بسم الله الرحمن الرحيم

Sudan University of Science and Technology
College of Graduate Studies

Quantum Correlation of Laser Entangled Photons Calculated Via Event-Based Method by Using Matlab Simulation

حساب الإرتباط الكمي لفوتونات ليزر مترابطة بطريقة الحدث المنفرد باستخدام محاكاة الماتلاب

A Thesis Submitted in Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Laser Applications in Physics

By:

Ahmed Mohammed Gomaa Mohammed

Supervised by:

Dr. Khalid Mohammed Haroun Mohammed

March 2019

الآيـة

قال تعالى:

(اللَّهُ نُورُ السَّمَاوَاتِ وَالْأَرْضِ مَثَلُ نُورِهِ كَمِشْكَاةٍ فِيهَا مِصْبَاحٌ الْمِصْبَاحُ فِي زُجَاجَةٍ الزُّجَاجَةُ كَأَنَّهَا كَوْكَبٌ دُرِّيٌّ يُوقَدُ مِنْ شَجَرَةٍ مُبَارَكَةٍ زَيْتُونَةٍ لَا شَرْقِيَّةٍ وَلَا غَرْبِيَّةٍ يَكَادُ زَيْتُهَا يُضِيءُ وَلَوْ لَمْ تَمْسَسْهُ نَارٌ نُورٌ عَلَى نُورٍ يَهْدِي اللَّهُ لِنُورِهِ مَنْ يَشَاءُ وَيَضْرِبُ اللَّهُ الْأَمْثَالَ لِلنَّاسِ وَاللَّهُ بِكُلِّ شَيْءٍ عَلِيمٌ)

صدق الله العظيم

سورة النور الآية (35)

Dedication:

Dedicated :

To my mother,

The first one whom taught me a letter.

To my father,

From whom I know the meaning of life.

To my brothers and sisters,

The light of my way.

To my family,

Whom I love.

Acknowledgement

My primary thanks to Allah, the most beneficent, the most merciful.

Thank to my supervisor, **Dr. Khalid Mohammed Haroun**, thanks for the opportunity to join you. Thanks for your guidance . I have learned a lot from you.

I would like to thank Prof. Dr. Nafie Abd Allatif for help he gave me through my this study. I have learn a lot from him.

Thanks to the supporting staff of the Laser institute library.

To all my fellow students and postdocts. thank you all. Special thanks to **Dr. Yousif Hassan** and **Dr. Sulaiman Addoud**

Finally, thanks to my parents, Mohammed Gomaa and Saida Adam.

Abstract

Quantum correlations between particles are usually formulated by assuming the persistence of an entangled state after the particles have separated. When entanglement is present, Bell's Inequalities are violated but when entanglement is destroyed, Bell's inequalities are satisfied.

The aim of this work is to build computer program using Matlab software to simulate Ekert protocol of quantum cryptography by implement event-based simulation method. And by used two types of probabilistic polarizing beam splitter. Since we used the argument of Malus intensity law to represent the quantum probability amplitude for each single photon in type1 and the Hadamard transformation of single photon to represent quantum probability amplitude for each single photon in type2. The program calculated the quantum correlation of each two polarized entangled photons as a value of Bell inequality (S) . The obtained results of (S) value after implemented suitable time tag model was in average S = 2.6 for type1, and S = 2.7 for type2. And this results investigated strong quantum correlation, and very agreement with that result of maximum correlation expected by quantum mechanics theory calculated for polarized entangled photons (S =2.83).

After running the simulation program of Ekert protocol the results of established secret key between two legitimate users and the variation of (S) value showed very good ability of program for detecting eavesdropper, that by an obvious decrease in (S) value. When eavesdropper was present the value of (S) decreased to S = -0.29 and S = 0.19for type1 and type2 respectively.

المستخلص

الارتباط الكمي بين الجسيمات يبرهن عادة بافتراض وجود حالة ترابط بين الجسيمات بعد أن تفصل بينها مسافة. ففي حالة وجود الترابط فان قيمة الارتباط الكمي تتعدى مدى متراجحة بيل(Bell) وعند فقدان حالة الترابط فان قيمة الترابط الكمي تكون في مدى متراجحة بيل (Bell).

تهدف هذه الدراسة لبناء برنامج حاسوب باستخدام برمجية الماتلاب لمحاكاة نموذج Ekert للتشفير الكمي و ذلك بتوظيف طريقة الحدث المنفرد لعمل نوعين من المستقطبات الضوئية ذات المحاكاة الاحتمالية. حيث استخدمنا قانون مالوس للشدة الضوئية لتمثيل السعة الاحتمالية لكل فوتون على حدا بالنسبة للنوع الأول، و تحويلات هادمارد للفوتون لتمثيل السعة الاحتمالية في النوع الثاني.

تم حساب الارتباط الكمي للفوتونات المترابطة إستقطابيا و ذلك بحساب قيمة متراجحة Bell(S). النتائج المتحصله لقيمة (S) بعد توظيف نموذج مناسب للتطابق الزمني وجد أن قيمة (S) في المتوسط S=2.6 بالنسبة للنوع الأول و S=2.7 للنوع الثاني، و هذه النتائج توضح ارتباط كمي قوي و تتوافق بشدة مع قيمة الارتباط الكمي العظمى المتوقعة حسب نظرية ميكانيكا الكم (S=2.83).بعد تشغيل برنامج محاكاة نموذج Ekert ، وجد أن نتائج المفتاح المتوزع بين المستخدمين و التغير في قيمة (S) توضح إمكانية عالية للنموذج في كشف المتجسس و ذلك بملاحظة النقصان الواضح في قيمة (S). حيث نقصت قيمة S إلى S=-0.29 و S=0.19 للنوع الأول و الثاني على التوالي.

Table of Contents

CHAPTER THREE
Cryptography

CHAPTER FOUR

Event-based simulation of quantum physics experiments

List of Figures

Chapter one
Introduction

1.1. Introduction*:*

Cryptography from Greek Krypto's "hidden" and graphein "writing" (Thomase. Copeland, 2000) is the art of creating secure codes, whereas cryptanalysis deal with breaking this codes.

The need of safety communication has increased tremendously during the last decade , since more and more sensitive information are transported and more people are concerned .

Cryptography has been used for long time to safeguard military and diplomatic communications. But the downing of the information age revealed an urgent need for cryptography in the private sector(Dannis Luciano, Gorden Prichett 19987). A Cryptography is a tool used to protect information in computing system. It is used everywhere and by millions of people worldwide on a daily basis. It used to protect data at rest and data in motion.

The basic terminology is that cryptography refers to the science and art of designing ciphers." Cryptography is the mathematical foundation on which one build secure system. It studies ways of securely storing, transmitting, and processing information(Luca Travisan 2009). Cryptography is where security engineering meets mathematics (John F.kenny 2009). It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems.

Classical cryptography use keys to encode and decode messages. The encoding of a message, makes it unavailable to any party who does not have the private key .

The one-time pad cipher is an example of a classical secure algorithm. In the one-time pad, the sender and receiver share a secret random key. The secret key is composed of a sequence of random bits and it must be as long as the message to be encrypted. The problem with the one-time pad cipher is that the key has to be transfer between two parties securely.
But Quantum key Distribution (QKD) is a proposal to solve the problem of key distribution between two distant parties by using the quantum properties of single photons .

Actually, QKD is a new emerging technology for protecting sensitive data during transmission process in a new communications environment. So, many researchers have focused on the simulation of QKD to achieve a secure communication for files depending on different simulator environments.

1.2 Research problem:

Quantum cryptography is one of the important modern information science branch ,and the need of security communication is increasing every day.

Classical cryptography algorithms have a real problem in key distribution, and quantum mechanics concepts propose to solve it.

The use of quantum key distribution(QKD) began science 1984 (BB84 protocol), after that many projects and experiments had done for security purpose.

The set up of QKD experiments now a days is not available in our country, that it is not able to do real experiments in QKD field. Instead of that one can use simulation computer programs to modeling QKD protocols .

To observe how the eavesdropping effect can be detected in EKERT protocol this work aims to make simulation program of EKERT protocol with and without the present of eavesdropper to check what variation that well be happen by compare the values of CHCH's inequality.

1.3 Objectives:

The general objective of this work is to study the quantum cryptography simulation by using Matlab, and the specific objectives helping to complete the general one are:

- Using MATLAB program to build a model of event based simulation of polarizing beam splitter (PBS) to analyze single photon polarization on quantum mechanics concept .
- Using the PBS to model an EKERT protocol simulation program to establish a secret key between two users.
- To verify that the simulation program can easy detect eavesdropper .

1.4 Research Methodology:

The methodology of this thesis is the using theoretical and modeling of quantum cryptography protocols implementing Matlab software package.

1.5 Thesis Layout:

The first chapter of this thesis was a brief description of the research methodology, problem statement and objectives. Theoretical aspects of quantum fundamental concepts are presented in chapter two. Chapter three describes the cryptography, and quantum cryptography in general in addition to the literature review.

Chapter four presents and discussed the event based simulation of quantum experiments, then the event based simulation was used in implementation of Ekert protocols, and also the chapter contains the results and discussion of the simulated experiments. Finally, the chapter presented the conclusion and recommendations for future work.

Chapter Two

Quantum mechanics background:

2.1-Introduction:

Quantum mechanics is the mechanics that describe the behavior and properties of very small objects , like electrons, photons, and atoms.(en.wikipedia.org/wiki/) And Quantum mechanics is often seen as the mathematics of objects that are sufficiently small and of sufficiently low energy that the act of observing one of them by hitting it with a photon of light disturbs the object that is being observed- alter its momentum or position or energy.

In the macroscopic world it is presumed the hitting an object , say a cricked ball , with a photon of light to observe it will not disturb the object. It is disturbance or non disturbance by observation that is seen as differentiating the very small objects of quantum mechanics from the macroscopic objects of Newtonian mechanics . This disturbance is often associated with uncertainty in the values of some of the dynamic variables. And Uncertainty is a central feature of quantum mechanics. Quantum mechanics is formulated as mathematical operators , eigen-functions , and eigen-values. The continuous dynamic variables such as energy or momentum of Newtonian mechanics are each taken to be associated with operator. For each variable there is one, and only one corresponding operator.

In Newtonian mechanics the variable can take any real value . since in quantum mechanics the only allowed values of variables are the eigen-values of the associated operator . These eigen-values are often discreet rather than continuous.

Operators are also different from Newtonian variables in that they often do not commute with each other. There is no concept to non commutation in Newtonian mechanics.

2.2-Dirac notation

Dirac introduced the symbol $|\psi\rangle$, pronounced 'ket psi', to denote a complete set of amplitudes for the system. If the system consists of a particle trapped in a potential well, $|\psi\rangle$ could consist of the amplitudes of the spectrum of possible energies, or it might consist of the amplitudes $\psi(x)$ that the particle is found at x, or it might consist of the amplitudes $\psi(p)$ that the momentum is measured to be p.

Using the abstract symbol $|\psi\rangle$ enables us to think about the system without committing ourselves to what complete set of amplitudes we are going to use, in the same way that the position vector x enables us to think about a geometrical point independently of the coordinates (x, y, z), (r, θ, ϕ) or whatever by which we locate it. That is, $|\psi\rangle$ is a container for a complete set of amplitudes in the same way that a vector x is a container for a complete set of coordinates (James Binnery, David skinner 2014).

2.3-Linear vector spaces

The analogy between kets and vectors provides ability to using kets as a to represent the vectors.

By describe scalars (complex numbers) by *a*, *b*, *c*,…., and vectors by $|\alpha\rangle,|\beta\rangle,.....$

A linear vector space *V* is a set of vectors($|\alpha\rangle,|\beta\rangle,.....$) which are closed under addition and scalar multiplication. That is, if $|\alpha\rangle and|\beta\rangle$ are in *V*, then

$|C\rangle = a|\alpha\rangle + b|\beta\rangle$ is also in (2.1)

We usually write vectors as column matrices:

$$|C\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \qquad (2.2)$$

A set of vectors $|\,e_1\rangle$; $|\,e_2\rangle$;. . . ; $|\,e_N\rangle$, are linearly independent if the relation,

$$\sum_{n=1}^{N} c_n |e_n\rangle = 0 \qquad (2.3)$$

can only be true if: $c_n = 0$,for $n = 1; \ldots ; N$. Otherwise, the set of vectors are linearly dependent, which means that one of them can be expressed as a linear combination of the others.

The maximum number N of linearly independent vectors in a vector space V is called the dimension of the space, in which case the set of vectors provides a basis set for V. Any vector in the space can be written as a linear combination of the basis vectors.

Let $|\,e_n\rangle$, be a basis in V. Then any vector $|\,\alpha\rangle$ in V can be represented by:

$$|\alpha\rangle = \sum_{n=1}^{N} a_n |e_n\rangle \qquad (2.4)$$

where a_n is a complex numbers. Thus the component a_n is unique for the basis set $|\,e_n\rangle$.

An inner product maps pairs of vectors to complex numbers. It is written as: $\langle\alpha|\beta\rangle$

The inner product must have the properties:

1. $\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle^*$ = a complex number.
2. $\langle a\alpha + b\beta|\gamma\rangle = a^*\langle\alpha|\gamma\rangle + b^*\langle\beta|\gamma\rangle$. (2.5)
3. $\langle\gamma|a\alpha + b\beta\rangle = a\langle\gamma|\alpha\rangle + b\langle\gamma|\beta\rangle$
4. $\langle\alpha|\alpha\rangle \geq 0$, with the equality holding only if $|\,\alpha\rangle = |\,0\rangle$.

The norm, or length, of a vector is defined by $\|\alpha\|^2 \equiv \langle\alpha|\alpha\rangle > 0$.

Hilbert space is a linear vector space with an inner product for each pair of vectors in the space. Using our examples of linear vector spaces, one possible definition of the inner products is:

$$\langle a|b\rangle = a_1^* b_1 + a_2^* b_2 + \cdots + a_N^* b_N \; ; \qquad (2.6)$$

A basis set e_n , are orthonormal if

$$\langle e_i | e_j \rangle = \delta_{ij} \; : \qquad (2.7)$$

Where $\delta_{ij} = 0$; when $i \neq j$.

$\delta_{ij} = 1$; when i = j.

the important property of the inner product is: the Schwartz inequality. The Schwartz, or triangle, inequality states that for any two vectors in V,

$$\|\psi\|.\|\phi\| \geq |\langle \psi | \phi \rangle| . \qquad (2.8)$$

Physical systems are represented in quantum theory by a complex vector space *V* with an inner product. The state of the system is described by a particular vector $|\psi\rangle$ in this space. All the possible states of the system are represented by basis vectors in this space. Observables are represented by Hermitian operators acting in this vector space. The possible values of these observables are the eigen values of these operators (John F.D., 2009).

2.4-Operators

An operator **A** is an object that maps a vector $|\alpha\rangle \in V$ to another vector $|\beta\rangle \in V$. We write:

$$\mathbf{A}|\alpha\rangle = |\beta\rangle . \qquad \mathbf{(2.9)}$$

For any operator A, if we can find a complex number a and a ket $|a\rangle$ such that

A| a⟩ = a| a⟩ ;

then a is called the eigen value and | a⟩ is the eigenvector.

2.5-Pauli operators

Physics properties can be associated with operators A, with linear maps of the form $A|\psi\rangle = a|\psi\rangle$.

The famous , important matrices operators are the Pauli matrices operators ($\sigma_x, \sigma_y, \sigma_z$) . let us consider an example: The Pauli-z-matrix σ_z acts as:

$$\sigma_z|0\rangle = |0\rangle$$
$$\sigma_z|1\rangle = -|1\rangle \qquad (2.10)$$

We hence note that the vectors $|0\rangle and |1\rangle$ are eigenvectors of σ_z : Up to a complex number +1 and -1, the respective eigen values we obtain again the same vector if we apply σ_z to it. Similarly, we find that the Pauli-x matrix σ_x acts as:

$$\sigma_x|+\rangle = |+\rangle$$
$$\sigma_x|-\rangle = -|-\rangle \qquad (2.11)$$

And the Pauli-y-matrix σ_y has the property that

$$\sigma_y|\times\rangle = |\times\rangle$$
$$\sigma_y|\Theta\rangle = -|\Theta\rangle \qquad (2.12)$$

Physical properties are associated with operators, in fact with Hermitian operators, such Hermitian operators are called observables. Pauli operators are examples of Hermitian operators. A measurement along the z axis corresponds to the Pauli-z-matrix, and similarly for the other Pauli matrices. So the first measurement corresponds to a "measurement of the observable Pauli-z". After the measurement, the system will be in an eigenvector of the respective observable, the outcome of the measurement being the eigen value of the

eigenvector. For example, we measure the spin along the z axis, hence "measure the observable Pauli-z". If we get the value +1, we will obtain the state vector $|0\rangle = \sigma_x|0\rangle$ after the measurement, corresponding to spin up. In case of the value -1, we obtain the state vector $|1\rangle = -\sigma_x|1\rangle$ after the measurement. Since $|0\rangle$ is an eigenvector of σ_z, if we will repeat measuring σ_z, we will repeatedly get the outcome +1 and the post measurement state vector $|0\rangle$. This is why then the spin is always pointing into the same direction. If we at some point measure along the *x* axis, the situation is quite different. Neither $|0\rangle$ not $|1\rangle$ are eigenvectors of σ_x. We will see that this fact is essentially responsible for the two outcomes, spin left and spin right, being obtained in a probabilistic fashion. After the measurement, the state vector is an eigen state of the observable measured, i.e.,

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \sigma_x \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

and (2.13)

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = -\sigma_x \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The matrix form of the Pauli operators are :

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (2.14)$$

The vectors $|0\rangle$ and $|1\rangle$ are already eigenvectors of σ_z, so we should not be surprised to see that the matrix form is diagonal. Similarly, the matrix form of the other two Pauli operators as

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad (2.15)$$

2.6-Superposition Principle:

When two waves meet they overlap and interact. Sometimes they add to make a wave bigger, sometimes they cancel each other out, and often it's a combination of both. Noise-cancelling headphones listen to regular and constant noise around you and play the exact opposite sound to cancel annoying noises like jet planes engines. This phenomenon is known as superposition.

