Modeling and Simulation of Schematic Quantum Cryptography System Based Entangled Photons

Siddeeq Y. Ameen*, Mohammed A. Abdala and Salih H. Ali***

Received on :27/12/2005
Accepted on :1/6/2006

Abstract

The paper investigates many problems in quantum systems by using the modeling of optical components using Jones matrices. These methods give high flexibility to choose perfect model and ideal measurements base of Alice and Bob. The simulated source uses polarization entangled photons from spontaneous parametric down-conversion. The proposed model of Ekert's quantum cryptography protocol, is also simulated based on modeling the optical components by Jones matrices. Bell's inequality is computed to detect the eavesdropper. The results show the effect of the eavesdropper on the Bit Error Rate (BER) and S factor of Bell's inequality. The eavesdropper affects more on the results of S and BER when he doesn't know the base measurements of Alice and Bob.

الخلاصة

أكتشف البحث عدد من المشاكل بأنظمة التشفير الكمية معتمدا على طرق تمثيل الأجزاء الضوئية بأستخدام مصفوفات Jones والتي توفر مرونة عالية في أختيار التمثيل الأفضل والأختيار الأمثل لمستوى زوايا قياس الفوتونات المستقطبة من قبل Alice & Bob.

تم محاكاة الحاسبة لتمثيل مصدر فوتونات (SPDC type II) لتوليد ازواج الفوتونات المتعاقده استقطابيآ وتم محاكاة الحاسبة لتنفيذ نموذج مقترح لبروتكول Ekert مستخدمآ تمثيل الاجزاء الضوئيه في النظام باستخدام ممفوفا ت Jones وتم حساب متراجحة Bell لكشف الاستراق . اظهرت النتائج تأثير الاستراق على (BER) و (المعامل S لمتراجحة Bell) فأن المسترق سوف يكون تأثيره كبير وواضحآ على (BER) و (S) في حالة عدم معرفة المسترق لمستوى زوايا القياس الذي يستخدمه كل من (Alice) و (Bob).

1. Introduction

Usually the encryption and decryption algorithms are publicly known, and the security of the cryptogram depends entirely on the secrecy of the key. This key should supply together with the plaintext as an input to the encrypting algorithm, and together with the cryptogram as an input to the decrypting algorithm [1]. In classical cryptography although there is truly unbreakable system (perfectly secure one time pad) there is a snag, it is called key distribution [2]. Once the key is established subsequent communication involves sending cryptogram over channel, even one which is vulnerable to total passive eavesdropping. In principle any classical key distribution can always be passively monitored, without the legitimate users being a ware that any eavesdropping has taken place. To solve

the key distribution problem, there are two very interesting solutions, one mathematical and one physical. The public key cryptography is the mathematical one. The physical one is referred to as quantum cryptography.

Quantum cryptography ensures the perfect security based on the accepted natural laws of quantum mechanics. The origins quantum cryptography can be traced to the work of Wisner in the early 1970s, who proposed that if single quantum states could be stored for long periods of time they could be used as counterfeit proof money.

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 uses single photons transmitted from Alice to Bob, who are prepared at random in four partly orthogonal polarization states 0°, 45°, 90°, and 135° [3]. 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. Other protocols based on non orthogonal quantum states uses single photons transmitted from Alice to Bob [4, 5]. The security of these protocols relies on the impossibility of measuring the wave function of a quantum system without imposing a back action on the state. This back action will usually result in an increase in errors across the communication channel.

In 1991, Ekert proposed the well known protocol that quantum key distribution could also be implemented using entanglement between quantum systems [6]. This scheme is based on the Bohm's well known version of the Einstein-Podolsky-Rosen (EPR) gendanken experiment [7]. The generalized Bell's theorem (Clauser-Horne-Shimony-Holt inequalities) is used to detect the eavesdropping [8]. The idea of using entangled photons for quantum cryptography was extended by Bennett, Brassad, and Mermin to the two photon variant of BB84 [9]. In 1995, Kwiat proposed a new high-intensity source of polarization- entangled photon pairs. This source type II non collinear phase matching in parametric down conversion produces true entanglement. No part of the wave function must be discarded, in contrast to previous schemes. The new source allowed ready preparation of all four of the EPR- Bell states. Anton Zeilinger *et al.* utilizes this new source to establish highly secure keys by realizing a quantum cryptography system based on polarization entangled photon pairs. The naval key distribution scheme was implemented using Wigner's inequality to test the security of the quantum channel [10]. Kwiat used polarization-entangled photons from spontaneous parametric down conversion to implement Ekeret's quantum cryptography protocol. The presence of an eavesdropper is continually checked by measuring Bell's inequalities [11]. By using polarization entangled photons from spontaneous parametric down-conversion, the Ekert's quantum cryptography protocol was simulated based on modeling the optical components by Jones matrices. Bell's inequality is computed continually to check or detect the eavesdropper.

