Effect of Number of Entangled Photons on Number of Coincidences, Bell's values |S| and Error Rate Using Delphi Program

Abstract:

Background: Quantum cryptography is science that relies on the use of protocol designed to exploit quantum mechanical phenomena to achieve the secrecy of cryptographic keys.

Method: This work aimed to generate quantum key based on polarization entangled photon pairs, and to eliminate the error by implementing BB89 protocol using Delphi language program in order to obtain a high degree of security.

Results: The results explain the effect of number of EPR photons pair running from (500-10000) photons on number of coincidences, expected error and Bell's parameter discussed as: Total coincidences of the Bell – CHSH increases with increasing of EPR pairs, and $|S|$ values were stable when EPR pairs were increased, there was a small random change in the expected error rate (in case of no eavesdropping).

Conclusions: This study conclude that Total coincidences of the Bell and expected error are affected by the number of entangled photons

Keyword: Quantum Key Distribution (QKD), Einstein- Podolesky- Rosen (EPR).

Introduction

The main goals of cryptography are the encryption and decryption of messages to render them unintelligible to third party. These goals can be obtained when the sender ("Alice") and recipient ("Bob") both have a secret Key using some cryptographic algorithm. The key distribution becomes possible if they communicate by using the emerging technology of quantum cryptography (QC), or quantum key distribution (QKD). In 1991 Ekert proposed the Einstein- Podolesky- Rosen (EPR) (Einstein et al., 1935) "entangled" two-particle states used to implement a quantum cryptography protocol whose security was based on "Bell's inequalities". (Bell et al., 1964), (Bopp., 2017)

For a review, see, for example, (Gisin et al., 2002), (Flamini et al., 2018)

In the not-too-distant future, quantum computing is anticipated to transform the paradigm of computing (Minal and Nisha., 2014).Researchers are faced with the challenge of creating new coding methods that would hold up in the era of quantum computing. Also, previous study (Nurhadi and Syambas., 2018). which showed that in order to provide security strength in key distribution, most conventional cryptography depends on mathematical complexity and the irrational amount of time required to crack the approach. However, it won't work if the procedure for distributing secret keys is faulty. Peter Shor published an algorithm in 1994 that can efficiently factorize big integer numbers using the principles of a quantum computer, posing a threat to some of the classical encryption. Recently, quantum key distribution (QKD) has drawn more attention from researchers as a potential solution to the key distribution issue. Using the principles of quantum physics,it has been shown that QKD is theoretically capable of providing communication that is 100 percent secure. Theoretically, QKD has been demonstrated to be capable of offering communication that is completely secure based on the laws of quantum mechanics.

In addition, previous study (Iovane., 2021) showed the quantity of data points the system can gather in a limited amount of time has a significant impact on the security of real-world quantum key distribution (QKD). Obtaining positive secret keys now requires block lengths in the order of 104 bits for state-of-the-art finite-key security evaluations. However, in fact, it can be very challenging to meet this condition, particularly in the case of entanglement-based satellite QKD, where the overall channel loss can reach 70 dB or higher. Here, we present an enhanced finite-key security analysis that lowers the required block length for typical channel and protocol parameters by 14% to 17%. Practically speaking, this reduction might spare weeks of measurement time and resources for entanglement-based satellite QKD, bringing space-based QKD technology closer to being a reality. We demonstrate the recently revealed Micius QKD satellite's ability to generate positive secret keys with a 105-security level using the improved analysis as an application. Using the commercial Optic System TM optical simulation, a framework for modeling and simulating quantum key distribution algorithms is presented. This simulation methodology is based on the empirical components of a quantum key distribution. The BB84 process was also simulated using the noise immune switching distribution and different security attack scenarios. In terms of the experimental arrangement, the effectiveness of the visual simulator's component parts was also examined. These simulations were used to examine how the experimental optical components affected the quantum key distribution process (Buhari et al., 2012).

According to (Iovane., 2021), (Kalra., 2019),The most recent development in quantum cryptography is quantum key distribution. There are numerous QKD protocols, including BB84, B92, Ekert91, COW, and SARG04, the earliest of which was created in 1984. The BB84 protocol's work was discussed, and after that, a new protocol that is a variation of the BB84 protocol was proposed. Next, the design of the simulation setup was discussed. Finally, the BB84 protocol's performance was compared with the proposed protocol, and the latter performed significantly better in terms of amplitude and error estimation. Both the BB84 protocol and the new protocol's simulation design employed an object-oriented methodology.