Confusingly, however, in the quantum world superposition can mean something different entirely. At the quantum scale, particles can also be thought of as waves. Particles can exist in different states, for example they can be in different positions, have different energies or be moving at different speeds. But because quantum mechanics is weird, instead of thinking about a particle being in one state or changing between a variety of states, particles are thought of as existing across all the possible states at the same time. It's a bit like lots of waves overlapping each other. This situation is known as a superposition of states. If we are thinking in terms of particles, it means a particle can be in two places at once. This doesn't make intuitive sense but it's one of the weird realities of quantum physics.

However, once a measurement of a particle is made, and for example its energy or position is known, the superposition is lost and now have a particle in one known state. (Physics.org).

Consider a system with *k* distinguishable (classical) states. For example, the electron in a hydrogen atom is only allowed to be in one of a discrete set of energy levels, starting with the ground state, the first excited state, the second excited state, and so on.

If we assume a suitable upper bound on the total energy, then the electron is restricted to being in one of *k* different energy levels — the ground state or one

of k -1 excited states. As a classical system, we might use the state of this system to store a number between 0 and k - 1.

The superposition principle says that if a quantum system can be in one of two states then it can also be placed in a linear superposition of these states with complex coefficients.

Let us denote the ground state of our k-state system by $|0\rangle$, and the successive excited states by $|1\rangle,...,|k-1\rangle$. These are the k possible classical states of the electron.

The superposition principle tells us that, in general, the quantum state of the electron is

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + ... + \alpha_{k-1}|k-1\rangle$$

where $\alpha_0, \alpha_1, \alpha_2, ...\alpha_{k-1}$ are complex numbers normalized so that $\sum_j |\alpha_j|^2 = 1$

α_j is called the amplitude of the state $|j\rangle$. For instance, if k = 3,

the state of the electron could be

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle$$

or $$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{2}|1\rangle + \frac{i}{2}|2\rangle$$

or $$|\psi\rangle = \frac{1+i}{\sqrt{2}}|0\rangle - \frac{1-i}{2}|1\rangle + \frac{1+2i}{2}|2\rangle$$

The superposition principle is one of the most mysterious aspects about quantum physics. One way to think about a superposition is that the electron does not make up its mind about whether it is in the ground state or each of the k – 1 excited states, and the amplitude α_0 is a measure of its inclination towards the ground (www.inst.ees.berkeley.edu).

2.7-Quantum measurement :

Physics is about the quantitative description of natural phenomena. A quantitative description of a system inevitably starts by defining ways in which it can be measured. If the system is a single particle, quantities that we can measure are its x, y and z coordinates with respect to some choice of axes, and the components of its momentum parallel to these axes. We can also measure its energy, and its angular momentum. The more complex system is, the more ways there will be in which we can measure it (J Binney, D. Skinner, 2013).

Associated with every measurement, there will be a set of possible numerical values for the measurement (the spectrum of the measurement). For example, the spectrum of the x coordinate of a particle in empty space is the interval [-∞, ∞], while the spectrum of its kinetic energy is [0, ∞].

When the spectrum is a set of discrete numbers, we say that those numbers are the allowed values of the measurement. With every value in the spectrum of a given measurement there will be a quantum amplitude that we will find this value if we make the relevant measurement. Quantum mechanics is the science of how to calculate such amplitudes given the results of a sufficient number of prior measurements (J.Binnery 2008).
In practical if we about investigating some physical system: some particles in an ion trap, a drop of liquid helium, the electromagnetic field in a resonant cavity. What do we will know about the state of this system, there are two types of knowledge: first, a specification of the physical nature of the system (e.g., size & shape of the resonant cavity), and, second, the information about the current dynamical state of the system.

In quantum mechanics information of type one is used to define an object called the Hamiltonian 'H' of the system . And information of type two is more

subtle. It must consist of predictions for the outcomes of measurements you could make on the system.

Since these outcomes are inherently uncertain, your information must relate to the probabilities of different outcomes, and in the simplest case consists of values for the relevant probability amplitudes.
In quantum mechanics, then, knowledge about the current dynamical state of a system is embodied in a set of quantum amplitudes.

In classical physics, by contrast, we can state with certainty which value we will measure, and we characterize the system's current dynamical state by simply giving this value. Such values are often called 'coordinates' of the system. Thus in quantum mechanics a whole set of quantum amplitudes replaces a single number.
The state of a quantum system, $|\psi\rangle$, is a vector in a complex vector space. If the set of vectors $\{|n\rangle\}$, (where N may be ∞) is an orthonormal basis for this space, then we can always express $|\psi\rangle$ as $|\psi\rangle = \sum_n c_n |n\rangle$
for some complex coefficients c_n, where $\sum_n |c_n|^2 = 1$.
The basis of quantum measurement theory is the following postulate: We can choose any basis, and look which one of these basis states the system is in.

When we do so, we will find the system to be in one of these basis states, even though it may have been in any state $|\psi\rangle$ before the measurement. Which basis state we find is random.

If the system is initially in the state $|\psi\rangle$ then the probability that we will find state $|n\rangle$ is given by $|c_n|^2$.

A measurement like this, for which the result is one of a set of basis states, is called a Von Neumann measurement.

Quantum measurement theory springs from the theory of self-adjoin operators. Specifically, to every classical observable we associate a self- adjoin linear operator A which acts upon the elements of H. We then associate; the possible meter-readings which can result from A-measurement with the real eigen values of A; and the possible quantum state immediately subsequent to such a measurement with the eigenvectors of A. Each observable contrives spectrally to erect its own individual 'orthogonal scaffold ($|a\rangle$)" in the space of states (Nicholas Wheeler,2009). For the idealized measurement process if we have a System S, in unknown quantum state $|\psi\rangle$, is presented to the measurement device represented by the operator A . After the interaction is complete;
The device is in the state "a" reported by its read-out mechanism, and this is interpreted to mean that, the system S is in state $|a\rangle$.
Quantum mechanically fundamental is the fact that repetitions yield statistically scattered results, and we can obtain

$|a_1\rangle$ with probability $P_1 = |\langle a_1|\psi\rangle|^2$

$|a_2\rangle$ with probability $P_2 = |\langle a_2|\psi\rangle|^2$ (2.16)

$|a_n\rangle$ with probability $P_n = |\langle a_n|\psi\rangle|^2$

Quantum measurement is by this scheme a 'state-preparation process,' and measurement devices are, in effect, sieves the input state $|\psi\rangle$
and the device acts probabilistically to pass one of the eigen-components, and to annihilate all others.
We assert that a measurement has actually taken place on these grounds: if the output $|a_n\rangle$ of a measurement which registered an is immediately re-presented to an A-meter . And repeated A-measurement yield:
$|a_1\rangle$ with probability P1 = $|\langle a_1|\psi\rangle|2 = 0$
$|a_2\rangle$ with probability P2 = $|\langle a_2|\psi\rangle|2 = 0$

$|a_n\rangle$ with probability Pn = $|\langle a_n|\psi\rangle|2 = a_n$

which is to say: we recover (or 'confirm') the previous result with certainty. The expected average of many independent A-measurements i.e., of the results obtained when many identical copies of $|\psi\rangle$ are presented serially to an A-meter can be described

$$\langle a\rangle \equiv \sum_i^n a_i P_i = \sum_i a_i \left|\langle a_i|\psi\rangle\right|^2 = \langle\psi|(a_i|a_i\rangle\langle a_i|)|\psi\rangle = \langle\psi|A|\psi\rangle \qquad (2.17)$$

but alternative descriptions exist and are sometimes more useful. For example, let ($|n\rangle$)be some arbitrary orthonormal basis in the space of states. Drawing upon the completeness condition , we have

$$\langle\psi|A|\psi\rangle = \sum_n \langle\psi|n\rangle\langle n|A|\psi\rangle = \sum_n \langle n|A|\psi\rangle\langle\psi|n\rangle = \sum_n \langle n|A\rho_\psi|\psi\rangle$$

Where

$\rho_\psi \equiv |\psi\rangle\langle\psi|$ projects onto $|\psi\rangle$

$\langle\psi|A|\psi\rangle = trA\rho_\psi$

So $\langle a\rangle = \langle\psi|A|\psi\rangle = trA\rho_\psi$

Quantum mechanics attempts to describe not where the next particle will land on the detection screen' but statistical features of the pattern formed when many identically-prepared particles are directed at the screen (Nicholas Wheeler,2009).

2.8-Uncertainty principle:

In classical mechanics the state of a particle in a one-dimensional world is completely determined by the value of its position x(t) and momentum p(t), by its trajectory. The situation is radically different in quantum mechanics. The probabilistic interpretation of the wave function implies that we can at best obtain the probability density for a particle to be at a given position *x* at time *t*. As a consequence the concept of classical trajectory used in Newtonian mechanics does not make sense in quantum mechanics. The position and

momentum of the particle can be defined, but their values cannot be measured simultaneously.
On the other hand, when the scales in the problem are much larger than the Planck constant h, we expect to recover the classical results.
These two features are summarized in the so-called uncertainty relations, first derived by Heisenberg. The uncertainty relations state that, if the position and momentum are measured simultaneously, with respective precisions Δx and Δp, then:

$$\Delta x.\Delta p \geq \frac{\hbar}{2} \tag{2.18}$$

It is clear from equation above that if the position of the particle is known exactly, then the knowledge of its momentum is completely lost. In general the product of the two uncertainties has to be greater than $\frac{\hbar}{2}$

It is important to appreciate that Heisenberg's inequalities reflect a physical limitation. A better experimental apparatus would not allow a higher precision to be obtained. The uncertainty is a property of the dynamics of the system. They also encode the idea that in quantum mechanics the measurement of a quantity interferes with the dynamics. If we measure exactly the position of the particle, then we lose all knowledge of its momentum. Hence the concept of determinism is lost during the measurement process.

2.9-Photon's Polarization:

In order to predict the behavior of a quantum system, we need to know precisely the physical properties of all states. One of the most simple physical systems is the polarization of the photon. The dimension of its Hilbert space is just two, yet it is quite sufficient to show how amazing the world of quantum mechanics can be.
Suppose we can isolate a single particle of light, photon, from a polarized wave. The photon is a microscopic object and must be treated quantum-mechanically. To define the associated Hilbert space of photon. We first notice that the state of the photon obtained from a horizontally polarized wave, whose state we denote as $|H\rangle$, is incompatible with its vertical counterpart, $|V\rangle$ an

$|H\rangle$ photon can never be detected in a $|V\rangle$ state. If we prepare a horizontally polarized photon and send it through a polarizing beam splitter, it will always be transmitted and never reflected. This means that states $|H\rangle$ and $|V\rangle$ are orthogonal. So that states $|H\rangle$ and $|V\rangle$ form an orthonormal basis in the corresponding Hilbert space.
when, these states are orthogonal and thus they are linearly independent . And, any polarization state of the photon can be written as linear combination of states $|H\rangle$ and $|V\rangle$

$$|\psi\rangle = \alpha|H\rangle + \beta|V\rangle \qquad (2.19)$$

We will call the basis {|H⟩ , |V ⟩} the canonical basis of our Hilbert space. For a classical wave, shifting the phases of both horizontal and vertical component by the same amount does not change the polarization of the wave.

A similar rule applies to quantum states. Multiplying a state vector by $e^{i\phi}$ does not change the physical nature of a state. For example, |V⟩ i|V⟩ and - |V⟩ represent the same physical object, as well as, say, $\frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle) and \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$. This rule turns out to be very general: it works for all states in the entire domain of quantum mechanics.

Table 1.1: Important polarization states:

state	designation	Notation
$\cos\theta\|H\rangle + \sin\theta\|V\rangle$	linear polarization at angle θ to horizontal	|θ⟩
$\frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	+45◦ polarization	|+45◦⟩ or |+⟩
$\frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	-45◦ polarization	|-45◦⟩ or |-⟩
$\frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	Right circular polarization	|R⟩
$\frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	Left circular polarization	|L⟩

The ±45◦ polarization states are also called diagonal polarization states.

In classical, macroscopic physics, the concept of measurement is of technical rather than fundamental nature. This is because we can precisely measure the state and evaluate the system without disturbing it. In the quantum world, the situation is different: we are big and the things we want to measure are small. Therefore, any measurement will change the quantum state of our system.

Suppose a single photon in state $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ hits a polarizing beam splitter (PBS) [Fig. 2.1(a)]. If we were dealing with a classical wave, we would expected it to split: a part would be transmitted through the PBS, and the remainder reflected. But the photon is the smallest energy portion of light, and cannot be divided into parts. So what will happen to it? The experiment shows that the outcome will be random: the photon will go through the PBS with a probability $|\alpha|^2$, and be reflected with a probability $|\beta|^2$.

If a large number N of photons are incident on the PBS (e.g. in the case of a classical wave), on average $|\alpha|^2$N of them will be transmitted, and $|\beta|^2$N reflected. This means that the total flux of energy in the transmitted and reflected channels will be proportional to $|\alpha|^2$ and $|\beta|^2$, respectively. This is remarkably consistent with the classically expected .

As in classical, the part of the classical wave that is transmitted through the PBS will become horizontally polarized. The same happens with photons.

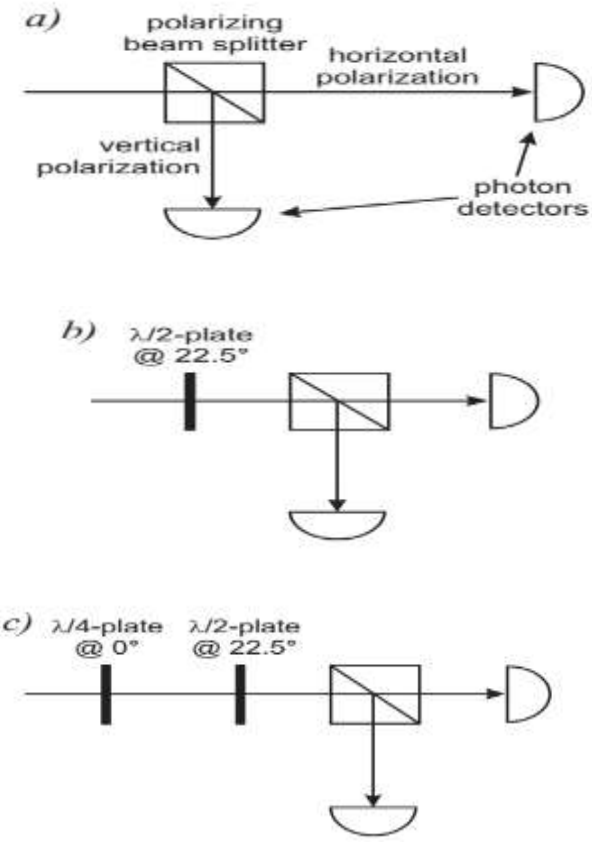
After the PBS, the photon state in the transmitted channel will become $|H\rangle$ (and in the reflected channel $|V\rangle$). If we place a series of additional PBS's in the transmitted channel of the first one, the photon will be transmitted through all of these PBS's.

The photon propagating through a PBS gives us an example of the photon polarization state measurement. Into both output channels of the PBS, we can place single-photon detectors — devices that generate a macroscopic electric pulse whenever a photon hit their sensitive areas. Of the two detectors, only one will click — thus providing us with some information about the photon's initial polarization.

Above, we discussed the apparatus for measuring the polarization of the photon in the canonical basis. What if we want to measure it in some other basis? We can take advantage of the optical element called the wave plate

which inter converts polarization states of a photon into one another. Here are some examples.

Fig 2.1(a-b-c)



The setup shown in Fig. 2.1(a) measures the photon polarization in the canonical ($|H\rangle, |V\rangle$) basis: A polarizing beam splitter sends the horizontal and vertical polarization components to different single-photon detectors. A "click" in one of the detector signifies that a measurement has occurred. This measurement is destructive, because the photon is absorbed by the detector photocathode.