2. Modeling of Optical Components Based on Ray Matrices

The optical axis is commonly defined as the z direction is shown in Fig. 1. The analysis of rays which are in the same plane as the z-axis is sufficient. The distance of such a ray from this axis is w and its slope is w'. Both parameters

are function of z and can be combined into the ray vector

$$\text{Ray vector} \begin{bmatrix} w(z) \\ w'(z) \end{bmatrix} \quad (1)$$

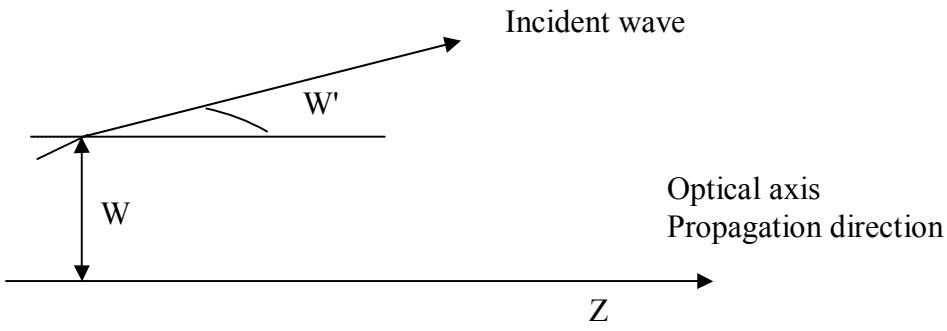

Fig. (1) Beam characteristics of optical rays in geometrical optics

When the rays are not in a plane with the z-axis, then the ray vector with four parameters is necessary as shown in Fig. 2. The four parameters, two distances u, v and two slops u', v' are analogous to the two parameters, case collected in a ray vector

$$\text{Ray vector} \begin{bmatrix} u(z) \\ v(z) \\ u'(z) \\ v'(z) \end{bmatrix} \quad (2)$$

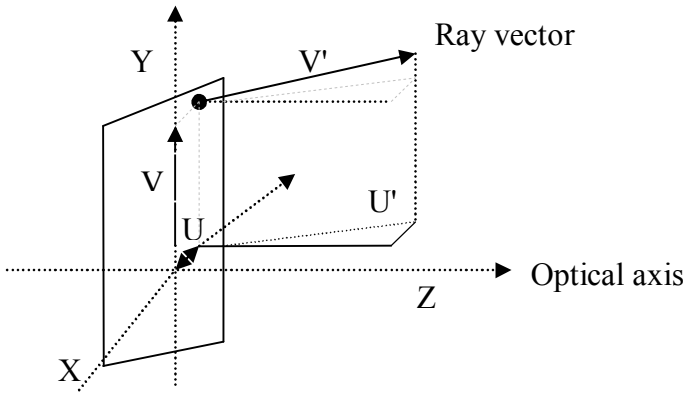

Fig. (2) Definition of parameters for rays not in planes with the z-axis

Imaging and illumination with incoherent light can be calculated to a good approximation by determining the beam propagation of the optical rays. This can be done with ray tracing or for paraxial rays with ray matrices. In ray tracing fore large number of geometrical optical rays the propagation is calculated and then superimposed for determining the intensity distributions. When many optical elements are in the path, the method of ray matrices is very handy. In this formalism the optical path including all optical elements is described with a ray matrix M as shown in Fig. 3

