Iraqi J. Laser, Part A, Vol. 3, pp. 1- 10 (2004)

IRAQI JOURNAL OF LASER

Quantum Cryptography and a Quantum Key Distribution Protocol

K. I. Hajim **Sheelan Kh. Tawfiq** and **Ahmed M. Meki**

Institute of Laser for Postgraduate Studies, University of Baghdad, P.0. Box 47314 Jadiriah, Baghdad, IRAQ

(Received 8 February 2004; accepted 29 October 2004)

Abstract: In this article, a short review on the feature of reality and locality in quantum optics is given. The Bell inequality and the Bell states are introduced to show their direct use in quantum computer and quantum teleportation. Moreover, quantum cryptography is discussed in some details regarding basic ideas and practical considerations. In addition, a case study involving distillation of a quantum key based on the given fundamentals is presented and discussed.

Introduction

Since the 1920's, when the quantum physics was invented, the discussions about understanding the theory correctly still exist. These discussions deal with important issues like Einstien- Podolosky- Rosen paradox, quantum non-locality and the role of the measurement in quantum physics [1] .

In 1933 it was realized that this modern theory has counter intuitive features that were very clear in the famous dialogue between Nils Bohr and Albert Einstein [2]. Two years later, this subject was given a much important role in a paper written by Einstein, Podolosky and Rosen. In this paper an essential imperfections of quantum theory was exposed [3].

The success of a physical theory could be judged by answering two questions; is the theory correct? and, does the description given by the theory is complete?. The theory may be said to be satisfactory if the answer of these two questions is positive [4].

We cannot determine by priori philosophical considerations the elements of the physical reality. These elements must be found by results of experiments and measurements.

The following criterion is sufficient to describe reality, if the value of a physical quantity can be predicted with certainty (i.e., probability equals to 1) then there exists an element of physical reality corresponding to this physical quantity [4].

It was proven that the quantum mechanical description of reality given by wave function is not complete [4]. Einstein, Podolosky and Rosen had advanced their paradox as an argument that quantum mechanics could not be a complete theory but should be supplemented by additional variables [5].

Until 1964, the paper submitted by Einstein, Podolosky and Rosen (EPR) remained purely philosophical. By 1964, a statement which is in principle experimentally testable was derived by Bell. He started from EPR's example in the version given by Bohm in 1957 [6]. He found that in any model, the correlation predicted between two measurements must necessarily comply with a set of inequalities nowadays known as Bell inequalities [6]

$$S(a,b,a',b') = |E(a,b) - E(a,b')| + |E(a',b')+E(a',b)| \leq 2 \quad (1)$$

where E(a,b) is the correlation coefficient of measurements along a,a' and b, b', while S represents the Bell parameter; it was the meaning of second order correlation.

In practice, the correlation coefficients that determine the Bell parameter are calculated from what is known as coincidence counts, R's. For example, E(a,b) can be obtained by the expression:

$$E(a,b)=\frac{R_{++}(a,b)+R_{--}(a,b)-R_{+-}(a,b)-R_{-+}(a,b)}{R_{++}(a,b)+R_{--}(a,b)+R_{+-}(a,b)+R_{-+}(a,b)} \quad (2)$$

where, $R_{\pm}$ (a,b) is the number of coincident events of detecting ±1 at site 1 apparatus with the analyzer oriented at an angle (a) and detecting ±1 at site 2 apparatus with the analyzer oriented at an angle (b).

It was found that this inequality will be violated with $S=2\sqrt{2}$ for a singlet state of two spin–half particles (ψ^- Bell state). It is concluded that a system that can be described by a local theory cannot mimic the behavior of entangled states and hence the quantum theory must be a non- local theory [6].

The general setup for Bell experiment is shown in Fig. (1). In this setup, correlated particles are emitted by the source. The qubits fly back to back towards two analyzers to make projection measurement in bases defined by the analyzers' parameters a and b respectively. The measurements' outputs are correlated in order to enable them to be tested using Bell inequalities whether the two–particle system can be described by a local or by a non-local theory [6].

The Quantum Bits (Q bits) and Bell States

The bit is the most fundamental entity in information science. It carries two possible values, "0" and "1". It can be defined as a system which is designed to have two distinguishable states, such that the energy barrier between them is sufficiently large so that no spontaneous transition can occur between them [2]. The Q bit, is a two- state system which is the quantum analog of a bit. The two states are simply called $|0\rangle$ and $|1\rangle$. Any quantum system which has at least two states can serve as a quantum bit.