The uses of quantum information science are expanding into better and more expansive aspects for the upcoming technologies. In the fields of quantum computation and cryptography, there have already been a number of ground-breaking physical products and promising outcomes. One of the more developed fields of quantum mechanics is quantum cryptography, and the equipment is already on the market. The current level of quantum cryptography is still being researched in numerous ways in order to reach the heights of digital cryptography. However, because it uses both hardware and software, quantum cryptography is extremely difficult. The success of quantum cryptography experiments is delayed by the lack of an effective modeling tool for designing and analyzing the experiments. Therefore, in order to achieve a high level of security, a framework based on polarization entangled photon pairs utilizing the Ekert protocol is used in this paper. Additionally, the error is eliminated by implementing the BB89 protocol using a Delphi language application.

Theoretical background:

Aurther Ekert (Weier., 2003), (Bennett., 1992), (Ekert., 1991) proposed the entanglement-based quantum cryptography method which explained as: a source that emits entangled photon pairs (in the Bell state) in opposite directions is placed Between Alice and Bob, (Bell., 1964). Alice and Bob receive a photon and analyse its polarization on a different, randomly basis and exchange information about the bases were used (Ma et al., 2007), (Acin et al., 2007). After that branched the results into two groups: first group when they used the same basis of measurement used as keys of cryptography, the second when used different basis used to chick the eavesdropping. Since they cannot be utilized for the key transfer anyway, and make the findings of those measurements' public. With the use of these figures, they may determine whether the experimental data they collected is in violation of the so-called Clauser- Horne- Shimony- Holt (CHSH) inequality (Weier., 2003). This is a different interpretation of Bell's inequality, which was inspired by the EPR paradox. When Alice and Bob are measuring in distinct bases according to the Ekert protocol, the CHSH inequality provides a constraint for classically coupled particles that is maximally violated by quantum correlations. Calculating the violation of the CHSH inequality will allow Alice and Bob to be certain that no eavesdropper was present as these quantum correlations are the source of information utilized to derive the key (Weier., 2003).

A state of an EPR photon pairs that emitted in a single state of polarization used to carry out the key distribution is explained by (Maki., 2004):

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle_1|\uparrow\rangle_2 - |\uparrow\rangle_1|\rightarrow\rangle_2\right) \quad (1)$$

After the photons have separated, Alice and Bob, measure of incoming particles individually and arbitrarily selected bases and record the results in one of three bases that are created by rotating the basis along the z-axis at different angles:

$\Phi_1^a = 0,\ \Phi_2^a = \frac{\pi}{4}$ *and* $\Phi_3^a = \frac{\pi}{8}$ for Alice and by angles

$\Phi_1^b = 0,\ \Phi_2^b = -\frac{\pi}{8}$ *and* $\Phi_3^b = \frac{\pi}{8}$ for Bob.

The analyzers for Alice and Bob are indicated by the superscripts "a" and "b," respectively. There are two outcomes for each measurement. +1 (the photon is measured in the first polarization state of the selected basis) and -1 (the photon is measured in the other state of the selected basis), and each measurement has the ability to expose one piece of information.

The amount:

$$E(\Phi_i^a,\Phi_j^b) = P_{++}(\Phi_i^a,\Phi_j^b) + P_{--}(\Phi_i^a,\Phi_j^b) - P_{-+}(\Phi_i^a,\Phi_j^b) - P_{+-}(\Phi_i^a,\Phi_j^b) \quad (2)$$

E: is the correlation coefficient of the measurements performed by Alice in the basis rotated by Φ_i^a and by Bob in the basis rotated by Φ_j^b. Here $P_{\pm\pm}(\Phi_i^a,\Phi_j^b)$ denotes the probability that the result ± 1 has been obtained in the basis defined by Φ_i^a and ± 1 in the basis defined by Φ_j^b. According to the quantum rules (Maki., 2004):

$$E(\Phi_i^a,\Phi_j^b) = -\cos\left[2(\Phi_i^a - \Phi_j^b)\right] \quad (3)$$

And $E(\Phi_1^a,\Phi_1^b) = E(\Phi_3^a,\Phi_3^b) = -1$ (4)

We can define the quantity S that composed of the correlation coefficients when Alice and Bob used analyzers of different orientation:

$$S = E(\Phi_1^a,\Phi_3^b) + E(\Phi_1^a,\Phi_2^b) + E(\Phi_2^a,\Phi_3^b) - E(\Phi_2^a,\Phi_2^b) \quad (5)$$

Which the same S that is generalized the Bell theorem proposed by Clauser, Horne, Shimony and Holt, and known as the CHSH inequality (Guillermin and Dedeurwaerdere., 2013). Quantum mechanically S must be equal: $S = -2\sqrt{2}$ (6).