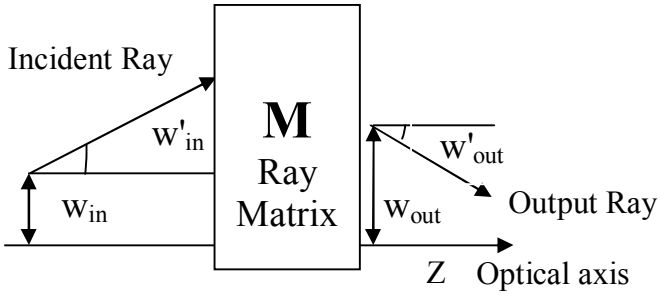

Fig. (3) Optical ray passes optical elements with the total matrix M

The ray vector behined a system of optical elements, including the optical paths in vacuum (or air), can be calculated from the incident ray vector and the total ray matrix M total as a simple multiplication

$$\begin{bmatrix} w_{out} \\ w'_{out} \end{bmatrix} = M_{total} \begin{bmatrix} w_{in} \\ w'_{in} \end{bmatrix} \qquad (3)$$

where

$$M_{total} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad (4)$$

or

$$\begin{bmatrix} u_{out} \\ v_{out} \\ u'_{out} \\ v'_{out} \end{bmatrix} = M_{total} \begin{bmatrix} u_{in} \\ v_{in} \\ u'_{in} \\ v'_{in} \end{bmatrix} \qquad (5)$$

where

$$M_{total} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \qquad (6)$$

The light beams should be paraxial with sufficiently low divergence similar to the ray optics. Gaussian beams are characterized by the Gaussian shape of the transversal profile of the beam. The electric field is given by in the transversal x or y directions which are replaced by r and the propagation direction z as [12]:

$$|E(z,r\}| = \mathrm{Re}\{E_A(z,r)\}\ \ \mathrm{Re}\{e^{i(2\pi\nu t - k_\circ z)}\} \tag{7}$$

Where

ν is the optical frequency

$k_\circ$ is the wave vector in free space

$$E_A(z,r) = \frac{|E_\circ|}{1-\frac{iz\lambda}{w_\circ^2 n\pi}}\ e^{-\frac{r^2/w_\circ^2}{1-iz\lambda/w_\circ^2 n\pi}} \tag{8}$$

with a maximum $|E_\circ|$ at z = 0.

The beam radius w (z) of Gaussian beams are completely determined by the position $z_{w_\circ}$, the size of the waist $w_\circ$, wavelength λ and material refractive index n by [12]

$$\text{beam radius } w(z) = w_\circ\sqrt{1-(\frac{z_{w_\circ}\lambda}{w_\circ^2 n\pi})^2} \tag{9}$$

Which can be written by using the Rayleigh length as [12]

$$w(z) = \sqrt{\frac{\lambda}{n\pi}(z_R + \frac{z_{w_\circ}{}^2}{z_R})} \tag{10}$$

where z_R is the Rayleigh length of a Gaussian beam given by

$$z_R = \frac{n\pi}{\lambda_\circ}w_\circ^2 = \frac{|k|}{2}w_\circ^2 \tag{11}$$

with wave vector k and refractive index of material n.

The shape of the phase fronts of the Gaussian beam can also be derived. They have a spherical shape their radius R (z) is given by wave front radius

$$R(z) = z + \frac{1}{z}(\frac{w_\circ^2 n\pi}{\lambda})^2 \tag{12}$$

The ray matrices can be used for theoretical propagation of simple rays in the sense of geometrical optics or for the propagation of diffraction limited Gaussian beams described by their beam parameter. Ray matrices can be derived by calculating the ray or beam parameters behind the optical element using Maxwell's equations or derived formulas and comparing the coefficients of these equations with the matrix elements. Fig. 4 represents the simplest case of ray propagation over length L in free space.

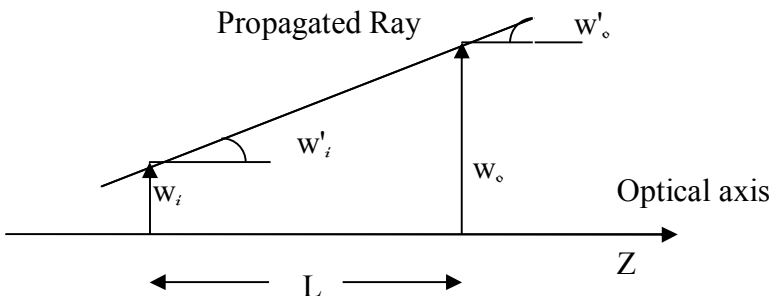

Fig. (4) Ray propagation over length L in free space

The ray equations would be

$$w_\circ = w_i + w_i'.L$$
$$w_\circ' = w_i' \qquad (13)$$

and matrix multiplication

$$\begin{pmatrix} w_\circ \\ w_\circ' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} w_i \\ w_i' \end{pmatrix} \qquad (14)$$