The possibility of coherence and super-position is the most general property of quantum states when used to encode bits [2]. The general state is,

$$|Q\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad (3)$$

with $|\alpha|^2 + |\beta|^2 = 1$

This means that the qubit is in a superposition of both states. If the qubit is measured, it will be found with a probability $|\alpha|^2$ to carry the value "0" and with a probability of $|\beta|^2$ to carry the value "1", i.e.,

$$p(\text{"0"}) = |\alpha|^2 \quad \text{and} \quad p(\text{"1"}) = |\beta|^2 \quad (4)$$

Photons, electrons, atoms, quantum dots and so on can all be used as qubits. Internal states such as the energy levels in an atom, and external states such as the direction of propagation of a particle are also possible to be used as qubits [1].

For a pair of two- states particles, there are four possible Bell states that are a widely used choice of superposition.
The two states are |0> and |1>, the qubits are labeled by the subscripts 1 and 2. The four states are

$$\begin{aligned}
|\Psi^+\rangle &= (1/\sqrt{2})\,(|0\rangle_1\,|1\rangle_2 + |1\rangle_1|0\rangle_2)\\
|\Psi^-\rangle &= (1/\sqrt{2})\,(|0\rangle_1\,|1\rangle_2 - |1\rangle_1|0\rangle_2)\\
|\Phi^+\rangle &= (1/\sqrt{2})\,(|0\rangle_1\,|0\rangle_2 + |1\rangle_1|1\rangle_2)\\
|\Phi^-\rangle &= (1/\sqrt{2})\,(|0\rangle_1\,|0\rangle_2 - |1\rangle_1|1\rangle_2)
\end{aligned} \quad (5)$$

Each Bell state represents a coherent superposition of two possibilities. In this superposition, the single– particle states are direct product of complete states of each individual particle. If A and B represent two subsystem, $|i\rangle$ and $|j\rangle$ are a basis for A and B then a combined state is entangled if it can not be written in the form [7]

$$\left(\sum_I C_i^{(A)}|i\rangle_A\right)\left(\sum_J C_j^{(B)}|j\rangle_B\right) \quad (6)$$

Given a state in the general form

$$|\psi\rangle_{AB} = \sum_{i,j} C_{ij}|i\rangle_A|j\rangle_B \quad (7)$$

it is easy to determine whether it is entangled or not. If each subsystem is in a mixed state then it can be shown that it is entangled. If a local measurement is made on a subsystem of an entangled state, the other system will be in a mixed state [7].

Entanglement and the EPR Pairs

Entanglement is related to the issue of non-locality in quantum theory. If two particles in an entangled state, are widely separated, then any measurement applied on one will immediately influence the quantum state of the other one. The particles seem as they are communicating faster than the speed of light but special relativity is not violated because no information is exchanged [1]. Entanglement

describes correlations between quantum systems that are much stronger than any classical correlations.

Entanglement can be achieved in the laboratory by performing experiments in such a way that it is possible to find , even in principle , which particle is in which state .

Consider a source that emits a pair of particles such that one particle emerges to the left and the other to the right as shown in Fig. (2). The particles from this source are emitted with opposite momenta, the particles 1, 2 and in qubit language are said to carry different bit values. Either particle 1 carries "0" and particle 2 definitely carries "1", or vice versa. In this source, if particle 1 emerging to the left is found in the upper beam, then particle 2 traveling to the right is found in the lower beam and vice versa. Quantum mechanically this is a two-particle superposition state of the form:

$$(1\sqrt{2})\,(|0\rangle_1\,|1\rangle_2 + e^{i\phi}\,|1\rangle_1\,|0\rangle_2) \qquad (8)$$

The phase ϕ is just determined by the internal properties of the source and for simplicity ϕ is assumed to be equal to zero. Equ. (8) describes what is called entanglement [2].

Quantum computers, quantum teleportation and quantum cryptography, are direct possible applications of quantum optics.

Quantum Computer and Quantum Teleportation

Quantum computer

The advantage of quantum computation as compared to classical factoring appears in providing exponential speedup for factoring and quadratic speedup of search [8]. For example a classical problem requires eight months to be solved with the aid of hundreds of computers.

In digital computers for example, a bit of information can be represented by the voltage between the plates of a capacitor. A charge on the capacitor denotes 1 and the absence of the charge denotes 0.

Two different polarizations of light or two different electronic states of an atom can be used to encode one bit of information. In quantum mechanics, if a bit can exist in either of two distinguishable states, it can also exist in coherent superposition of them; this means that we have further states that have no classical analogous [2].