The setup in Fig. 2.1(b) performs the measurement in the diagonal ($|\pm 45^\circ\rangle$) basis: A $\lambda/2$ wave plate at 22.5◦ first converts the +45◦ and -45◦ components into horizontal and vertical and then a polarizing beam splitter sends these into separate detectors .

Measurement in the circular polarization ($|R\rangle$, $|L\rangle$) basis [Fig. 2.1(c)]: a $\lambda/4$ at 0◦ first converts the circular components into ±45◦ components, then a $\lambda/2$

wave plate, again at 22.5◦, converts them into horizontal and vertical components which are then split by a polarizing beam splitter.

Although a single measurement provides us with some information about the initial state of a quantum system, this information is very limited. For example, suppose we have measured a photon in the canonical basis and found that the photon has been transmitted through the PBS. The only thing we learn from this measurement is that the photon was not vertically polarized. But for any other initial state, the result obtained is fully possible.

Suppose now we have performed the same measurement many times. Now we know much more! Since we have the statistics, we can calculate, with some error,

$P_H = |\langle H|\psi\rangle|^2$ and $P_V = |\langle V|\psi\rangle|^2$, i.e. learn about the absolute values of the state components. But the complex phases of these components are still unknown. For example, if we observe $P_H = P_V = 1/2$, state $|\psi\rangle$ could be $|H\rangle$ or $|V\rangle$ or $|+\rangle$ or $|-\rangle$ or many other options. What can we do about this? if we perform additional sets of measurements in other bases. Then we obtain additional numbers, and it is easier for us to solve the equations for α and β. As it turns out, this approach to measuring quantum states can be generalized to other quantum systems, including those of higher dimension. The procedure of obtaining complete information about the quantum state by performing series of measurements in several different bases on the state's multiple identical copies is called quantum tomography.(Noah 2014)

2.10-Polarization qubit:

Let us consider an elementary experiment with light polarization. A light beam is sent to (PBS) whose output ports are monitored by photo detectors. The intensities measured by the detectors will be proportional to squared absolute values $|E_x|^2$ and $|E_y|^2$ of the elements of the Jones vector describing the input beam. Suppose now that we decrease the amplitude of the incident wave and detect light with very sensitive photo detectors, such as photomultipliers. A meaningful question one may now ask is what happens if we send a single

photon to the (PBS)—which of the two detectors will register it? All experimental facts conclude that the outcome is probabilistic: everything that can be predicted is the chance that one or another detector will click.

The polarization of a single photon is described by an object analogous to the Jones vector. It has two complex components α and β, but their interpretation is now different: their squared absolute values $|\alpha|^2$ and $|\beta|^2$ specify the probabilities that the photon will generate a click on one or another detector. Because there is no other path for the photon to take at the exit, we require that the normalization condition

$|\alpha|^2 + |\beta|^2 = 1$ is satisfied. A macroscopic light beam can be thought of as composed of a large number of photons with the same polarization. Therefore it is natural to assume the polarization state of an individual photon is described by the Jones vector rescaled to satisfy the normalization condition. When many photons are sent to the (PBS), this will reproduce the division of classical intensities between the output port. For example, a photon polarized linearly at an angle θ will be described by a vector

$$\begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} \qquad (2.20)$$

and the probabilities of clicks are $\cos^2\theta$ and $\sin^2\theta$. This is the quantum analog of the Malus law.

It will be useful to denote horizontal and vertical polarization states of a single photon with:

$$|H\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |V\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad (2.21)$$

The states $|H\rangle$ and $|V\rangle$ can be identified unambiguously using a (PBS). If we are tasked with encoding a classical message in the form of a string of bits into the polarization of a train of photons, the solution is straightforward: send the

bit value 0 as $|H\rangle$, the bit value 1 as $|V\rangle$ and tell the receiving party to read out the message using a (PBS) and two single-photon detectors.

However, quantum mechanics offers us a possibility to prepare an arbitrary superposition state which can be seen most directly by rewriting ,

$|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$

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

This quantum mechanical generalization of the bit is called a qubit (Banaszek et al., 2012).

Chapter Three

Cryptography

3.1History of Cryptography:-

Human desire to communicate secretly is at least as old as writing itself and goes back to the beginnings of civilization. Methods of secret communication were developed by many ancient societies, including those of Mesopotamia, Egypt, Sudan, India, China, and Japan, but details regarding the origins of cryptology, i.e., the science and art of secure communication, remain unknown.

The ancient Egyptian civilizations left behind document of Hieroglaphs in the Giza pyramids, some of them are attempted to be an early example of secret writing.

The modern history of cryptography can be retained back to Julius Caesar cipher. "Julius Caesar enciphered his dispatches by writing D for A, E for B and so on" (sergienko, 2005). Then Augustus Caesar changed the imperial cipher system to be C written for A, D for B, and so on. The Arabs generalized this idea to the mono alphabetic substitution, in which a keyword is used to permute the cipher alphabet.

There are basically two ways to make a stronger cipher: the stream cipher and the block cipher. In the first one, the encryption rule depend on a plaintext symbol's position in the stream of plaintext symbols, while in the second it encrypt several plaintext symbols at once in a block.

3.2 Cryptographic algorithms:

Encryption and decryption in cryptography are performed by what are so called cryptographic algorithms. They may be mathematical or otherwise. Cryptographic algorithms all in two types :

3.2.1 Restricted cryptographic algorithms:

In which a key is not used in the process of encryption and decryption , and security is based on keeping the way that algorithms ways secret. Unfortunately they are easily broken, so they can be used in low security applications.

3.2.2 key- based cryptographic algorithms:

This cryptography depend on using a secret key, and the key used in the process of encryption and decryption.

The Key-based cryptography has two types: Symmetric and Asymmetric algorithms.

a. Symmetric algorithms:

In symmetric algorithms the process of encryption and decryption requires each party access to the same secret key. This needs to be known to both sides , but need to be kept secret. And this key use by sender to encrypt the message and by the receiver to decrypt it.

Encryption algorithms which have this property are called symmetric cryptosystems or secret key cryptosystems. In fact all historical ciphers pre 1960 are symmetric.

b. Asymmetric algorithms:

There is a form of cryptography which uses two different types of key, one is publicly available and use for encryption whilst the other is private and used for decryption.

These types of cryptosystems are called A symmetric cryptosystems or public key cryptosystems.

Usually in cryptography the communicating parties are denoted by A and B . However often one uses the more user – friendly names of **Alice** and **Bob**. But it is not assume that the parties are necessarily human, one could be describing a communication being carried out between two machines. The Eavesdropper, bad girl, adversary or attacker is usually given the name **Eve.**

3.3 Kirchhoff's Principle :

Cryptosystem are designed to cope with the worst case scenario. If adversary has infinite computing resources , can gain access to plaintext / cipher text pairs and thus can study the relationship between each pair ,and knows the encryption and decryption algorithm. So can abstracts plaintext from cipher text values at will. The only element not accessible to this adversary is the secret key, and thus the security of a cryptosystem depends completely on the security of the key. This is a long standing design philosophy first established by Auguste Kerckhoff 1883: "The security of a cryptosystem must not depend on keeping the secret of the cryptoalgorithm. The security must depends only on keeping the secret of the key" (Kennedy, 2008).

3.4 Key Distribution:

Key establishment is important stage, indeed, cryptography itself would probably vanish if keys could not be produced successfully. However, there is another important task is a key distribution.

Traditionally, symmetric encryption suffered one enormous shortcoming, it was necessary for either the sender or the recipient to create a key and then send it to the other party. While the key was in transit, it could be stolen or copied by a third party who would then be able to decrypt any ciphertexts encrypted with that key.

The one-time pad cipher used physical way to distribute the keys. Users have to agree secretly on the key, a long, random sequence of 0's and 1's. Once they have done this, they can use the key for enciphering and deciphering, and the resulting cryptograms can be transmitted publicly, for example, broadcasted by radio, posted on the Internet, or printed in a newspaper, without compromising the security of the messages. But the key itself must be established between the sender and the receiver by means of a secure channel for example, a secure telephone line, or via a private meeting or hand delivery by a trusted courier.

Such a secure channel is usually available only at certain times and under certain circumstances. Furthermore, even if a secure channel is available, this security can never be truly guaranteed. A fundamental problem remains because, in principle, any classical private channel can be monitored passively, without the sender or receiver knowing that the eavesdropping has taken place. This is because classical physics allows all physical properties of an object to be measured or copied without disturbing those properties. And this is not the same case in quantum theory, which forms the basis for quantum cryptography.

3.5 Quantum cryptography:

Classical cryptography" relies on the use of 'keys' (specific sequence of bits) to encode and decode private messages. In this way the security of a message in transmission through a public channel depends on the security of the key that was used to encode it.

The one-time pad cipher is an example of classical cryptography. In the one-time pad, the sender and receiver share a secret random key. The secret key is composed of a sequence of random bits and it must be as long as the message to be encrypted. The sender encodes the private message with the random

secret key via the addition of each bit of the message with a bit of the key. The receiver, who knows the random secret key, decodes the encrypted message by adding it with the secret key. The security of the one-time pad was mathematically proven by Shannon . And One-time pad If implemented correctly, cannot be broken at any point, even if the eavesdropper has unlimited computational power.

The problem with One-time pad is that the key has to be as long as the message, random, kept secret, and it should be used only once for encryption. Without these conditions, the security of the private message cannot be proven. Hence, the problem of secure communication between two parties translates into a problem of distributing random secret keys between them.
Quantum key distribution (QKD) is a proposal to solve the problem of key distribution between two distant parties.

The first protocol for QKD was proposed in 1984 by Charles Bennett and Gilles Brassard, a protocol that is still widely used . The goal of QKD is to establish a secure key between two parties, typically named Alice (the sender) and Bob (the receiver) who are communicating through a public channel.

The idea behind QKD is to use quantum properties of single photons to distribute a secure key. These properties include the fact that the state of single photons are perturbed when they are measured and also that it is not possible to create a perfect copy of them .

If Alice encodes information in single photons and sends them to Bob, then the two parties can establish an identical and random sequence of bits that is only known to them and nobody else. This string of bits can used as a secret key. An eavesdropper (Eve) can try to intercept the photons in transmission and measure them, but it is impossible to do that without leaving a trace. Also Eve cannot copy the quantum signals and therefore the security of the key in

transmission is, in principle, guaranteed.

The goal of Eve is to obtain full or partial information about the key that is being distributed between Alice and Bob. If Eve obtains information about the key then she can obtain information about the private message. Any errors found in the secret key are attributed to information about the key that Eve has learned through some form of eavesdropping. Note that this means that Alice and Bob can quantify the amount of information that the eavesdropper has about the key. If the disturbance from eavesdropping is below a specific limit, the information that Eve learned can be removed through classical post-processing .

The possibility to verify the security of the key before it is used for encoding is a feature of QKD and is not possible with any classical protocol (William K. Wootters and H. Zurek, 2009).

3.6 Elements of quantum cryptography:

In this content we will mention some of quantum concepts which regard as elements of Quantum Key Distribution.

a-Qubit:

The classical unit of information is the Bit, it can take the values 0 or 1 and it can be identified with the state of a classical system (on-of). In the quantum counterpart the unit of information is the quantum bit or Qubit. A qubit can be implemented using a quantum system; that is to say a system described by two orthogonal basis states.

In mathematical terms, the state of a qubit is a normalized vector in a two-dimensional complex vector space with an inner product $\langle\psi|\psi\rangle = 1$.

Unlike classical bits, qubits can also be in a linear superposition of the basis states: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α and β are complex numbers that satisfy $|\alpha|^2 + |\beta|^2 = 1$.

There are different ways to create qubits. Any degree of freedom belonging to a two-level quantum system can be used. The most relevant using are photons polarization, which give rise to the so-called photonic qubits. The polarization of the photon can be use to form polarization qubits .

When using polarization, the two orthogonal basis states are horizontal $|H\rangle \equiv |0\rangle$ and vertical $|V\rangle \equiv |1\rangle$.

Moreover, a pair of linear superposition of the basis states are defined, for example, by the diagonal polarization states:

$|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$ in which the states $|+\rangle$ and $|-\rangle$ also form a basis.

Another difference between bits and qubits is the measurement process and result. When a classical bit is measured it outputs one of two values, '0' or '1', according to the value that the bit has.

A measurement on a qubit is different since measuring a qubit is only an attempt to determine its state. When a quantum state $|\psi_i\rangle$ is measured, its state is projected onto the subspace $|m\rangle\langle m|$, where $|m\rangle$ is a label of the possible results of the measurement. The probability of projecting onto $|m\rangle$ is given by:

P = $|\langle m|\psi_i\rangle|^2$

This means that the result of the measurement depends on the basis chosen to measure the qubit. For example if the state to be measured is $|\psi\rangle = |0\rangle$ and we measure it in the basis $\{|0\rangle, |1\rangle\}$ then it is projected onto the state $|0\rangle$ 100% of the

time. However, if the state to be measured is $|\psi\rangle = |0\rangle$ and we measure it in the basis $\{|+\rangle, |-\rangle\}$ then it is projected onto the state $|+\rangle$ only with probability $P = \frac{1}{2}$.

In addition , a measurement on a qubit disturbs or modifies its state and the quantum state resulting from the measurement is the new state after the measurement.

Bennet and Brassard realized the use of this fundamental property of quantum states for cryptographic purposes. If the eavesdropper tries to obtain information about the qubits while they are in transmission she must measure them. However, when performing the measurement she changes the quantum state if the basis she chooses to measure is not the same in which the qubit was prepared in, leaving a trace or creating an error that Alice and Bob can detect. In addition, it is fundamentally impossible for Eve to measure a single qubit in two different bases simultaneously (William K. Wootters and H. Zurek, 2009)

b-Nocloning theorem:

The principle of superposition is a cornerstone of quantum mechanics. It says that when two evolving states solve the Schrödinger equation, any linear combination of the two is also a solution. For that reason, waves from the two slits in the double-slit experiment simply add together to create the familiar interference pattern. The superposition principle also prohibits the arbitrary copying of quantum states.

By imagine a machine that can copy the state of a photon or an electron. When the original enters, two copies come out, each having the same state as the original. If such a machine were successful, it would convert the state $|0\rangle$ to $|00\rangle$ and $|1\rangle$ to $|11\rangle$. The problem arises when we send a linear combination, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, through the hypothetical cloner. If $|0\rangle$ and $|1\rangle$ are cloned correctly, then because of the linearity of quantum mechanics, the output for

their superposition must be the superposition of the outputs,

$$|\phi\rangle = \alpha|00\rangle + \beta|11\rangle. \qquad (3.1)$$

But we want $|\psi\rangle\,|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$, the original and a copy of $|\psi\rangle$. That is not the state $|\phi\rangle$ we get! .

Perfect copying can be achieved only when the two states are orthogonal, and even then one can copy those two states (or perhaps a larger collection of mutually orthogonal states) only with a copier specifically built for that set of states. Thus, for example, one can design a copier for any orthogonal pair of polarization states of a photon, but a copier that works for $\{|0\rangle, |1\rangle\}$ will fail for $\{|+\rangle, |-\rangle\}$, and vice versa.

In sum, one cannot make a perfect copy of an unknown quantum state, since, without prior knowledge, it is impossible to select the right copier for the job.

The impossibility of cloning may seem at first an annoying restriction, but it can also be used to one's advantage , for instance, in a quantum key distribution protocols (Itzel, 2013)

c-Entanglement

Entanglement is a purely quantum phenomenon, it is not supplied with a classical counterpart; it is in this way that the quantum state of two or more physical systems depends on the states of everyone of the systems that compose it (Danny Laghi,2013).

For a system of two qubits. Consider the two single photons , each regarded as a 2-state quantum system. Since each photon can be in either of the horizontal $|0\rangle$ or vertical $|1\rangle$ polarization state, classically the two photons are in one of four states – 00, 01, 10, or 11 – and represent 2 bits of classical information.

By the superposition principle, the quantum state of the two photons can be any linear combination of these four classical states:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \qquad (3.2)$$

where $\sum_{ij}|\alpha_{ij}|^2 = 1$

Suppose the first qubit is in the state $\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$, and the second qubit is in the state $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, then the joint state of the two qubits is

$$(\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle)(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle) = \frac{3}{5\sqrt{2}}|00\rangle - \frac{3}{5\sqrt{2}}|01\rangle + \frac{4}{5\sqrt{2}}|10\rangle - \frac{4}{5\sqrt{2}}|11\rangle$$

In fact, there are states such as

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad (3.3)$$

which cannot be decomposed in this way as a state of the first qubit and that of the second qubit. Such a state is called an entangled state. When the two qubits are entangled, we cannot determine the state of each qubit separately. The state of the qubits has as much to do with the relationship of the two qubits as it does with their individual states.

