Distribution of data dependent on Alice's and Bob's respective phase setting α_i and β_j

		Alice			
		$\alpha_1 = \pi/4$	$\alpha_2 = \pi/2$	$\alpha_3 = 3\pi/4$	$\alpha_4 = \pi$
Bob	$\beta_1 = 0$	S	-----	S	Key
	$\beta_2 = \pi/4$	-----	S'	Key	S'
	$\beta_3 = \pi/2$	S	Key	S	-----
	$\beta_4 = 3\pi/4$	Key	S'	-----	S'

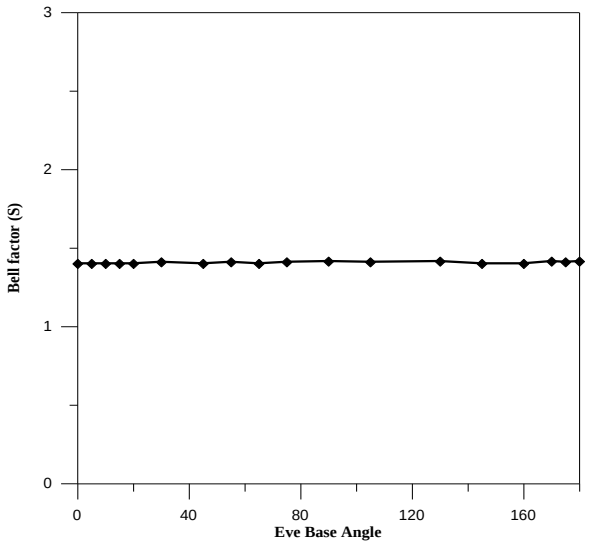
As shown in **Table (2)**, only 1/4 of the data actually contribute to the raw cryptographic key; 1/2 of data are used to test Bell's inequalities; and 1/4 of data are not used at all. In this version the authors used elliptical polarization analysis (i.e. on the plane containing the circularly polarized poles of the sphere and the ± 45° linearly polarized states), instead of using linear polarization analysis (i.e. in the equatorial plane of the Poincar'e sphere). In particular, the Bell parameters [7].

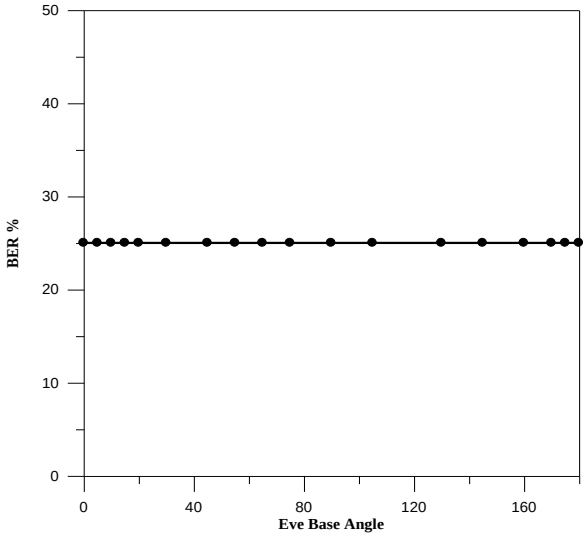
$$S = -E(\alpha_1,\beta_1) + E(\alpha_1,\beta_3) + E(\alpha_3,\beta_1) + E(\alpha_3,\beta_3),$$
$$S' = E(\alpha_2,\beta_2) + E(\alpha_2,\beta_4) + E(\alpha_4,\beta_2) - E(\alpha_4,\beta_4) \quad \text{..... (6)}$$

where:

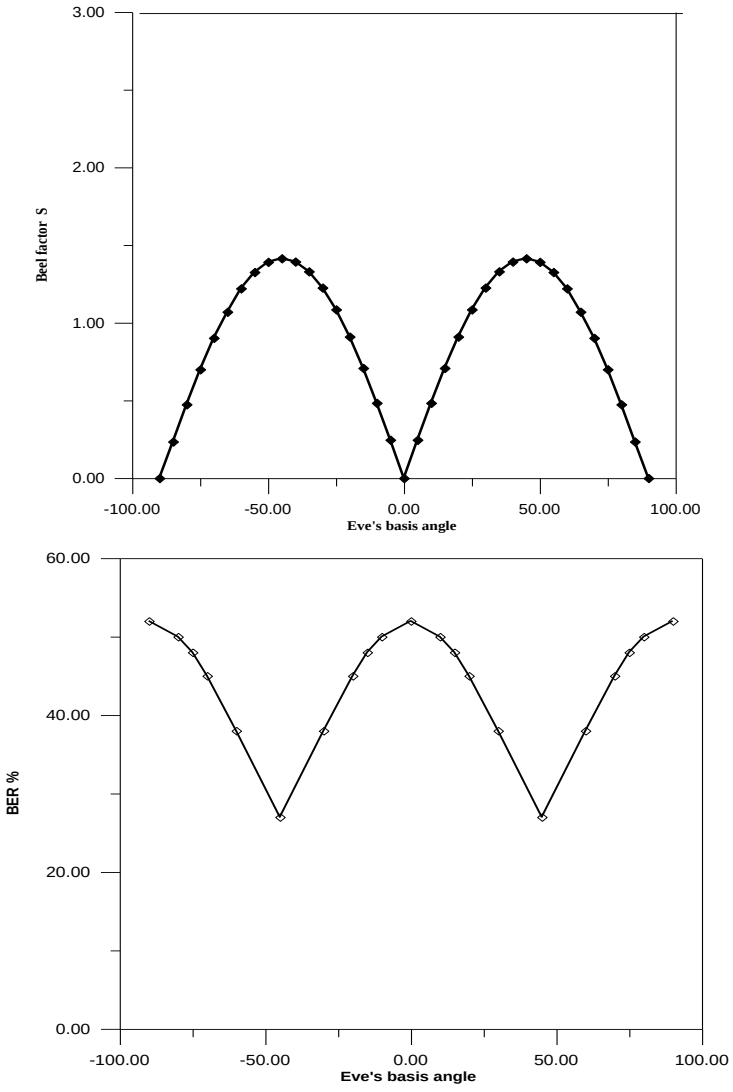
$$E(\alpha,\beta) = \frac{R_{12}(\alpha,\beta) + R_{1'2'}(\alpha,\beta) - R_{12'}(\alpha,\beta) - R_{1'2}(\alpha,\beta)}{R_{12}(\alpha,\beta) + R_{1'2'}(\alpha,\beta) + R_{12'}(\alpha,\beta) + R_{1'2}(\alpha,\beta)} \quad \text{..... (7)}$$

And the R's are the various coincidence counts between Alice's and Bob's detectors. For any local realistic theory $|S|,\ |S'| \le 2$, while for the combinations of α and β indicated in **Table (2)**, the quantum mechanically expected values of $|S|,\ |S'|$ **are** $2\sqrt{2}$. In fact if the eavesdropper measures one photon from every pair, then $|S_{eve}| \le \sqrt{2}$ [6]. Because high values of $|S|,\ |S'|$ have been observed in this system, the presence of an eavesdropper could thus be detected in ~1 sec of data collection. The simulated eavesdropper thus makes the projective measurement $|X\rangle\langle X|$. The effect on the measured value of S and S' and BER depend strongly on what eavesdropping basis $|X\rangle$ is used [8]. Theoretical predications and results for bases in two orthogonal planes in the Poincare sphere are shown in **Fig.(6)**.





(a)



(b)

Figure (6) Shows the effect of the eavesdropper on S and BER for various attacks bases:

(a) $|H\rangle + e^{i\phi}|V\rangle$, **(b)** $\cos\theta|H\rangle + \sin\theta|V\rangle$

Anton Zeilinger investigates other scheme utilizes Wigner's inequality [9], for establishing the security of the quantum channel, based on polarization entangled photon pairs in the single state:

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left[\left|H\right\rangle_1\left|V\right\rangle_2 - \left|V\right\rangle_1\left|H\right\rangle_2\right]$$

where, photon 1 is sent to Alice and photon 2 is sent to Bob, H and V are the horizontal and vertical linear polarization, respectively. This state shows perfect anti correlation for polarization measurements along parallel but arbitrary axes. However, the actual outcome of an individual measurement on each photon is inherently random. These perfect anti correlations can be used to generate the keys, yet the security of the quantum channel remains to be ascertained by implementing a suitable procedure. In order to implement quantum key distribution, Alice and Bob vary the analyzers randomly between two settings, Alice ($\alpha_1 = -30^{\circ}, \alpha_2 = 0^{\circ}$) and Bob ($\beta_1 = 0^{\circ}, \beta_2 = 30^{\circ}$), This allows the generation of keys via the perfect anti correlations, with the possible results +1 and -1 on photon 1, 2. Polarization parallel to the analyzer axis corresponding to a +1 result, and polarization orthogonal to the analyzer axis corresponds to -1. The probabilities for obtaining +1 on both sides, P_{++} must obey Wigner's inequality;

$$\mathbf{W = P_{++}(\alpha_1,\beta_2) + P_{++}(\alpha_2,\beta_2) - P_{++}(\alpha_1,\beta_2) \geq 0} \quad \text{..... (8)}$$

where, $\mathbf{P_{++}^{qm}(\alpha,\beta) = \frac{1}{2}\sin^2(\alpha-\beta)}$ is the quantum prediction for probabilities.

The analyzer setting at ($\alpha_1 = -30^{\circ}, \alpha_2 = 0^{\circ}$) and ($\beta_1 = 0^{\circ}, \beta_2 = 30^{\circ}$) leads to a maximum violation of Wigner's inequality:

$$\mathbf{P_{++}^{qm}(-30^{\circ},0^{\circ}) + P_{++}^{qm}(0^{\circ},30^{\circ}) - P_{++}^{qm}(-30^{\circ},30^{\circ}) = \frac{1}{8}+\frac{1}{8}-\frac{3}{8} = -\frac{1}{8} < 0}$$

Because Alice and Bob operate independently, four possible combinations of analyzer setting will occur, of which three oblique settings allow a test of Wigner's inequality and the remaining combination of parallel settings (α=0, β=0) allows the generation of keys via the perfect ant correlations, where either Alice or Bob has to invert all bits of the key to obtain identical keys. As seen in **Table (3)**, 1/4 of the data actually contribute to the raw cryptographic key; 3/4 of the data are used to test Wigner's inequality; there is no data that are not used.

Table (3) Distribution of data dependent on Alice's and Bob's respective phase setting α_i and β_j

		Alice	
		$\alpha_1 = -30^\circ$	$.\alpha_2 = 0^\circ$
Bob	$\beta_1 = 0^\circ$	W	Key
	$\beta_2 = 30^\circ.$	W	W

5. Conclusion

In summary, the paper presented the first implementation of Ekert quantum cryptography protocol using entangled photon pairs, with different numbers of combinations depending on the analyzer setting of Alice and Bob. These systems are secure even though no rapid switching is employed, since only one photon pair event is used for any particular $\alpha - \beta$ setting. From the analysis presented, it is believed that this work demonstrates that entanglement based cryptography can be a tomorrow's technology.

6. References

1. Shor, ***"Algorithms for Quantum Computation Discrete Log and Factoring"***, Proceedings of the 35th Annual Symposium on Foundation of Computer Science, Institute of Electrical and Electronic Engineers computer Society Press, 1994.

2. M. Agrawal, and Saxena N. Primes in ***http://www.cse.iitk.ac.in/news/primality.pdf***, 2002.

3. Dirac, ***"The Principles of Quantum Mechanics"***, 4th Edition, Oxford University Press, 1958.

4. C. H., Bennett, and G., Brassard, ***"Quantum Cryptography: Public Key Distribution and Coin Tossing"***, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984, pp. 175-179.

5. A. K., Ekert, ***"Quantum Cryptography Based on Bell's Theorem"***, Phys. Rev. Lett., Vol. 67, No. 6, 1991, pp. 661-663.

6. D. S., Naik, and et. al., ***"Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol"***, Phys. Rev. Lett., Vol. 84, No. 20, 2000, pp. 4733-4736.

7. J. S., Bell., ***"The Generalized Bell's Theorem"***, Physics, Long Island City, N. York, 4, 195, 1965.

8. C. H., Bennett, ***"Quantum Cryptography Using any Two Nonorthogonal States"***, Phys. Rev. Lett., Vol. 68, 1992, pp. 3121-3124.

9. T., Jennewein, and et. al., ***"Quantum Cryptography with Entangled Photons"***, Phys., Rev., Lett., Vol. 84, N. 20, 2000, pp. 4729-4732.