Quantum teleportation

Teleportation is the ability to travel by simply reappearing at some distant location. The properties of the teleported object can be used to characterize it. At the distant location, a copy of the object is made by sending the scanned information so that it can be used to reconstruct the object. Bennett *et al*. have suggested that it is possible to transfer the quantum state of a particle onto another particle, i.e. the process of quantum teleportation, without getting any information regarding the state in the course of this transformation. Entanglement can be used to fulfill this requirement, which is the essential feature of quantum mechanics [9].

Fig. (3) shows the principle of quantum teleportation. Particle 1 is in its initial state which Alice wants to teleport it to Bob from her quantum system. Also, an ancillary entangled pair of particles 2 and 3 is shared between Alice and Bob and is emitted by EPR – source.

A joint Bell state measurement (BSM) is performed by Alice on the initial particle and one of the ancillaries, projecting them also onto an entangled state. The result of measurement, done by Alice, is sent to Bob as classical information followed by performing a unitary transformation (U), done by Bob, on the other ancillary particle which will result in it being in the state of the original particle.

Quantum Cryptography

One of the mature application of quantum optics out of the three famous ones, quantum teleportation, quantum computer and quantum communication, is quantum cryptography in communication.

In cryptography, two parties, Alice and Bob, are enabled to mask confidential messages, so that the transmitted data are illegible to any unauthorized third party, Eve. A shared secret key is used to achieve this. The quantum key distribution recent development covers this major loophole of classical cryptography. Alice and Bob are allowed to establish two completely secure keys by a transmission of a single quantum (qubits) along a quantum channel. The basic principle of quantum key distribution depends on the prohibition of nature from

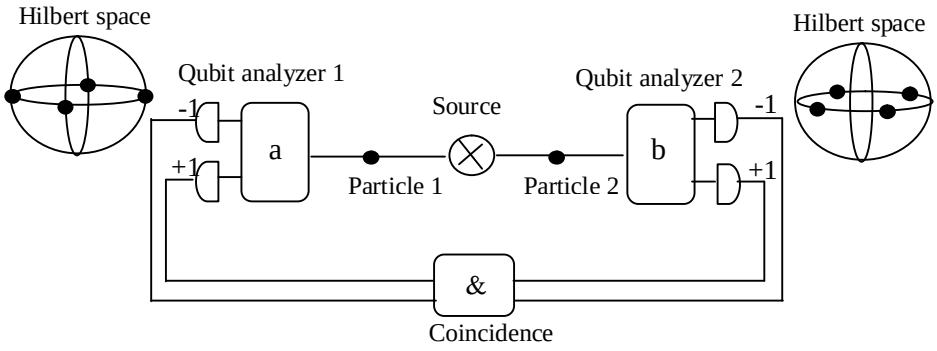

Fig. (1): The general setup for Bell experiment [6]

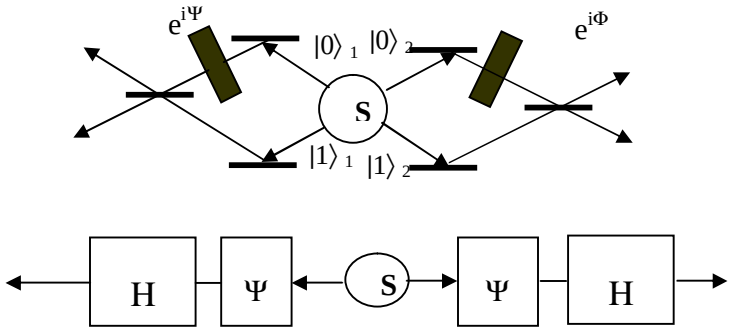

Fig. (2): A source emits two qubits in an entangled state [2]

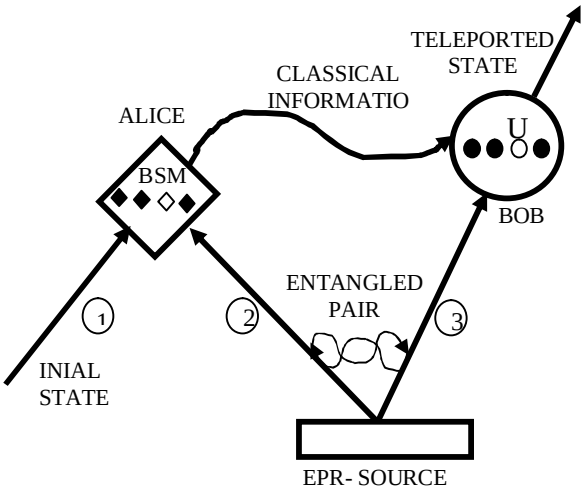

Fig. (3): Principle of quantum teleportation [2]

gaining information on the state of a quantum system without disturbing it. In classical channels eavesdropping can take place without the sender or receiver knowing, in quantum cryptography this is not true where the measured sequence will be disturbed by eavesdropping [10]. To achieve an absolute secure communication, the secure keys can be used in a one– time pad protocol [11].