Quantum Calculation of the Correlations in Bell's Theorem

A state vector $|\Psi\rangle$ which described by quantum calculation for the probability of a spin-1/2 particle passing through a Stern- Gerlach apparatus (SGA) oriented at angle θ is given by (Guillermin and Dedeurwaerdere., 2013):

$$P_\Psi(\theta) = |\langle\theta|\Psi\rangle|^2 \quad (7)$$

$|\theta\rangle$ is formed by rotating a "spin up "state about the Y-axis:

$$|\theta\rangle = e^{-i\theta\sigma_y/2}|\uparrow\rangle \quad (8)$$

recall that:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (9)$$

and:

$$|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \text{ and } |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (10)$$

$P_\Psi(\theta)$: is the probability that may be rewritten as:(Scully and Zubairy., 1969):

$$P_\Psi(\theta) = \langle\Psi|\theta\rangle\langle\theta|\Psi\rangle \quad (11)$$

The probability of simultaneous passage through SGAs at $\theta_a$and $\theta_b$by the particles after a little algebra, described by the spin singlet state (Rau et al., 20014):

$$\left|\Psi_{1,2}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow_1,\downarrow_2\right\rangle - \left|\downarrow_1,\uparrow_2\right\rangle\right) \quad (12)$$

is:

$$P_{ab} = \left\langle \Psi_{1,2}\left|\pi_{\theta_a}^{(1)},\pi_{\theta_b}^{(2)}\right|\Psi_{1,2}\right\rangle \quad (13)$$

The projection operators in this expression correspond to particles 1 and 2. After a little algebra, one finds:

$$P_{ab} = \frac{1}{4}\left[1-\cos(\theta_a-\theta_b)\right] = \frac{1}{2}\sin^2\left[\frac{(\theta_a-\theta_b)}{2}\right]$$

(14)

in this work photons are involved along so that the optical polarization property, an expression for the probability will also be established; however, it will only apply to the scenario of a source of photon pairs emitting to two receivers that measure photons by filters (analyzers) then detectors, as shown in figure (1).

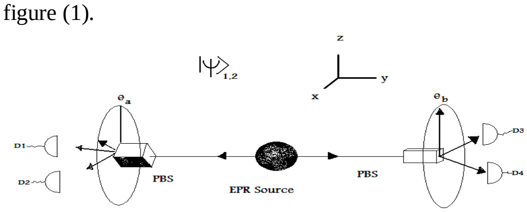

Figure (1): correlations measurements between Alice's and Bob's detection events for different choices for the detection bases (indicated by the angles θa and θb for the orientation of their polarizing beam splitter, PBS) lead to the violation of Bell's inequality (Zeilinger., 1998).

The polarization state of the two photons, after passage through the filters, is:

$$\left|\Psi_{1,2}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|r_1\right\rangle\left|r_2\right\rangle + \left|l_1\right\rangle\left|l_2\right\rangle\right) \quad (15)$$

r and l represent the photon polarizations being right and left circular and the subscripts 1 and 2 represent the photons having frequencies $\nu_1$and ν_2 respectively (Maki et al., 2004). A change of basis to linear polarization states $\left|x\right\rangle,\left|z\right\rangle$ allows the state vector $\left|\Psi_{1,2}\right\rangle$ above to be rewritten as:

$$\left|\Psi_{1,2}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|z_1\right\rangle\left|z_2\right\rangle + \left|x_1\right\rangle\left|x_2\right\rangle\right) \quad (16)$$

The measurement of joint linear polarization by polarizer's at angles θ_a and θ_b to the z-axis projects the latter state above onto the two polarization states:

$$\left|\theta_a\right\rangle = \cos\theta_a\left|z_1\right\rangle + \sin\theta_a\left|x_1\right\rangle \quad (17)$$
$$\left|\theta_b\right\rangle = \cos\theta_b\left|z_2\right\rangle + \sin\theta_b\left|x_2\right\rangle$$

The probability for passage through the two-polarization analyzers quantum mechanically is given by:

$$P_{1,2}(\theta_a,\theta_b) = \left|\left\langle\theta_a\right|\left\langle\theta_b\right|\Psi_{1,2}\right\rangle\right|^2 \Rightarrow P_{1,2}(\theta_1,\theta_2) = \frac{1}{2}\cos^2(\theta_a-\theta_b)$$