will lead to:

$$w_\circ = aw_i + bw_i'$$
$$w_\circ' = cw_i + dw_i' \qquad (15)$$

then a=1, b=L, c=0 and d=1

Thus the matrix for any optical element can be developed as long as the light path through these elements is reversible. If light passes n optical elements each recognized by one matrix *Mi* as shown in Fig. 5. The total matrix is then simply given by the product of all these matrices in the right order:

$$M_{total} = M_n.M_{n-1}.....M_2.M_1 \qquad (16)$$

It should be noted that the passed optical element first, with the matrix M_n is the last one to be multiplied as given in formula above.

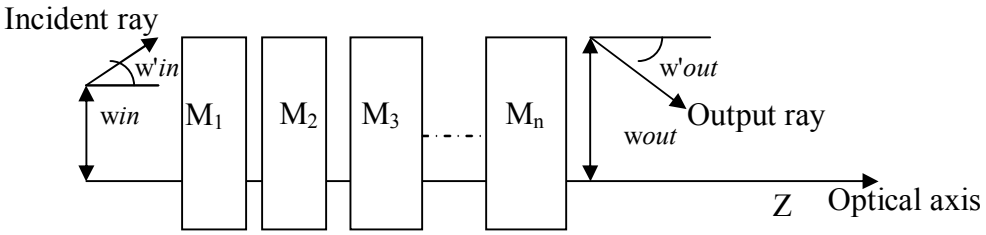

Fig. (5) Light passing through a sequence of optical elements as described by their matrices Mi

For the description of linear, circular or elliptical polarized light with Jones vectors. Cartesian coordinates are assumed with z axis pointing in the beam propagation direction as shown in Fig. 6.

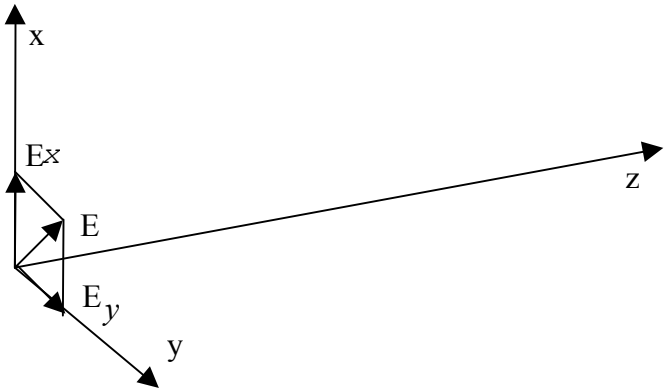

Fig. 6 Components of the electric light wave field at a certain moment.

In the case of linear polarized light, these components can describe by:

$$E_x(z,t) = E_{\circ,x} e^{i(2\pi\nu t - kz + \varphi_x)}$$
$$E_y(z,t) = E_{\circ,y} e^{i(2\pi\nu t - kz + \varphi_y)} \quad (17)$$

and by using the total amplitude of the electric field Eo:

$$|E_\circ| = \sqrt{E_{\circ,x}^2 + E_{\circ,y}^2} \quad (18)$$

The linear polarization of this light beam can be described by the Jones vector J of linear polarized light as:

$$J = \frac{1}{|E_\circ|}\begin{pmatrix} E_{\circ,x} e^{i\varphi_x} \\ E_{\circ,y} e^{i\varphi_y} \end{pmatrix} \quad (19)$$

3. Schematic Simulation of QC System Based on Entangled Photons

Fig. 7 represents the schematic of quantum cryptography system which used in the proposed model of Ekert protocol