If an unauthorized third party obtained any information about the exchanged key, the quantum bit error rate (QBER) of the transmitted data, which can be checked using a suitable subset of the data will increase.

4The QBER consists of two parts, the first part is the $QBER_{opt}$ which represents the fraction of photons whose polarization or phase is determined with an error. The second part, $QBER_{det}$, is due to the dark count rate [12]. As long as the quantum bit error rate of the sifted key is below a certain threshold, Alice and Bob can still distill a secure key by means of classical error correction and privacy amplification protocols. Then an exchange of a confidential message in a complete privacy can be achieved by using a secret key together with the one – time pad protocol [6].

Practical Experiments in Quantum Cryptography

The work of Wiesner in 1970 is considered as the origin of quantum cryptography. Wiesner proposed that storing single –quantum states for a long period of time leads to the ability of using them as counterfeit – proof money. Wiesner's ideas were published in 1983, but they were largely of academic interest. Later, Bennett and Brassard realized that single quanta can be used for information transmission rather than being used for information storage. In 1984 the first quantum cryptography protocol was published by them. The protocol was known as BB84 [13].

In BB84 scheme, single photons are transmitted from Alice to Bob. Alice and Bob can detect any error caused by Eve if she tries to extract information about the polarization of the photons. Detection of errors by Bob and Alice is done by comparing random subsets of the generated keys [11]. Table (1) illustrates the protocol with the example of four polarization qubits [2].

In this protocol, a random sequence of the four canonical kinds of polarized photons is sent from Alice to Bob. For each photon, the rectilinear or diagonal polarization is chosen randomly and independently by Bob. The kind of measurement, not the result, made by Bob is announced publicly by Bob and Alice tells him publicly whether he made the correct measurement. The data from these correctly – measured photons are kept by Alice and Bob, all the rest are discarded [14].

The system based on the BB84 protocol was implemented by Bennett et al. [14] in 1992. The system was realized by exchanging faint laser pulses containing less than one photon on average over a distance of 30 cm in air. This experiment was very important because it had proved the ability of using single photons instead of classical pulses for encoding bits.

Fig. (4) shows a typical system for quantum cryptography with the BB84 four state protocol using the polarization of photons. Such a system was used by Muller and his coworkers at the University of Geneva in 1993 to perform quantum cryptography experiments over optical fibers. A key was created over a distance of 1100m with photons at 800nm. The transmission distance was increased by repeating the experiment with photons at 1300 nm and a key was created over a distance of 23 km [1].

In 1991, further advances in theoretical quantum cryptography took place when EPR "entangled" two-particle states were proposed by Ekert to be used in implementing a quantum cryptography protocol whose security was based on Bell's inequalities [13]. One particle out of the entangled pair is received by both Alice and Bob. Alice and Bob perform measurements along at least three different directions by rotating the $\oplus$ basis around z- axis by certain angles on each side specifically, these angles are $\phi_1^a = 0$, $\phi_2^a = \pi/4$, $\phi_3^a = \pi/8$ for Alice and $\phi_1^b = 0$, $\phi_2^b = -\pi/8$, $\phi_3^b = \pi/8$ for Bob, as the superscripts imply [2].

To generate the keys, measurements along the parallel axis are used, while testing the inequality is done using oblique angles, namely (ϕ_1^a, ϕ_3^b), (ϕ_1^a, ϕ_2^b), (ϕ_2^a, ϕ_3^b) and (ϕ_2^a, ϕ_2^b) [2]. Ekert pointed out that eves dropping reduces the degree of violation of Bell's inequality because it inevitably affects the entanglement between the two constituents of a pair [9].

In Ekert scheme the correlation coefficients of the measurements performed by Alice along a_i and by Bob along the b_j are [16]

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j) \quad (9)$$

Table (1): Example of polarization protocol

1. Alice random basis	⊗	⊕	⊗	⊗	⊕	⊗	⊗	⊕
2. Alice bits	1	1	0	1	0	0	0	0
3. Polarization states sent to Bob	↘↙	↔	↙	↘↙	↕	↙	↙	↕
4. Bob random basis	⊕	⊕	⊗	⊗	⊗	⊕	⊕	⊕
5. Bob bits	0	1	0	1	1	0	1	0
6. Same basis for both Alice and Bob?		√	√	√				√
7. Sifted key		1	0	1				0