If the first or second qubit of $|\phi^+\rangle$ is measured then the outcome is 0 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$. However if the outcome is 0, then a measurement of the second qubit results in 0 with certainty. This is true no matter how large the spatial separation between the two particles.

The state $|\phi^+\rangle$, which is one of the Bell basis states, has a property which is even more strange and wonderful. The particular correlation between the measurement outcomes on the two qubits holds true no matter which rotated basis are used to measure in. if we use a rotated basis $|v\rangle and |v^\perp\rangle$ where:

$|0\rangle = \alpha|v\rangle + \beta|v^{\perp}\rangle$ and $|1\rangle = -\beta|v\rangle + \alpha|v^{\perp}\rangle$ this can be seen as

$$|\phi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) =$$

$$\frac{1}{\sqrt{2}}((\alpha|v\rangle + \beta|v^{\perp}\rangle)) \otimes ((\alpha|v\rangle + \beta|v^{\perp}\rangle)) - \frac{1}{\sqrt{2}}((-\beta|v\rangle + \alpha|v^{\perp}\rangle)) \otimes ((-\beta|v\rangle + \alpha|v^{\perp}\rangle))$$

$$= \frac{1}{\sqrt{2}}((\alpha^2 + \beta^2)|vv\rangle + (\alpha^2 + \beta^2)|v^{\perp}v^{\perp}\rangle) = \frac{1}{\sqrt{2}}(|vv\rangle + |v^{\perp}v^{\perp}\rangle) \qquad (3.4)$$

d-Entangled Photon Sources:

The ability to produce single photons and entangled photon pairs in desired quantum states is essential in any system intended to handle quantum information. Single photons serve as qubits in quantum computers, and the most powerful operations in those computers are performed by entangling them. Further, entangled pairs of photons are the carriers for signals in quantum cryptography.

Traditionally, single photons could only be produced by the aggressive attenuation of stronger signals. Entangled photons were traditionally produced by spontaneous parametric down conversion. In the latter process, a nonlinear optical crystal annihilates a high-frequency photon and creates two lower-frequency photons. This is a random process with a very low probability of happening, so it requires a very high-intensity source at the input, but this is relatively easy to supply, so SPDC remains a proven method of generating entangled photons.

As random processes, these two methods share a pair of distinct but

related disadvantages: First, it seriously limits the system's ability to produce a photon at a specific time, which is an impediment to creating any kind of clock-based quantum system. Second, it means that there may be multiple photons created at a given time, which destroys the absolute security of quantum cryptography.

The condition that photons should be separated in time may be called Anti bunching or sub-Poisson behavior. These are the photon producers that may properly be called sources of single and entangled photons, and the desire to create effective implementations of them has driven much of the recent research in quantum optics. In the last decade in particular, many novel sources have been developed to address this need (Sources of Single and Entangled Photons Scott Barker November 1, 2011).

It is important to point out that exists a wide variety of nonlinear crystals that can be used for SPDC in a given range of frequencies [6]. That is the case of KTiPO3, RbTiPO4, LiNbPO3, LiTaO3 and BaB2O4. In fact, most of the nonlinear crystals are birefringent, therefore they produce two types of phase matching, or regimes where we have constructive interference. Such phase matching condition obeyed the conservation of energy and momentum. We have two types of phase matching , type I and type II. In type I the down-converted photons are parallel to each other and perpendicular to the pump photon, while type II the down-converted photons have orthogonal polarizations.

Other important sources are semiconductor nanostructures, particularly quantum dots, where electrons and holes can be trapped to form excitonic

complexes (states consisting of bound electron–hole pairs) that eventually will suffer radioactive decay similarly to atomic cascades.

In fact this technique is closely related to the generation of entangled photons in single atoms, therein the reason to call quantum dots as artificial atoms. In such radioactive decay process photons emits entangled photons with certain polarization that can be controlled. It is important to mention that this technology has made real the possibility to have compact sources of entangled photons. Example of that can be devices like semiconductor light emitting diodes.(O.S. Magaña 2010)

The most popular method of producing entangled photons is through spontaneous parametric down conversion (SPDC). A 100mW ion-argon laser pump beam is incident on a pair of orthogonally polarized type I Beta Barium Borate crystals. As the pump beam interacts with these nonlinear crystals, single photons split into entangled "signal" and "idler" photons with wavelengths longer than the pump. Because a type I crystal is used, the polarization of the signal and idler photons will be identical but opposite of the pump polarization.(*Graham Jensen* 2017).

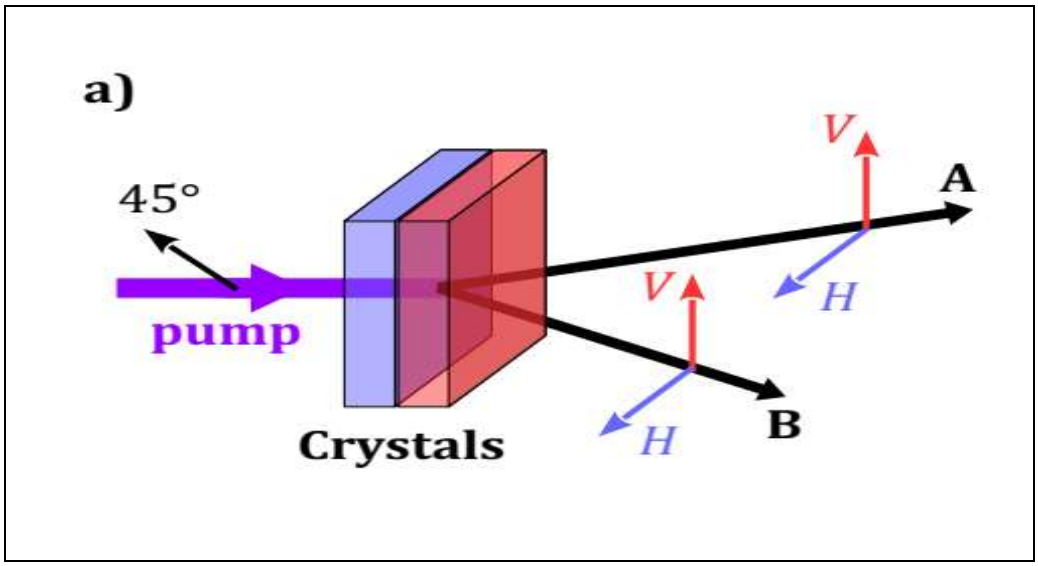


Fig.3.1 generation of polarizing-entangled photon states with nonlinear crystal. (Adeline.al 2017)

3.7 Electro-optic modulator (EOM):

EOM is an optical device in which a signal-controlled element exhibiting the electro-optic effect is used to modulate a beam of light. The modulation may be imposed on the phase, frequency, amplitude, or polarization of the beam. Modulation bandwidths extending into the gigahertz range are possible with the use of laser-controlled modulators.

The electro-optic effect is the change in the refractive index of a material resulting from the application of a DC or low-frequency electric field. This is caused by forces that distort the position, orientation, or shape of the molecules constituting the material. Generally, a nonlinear optical material (organic polymers have the fastest response rates, and thus are best for this application) with an incident static or low frequency optical field will see a modulation of its refractive index.

The simplest kind of EOM consists of a crystal, such as lithium niobate, whose refractive index is a function of the strength of the local electric field. That means that if lithium niobate is exposed to an electric field, light will travel more slowly through it. But the phase of the light leaving the crystal is directly proportional to the length of time it takes that light to pass through it. Therefore, the phase of the laser light exiting an EOM can be controlled by changing the electric field in the crystal.

Note that the electric field can be created by placing a parallel plate capacitor across the crystal. Since the field inside a parallel plate capacitor depends linearly on the potential, the index of refraction depends linearly on the field (for crystals where Pockels effect dominates), and the phase depends linearly on the index of refraction, the phase modulation must depend linearly on the potential applied to the EOM.

The voltage required for inducing a phase change of $\frac{\pi}{2}$ is called the half-wave voltage. For a Pockels cell, it is usually hundreds or even thousands of volts, so that a high-voltage amplifier is required. Suitable electronic circuits can switch such large voltages within a few nanoseconds, allowing the use of EOMs as fast optical switches.

Depending on the type and orientation of the nonlinear crystal, and on the direction of the applied electric field, the phase delay can depend on the polarization direction. A Pockels cell can thus be seen as a voltage-controlled wave plate, and it can be used for modulating the polarization state. For a linear input polarization (often oriented at 45° to the crystal axis), the output polarization will in general be elliptical, rather than simply a linear polarization state with a rotated direction.

3.8 EPR Paradox:

In 1935 Albert Einstein, Boris Poldosky, and Nathan Rosen published the paper, Can quantum-mechanical description of physical reality be considered complete?. The problem lined out therein was later named the EPR paradox, after its authors (Qubits and Quantum Measurement ,Chapter 1, 2018).The aim of the paper was to demonstrate, on theoretical grounds, that quantum theory, and more specifically the quantum wave function, does not contain all the information about a system. In other words, all Information that interpreted as the theoretical elements, should be have a corresponding element in physical reality.

That means the results predicted by the theory agrees with what can be observed by experiments. And secondly that all things that have a physical reality have a theoretical counterpart in the theory. In other words the theory should describe all of reality and be correct.

By consider a system of one particle that has only one degree of freedom and is described by the wave function . And the observable physical quantity $|\psi\rangle$ of this system corresponding to the quantum mechanical operator **A**, since $A|\psi\rangle = a|\psi\rangle$: If *a* is a number it is true that the physical quantity $|\psi\rangle$has the value *a*. According to the criterion of physical reality we may regard there is an element of physical reality corresponding to the measured value of$|\psi\rangle$. In other words we have measured something that exists. In quantum mechanics it is true that if two different physical quantities have the non commuting operators *X* and *Y* , so that XY ≠ Y X, then it is not possible to know them both simultaneously. This means for the previously stated, that quantum mechanics is either incomplete as it cannot describe both of the physical quantities corresponding to the operators at once, or that the physical quantities themselves do not exist simultaneously. This is referred to as the quantities not having simultaneous reality(Danny Laghi, 2013)

The main argument of EPR is based on three requirements:

a-Completeness: Every element of physical reality must have a counterpart In the physical theory in order for the theory to be complete.

b-Realism: If the value of a physical quantity can be predicted with certainty, without disturbing the system, then the quantity has physical reality.

c-Locality: There is no action at a distance. Measurements on a (sub)system do not affect measurements on (sub)systems that are far away.

EPR then conclude that under certain circumstances quantum mechanics is not a complete theory.

To understand this claim, let us consider two spin $\frac{1}{2}$ particles in the spin entangled state $|\Psi^-\rangle$, (the antisymmetric Bell state) , and let them propagate

in opposite direction along x-axis from the source . let then two observers , Alice and Bob , perform spin measurement along the z-direction . quantum mechanics tell us that for state,

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle\right) \qquad (3.5)$$

The result measured by Alice undetermined , i.e. either ↑ or ↓ , but if Alice measure ↑ , then Bob will measure ↓ with certainty and vice versa, which a sings physical reality to the spin of Bob's particle in the sense of EPR. Since there is no disturbance or action at a distance , EPR conclude , quantum mechanics does not contain any information about predetermined measurement outcomes and is there for incomplete.

To account for the missing information , there must be some inaccessible parameter, a hidden variable , to determine which spin eigen value is realized in the measurement . EPR then demand a hidden variable theory (HVT) to explain this problem.

In the same year as the EPR paper was published , Bohr replied (using the same title for his paper as EPR , i,e. "can quantum- mechanical description of physical reality be considered complete ?" criticizing their perception of reality and sweeping away their arguments without really answering the interesting paradox presented in the EPR paper. But due to Bohr's great authority the physical community followed his view that the quantum mechanics is complete and the case rested for nearly 30 years until John Bell published his famous article in 1964 , presenting away to solve the debate (A. EINSTEIN, 1935).

3.9 Bell's Theorem

John Bell published his paper On the Einstein Podolsky Rosen Paradox in

1964, and in it he proved that any local deterministic hidden variable theory is incompatible with the predictions of quantum mechanics.

The hidden variable idea rests on the thought that quantum mechanics as we know it only offers a statistically correct description of reality, and that there are some finer details (hidden variables) that are waiting deeper down.

Bell's work produced, among other things, the Bell inequalities, a set of inequalities which any local hidden variable theory that takes separability into consideration must satisfy in some form. Quantum mechanics does not satisfy these, and hence the predictions of hidden variable theories and quantum mechanics are differ.

3.9.1 Derivation of Bell's First Inequality

Arguing against the simplified form of the EPR paradox presented by David Bohm, Bell derived his result as follows.

The spin of the two particles is denoted as σ_1, σ_2. The spins can be measured along the unit vectors **a** and **b** to yield the results A = $\sigma_1 \cdot$ **a** and B = $\sigma_2 \cdot$**b** respectively. The assumption is made that the orientation of the measurement vectors **a** and **b** can be chosen independently of each other. Hidden variable theories hold that the spin of the particles are described by one or more parameters in such a way as to form a more complete description of the state than the description given by quantum mechanics. Let this parameters be λ, the measurement of $\sigma_1 \cdot$ **a** yielding **A** can then be described by **a** and λ. And similarly $\sigma_2 \cdot$**b** yielding **B** can be described by **b** and λ. The dependences of **A** and **B** on λ are not restricted by any assumptions apart from the locality assumption which may be formulated as

$$[A(\mathbf{a})B(\mathbf{b})](\lambda) = A(\mathbf{a}, \lambda)B(\mathbf{b}, \lambda) \qquad (3.6)$$

This equation states that A and B have a separate dependence upon λ. They can be described as separate systems.

The possible results of a spin measurement on a spin-$\frac{1}{2}$ particle are $\pm\frac{\hbar}{2}$. To simplify it is assumed instead that

$$A(\mathbf{a}, \lambda) = \pm 1; \quad B(\mathbf{b}, \lambda) = \pm 1 \tag{3.7}$$

Let $\rho(\lambda)$ be the probability distribution of the hidden variable parameter. The only assumption made about this distribution is that it is normalized and therefore must equal unity when integrated over all the possible values of λ,

$$\int \rho(\lambda) d\lambda = 1 \tag{3.8}$$

The quantum mechanical expectation value of the product of A and B is

$$E_{QM} = \langle \psi | (\sigma_1.a).(\sigma_2.b) | \psi \rangle = -a.b \tag{3.9}$$

whence it follows that if

$$a = b \Rightarrow \langle \psi | (\sigma_1.a).(\sigma_2.b) | \psi \rangle = -1 \tag{3.10}$$

The above equation expresses spin conservation and it is important to note that given the locality assumption (3.7) and the assumption that the measurement directions **a** and **b** can be chosen independently the above equation implies determinism. If the two measurements and systems cannot affect each other, occur along the same axis and we know that one will measure as spin up and the other as spin down (3.5), then they must have had those properties all along.

If hidden variable expectation value E is given by,

$$E = \int \rho(\lambda) A(a, \lambda) B(b, \lambda) d\lambda \tag{3.11}$$

Taking (3.7) and (3.8) into account it follows that E (equation (3.6)) cannot be lower than -1. Furthermore E is equal to -1 for a = b if and only if

$$B(b, \lambda) = -A(a, \lambda)$$

Assuming $B(b, \lambda) = -A(b, \lambda)$ according to (3.11) for all possible values of λ, yields the expectation value

$$E = -\int \rho(\lambda) A(a, \lambda) A(b, \lambda) d\lambda \tag{3.12}$$

Now introducing a third unit vector **C** as a direction for the spin measurement.

The result of a measurement **C** of the **c** component of the spin depends on the hidden variable parameter λ though again no assumptions are made as to the nature of that dependence.

Defining the expectation value of the measurement of the product of A and C following the same procedure as led up to equation (3.12) allows us to write the expectation value difference

$$E(a,b)-E(a,c)=-\int \rho(\lambda)[A(a,\lambda)A(b,\lambda)-A(a,\lambda)A(c,\lambda)]d\lambda \qquad (3.13)$$

Using the fact that $A(b;\lambda)^2 = 1$ which is a consequence of (3.7), equation (3.13) can be written as

$$E(a,b)-E(a,c)=\int \rho(\lambda)A(a,\lambda)A(b,\lambda)[A(b,\lambda)A(c,\lambda)-1]d\lambda \qquad (3.14)$$

From (3.7) we have that

$$\left|A(b,\lambda)A(c,\lambda)-1\right|=1-A(b,\lambda)A(c,\lambda)$$

and also that

$$\left|A(a,\lambda)A(b,\lambda)\right|=1$$

Rewriting (3.14) as $\int f(a,b,c,\lambda)d\lambda$

where f is a function of a, b, c, and λ, it must hold that

$$\left|\int f(a,b,c,\lambda)d\lambda\right|\le\int|f(a,b,c,\lambda)|d\lambda \qquad (3.15)$$

Therefore Bell's inequality can be derived from equation (3.9)

$$\left|E(a,b)-E(a,c)\right|\le\int\rho(\lambda)d\lambda(1-A(b,\lambda)A(c,\lambda)) \qquad (3.16)$$

The second term on the right side of the inequality is precisely the expectation value of a measurement of the product of B and C (equation (3.7) with a = c). And so the inequality can be written as

$$\begin{aligned}&\left|E(a,b)-E(a,c)\right|\le\int\rho(\lambda)d\lambda-\int\rho(\lambda)d\lambda A(b,\lambda)A(c,\lambda)\Rightarrow\left|E(a,b)-E(a,c)\right|\le 1+E(b,c)\\&\Rightarrow\left|E(a,b)-E(a,c)\right|-E(b,c)\le 1\end{aligned} \qquad (3.17)$$

This is Bell's inequality, and all deterministic hidden variable theories preserving locality must satisfy it. Straying from Bell's original paper the disagreement between quantum mechanics and local hidden variable theories

can be illustrated using the following counterexample first presented by Clauser and Shimony .