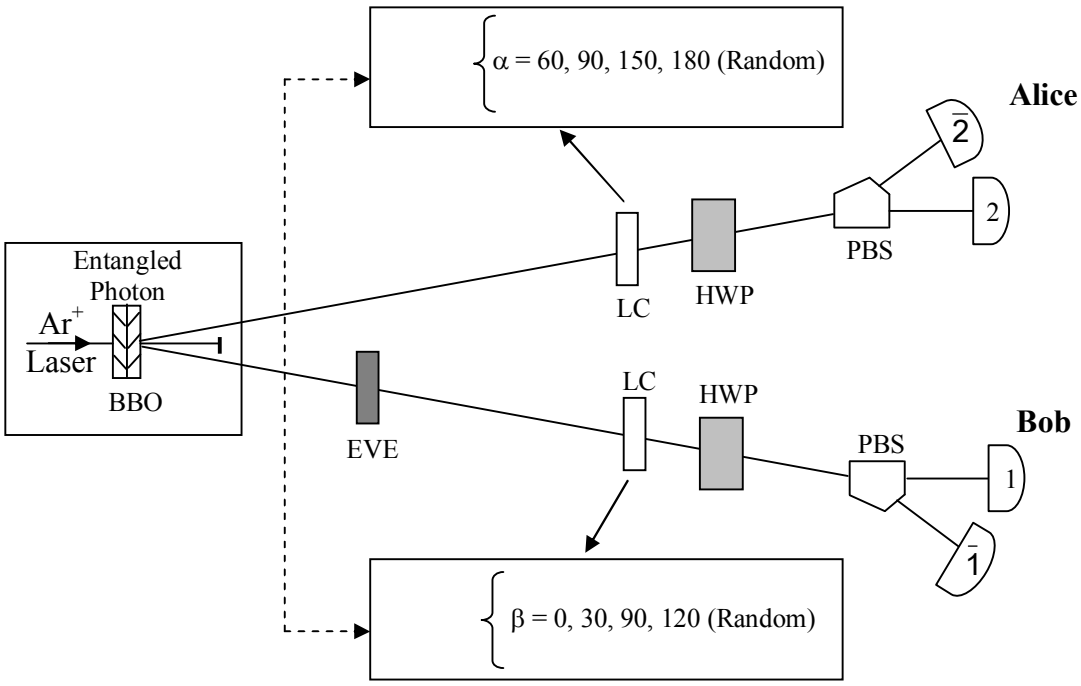

Fig. (7) The schematic of proposed model of quantum cryptography system

An Argon ion laser is used to pump two perpendicularly oriented nonlinear optical crystals (BBO), the resultant entangled photons are sent to Alice and Bob, where each analyze them in one of four randomly chosen bases. The photon pairs are then created in the maximally entangled state $|\phi^+\rangle$. Alice's and Bob's analysis systems each consists of a randomly driven liquid crystal (LC) (to set the applied phase shift), a half wave plate (HWP) and Calcite Glan-Thompson prism (PBS). The silicon avalanche photodiodes are used to detect

the photons from the horizontal and vertical polarization output of the prism. This version is simulated using Jones matrices for HWP and LC polarizer as shown in Table 1.

Table 1. Jones matrices for some optical components are used in the schematic quantum system

Polarizer in x direction (LC in $\alpha,\beta=0$)	$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$
Polarizer in y direction (LC in $\alpha,\beta=90$)	$\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$
Polarizer 45 (LC in $\alpha,\beta=45$)	$\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}$
Polarizer 135 (LC in $\alpha,\beta=135$)	$\frac{1}{2}\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}$
Half wave plate	$\mathrm{i}\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$
Rotator: angle β (LC in $\alpha,\beta=\beta$)	$\begin{pmatrix}\cos\beta & \sin\beta\\ -\sin\beta & \cos\beta\end{pmatrix}$

In the proposed model, Alice and Bob each receive one photon of a polarization-entangled pair in the state $|\phi^+\rangle=\frac{1}{\sqrt{2}}(|H_1H_2\rangle+|V_1V_2\rangle)$ where H (V) represents horizontal (vertical) polarization. Each, respectively, measure the polarization of their photons in the bases

$$|H_1\rangle+e^{i\alpha}|V_1\rangle \quad and \quad |H_2\rangle+e^{i\beta}|V_2\rangle,$$

where α *and* β are randomly taken values

$\alpha_1=60^\circ,\alpha_2=90^\circ,\alpha_3=150^\circ,\alpha_4=180^\circ;$

$\beta_1=0^\circ,\beta_2=30^\circ,\beta_3=90^\circ,\beta_1=120^\circ$

Then they disclose by public discussion which bases used are disclosed, but not the measurement results. For the state $|\phi^+\rangle$, the probabilities for a coincidence between Alice's detector 2 or 2', which detects the orthogonally polarized photons and Bob's detectors 1 (1') are given by [11],

$$P_{12}(\alpha,\beta)=P_{1'2'}(\alpha,\beta)=\frac{1}{4}(1+\cos(\alpha+\beta))$$

$$P_{12'}(\alpha,\beta)=P_{1'2}(\alpha,\beta)=\frac{1}{4}(1-\cos(\alpha+\beta)) \quad (20)$$