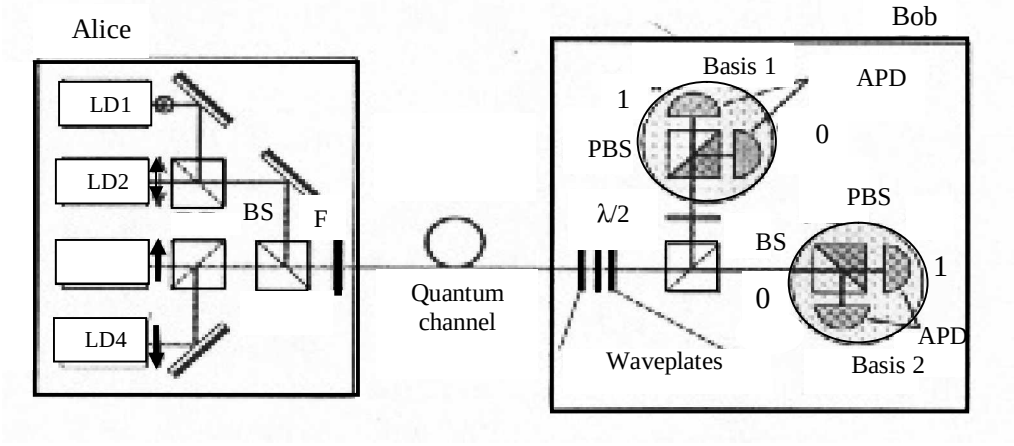

Fig. (4): Typical system for quantum cryptography with the BB84 four- state protocol using the polarization of photons [15].

where, $P_{\pm\pm}(a_i, b_j)$ is the probability that result ±1 has been obtained along a_i and ±1 along b_j..

For the two pairs of analyzers of the same orientation (a_2, b_1 and a_3, b_2) quantum mechanics total anti-correlation of the results obtained by Alice and Bob:

$$E(a_2,b_1) = E(a_3,b_2) = -1 \quad (10)$$

The correlation coefficient for which Alice and Bob used analyzers of different orientation is,

$$S= E(a_1,b_1) - E(a_1,b_3) + E(a_3,b_1) + E(a_3,b_3) \quad (11)$$

where quantum mechanics requires that $S=-2\sqrt{2}$ [16]. Then the measurements are divided into two groups, the first for which they used different orientations of analyzers, and a second for which they used the same orientation of their analyzers. The measurements in which they failed to register a particle are discarded. Subsequently, the results obtained within the first group of measurement are only revealed. This allows them to establish the value of S, which should reproduce the result of $(-2\sqrt{2})$. This assures the legitimate users that the results they obtained within the second group are uncorrelated and can be converted into a secret key, which can be used in conventional cryptographic system [16].

Through the two experiments, polarization transformation induced by long optical fiber was found to be unstable over time. When QBER was monitored for these two systems, it was found that although if remained stable and low for some time (several minutes), it will increase suddenly after a while, which is an indication for a modification of the polarization transformation in the fiber. This means that an active alignment for compensation for this evolution is required in real quantum cryptography system.

An active feedback alignment system was implemented by Franson in 1995 [13]. It is interesting to note that using polarization maintaining fibers instead of standard fibers does not solve the above problem. In 1998, a

polarization encoded system for quantum cryptography was investigated by Paul Townsend of BT laboratories .The experiment was investigated on short-span links up to 10 km with photons at 800nm. In this experiment, single mode propagation was assured by carefully controlling the launching conditions although standard telecommunication fibers were used [15]. As discussed above, it was shown that using polarization coding does not seem to be the best choice for quantum cryptography in optical fibers [15].

In 1999, quantum cryptography based on the properties of entangled photons was demonstrated by three groups .The main advantage of using photon pairs for quantum cryptography, lies in the fact that empty pulses can be removed, since the detection of one photon of a pair reveals the presence of a companion. Thus, it is possible to have a probability of emitting a non-empty pulse equal to one. In Fig. (5), a typical system for quantum cryptography based on photon pairs entangled in polarization is shown.

In this scheme, a two photon source emits pairs of entangled photons flying back to back towards Alice and Bob. The polarization-entangled pairs are prepared using the process of spontaneous parametric down conversion in a nonlinear crystal [13, 17]. Two identically cut adjacent crystals, BBO, are oriented in such a way that their optic axes lie in a plane perpendicular to each other. A polarization beam splitter is used to analyze the photon. The orientation of polarizing beam splitter with respect to a common reference system can be changed rapidly [13, 17].