Take a, b and c to lie in the same plane with the angle from a to b being $\frac{\pi}{3}$ radians. And c is such that the angle from b to c is also $\frac{\pi}{3}$ radians thereby making the angle between a and c $2\frac{\pi}{3}$ radians. Using the fact that $\frac{a.b}{|a|.|b|} = \cos\theta$, where θ is the angle between the vectors, we have that

$$a \cdot b = b \cdot c = \cos\frac{\pi}{3} = \frac{1}{2}; \quad a \cdot c = \cos 2\frac{\pi}{3} = -\frac{1}{2} \qquad (3.18)$$

because a, b and c are unit vectors and therefore their magnitude is unity. Using the quantum mechanical expectation values (3.4) instead of the expectation values for the hidden variable description of reality in the inequality (3.12) yields

$$\left|-\frac{1}{2}-\frac{1}{2}\right| \le 1-\frac{1}{2} \Rightarrow 1 \le \frac{1}{2} \qquad (3.19)$$

This is a clear violation of Bell's inequality. Quantum mechanics and in other side all deterministic hidden variable theories preserving locality ,give different predictions of experimental outcomes and therefore different descriptions of reality. But many experiments have validated the predictions made by quantum mechanics.

3.9.2 CHSH inequality:

The original Bell inequality (3.12) relies strongly on the fact that equation (3.5) holds perfectly. An experiment testing this Bell inequality requires the use of perfect analyzers and detectors. Such devices do not exist (A. EINSTEIN et al., 1935). Therefore Bells theorem cannot be verified using this relation. In 1969 J.F. Clauser, M.A. Horne, A. Shimony and R.A. Holt presented the CHSH

inequality, which is a Bell inequality that does not use this assumption and is therefore more suitable for experimental verification (Hoglund, 2013).

Labeling λ the set of additional parameters and A(λ, a) and B(λ, b) the results respectively obtained from analyzer 1 oriented respectively along **a**, and analyzer 2 oriented along **b,** these quantities can only assume values ± 1 hence the quantity $\frac{1}{2}[1+A(\lambda,a)]$ could assume only values +1 (in case of result +1 and 0 otherwise), and analogously, the quantity

$$\frac{1}{2}[1-A(\lambda,a)] \qquad (3.20)$$

could assume only values +1 (in case of result -1 and 0 otherwise). Hence, given the probability distribution of λ, that is $\rho(\lambda)$, the expectation values for single detection are found to be:

$$P_{\pm}(a)=\frac{1}{2}\int d\lambda\rho(\lambda)[1\pm A(\lambda,a)]$$

$$P_{\pm}(a)=\frac{1}{2}\int d\lambda\rho(\lambda)[1\pm B(\lambda,b)] \qquad (3.21)$$

Whereas for combined detections:

$$P_{++}(a,b)=\frac{1}{4}\int d\lambda\rho(\lambda)[1+A(\lambda,a)][1+B(\lambda,b)]$$

$$P_{--}(a,b)=\frac{1}{4}\int d\lambda\rho(\lambda)[1-A(\lambda,a)][1-B(\lambda,b)]$$

$$P_{+-}(a,b)=\frac{1}{4}\int d\lambda\rho(\lambda)[1+A(\lambda,a)][1-B(\lambda,b)]$$

$$P_{-+}(a,b)=\frac{1}{4}\int d\lambda\rho(\lambda)[1-A(\lambda,a)][1+B(\lambda,b)] \qquad (3.22)$$

Substituting these quantities in correlation coefficient,

$$E(a,b) = P_{++}(a,b) + P_{--}(a,b) - P_{+-}(a,b) - P_{-+}(a,b)$$

After some straightforward passage, find that the correlation coefficient, averaged over the distribution of λ, is given by:

$$E(a,b) = \int d\lambda \rho(\lambda) A(\lambda,a) B(\lambda,b) \qquad (3.23)$$

Now define a new quantity, that allowed us to write the inequalities representing in explicit form, the correlation coefficient quantity which can be denoted by,

$$\begin{aligned} S(\lambda,a,a',b,b') &= A(\lambda,a)B(\lambda,b) - A(\lambda,a)B(\lambda,b') + A(\lambda,a')B(\lambda,b) + A(\lambda,a')B(\lambda,b') \\ &= A(\lambda,a)[B(\lambda,b) - B(\lambda,b')] + A(\lambda,a')[B(\lambda,b) + B(\lambda,b')] \end{aligned} \qquad (3.24)$$

since A and B can assume only the value ± 1, then

$$S(\lambda,a,a',b,b') = \pm 2, \qquad (3.25)$$

From which averaging over the distribution of λ one gets,

$$-2 \le \int d\lambda \rho(\lambda) S(\lambda,a,a',b,b') \le +2$$

That yield

$$-2 \le [S = E(a,b) - E(a,b') + E(a',b) + E(a',b')] \le +2 \qquad (3.26)$$

These inequalities are well-known as BCHSH inequalities. These inequalities are based on a combination of four correlation coefficient of polarization, measured along four orientations of the polarizers. Then S is measurable quantity.

However, CHSH inequalities in some particular situations are in conflict with Quantum Mechanics. Indeed if we put the system in the angles,

$$\theta_{ab} = \theta_{a'b} = \theta_{a'b'} = \frac{\pi}{8}$$

$$\theta_{ab'} = \theta_{ab} + \theta_{a'b} + \theta_{a'b'} = 3\frac{\pi}{8}$$

Substituting the quantities E with their quantum mechanical values we get,

$$S = E(a,b) - E(a,b') + E(a',b) + E(a',b')$$

$$S = E(22.5) - E(67.5) + E(22.5) + E(22.5) \quad \text{and,}$$

$$E_{QM}(a,b) = \cos(2\theta_{ab})$$

So,

$$S_{QM} = \cos(45) - \cos(135) + \cos(45) + \cos(45)$$

$$S_{QM} = 2\sqrt{2} \qquad (3.27)$$

This quantum prevision deeply violates the upper limit of inequalities.

With respect of three independent angle when

$\theta_{ab} = \theta_{a'b} = \theta_{a'b'} = \theta$ one find

$$S_{QM}(\theta) = 3\cos(2\theta) + \cos(6\theta) \qquad (3.28)$$

This equation representing the behavior of S varying with angle θ.

In conclusion, Bell's Theorem brings out a conflict between theories with hidden variables and certain quantum mechanical previsions and provides a quantitative criterion to clarify this conflict (William K. Wootters and H. Zurek 2009).

3.10 Quantum Channels

Quantum states can be used to transmit information between two authorized parties, conventionally named Alice and Bob. Theoretically, it will make no difference whether atoms, ions, molecules, electrons or any other quantized particles are involved in the exchange. From a practical perspective, however, it is the quantum of light – the photon – which is the preferred option, because photon quantum states can be transmitted over longer distances without

decoherence than the other quantum candidates. There are losses due to scattering, but provided they are accounted for and dealt with effectively they do not affect the overall security of a QKD protocol.

Any medium which allows light to propagate will henceforth be referred to as a ‘quantum channel’. (Examples are line-of sight free space or optical fibers.). The channel itself is not quantum, it merely carries quantum information.

3.11 Quantum Theory and Quantum Key Distribution

Quantum key distribution uses basic quantum properties to detect eavesdroppers in one of two ways: either by relying on the Heisenberg Uncertainty Principle or by the violation of Bell’s Inequalities in entanglement based schemes. Heisenberg - based protocols use the fact that measuring a quantum state changes it: the eavesdropper will introduce errors into the information transfer along a quantum channel which should always be detected by the protocol.

Entanglement - based protocols do not have any information to eavesdrop! Information only springs into existence when the entangled quanta are measured: the eavesdropper’s only potential ploy is to attempt to inject extra quanta into the protocol. The extra quanta decrease the value of Bell’s inequality, and so the eavesdropper will also be detected in this case. Quantum no-cloning further ties the eavesdropper’s hands, as no copies of quanta can be taken for processing later.

3.12 Quantum Key Distribution Protocols, general methodology :

quantum mechanical properties can be used to transfer information from Alice to Bob, and any attempted eavesdropping by Eve will always be detectable.

But how can this be turned into a working cryptographic key distribution protocol? A combination of quantum processing and well established classical procedures is needed.

Three distinct stages are needed: raw key exchange, key sifting and key distillation, with the option to discard the secret key at any of the stages if it is deemed that not enough security could be obtained from it.

3.12.1.Raw Key Exchange

This is the only quantum part of Quantum Key Distribution! Alice and Bob exchange 'some quantum states' so quantum information is passed along a quantum channel from Alice to be measured by Bob, with or without the presence of Eve.

3.12.2.Key Sifting

Alice and Bob decide (classically) between them which of the measurements will be used for the secret key. The decision making rules depend on which protocol is being used, and some measurements will be discarded e.g. if the settings used by Alice and Bob did not match.

3.12.3.Key Distillation

The need for further processing after the key sifting stage was determined by Bennett et al when reviewing experimental results (practical channels are lossy, and the protocol needs to be workable even in the presence of transmission errors) and how the use of an authenticated public channel could repair the information losses from an imperfect private channel. Thus error correction and privacy amplification are required, which are the first two steps in the key distillation stage of the classical post-processing of the remaining secret key bits. The third (and arguably most important!) final process is authentication, which counteracts man-in-the-middle attacks (MITM).

3.13.BB84 Protocol

The BB84 protocol is the most popular QKD protocol at the moment. It is named after its inventors, Bennett and Brassard .

The procedure of BB84 is as follows .

• In BB84, Alice sends Bob a sequence of photons, each independently chosen from one of the four polarizations vertical, horizontal, 45-degrees and 135-

degrees.

•For each photon, Bob randomly chooses one of the two measurement bases (rectilinear and diagonal) to perform a measurement.

• Bob records his measurement bases and results. Bob publicly acknowledges his receipt of signals.

• Alice broadcasts her bases of measurements. Bob broadcasts his bases of measurements

Table 3.1: Procedure of BB84 protocol:

Alice's bit sequence	1	0	1	1	0	1	0	0	0	1
Alice's basis	×	+	+	+	×	+	×	×	+	×
Alice's photon polarization	↘	↔	↕	↕	↗	↕	↗	↗	↔	↘
Bob's basis	+	+	×	+	+	×	×	+	+	×
Bob's measured polarization	↕	↔	↘	↕	↔	↗	↗	↕	↔	↘
Bob's sifted measured polarization		↔		↕			↗		↔	↘
Bob's data sequence		0		1			0		0	1

• Alice and Bob discard all events where they use different bases for a signal. The remaining bits are defined as \sifted bits".

• Alice and Bob each convert the polarization data of all remaining data into a binary string called a raw key (by, for example, mapping a vertical or 45-degrees photon to \0" and a horizontal or 135-degrees photon to \1"). They can perform classical post-processing such as error correction and privacy amplification to generate a final key.

3.14 B92 Protocol

The B92 protocol is a variant of the BB84 scheme, still using polarized photons, but this time with non-orthogonal quantum states for encoding information. Two quantum states are used, instead of the four required in BB84. Alice randomly chooses one or other of these quantum states and sends them to Bob via a quantum channel. Bob has two methods to measure the arriving photons, which will either register “detection” or “no detection”.

During the Key Sifting stage, Bob tells Alice which photons he "detected", but not his actual measurement, and all other photons are discarded. Error correction and privacy amplification continue as normal, to verify that the secret key is the same for both Alice and Bob.

3.15 E91 Protocol

In 1991, Ekert proposed a method of using Bell's inequalities to perform key distribution via entangled polarized photons in a quantum channel. These entangled photons can be created by Alice, Bob or a trusted third party (TTP), and each pair is separated in a way that results in Alice and Bob receiving one of each pair. This is arguably a more secure method of using polarized photons, as there is not information to be eavesdropped: it only springs into existence at the moment of measurement.

Alice and Bob both independently and randomly choose from two different orientations of their analyzers to measure the polarizations of the photons, and the choice of analyzer is the basis for the publicly discussed key sifting stage. The measurements are divided into two groups: the first is when different orientations of the analyzer were used, and the second when the same analyzer orientation was employed. Any photons which were not registered are discarded. Alice and Bob then reveal the results of the first group only, and check that they correspond to the value expected from Bell's inequality ($2\sqrt{2}$): if this is so, then Alice and Bob can be sure that the results they obtained in the second group are correlated and can be used to produce a secret key string (Sheila Cobourne,2011).

3.16 Literature review:

Quantum Key Distribution(QKD) is a new technology for protecting sensitive data during transmission process in a new communications environment. So, many researchers have focused on the simulation of QKD to achieve a secure communication for files depending on different simulator environments.

(Shuang Zhao1.al 2007) proposed an event-by-event simulation model and polarizer as the simulated component for QKD protocols i.e. BB84 protocol by Bennet and Brassard and Ekert's protocol with presence of Eve and misalignment measurement as scenarios. they used Wigner inequality and 10^8 photon pairs.

D. S. Naik et al., in (1999) proposed the ways of Eavesdropping on the Ekert's protocol. They investigated several possible eavesdropper strategies, including pseudo-quantum non-demolition measurements. and they discuss a procedure to increase her detectability. In a typical 10 minute run of their system, they observed S=2.67 for the 40 minutes of collected data(real experiment).

Sara Idris Babiker Mustafa in 2005. Presented simulation software for a quantum cryptography based on Ekert . they considered Bell's theorem in simulation . there work without representing Eavsdropper.(S=2.5)

Dietrich Dehlinger and M. W. Mitchell in (2002). used polarization-entangled photon pairs to demonstrate quantum non-locality in an experiment. The photons are produced by spontaneous parametric down conversion using a violet diode laser and two nonlinear crystals. they demonstrated polarization correlations of the entangled photons. A test of the Clauser, Horne, Shimony, and Holt version obtained S= 2.30760.035. (real experiment).

Siddeq Y.Ameen et al. in (2006) proposed a model of Ekert protocol using more than three angles to calculate Bell's inequality . and they used Jones matrices to model the optical components.

H. De Raedt.al (2010) they discuss recent progress in the development of simulation algorithms that do not rely on any concept of quantum theory but are nevertheless capable of reproducing the averages computed from quantum theory through an event-by-event simulation. The simulation approach is illustrated by applications to Einstein–Podolsky–Rosen–Bohm experiments with photons. They used 10^6 photons pairs and obtained S=2.73.

K. Michielsen.al (2014) . they found S = 2:62 which compares very well with the values between 2 and 2.57 extracted from different sets of experimental data of Weihs *et al.* However, for W = 2 ns (results not shown), the results for the two-particle correlations fit very well to the prediction of quantum theory for the EPRB experiment. From these data we extract S = 2:82.

CHAPTER FOUR

Event-based simulation of quantum physics experiments

4.1 Introduction:

Computer simulation is widely regarded as complementary to theory and experiment (D.P. Landau, K.al 2000). The standard approach is to start from one or more basic equations of physics and to employ a numerical algorithm to solve these equations. This approach has been highly successful for a wide variety of problems in science and engineering. However, there are a number of physics problems, for which this approach fails, simply because there are no basic equations to start from. Indeed, as is quantum theory has nothing to say about individual events . Reconciling the mathematical formalism that does not describe individual events with the experimental fact that each observation yields a definite outcome is referred to as the quantum measurement paradox and is the most fundamental problem in the foundation of quantum theory .
In view of the quantum measurement paradox, it is unlikely that we can find algorithms that simulate the experimental observation of individual events within the framework of quantum theory. Of course, we could simply use pseudo-random numbers to generate events according to the probability distribution that is obtained by solving the time-independent Schrodinger equation. However, the challenge is to find algorithms that simulate, event-by-event, the experimental observations of, for instance, interference without first solving the Schrodinger equation(H. De Raete.al 2010)

The mathematical framework of quantum theory allows for calculation of numbers which can be compared with experimental data as long as these numbers refer to statistical averages of measured quantities, such as

an interference pattern, and the specific heat (Michielsen and Raedt, 2010) .