Completely correlated results will be available, when $\alpha+\beta=180$, which then constitute the quantum cryptography key. Only 1/4 of data actually contribute to the raw cryptography 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"). In particular, the Bell parameters [8]

$$S = -E(\alpha_1,\beta_1) + E(\alpha_1,\beta_3) + E(\alpha_3,\beta_1) + E(\alpha_3,\beta_3),$$
$$S' = E(\alpha_2,\beta_2) + E(\alpha_2,\beta_4) + E(\alpha_4,\beta_2) - E(\alpha_4,\beta_4) \quad (21)$$

where

$$E(\alpha,\beta) = \frac{R_{12}(\alpha,\beta) + R_{1'2'}(\alpha,\beta) - R_{12'}(\alpha,\beta) - R_{1'2}(\alpha,\beta)}{R_{12}(\alpha,\beta) + R_{1'2'}(\alpha,\beta) + R_{12'}(\alpha,\beta) + R_{1'2}(\alpha,\beta)} \quad (22)$$

The R's are the various coincidence count between Alice's and Bob's detectors.

Table 2. Distribution of Data dependent on Alice's and Bob's respective phase setting α_i and β_j

		Alice			
		$\alpha_1 = 60$	$\alpha_2 = 90$	$\alpha_3 = 150$	$\alpha_4 = 180$
Bob	$\beta_1 = 0$	S	NU	S	Key
	$\beta_2 = 30$	NU	S'	Key	S'
	$\beta_3 = 90$	S	Key	S	NU
	$\beta_4 = 120$	Key	S'	NU	S'

There are 1/2 of data used to test Bell's inequalities. The quantum mechanically expected values of $|S|$, $|S'|$ are $2\sqrt{2}$ for the combinations of α *and* β . For any local realistic theory $|S|$, $|S'| \le 2$. Because of high values of S have been observed in this system, the presence of an eavesdropper could thus be detected in very fast time in the data collection. The simulated eavesdropper thus makes the projective measurement $|X\rangle\langle X|$. The effects on the measurement of S and S' and BER depend strongly on what eavesdropping basis $|X\rangle$ is used [4]. Figs (8 and 9) show the effect of the eavesdropping on S and BER for the attack base $\cos\theta\ |H\rangle + \sin\theta\ |V\rangle$.

The eavesdropper in this attack base does not know the plane of measurement bases of Alice and Bob and causes average BER equal 32% and average value of S is equal to 0.7.

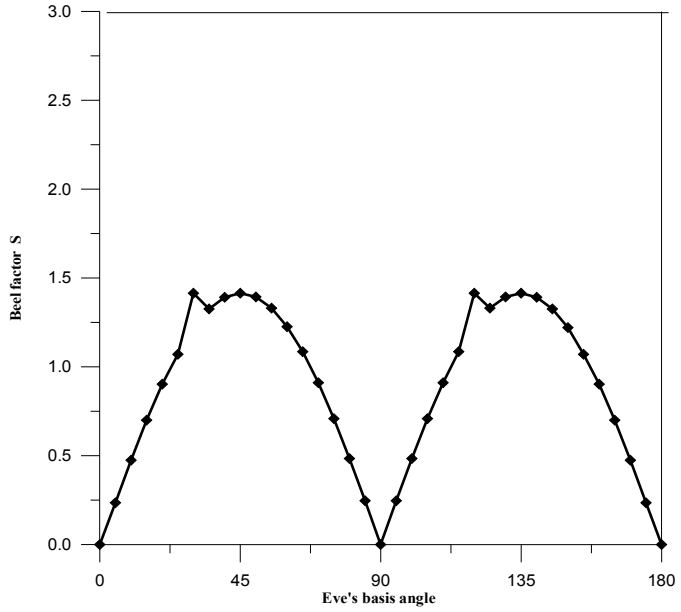

Fig.(8) The effect of the eavesdropper on S when the attack's base $\cos\theta \ |H\rangle + \sin\theta|V\rangle$