In 2000, two experiments were carried out by Jennewein and Naik. In both experiments, photon pairs at a wavelength of 700nm were used. The photons were detected with commercial single photon detectors based on silicon APD's [15]. A BBO crystal pumped by argon-ion laser was used in both experiments to create photon pairs. The polarization state of the photons was rotated by analyzers consisted of fast modulators [15].

Such a crypto system was demonstrated by the group of Anton Zeilinger, then at the University of Innsbruck over a distance of 360m, in 2000 [15] . The group of Paul Kwiat from Los Alamos National Laboratory demonstrated the Ekert protocol in the year 2000. The source and analyzers were separated only by few meters with a table- top realization [15].

Practical Considerations

Photon Sources

In optical quantum cryptography, single photon Fock states are used. Experimentally, these states are difficult to realize. Faint laser pulses or entangled photon pairs are used nowadays for practical implementations. In entangled photon pairs, where both the photon are well as the photon pair number distribution underlies Poisson statistics [13].

Faint laser pulses

Coherent states with an ultra-low mean photon number μ can be considered as a very simple solution to approximate single photon Fock states. These states can be realized with only standard semi-conductor lasers and calibrated attenuators. The probability to find n photons in such a coherent state follows the Poisson statistics:

$$P(n,\mu) = \frac{\mu^n}{n}\, e^{\mu} \qquad (12)$$

where μ is the mean photon number.

Also the probability that a non-empty weak coherent pulse contains more than one photon,

$$P(n>1|n>0,\mu) = \frac{1 - P(0,\mu) - P(1,\mu)}{1 - P(0,\mu)} = \frac{1 - e^{\mu} - (1+\mu)}{1 - e^{\mu}} \cong \frac{\mu}{2} \qquad (13)$$

can be made arbitrarily small .

Weak pulses are extremely practical and have been used in wide range of experiments, but they have one major drawback, when μ is small most pulses are empty: P (n=0) ≈ 1μ. Nowadays experiments rely on μ=0.1, meaning that 5% of the non empty pulses contain more than one photon [13].

Photon pairs generated by parametric down conversion

Single- photon states could be created by the generation of photon pairs and then using one photon as a trigger for the other one. In contrast to the sources discussed before, the second detector must be activated only when a photon is detected by the first one, hence when μ=-1, and not whenever there is an emission of a pump pulse this will solve the problem of empty pulses.

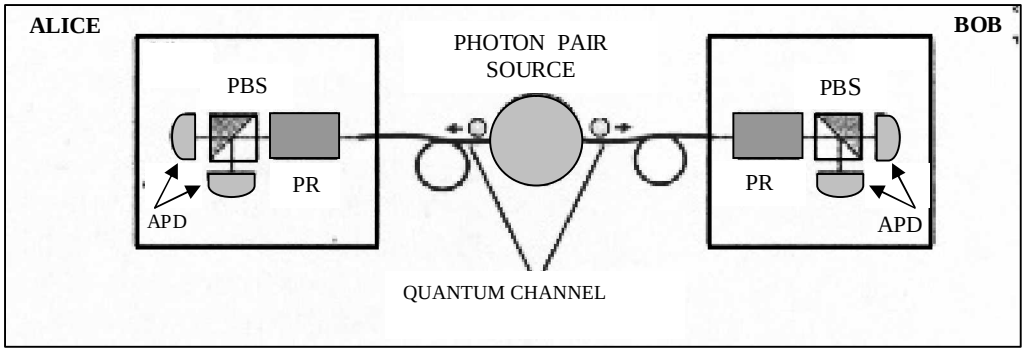

Fig. (5): Typical system for quantum cryptography based on photon pairs entangled in polarization [12]

Spontaneous parametric down conversion technique is a $\chi^{(2)}$ non-linear crystal is used to generate photon pairs. In this process which represents the inverse of the well known frequency doubling, a photon spontaneously splits into two daughter photons with concerning total energy and momentum. The momentum conservation is called phase matching. Phase matching can be achieved by exploiting the birefringence of non-linear crystal .

Photon pairs generated by parametric down conversion have an advantage if their entanglement is exploited rather than a single photon source [13]. The current schemes for down–conversion employ the natural birefringence of specific nonlinear crystals, like β-barium–borate (BBO). Also semiconductors such as GaAs or GaP have $\chi^{(2)}$ about two orders of magnitude larger than that of commonly used crystals such as BBO. This together with the existence of well developed microfabrication techniques for these materials, makes it attractive to explore ways of creating semiconductor based entangled photon sources [18].

Photon guns

The ideal single photon source is a device that when one pulls the trigger, and only then emits one photon. This is known as a photon gun.

The development of efficient solid-state single-photon sources is an important pre-request for a large scale implementation of secure telecommunication systems based on quantum cryptography.