But in some experiments like single-particle interference experiments the interference pattern is built up by successive discrete detection events, and in Bell-test experiments the two-particle correlations are computed as averages of pairs of individual detection events recorded at two different detectors and seen to take values which correspond to those of the singlet state in the quantum theoretical description.

So why individual entities which do not interact with each other can exhibit the collective behavior that gives rise to the observed interference pattern and why two particles, which only interacted in the past, after individual local manipulation and detection can show correlations corresponding to those of the singlet state.

An event-based simulation model provide answer by reproduces the statistical distributions of quantum theory without solving a wave equation but by modeling physical phenomena as a sequence of events whereby events can be particle emissions by a source, signal generations by a detector, interactions of a particle with a material and so on.

The assumption of the event-based simulation approach is that from current scientific knowledge derives from the discrete events which are observed in laboratory experiments and from relations between those events, event-based simulation approach can provide what we can say about these experiments but not what \really" happens in Nature. The general idea of the event-based simulation method is that simple rules define discrete-event processes which may lead to the behavior that is observed in experiments. The basic strategy in designing these rules is to carefully examine the experimental procedure and to devise rules such that they produce the same kind of data as those recorded in experiment.

Event based model started by search for useful rules by asking question in example by what kind of discrete-event rule should a beam splitter operate in order to mimic the build-up, event-by-event, of the correlation observed in the EPR experiment.

The event-based approach has successfully been used for simulations of Mach-Zehnder interferometer experiments and quantum cryptography protocols.

In this chapter, we used the event-based simulation method to build Ekert's protocol of quantum cryptography a summing that the source of entangled photon operate by using laser beam. And we will test whether or not a Bell-CHSH (Clauser Horne-Shimony-Holt) inequality can be violated. And we will use the variation in CHSH value to detect the case of eavesdropping.

4.2 Ekert's Protocol:

In 1991, Artur K. Ekert suggested a different approach for quantum key distribution . His idea is based on entangled particles with the help of Bell's theorem, it can be tested if eavesdropping has take place. The Ekert protocol, also called Einstein-Podolsky-Rosen protocol due to its direct connection to the EPR paradox.

The protocol works as follows:

A source emits pairs of qubits in a maximally entangled state like:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad (4.1)$$

• Alice and Bob choose randomly between three bases, obtained by rotating the horizontal-vertical basis $\oplus$ around the z-axis by angles :

$$\phi_1^a = 0 \quad , \quad \phi_1^b = 0$$

$$\phi_2^a = \frac{1}{8}\pi \quad , \quad \phi_2^b = \frac{1}{8}\pi \qquad (4.2)$$

$$\phi_3^a = \frac{1}{4}\pi \quad , \quad \phi_3^b = -\frac{1}{8}\pi$$

Where ϕ^a is the Alice choice angle, and ϕ^b is Bob choice angle.

• After the transmission has taken place, Alice and Bob release publicly which basis they have chosen for each measurement. They separate the measurements into three groups:

First group: Consisting of measurements using different orientation of the analyzers.

Second group: Consisting of measurements using the same orientation of the analyzers.

Third group: Consisting of measurements in which at least one of them failed to register a particle.

Note that the first group is used to test Bell's inequalities and the second group to establish a secure key, while the third group is discarded.

• Finally, Alice and Bob announce publicly only their results of the first group. Thus, they can check if eavesdropping has taken place.

If no eavesdropper has perturbed the system, Alice and Bob can use the measurements of the second group to obtain a secret string of bits, known as the key.

Assuming a source that emits pairs of photons, each measurement can yield two results:

• +1 for photons that are measured in the first polarization state of the chosen basis

• -1 for photons that are measured in the second polarization state of the chosen basis

Revealing the basis, Alice and Bob can obtain a bit of information. Alice and Bob calculate statistic correlation using equation(4.3),In order to check the eavesdropping.

$$E(\phi_i^a,\phi_j^b) = P_{++}(\phi_i^a,\phi_j^b) + P_{--}(\phi_i^a,\phi_j^b) - P_{+-}(\phi_i^a,\phi_j^b) - P_{-+}(\phi_i^a,\phi_j^b) \qquad (4.3)$$

which is the correlation coefficient of the measurements performed by Alice and Bob in the independently and randomly chosen basis. $P_{+-}(\phi_i^a,\phi_j^b)$ denotes the probability that +1 has been obtained by Alice in the basis rotated by the angle ϕ_i^a and -1 by Bob in the basis rotated by the angle ϕ_j^a.

According to the quantum rules

$$E(\phi_i^a,\phi_j^b) = \cos[2(\phi_i^a - \phi_j^b)] \qquad (4.4)$$

For bases with the same orientation, in this case ϕ_1^a ; ϕ_1^b and ϕ_2^a; ϕ_2^b, quantum mechanics predicts total correlation. So Alice and Bob obtain

$$E(\phi_i^a,\phi_j^b) = \cos[2(\phi_i^a - \phi_j^b)] = 1 \qquad (4.5)$$

The correlation coefficients for which Alice and Bob used bases with different orientation can be composed to define the quantity S,

$$S = E(\phi_1^a,\phi_2^b) + E(\phi_1^a,\phi_4^b) + E(\phi_3^a,\phi_2^b) - E(\phi_3^a,\phi_4^b) \qquad (4.6)$$

This quantity S is the generalized Bell's theorem proposed by Clauser, Horn, Shimony and Holt, better known as CHSH inequality . Quantum mechanics predicts,

$$S = 2\sqrt{2} \qquad (4.7)$$

CHSH inequality can be used to guarantee a secure key distribution. Recalling that the Alice and Bob have divided their measurements into three groups, they can now use their results of the first group (measurements with different orientation) to establish the value of *S*. If

the particles were not directly or indirectly disturbed by Eve, they should reproduce the result of equation (4.7).This assures that the results of the second group (measurements with the same orientation) are correlated and can be used to establish a secure key .

4.2.1 Eavesdropping:

Eve always trays to get information about the transmitted key. In order to emphasis that Bell's theorem can indeed detect eavesdropping, it is useful to take a closer look at an eavesdropper, strategies. Eve gets no useful information, if she intervenes during the transmission, because at this time no information is encoded in the particles. The requested information is "formed" only after the measurements done by the legitimate users and the public announcement have taken place.

One strategy may be that Eve substitutes her own prepared data for Alice's and Bob's data to misguide them. But because she does not know which orientation of the analyzers the two will choose, Eve's tampering will eventually be detected. In this case, Eve's intervention will be the same as introducing elements of physical reality to the polarization directions and will lower S below its quantum value.
The most favorable method for eavesdropping is Eve herself prepares each particle separately giving her total control over the state of individual particles. The well defined polarization directions may vary from pair to pair. Therefore, it is convenient to introduce the probability $P(\theta_a, \theta_b)$ with which Eve prepares Alice's particle in state $|\theta_a\rangle$ and Bob's particle in state $|\theta_b\rangle$. However, Alice and Bob will detect Eve by estimating the value of S.

The density operator is of Eve measurement given by:

$$\rho = \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} P(\theta_a, \theta_b) \left|\theta_a\right\rangle\left\langle\theta_a\right| \otimes \left|\theta_b\right\rangle\left\langle\theta_b\right| d\theta_a d\theta_b \qquad (4.8)$$

This lead to new correlation coefficient given by

$$E = \cos[2(\varphi^a - \theta_a)]\cos[2(\phi^b - \theta_b)$$

Rewriting CHSH S equation (4.6) with modified correlation coefficients, one obtain:

$$S = \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} P(\theta_a, \theta_b) d\theta_a d\theta_b (\cos[2(\varphi_1^a - \theta_a)]\cos[2(\phi_2^b - \theta_b)]$$

$$+ \cos[2(\varphi_1^a - \theta_a)]\cos[2(\phi_4^b - \theta_b)]$$

$$+ \cos[2(\varphi_3^a - \theta_a)]\cos[2(\phi_2^b - \theta_b)]$$

$$- \cos[2(\varphi_3^a - \theta_a)]\cos[2(\phi_4^b - \theta_b)])$$

This is lead to

$$S = \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} P(\theta_a, \theta_b) d\theta_a d\theta_b \sqrt{2} \cos[2(\theta_a - \theta_b)] \qquad (4.9)$$

which implies that S will be $-\sqrt{2} \geq S \leq \sqrt{2}$ -- (4.10).

The result of equation (4.10) confirms the assumption that Alice and Bob will notice Eve's tampering, because the result (4.10) will always be smaller than the requested one ($|S| = 2\sqrt{2}$) (Petra Pajic, 2013).

4.3 Event -based simulation procedure of Ekert's protocol (E91):

Computer simulation is a powerful methodology to model physical phenomena, but within the framework of quantum theory, no algorithm has been found to perform a simulation of quantum phenomena. But from a computational viewpoint, quantum theory provides us with a set of rules (algorithms) to compute probability amplitudes. Therefore we will use this algorithms to perform an event-based simulation of the E91 without using the machinery of quantum theory. The present simulation rules are out of any method based on the solution of the (time-dependent) Schrodinger equation and outside of the framework that quantum theory provides.

4.3.1 Entangled photons source:

To simulate the source of entangled photons we used random generation function to generate angles in the range of [0 , 360], to represent emitted photons polarization. Then the typical two polarized photons are traveled one to Alice and the other to Bob at the same time.

A schematic diagram of the simulation procedure is shown in fig(4.1). In the simulation algorithm, the source generates pairs of photons 1 and 2 travel to Alice and Bob, respectively.

Each photon carries a two-dimensional unit vector given by $P_{1,n} = (\cos\varphi_n + \sin\varphi_n)$

$$P_{2,n} = (\cos\varphi_n + \sin\varphi_n) \qquad (4.11)$$

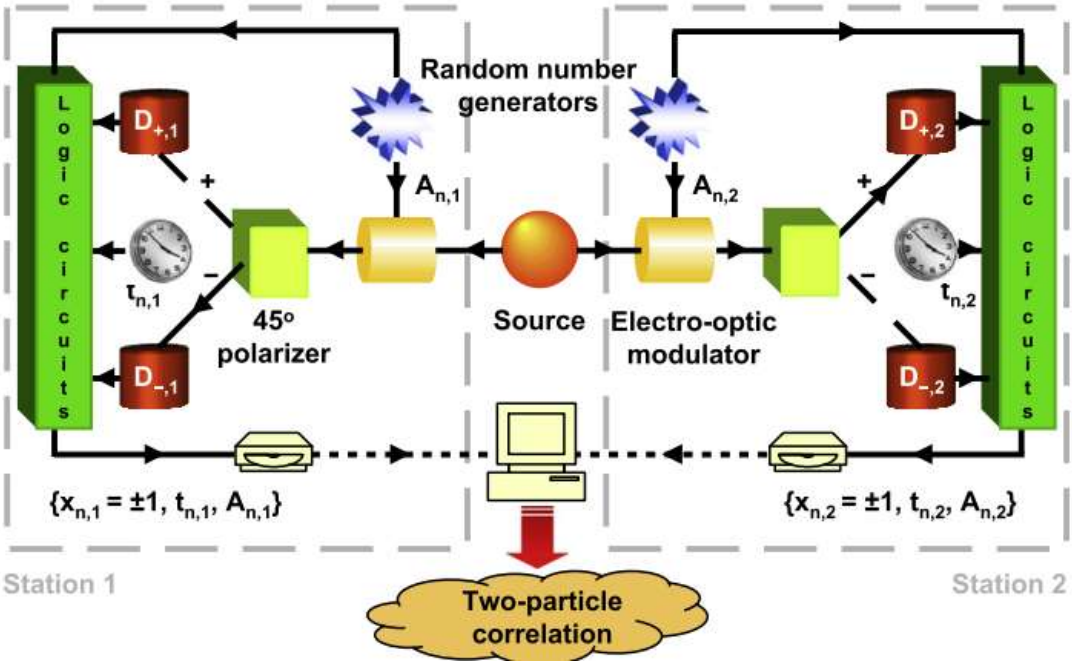


Fig:4.1 EPR experiment setup .

where φ_n represent the photon polarization ,and *n* labels the number of the photon (number of event). The distribution of φ_n is taken to be uniform over the interval [0,2π]. And we assumed the pair of photons travel through free space in ideal quantum channel with no effect on their polarization.

4.3.2 Electro-optic modulator (EOM):

When the photon arrives at Alice/Bob station , it passes through a modulator that rotates the polarization of the photon by an angle chosen randomly from [$\theta_1^a = 0$, $\theta_2^a = \frac{1}{8}\pi$, $\theta_3^a = \frac{1}{4}\pi$] for Alice,

and from [$\theta_1^b = 0$, $\theta_2^b = \frac{1}{8}\pi$, $\theta_3^b = -\frac{1}{8}\pi$] for Bob.

The EOM in station *i* = 1, 2 rotates the polarization of the incoming photon by an angle θi, and the new polarization angle of photon becomes $\emptyset_n = (\varphi_n - \theta_i)$. Alice and Bob choose θi randomly and independently.

Furthermore, to realize the Ekert protocol on the computer, we assume that the orientation of each a modulator can be changed at any time.

4.3.3 Polarizing beam splitter (PBS):

A polarizing beam splitter PBS is used to redirect photons depending on their polarization. For simplicity, we assume that the coordinate system used to define the incoming photons coincides with the coordinate system defined by two orthogonal directions of PBS.

Polarizing beam splitter, is an important part in quantum cryptography .

For event-based simulation of quantum mechanics , there are two methods to simulate polarizing beam splitter:

Deterministic polarizing beam splitter (DP) and probabilistic polarizing beam splitter (PP).

4.3.4 Probabilistic polarizing beam splitter (PP):

In this work we modeled two types of PP , and used them for simulation an Ekert's protocol.

The simulation model for a probabilistic polarizing beam splitter is defined by the rule

if $\cos^2 \emptyset i > 0.5$ $x_n = 0$

if $\cos^2 \emptyset i < 0.5$ $x_n = 1$ (4.12)

where $\emptyset i$ is angle different between polarization of incident photon and EMO rotation . It is easy to see that for fixed $\emptyset i$, this rule generates events such that the distribution of events complies with Malus law.

In this work also we built a probabilistic polarizing beam splitter using Hadamard gate transformation and we called it as (PPH).

The Hadamard gate (H) turns basis states into superposition states:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The Hadamard gate transformations is analogous to polarizing beam splitter transformations, turns basis states into superposition states:

$$H|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad (4.13)$$

And for general Qubit $|Q\rangle = \alpha|0\rangle + \beta|1\rangle$

$$H|Q\rangle \rightarrow \frac{1}{\sqrt{2}}((\alpha+\beta)|0\rangle + (\alpha-\beta)|1\rangle) \qquad (4.14)$$

Where $(\alpha+\beta)$ is now the probability amplitude to find the photon in the upper outgoing beam, and $(\alpha-\beta)$ is the probability amplitude for finding it in the lower outgoing beam.

For the specific case of either $\alpha = 0$ or $\beta = 0$, we find that the photon will be found with equal probability in either of the outgoing beams.

For another specific case, $(\alpha = \beta)$, we find that the photon will definitely be found in the upper beam and never in the lower beam.

Using above probability amplitudes we simulate a (PPH), and by using suitable time tag we implement this (PPH) to model an Ekert protocol.

4.3.5 Time tag:

In any real EPR experiment, one needs a criterion to decide whether two photons form a single two-particle system (entangled) or whether they may be considered as two single-particle systems. As EPR experiments with photons used coincidence in time to identify a single pair of two

photons. And because time coincidences play an essential role in real quantum cryptography experiments. In practice, Alice and Bob add time tags to their detection events in order to be able to count coincidences.

As the optical components (polarizer) induce time delays, it is reasonable for a photons to experience a time delay when it passes through the detection system. To mimic this, we introduce the time delay into our simulation algorithm. At each station, we generate a time tag that depends on the local settings only. Then, we compare the difference between the two time tags with a certain time window W.
If this difference is smaller than W , the detection events are considered to be coincident. Otherwise, they are discarded.

When light passes through an EOM (which is essentially a tune able wave plate), it experiences a retardation depending on its initial polarization and the rotation by the EOM. Therefore, in the case of single-particle experiments, we hypothesize that for each photon this delay is represented by the time tag ,(K.Michielsen.al 2014).

$$T_{ni} = F(\emptyset_n) r_n \qquad (4.15)$$

Where $0<r_n<1$ is a uniform pseudo random number, $\emptyset$ is angle between polarization of incident photon and EMO rotation .

For $T_{ni} = F(\emptyset_n) = T_0 \sin^4(\emptyset_n)$ (4.16)

This time-tag model, in combination with the model of the polarizing beam splitter, rigorously reproduces the results of quantum theory of the EPR experiments . Where T_0 is an adjustable parameter. In this work ,

For (PP) we used T_0= 2000, W=2, and $\sin^4(2\emptyset)$. (4.17)

And for (PPH) we used T_0= 1000, W=2, and $\sin^4(\emptyset)$. (4.18)

The model of time tag assumes that the maximum time delay T_{ni} for photon passing through a polarizer depends only on the angle difference between the polarization of the incident photon and the internal orientation of the polarizer.