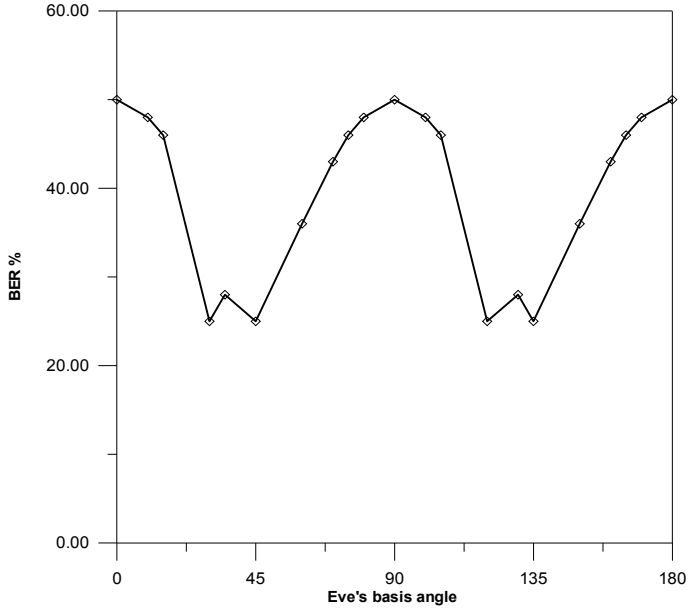

Fig (9) The effect of the eavesdropper on the BER when the attack base is $\cos\theta \ |H\rangle + \sin\theta|V\rangle$

When the eavesdropper know the plane of measurement of Alice and Bob (the attack base $|H\rangle + e^{j\phi}|V\rangle$). As shown in Figs. (10 and 11) the eavesdropper causes BER equal to 25% and S value equal to 1.4.

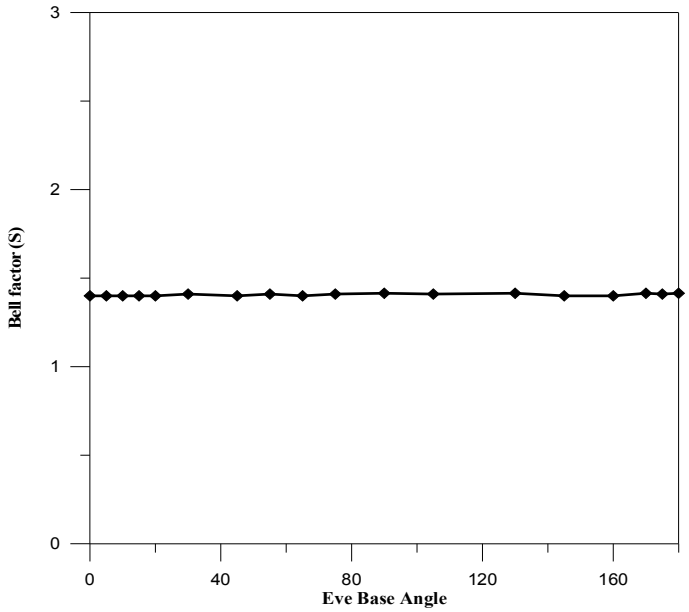

Fig.(10) The effect of the eavesdropper on S when the attack's base $|H\rangle + e^{j\phi}|V\rangle$.