Various solid state emitters including molecular, F-centers, semiconductor nano-crystals and self-assembled quantum dots (QDs) emit under proper excitation conditions untibunched light. QDs exhibit good stability, nearly unity quantum efficiency, short radiative lifetime, a quasi-monochromatic emission, and can easily be inserted inside semiconductor micro-cavities [16].

The most common way of creation of entangled photons at wavelength in the red or near infrared region is the spontaneous parametric down conversion. Most experiments suffer from low yield of the fluorescence process. A method is reported to optimize collection efficiency by matching the angular distribution of the parametric fluorescence to the spatial mode of an optical fiber [9].

Quantum channels - Single mode fibers and polarization effect

An ideal quantum channel is provided with a single-mode fiber with perfect cylindrical symmetry. But some asymmetries exist in all real fibers. As a result, the two polarization modes are no longer degenerated but each has its own propagation constant. A similar effect is caused by chromatic dispersion, where the group delay depends on the wavelength.

Common source of problems in all optical communication schemes are the polarization effects in single-mode fiber.

Nowadays, the remaining birefringence is small enough for the telecom industry, but any birefringence even extremely small, will always remain a concern in quantum communication.

This is clearly true for polarization based systems and also equally a concern for photon based systems because the interference visibility depends on the polarization states [13].

Single-photon detection

The possibility of detection of single photons determines the success of quantum cryptography. Various detection devices can be used to achieve this, like photomultipliers, avalanche photodiodes, and multichannel plates.
For photons in the range of wavelengths (600 – 800) nm, the commercially available single – photon counting modules based on silicon (Si) avalanche photodiodes (APDs') have high efficiencies and low – noise rates. Operating in this region will affect the data rate and error rate because the attenuation of single – mode fiber is quite high in this region (~ 3 db), on the other hand optical fibers have much lower attenuation in the infra – red at the 1.3 μm wavelength and more lower attenuation at 1.55 μm.

Although Ge and InGaAs APDs are commercially available, there are no commercially available single– photon modules. Nevertheless , it was shown that single photons at 1.3 μm can be detected by Ge APDs' by first cooling them to reduce noise and then be operated in so-called Geiger mode in which they are biased above breakdown [13].

Quantum Key: A Case Study

Results of 36-run process of simulation software are listed in Table (2). This software simulates a quantum cryptographic system based on photonic entanglement using the basic Ekert's protocol. The BB89 protocol is used for error elimination together with universal hashing technique by random binary matrix as a privacy amplification method. The simulated reality supposes an EPR-source emits maximally entangled photons prepared in Ψ^- –Bell's state, to the legitimate parties Alice and Bob. Eve, a malicious eavesdropper, attacks photons utilizing the intercept/resend strategy with strong filteration measurement of the attacked photons. Innocent noise is also taken into account.

Table (2) considers only three parameters: sifted key length, QBER, and Bell parameter when the EPR-source emits 5000 EPR pairs. One can notice the following:

i) In general, Bell parameter drops with increasing QBER (i.e., increasing Eve's attack level). For example, QBER=0 (i.e., Eve does not attack any photon at all) in run #21 and the corresponding $|\boldsymbol{S}|$= 2.8216, which violates Bell's inequality maximally. On the other extreme, QBER= 0.1266 in run #34 (the maximum among all the 36 runs) and the corresponding $|\boldsymbol{S}|$= 2.0305.

Actually, Eve must make a trade-off between her information gain and the induced QBER when she performs her attack, because if she intervenes severely she may gain large amount of information about the shared key between Alice and Bob but in the other hand she will be exposed by the Bell inequality which may not be violated in this case due to the high QBER.

ii) The sifted key has a maximum length in this assembly of samples in run #21, n_{sifted}= 1159 bits due to Eve's absence. It not necessary that when QBER be at its minimum extreme, the sifted key length be at its maximum one, because Eve attacks photons randomly (either photons at matched analyzer's orientations, mismatched ones, or destroyed photons due to innocent noise). Hence she may attack a large number of photons collectively, but the attack's share of the similar orientations group-photons (which are responsible for establishing the sifted key string) may be small. So, final discovered errors by Alice and Bob which determine QBER will also be small. In fact, the innocent noise pulses also play a vital role in deciding the sifted key length.