4.3.6 Detector:

As the photon leaves the polarizing beam splitter, it generates a signal in one of the two detectors. In the protocol, the firing of a detector is regarded as an event. We consider ideal experiments only, meaning that we assume that detectors operate with 100% efficiency.

We assume that the two stations are separated spatially and temporally such that the observation at station 1 cannot have any effect on the data registered at station 2 , and vice versa.

At the nth event, the data recorded at station 1, 2 consists of $x_n = \pm 1$, specifying which of the two detectors fired.(H.De Raedt.al 2010).

The simulation program generated the data sets Xi for N events, and analyzed these data sets in same manner as the experimental data are analyzed in EPR experiment, by using selection procedure to select photon pairs by a time-coincidence window W .

In this work we first made an event- based simulation model of Ekert's protocol by implementing a probabilistic polarizing beam splitter (PP) without using time tag for little number of photon pairs (100-500). After that and by using time tag(4.16) and parameters (4.17) for (10^3 ,10^4 , 10^5) photon pairs . The model calculated CHSH inequality ,with and without Eve.

Secondly we implement the Hadamard probabilistic polarizing beam splitter (PPH), for simulate event-based model of Ekert's protocol, using the time tag (4.16) and parameters (4.18) for (10^3 ,10^4 , 10^5) photon pairs , and we calculated CHSH inequality, with and without of Eve.

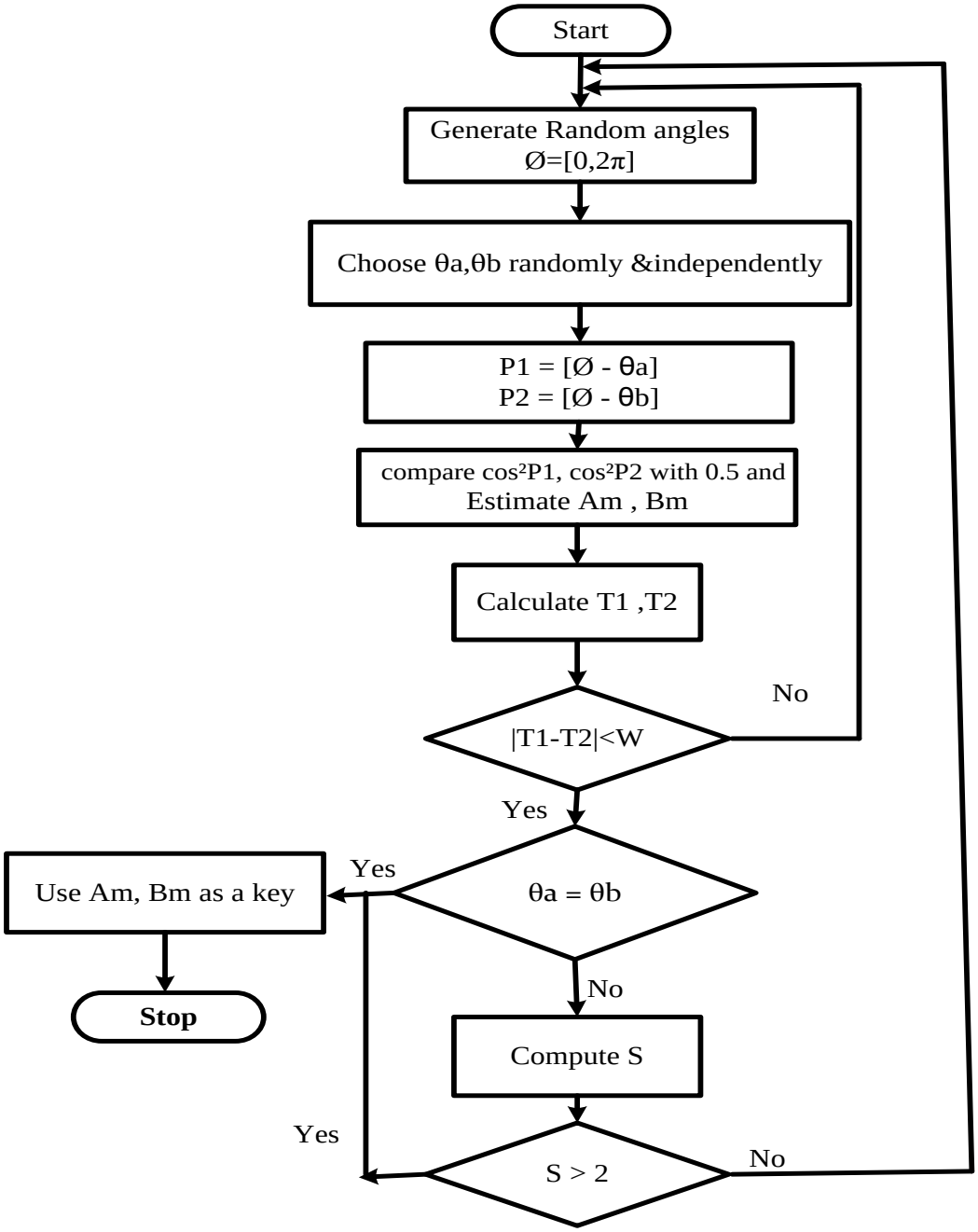


Fig: 4.2 Ekert protocol follow chart with time tag.

4.3.7 Eavesdropping :

To simulate Eavesdropper strategy we used two random generation functions to generate angles [0,360], to mimic Eve measurements for Alice and Bob sides.

4.4 Results:

First of all the equations was used to build the Matlab model.

Figure (4.3) shows the follow chart of model at first time using PP without time tag model as a semiclassical experiment .

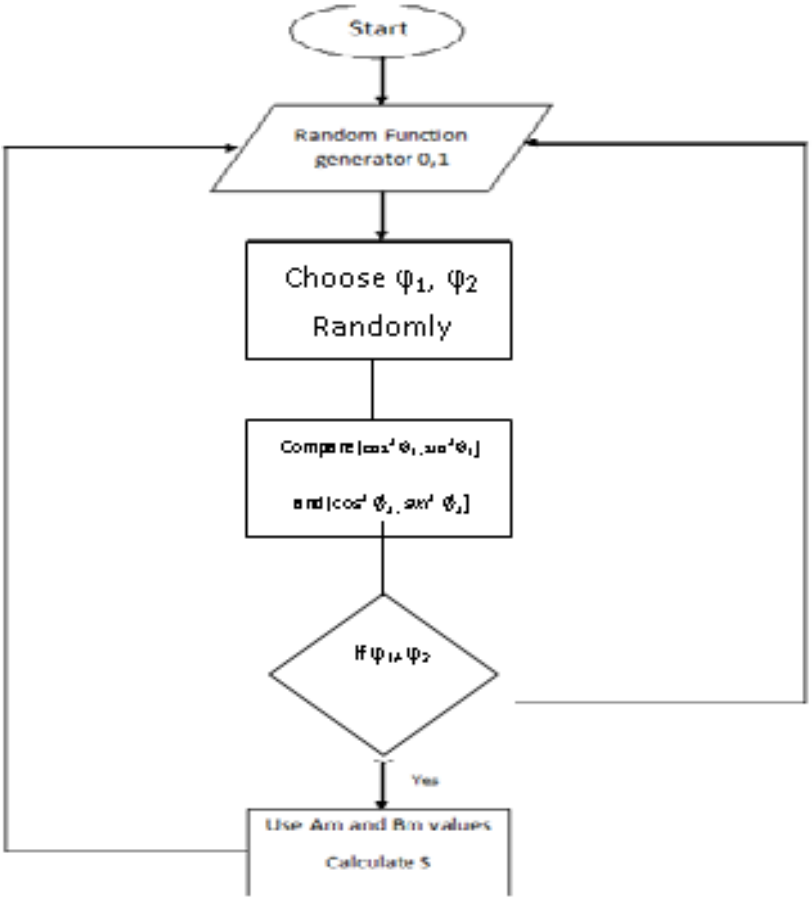


Fig.4.3: the flow chart of Ekert's protocol without using time tag.

The results of S as function of number of pairs obtained using probabilistic polarizing beam splitter without time tag is presented in table (4.1)

Table 4.1: result of S as function of number of pairs:

N	50	100	150	200	250	300	350	400	450	500
S	2.60	2.50	2.33	2.340	2.43	2.08	2.22	2.25	2.27	2.35
"	2.29	1.89	2.38	2.39	2.17	2.0	2.20	2.14	2.18	2.30
"	2	2.10	2.41	2.17	2.11	2.04	2.15	2.18	2.16	2.37
"	2.17	2.09	2.40	2.17	2	2.04	2.11	2.10	2.14	2.28
"	2.24	2.10	2.34	2.09	2.08	2.08	2.17	2.08	2.10	2.14
"	2.09	2.12	2.39	2.07	2.10	2.11	2.06	2.12	2.0	2.17
"	2.17	2.09	2.26	2.06	2.05	2.06	2.08	2.13	2.04	2.19
"	2.08	2.12	2.17	2.05	2.04	2.02	2.12	2.08	2.02	2.19
"	2.15	2.15	2.15	2.10	2.07	2.08	2.14	2.06	2.02	2.16
"	2.16	2.16	2.19	2.04	2.02	2.11	2.14	2.08	2.04	2.14

The results showing in table (4.1) is plotted in figure (4.2).

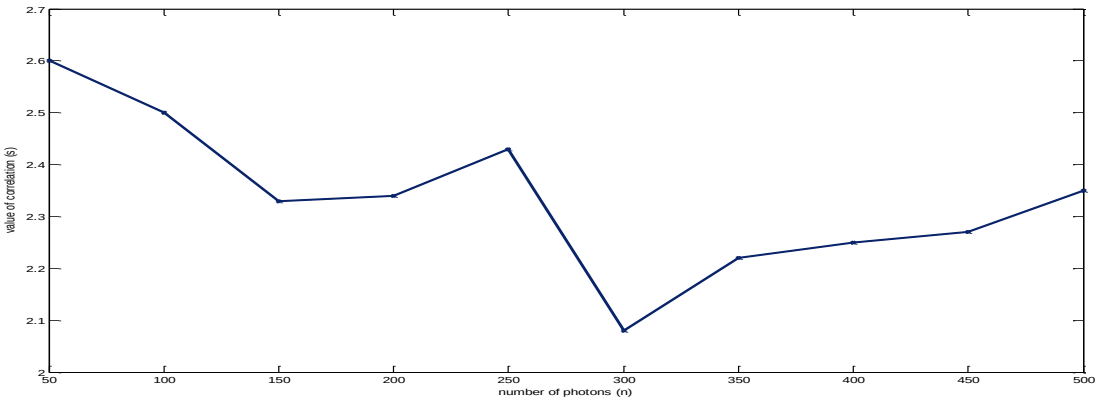


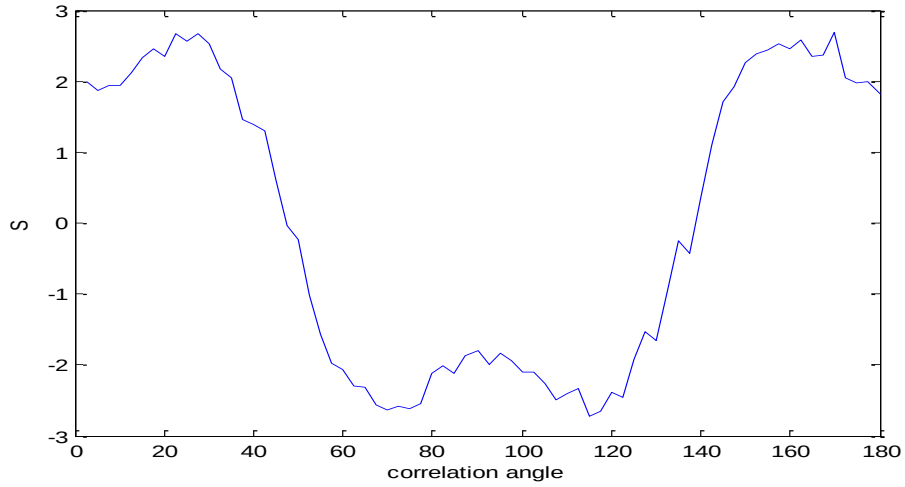
Figure 4.4 value of S as function of number of pairs

Table 4.2 : S value of different number of photon pairs (n)using PP with time tag model.

n = (10^3)	n = (10^4)	n = (10^5)
4	2.73	2.77
non	1.83	2.44
3	2.71	2.62
3.33	2.05	2.77
non	2.18	2.53
2.5	2.43	2.41
non	2.86	2.70
4	2.55	2.45
non	2.62	2.69
non	2.07	2.48

Table4.2 show the value of S of different numbers of photon pairs (10^3, 10^4, 10^5) using (PP) with time tag model.

Figure 4.5(a) shows the value of S as a function of angle difference between Alice and Bob polarizer using (PP) and suitable time tag.



(a)

Fig 4.5(a) : show the value of S as a function of angle difference between Alice and Bob polarizer using (PP) and time tag. every point plotted using 10^5 photon pairs.

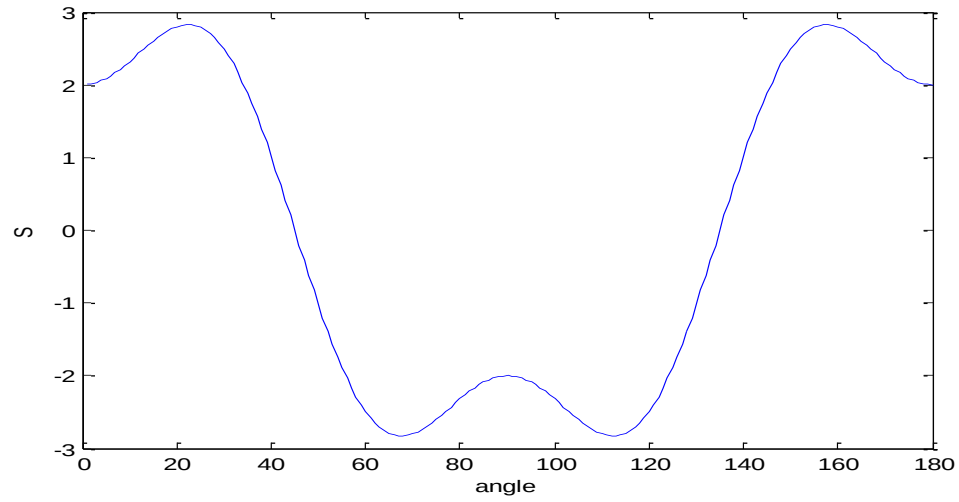


Figure 4.5(b) show quantum theory expectation $S(\theta) = 3\cos(2\theta) - \cos(6\theta)$ of S as function of angle difference between Alice and Bob polarizer.

Table (4.3) showed the results for 300, 600, and 1000 number of pairs obtained by used Hadamard gate as a beam splitter without time tag.

n	1000	600	300
S	2.84	2.84	2.96
"	2.76	2.70	2.53
"	2.78	2.76	2.61
"	2.76	2.70	2.59
"	2.70	2.64	2.57
"	2.73	2.64	2.49
"	2.74	2.67	2.55
"	2.74	2.68	2.55
"	2.73	2.67	2.58

The Correlation (S) when the number of photon pairs is 1000 is plotted in figure (4.6).

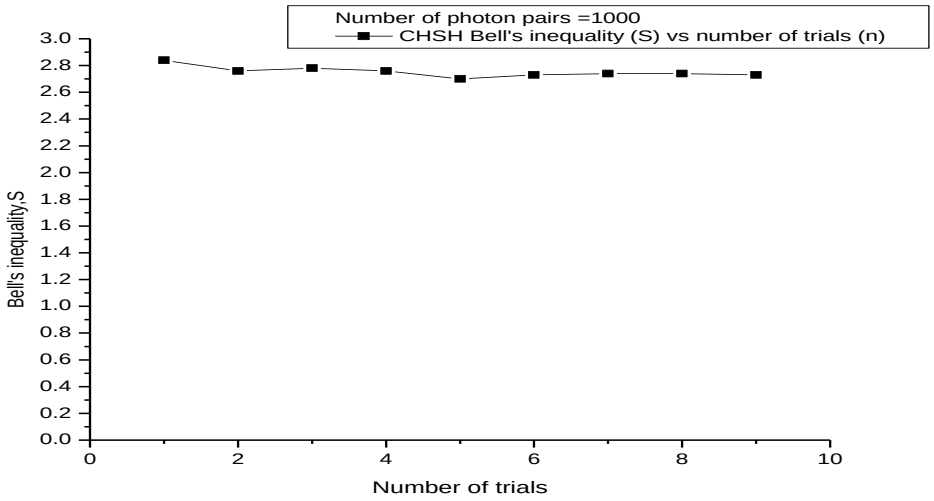


Figure 4.6 : Relation between CHSH bell's value (S) of (1000) photon pairs and number of trial (n).