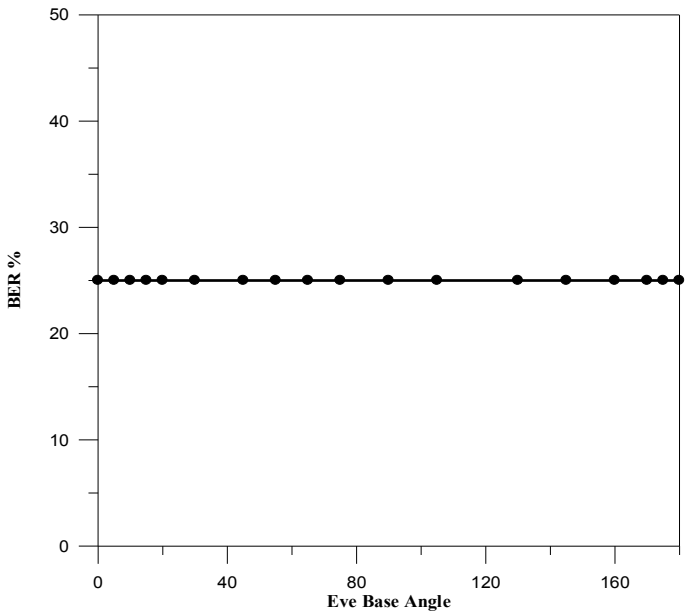

Fig (11) The effect of the eavesdropper on the BER when the attack base is $|H\rangle + e^{j\phi}|V\rangle$.

From the results we can improve the security and detect the eavesdropper at fast time if the eavesdropper doesn't know the measurement bases of Alice and Bob. We can build new strategy that satisfies this idea by used variant measurement bases in the same time of transmission. If the remain four combination in Table 2 used to calculate the factor NU, since $\alpha + \beta = 90 \; or \; 270$ in these combinations, therefore

$$P_{12}(\alpha,\beta) = P_{1'2'}(\alpha,\beta) = P_{1'2}(\alpha,\beta) = P_{12'}(\alpha,\beta) = 1/4$$

Then

$$E(\alpha,\beta) = P_{12}(\alpha,\beta) + P_{1'2'}(\alpha,\beta) - P_{1'2}(\alpha,\beta) - P_{12'}(\alpha,\beta)$$
$$= 0$$
$$NU = E(\alpha_2,\beta_1) + E(\alpha_1,\beta_2) + E(\alpha_4,\beta_3) + E(\alpha_3,\beta_4)$$
$$= 0 \qquad (23)$$

From simulation for noiseless channel and no eavesdropper NU = 0.
If the eavesdropper present we observed NU > 0, the exact value is unknown and cannot calculate from the formula of coincidence counts between Alice's and Bob's detectors, therefore these combinations are not used in the test of eavesdropping or in producing a cryptography key.

Conclusion

This paper presented proposed model of Ekert protocol based entangled photons. The modeling of optical components based Jones matrices are used to simulate the proposed model. This system is more secure if the eavesdropper does not know the base measurement of Alice and Bob. The average value of S is lower if the eavesdropper does not know the base measurement, and at the same time the BER is higher by comparison with the case when the eavesdropper knows the base measurement. By using variant measurement base of Alice and Bob in the time of transmission we can built more secure system.

References

[1] D. Bouwmeester, A. Zeilinger,"The Physics of Quantum Information", Institute for Experimental Physics University Wien, Austria

[2] W. Stallings, "Cryptography and Network Security: Principles and Practice", 2nd Edition, Prentice Hall, New Jersey, 2000.

[3] C. H.Bennet and G. Barassad, "Quantum Cryptography: Public Key Distribution and Coin Tossing" Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175-179, 1984.

[4] C. H. Bennet, "Quantum Cryptography Using Any Two Non orthogonal States", Phys. Rev. Lett. Vol. 68, pp 3121-3124, 1992.

[5] N. Gisin and S. Wolf, "Quantum Cryptography on Noisy Channels: Quantum Versus Classical Key-Agrement Protocols", Physical Review Letters, Vol. 83, No. 20, pp. 4200-4203, November 1999.

[6] A. K. Ekert, "Quantum Cryptography Based on Bell's

Theorem", Phys. Rev. Lett., Vol. 67, No. 6, pp 661-663, 1991.

[7] D. Bohm, "Quantum Theory", (Prentice Hall, Englewood Cliffs, NJ, 1951).

[8] J. S. Bell " Physics", Long Island City N,Y, 195 (1965); J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett , 23, 880 (1969)

[9] C. H. Bennett *et al*, "Experimental Quantum Cryptography", Journal of Cryptography, Vol.5, No.3, pp.3-28, 1992.

[10] A. Zeilinger and et-al. "Quantum Cryptography with Entangled Photons", Phys. Rev. Lett., Vol. 84, pp 4729-4732, 1999

[11] Kwiat, and et-al. "Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol", Phys. Rev. Lett., Vol. 84, No. 20, pp 4733-4736, 2000.

[12] Springer, " Photonics: Linear and Nonlinear Interactions of Laser Light and Matter, Verlag Berlin Hidelberg, New York, 2001.