References

1. A. Zielinger, "Fundamentals of Quantum Information", Physics World (1998) p 35.
2. A. Zielinger, "The Physics of Quantum Information", Springer (1998).
3. Commentary of Rosenfeld, *The Einstein-Podolosky-Rosen paper*, (1967).
4. A. Einstein, B. Podolosky and N. Rosen, "*Can quantum mechanical description of physical reality be considered complete?*", Phys. Rev. ***47***, 777 (1935)
5. J. S. Bell, *On the Einstein Podolosky Rosen Paradox*, Physics ***1***, 195 (1964)
6. W. Tittel and G. Weihs, *Photonic entanglement for fundamental tests and quantum communication*, Quantum Information and Computation ***1***, 1 (2001).

Table (2): Results of a 36-run process of the simulation software mentioned above, comprising the sifted key length n_{sifted}, quantum bit error rate QBER, and the absolute value of Bell parameter $|S|$.

Run index	n_{sifted} (bits)	QBER	$\|S\|$
1	981	0.0591	2.4824
2	1038	0.0684	2.3690
3	706	0.0650	2.4290
4	735	0.0571	2.4858
5	611	0.0491	2.5440
6	831	0.0902	2.2606
7	850	0.1000	2.1980
8	428	0.0771	2.3686
9	655	0.1022	2.1443
10	916	0.1157	2.0906
11	871	0.0459	2.5386
12	1083	0.0930	2.2615
13	678	0.0855	2.2590
14	864	0.0682	2.4300
15	547	0.0182	2.7140
16	404	0.1237	2.0850
17	518	0.0772	2.3107
18	570	0.0754	2.3695
19	1026	0.1174	2.0924
20	988	0.0182	2.7089
21	1159	0	2.8216
22	488	0.0778	2.3637
23	848	0.0094	2.7640
24	389	0.0694	2.4300
25	589	0.0288	2.6552
26	606	0.1204	2.0796
27	404	0.0198	2.7102
28	969	0.1217	2.0890
29	1046	0.0095	2.7686
30	979	0.0663	2.4283
31	529	0.0491	2.5405
32	701	0.0199	2.7073
33	1083	0.0295	2.6528
34	837	0.1266	2.0305
35	472	0.0381	2.5880
36	774	0.0465	2.5458

7. A. Abeyesinghe, *Review: Quantum entanglement from theory to new technology*, Dartmouth Undergraduate J. Science ***3***, No.1, (2000).
8. C. H. Bennett, "Quantum Information", IBM Research Yorktown, Apr. 2000, retrieved from www. research.ibm.com/quantuminfo .
9. D. Bouwmeester , Jian-Wei Pan , P. Mattle , M.Eibl, H. Weinfurter and A. Zeilinger *Experimental quantum teleportation*, Nature 390, 575 (1997).
10. M. O. Scully and M. S. Zubairy, "Quantum Optics", Cambridge University Press (1999).
11. T. Jennewein, C. Simon, G. Wies, H. Wienfurter and A.Zielinger, *Quantum cryptography with entangled photons*, Phys. Rev. Lett. ***84***, 4729 (1999).
12. H. Zbiaden, H. Bechmann- Pasquinucci, N. Gisin, G. Ribordy, Quantum Cryptography, Appl. Phys. ***B 67***, 743 (1998).
13. R. J. Hughes, W. Buttler and G. Paul, *Secure communication using quantum cryptography*, LA-UR -97-1099, pp 76-85.
14. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, *Experimental Quantum Cryptography*, J. Cryptology ***5***, No.3 (1992).
15. N. Gisin, G. Riburdy, W. Tittel and H. Zbindin, *Quantum cryptography*, Rev. Mod. Phys. ***74***, 145 (2001).
16. A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. ***67***, 661 (1991).
17. D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund and P. G. Kwiat, *Entangled state cryptography: Eavesdropping on Ekert protocol*, Phys. Rev. Lett. ***84***, 4733 (2003).
18. M. J. A. deDood, W. T. M. Irvine and D. Bouwmeester, *Nonlinear Photonic Crystals as a Source of Entangled Photons*, Phys. Rev. Lett. ***84***, 1 (2003).

التشفير الكمي وآلية توزيع المفتاح الكمي

خليل ابراهيم حاجم شيلان خسرو توفيق احمد محمد مكي

معهد الليزر للدراسات العليا ، جامعة بغداد ، بغداد ، العراق

الخلاصة

يتضمن المقال استعراضا قصيرا لخصائص الحقيقة والمكان في البصريات الكمية ، ويتم تقديم متباينة بيل وحالات بيل لبيان استخدامهم المباشر في الحاسوب الكمي والأنتقال عن بعد . كما يناقش التشفير الكمي بشيء من التفصيل فيما يتعلق بالأفكار الأساسية والأعتبارات العملية . بالأضافة الى ذلك يتم عرض ومناقشة دراسة حالة عن آلية توزيع مفتاح كمي يعتمد على الأساسيات المعطاة .