And to see the effect of the number of photon pairs on (S) 600 number of trials is used and the obtained results is shown in figure (4.5).

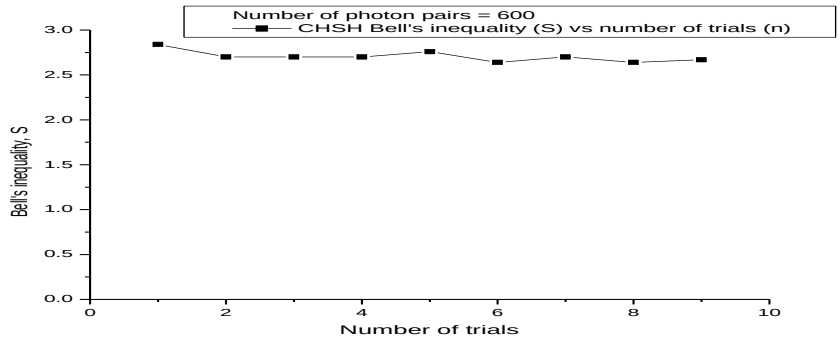


Figure 4.7: Relation between CHSH bell's value (S) of (600) photon pairs and number of trial (n).

And that when the number of trials was 300, is shown in figure (4.8).

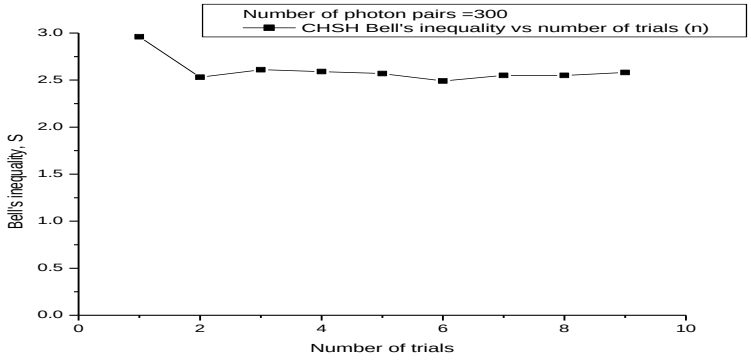


Figure 4.8: Relation between CHSH bell's value (S) of (300) photon pairs and number of trial (n).

Table4.4

$N = 10^3$	$n = 10^4$	$n = 10^5$
1.77	3.06	2.72
3.25	2.38	2.74
2.34	2.66	2.74
2.25	2.38	2.79
3.00	2.97	2.71
3.40	2.61	2.67
non	2.42	2.63
2.10	2.52	2.67
2.21	3.02	2.71
3.31	2.52	2.53

Table4.4 show the value of S of different numbers of photon pairs (10^3, 10^4, 10^5) using (PPH) with suitable time tag.

Figure 4.9 shows the quantum correlation using PPH and in the use of the time tag.

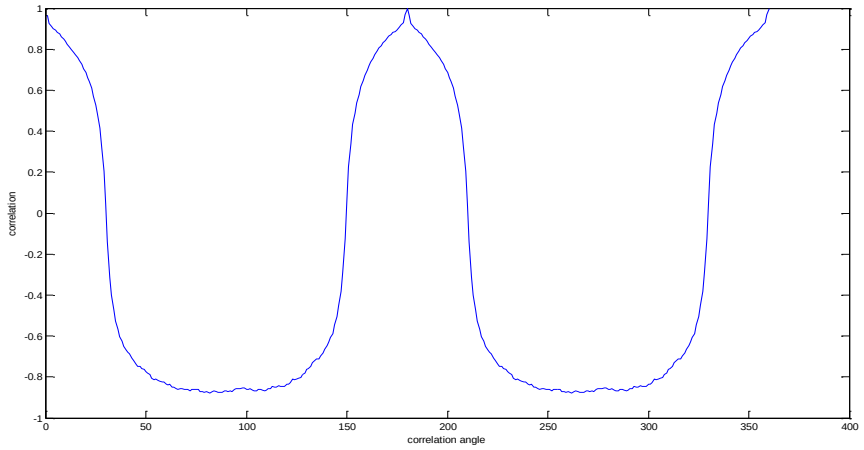


Fig.4.9(a): quantum correlation as function of angle obtained using (PPH).

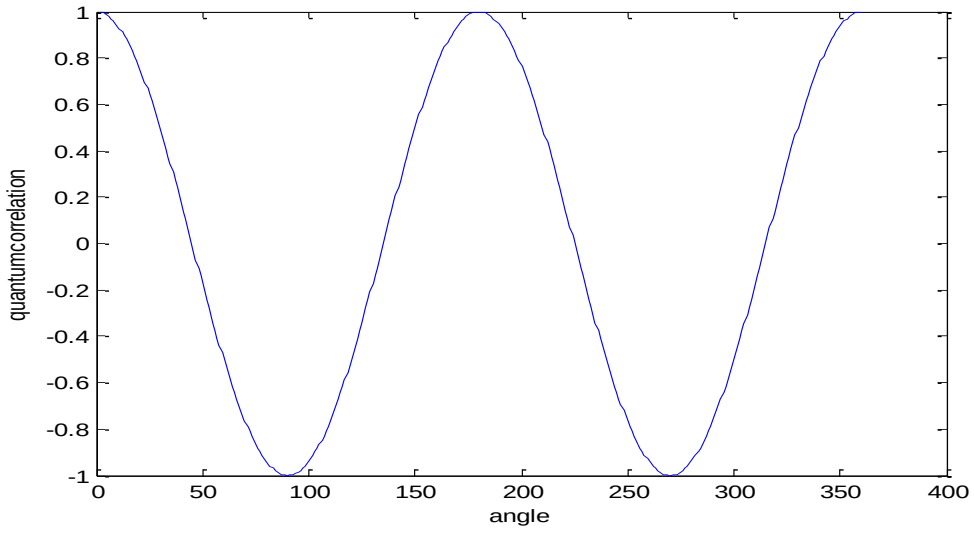


Fig4.9(b) show theoretical quantum correlation plotted for equation $E(\theta) = \cos 2\theta$. Where θ is the angle difference between Alice and Bob polarizer.

Table 4.5 results of First 100 running of Ekert's protocol simulation when Alice and Bob chose same angle randomly and independently. Using (PP) with time tag In the absent of Eave. S = 2.6306

Alice	0	1	0	0	1	1	0	1	1	1	0	1	0	1	0	1	0	1
Bob	0	1	0	0	1	1	0	1	1	1	0	1	0	1	0	1	0	1

Table4.6 results of First 100 running of Ekert's protocol simulation when Alice and Bob chose same angle randomly and independently. Using (PP) with time tag In the present of Eave. S = -0.2913

Alice	1	1	0	0	0	1	1	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0
Bob	1	1	0	0	1	0	0	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1	1

Table 4.7 results of First 100 running of Ekert's protocol simulation when Alice and Bob chose same angle randomly and independently. Using (PPH) with time tag In the absent of Eave. (S = 2.75).

Alice	1	1	1	1	0	0	0	1	0	1	0	1	0	0	0	1	0	0	1	0	1	0	1	0	0
Bob	1	1	1	1	0	0	0	1	0	1	0	1	0	0	0	1	0	0	1	0	1	0	1	0	0

Table4.8 results of First 100 running of Ekert's protocol simulation when Alice and Bob chose same angle randomly and independently. Using (PPH) with time tag In the present of Eave. S = 0.19.

Alice	0	0	0	0	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	1	1	0	0	0	0	1
Bob	1	0	1	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0

4.5 Discussion:

CHSH Bell's inequality for local hidden variables theory constrain that is $-2 \geq S_{LHV} \leq 2$. and Quantum mechanics prediction for CHSH is S_{QM} =2.83. By this comparison any result's of S value above "2" will recognized as a violation of classical correlation (S_{LHV}).

The results presented in fig 4.4 shows an obvious violation of S but the result was not stable (1.89 to 2.5) because the model described in fig 4.3, was not implement time tag to determine the coincident of photon pairs. And also the number of photon pairs was little (50 to 500) .since really EPR experiment requires about 10^5 photon pairs.

By using PP with suitable time tag in Ekert protocol model , the result presented in table 4.2 shows a good value of CHSH inequality S=(2.41 to 2.77), when number of photon pairs about 10^5 and by compare this result with the real experiment study done by (D. S. Naik et al., in (1999) S=2.67) result considered very good, and also comparing to result obtained using event-based simulation in study(H. De Raedt.al (2010) S = 2.73) the result consider in the same range. And by plotting S as a function of angle between Alice and Bob polarizer as shows in fig4.5(a) the results showed a very good agreement with that results predicted by quantum theory eq(3.28) that plotted in fig4.5(b) .

The relation between CHSH bell's inequality value (S) and number of trial (n) showed in fig (4.6 ,4.7 and 4.8). Figure 4.4 it was seen that the value of CHSH bell's inequality (S) above 2.7 and this value was near to the value that predicted by quantum mechanics 2.83. And also it was find that as the results showed there is a stability of the value (S) for all trials. And from figure 4.7 one find the value of CHSH bell's inequality (S) was found to be above 2.6 and this value is slightly different from the value predicted by quantum mechanics. And also it was found that there is some variations of the value (S) for the used trials. Figure 4.8 depicts the value of CHSH bell's inequality (S) as above 2.5 and the obtained value in this case is different also by small amount from the value that predicted by the quantum mechanics.

These values of CHSH in figures (4.6, 4.7 and 4.8) are good agreement with quantum predicted value (2.83). but this method of modeling of EPR by represent PP as Hadamard gate without using time tag is not sufficient to verify the value of CHSH that predicted by quantum mechanics for all angles.

By using specific time tag Eq.(4.16 and 4.18) we implemented the beam splitter transformations relations (Hadamard gate transformations Eq.(4.14)) to simulate event-based polarizing beam splitter and used it to model Ekert's protocol. The results showed in table (4.4) when $n=10^5$ (S=2.7) showed a very good agreement with that predicted by quantum theoretical (S=2.83).

The correlation of photons pair as function of angle between Alice and Bob polarizer showed in Fig (4.9a). The results obtained by using PPH in Ekert's protocol showed a good agreement with theoretical correlation predicted by quantum theory Eq.(4.4) which plotted in fig(4.9b).

After 100 times running of ekert protocol without present of Eve and by record the values of Alice and Bob measurements when they used same polarizing angles the results showed in tables(4.5, 4.7) were the same .

Tables (4.6, 4.8) showed results of Alice and Bob measurements when they chose same polarization angles in the present of Eve. In table 4.6 the disturbance caused by Eve is about (57%) and S value decrease from 2.63 to -0.29. And in table 4.8 the disturbance is about (43%) and S value down from 2.75 to 0.19.

This clear decrease of S enable protocol to detect Eavesdropping immediately.

4.6 Conclusion:

In this work the trial of modeling quantum cryptography and testing the quantum correlation by using MATLAB program model was established by representing the probability amplitude of single photon emerged from PBS and Hadamard gate transformation. And by treating the entangled pairs measurement independently the model calculated the CHSH Bell's inequality with and without eavesdropper and we observed that the model can easily check the present of eavesdropper . The result showed violation of classic constrains. So by this argument one can get results of CHSH Bell's inequality have value above '2'.. And the representing of polarizing beam splitter by just comparing ($\cos^2$) with($\sin^2$) without regarding time tag of photon pairs is not sufficient to give exact quantum prediction results.

Ekert's protocol is regarded as implementing of EPR experiment idea. And by results of correlation obtained above one can assume the event-based simulation of quantum cryptography is a good approach to obtain general quantum results from simple computational rules.

4.7 Recommendations:

Quantum cryptography is regarded as a modern searching field, there are daily progressing in simulation method. The recommendation can establish as follow:

• Make simulation of ekert protocol with study the effect of quantum channel .

• Built model of Ekert's protocol with other Eve strategies and how to detect it.

• Simulate ekert protocol and try to decrease the number of implemented photon pairs by searching for suitable time tag.

• Build model of Eve to attack Ekert's protocol without make disturbance on S value.

References:

A. EINSTEIN.al , (1935) , Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, Institute for Advanced Study, Princeton, New Jersey.

Alexander V.sergienko, (2005), Quantum communications and cryptography , CRC press Book ,New York

Chapter 1 Qubits and Quantum Measurement, www.inst.ees.berkeley.edu

http://www-inst.eecs.berkeley.edu/~cs191/sp12/notes/chap1&2.pdf

Dennis Luciano , Gordon Prichett-(1987)- Cryptology: From Caesar Ciphers to Public-Key Cryptosystems- The College Mathematics Journal, January 1987, Volume 18, Number 1, pp. 2–17.

Dietrich Dehlinger and M. W. Mitchella,(2002), Entangled photons, non locality, and Bell inequalities in the undergraduate laboratory. *Reed College, 3203 SE Woodstock Boulevard, Portland, Oregon 97202*

D.P. Landau, K. Binder, A Guide to Monte Carlo Simulation in Statistical Physics, Cambridge University Press, Cambridge, 2000

D. S. Naik1, C. G. Peterson1, A. G. White1,2, A. J. Berglund1, and P. G. Kwiat1,(1999)
Entangled state quantum cryptography: Eavesdropping on the Ekert protocol .Phys. Rev. Lett.

Danny Laghi ,Prof. Gianluca Grignani,(2013), EPR Paradox and Bell's Theorem .

Ekert, A.K., (1991),*Quantum cryptography based on Bell's theorem.* Physical Review Letters, 1991. **67**(6): p. 661-663.

*Graham Jensen***,** (2017)***, Entangled Photon Sources –***
Semiconductor devices for entangled photon pair generation

H. De Raedt1 , K. De Raedt2 and K. Michielsen1, (2005),

New method to simulate quantum interference using deterministic processes and application to event-based simulation of quantum computation

H. De Raedt a,, S. Zhao a, S. Yuan a, F. Jin a, K. Michielsen b, S. Miyashita c. (2010) Event-by-event simulation of quantum phenomena, Physica E 42 298–302

International Conference on Computer and Intelligent Systems (2012) & International Conference of Electrical, Electronics,

Introduction to quantum mechanics, en.wikipedia.org/wiki/

Itzel Lucio Mart´ınez(2014),Real world quantum cryptography , CALGARY ALBERTA,

John F. Dawson –(2009)-Quantum Mechanics: Fundamental Principles and Applications- *University of New Hampshire, Durham, NH 03824*
John F.Kennedy -security engineering : A guid to building dependable distributed system.

James Binney and David Skinner (2013) -The Physics of Quantum Mechanics, Published by Cappella Archive

John F.Kennedy ,security engineering : A guid to building dependable distributed system (2008)

Konrad Banaszek.al (2012) ,Quantum information 1/2

K.Miechielsen.al, Event-based simulation of quantum physics experiment. (2014), arxiv: 1312.6942V2(quantum-ph).

Luca Trevisan- Cryptography Lecture Notes from CS276,(2009) Stanford University

Magaña-Loaiza, (2011),Entangled Photon Source O.S., Quantum Optics and Quantum Information Laboratory, University of Rochester, NY, 14623)

Nicholas Wheeler- (2009)-Selected topics in Quantum Measurement Theory- Reed College Physics Department

Noah Graham (2014) Quantum Mechanics is Linear Algebra Middlebury College.

Niclas Hoglund,(2013), Bell's Theorem and Inequalities, with Experimental Considerations,
(920118-0677) nhoglu@kth.se Olof Jacobson (890222-0337)

O.S. Magaña-Loaiza, (2010),Entangled Photon Source Quantum Optics and Quantum Information Laboratory, University of Rochester, NY, 14623

Petra Pajic, ,(2013) Quantum Cryptography, Bachelor Thesis for the degree of Bachelor of Science at the University of Vienna

Quantum states and observables, http://www.physik.fu-berlin.de/en/einrichtungen/ag/ag-eisert/teaching/QMChapter2.pdf

30-S. Zhao1, S. Yuan1, H. De Raedt1 and K. Michielsen2 **(2**008).Computer simulation of Wheeler's delayed choice experiment with photons(a)
Shuang Zhao and Hans De Raedt (2007),Event-by-event Simulation of Quantum Cryptography Protocols .Nijenborgh 4, NL-9747 AG Groningen, The Netherlands.

Sara Idris Babiker Mustafa (2007), simulation of quantum cryptography based on Ekert protocol, (PhD thesis:Institute of laser. Sudan University of science and technology), Sudan

Sheila Cobourne , (2011), Quantum Key Distribution Protocols and Applications, Technical Report

Siddeq Y.al (2006) . Modeling and simulation of schematic quantum cryptography system Based Entangled photons. IJCCCE.VOL.No.2.2006.

Thomas e. copeland-(2000)- the information revolution
and national security- rummelr@awc.carlisle.army.mil.

William K.al ,(2009), The no-cloning theorem ,physics today

Zhao, S. and H. De Raedt,(2008), Event-by-event Simulation of Quantum Cryptography Protocols. Journal of Computational and Theoretical Nano science,. 5(4): p. 490-504.