(18)

By the way, the one useful form of the Bell inequalities (which is usually tested in experiments) is due to Clauser and Horne, and is defined by (Guillermin and Dedeurwaerdere., 2013):

$$S = \frac{P_{12}(\theta_a,\theta_b) - P_{12}(\theta_a,\theta_b') + P_{12}(\theta_a',\theta_b') + P_{12}(\theta_a',\theta_b')}{P_1(\theta_a') + P_2(\theta_b')} \le 1$$

(19)

S: known as the Bell parameter. By using:

$P_{1,2}(\theta_1,\theta_2) = \frac{1}{2}\cos^2(\theta_a-\theta_b)$ for any θ_1 and θ_2,

and : $P_1(\theta) = \frac{1}{2}$, $P_2(\theta) = \frac{1}{2}$, for any θ (may be θ_1 or θ_2), then the following is defined :

$$F = \frac{P_{12}(\theta_1,\theta_2)}{P_1+P_2} = \frac{\frac{1}{2}\cos^2(\theta_1-\theta_2)}{\frac{1}{2}+\frac{1}{2}} = \frac{1}{4}+\frac{1}{4}.\cos\left[2(\theta_1-\theta_2)\right]$$

(20)

Then S may be rewritten as:

$$S = F_1 + F_2 + F_3 + F_4 \le 1 \quad (21)$$

where the indices 1, 2,3 and 4 correspond to the angle combinations:

$(\theta_a,\theta_b),(\theta_a,\theta_b'),(\theta_a',\theta_b)$ *and* (θ_a',θ_b'),

respectively. By substituting for each F above in S expression yields (Maki et al., 2004):

$$S = \cos2(\theta_a-\theta_b) - \cos2(\theta_a-\theta_b') + \cos2(\theta_a'-\theta_b) + \cos2(\theta_a'-\theta_b')\ldots \le \frac{4}{2} = 2$$

(22)

$\therefore\ S \le 2$.

S: represent the Clauser and Horne form of Bell inequalities which adapted in the Ekert protocol for the quantum transmission in the quantum key distribution process, the correlation coefficients E_1,E_2,E_3 and E_4 defined in absolute by:

$$\left|E\right| = \cos\left[2(\theta_1-\theta_2)\right] \quad (23)$$

for any θ_1 and θ_2, where the indices 1, 2, 3 and 4 are as for the F's above.

Error correction stage

Error will strike Alice's and Bob's strings during quantum transmission, which parameterized by the quantum bit error rate (QBER) defined as the number of errors divided by total size of the cryptographic key. For example a QBER of 0.5 implies Alice and Bob have completely uncorrelated strings (Naik et al., 1999)..

The BB89 protocol (BB89 protocol is a modified version of the original protocol BB84 to produce a working QC apparatus at IBM in October 1989. It is called "BB" after the names of its inventors Bennett and Brassard) is adapted to eliminate the errors in the raw of quantum transmission (RQT) strings. Due to its simplicity and capability of eliminatory relatively high error rates is adapted in this work. (Faraj et al., 1999).

The input of this stage is the sifted key (which is an erroneous string output from the quantum transmission stage) and the output of the error elimination stage is the final key, which should be identical for both Alice and Bob at successful implementation for error elimination stage. The final key is smaller than the sifted key.

Simulation work:

The simulation of virtual reality features an EPR source that sends Bob and Alice the maximum number of maximally entangled photon pairs in the Bell's state. Additionally, the detectors' and polarized beam splitter's rules were concerned.

The random number generator function (RNG) was used to produce EPR photon pairs. One of the pair stored in Alice's array and the other stored in Bob's array. Alice and Bob randomly choose the base of measurement (state of analyzer) by using the detection angles are: $\theta_1^a = 0, \theta_2^a = \frac{\pi}{4}, \theta_3^a = \frac{\pi}{8}$ and

$\theta_1^b = 0, \theta_2^b = -\frac{\pi}{8}, \theta_3^b = \frac{\pi}{8}$ and substituted these angles in the rotational matrix which is defined by: $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.

The idea of quantum superposition and single particle interference explains why the EPR photons' random paths to the 1- or 0-detector at either side of the system—which are represented here by the product of multiplying the EPR photons by the analyzer's matrix (after placing them in a 1x2 matrix)—are justified.

When comparing their bases of measurement (state of the analyzer), Alice and Bob divided the data into two groups: the first group, which was used different bases of measurement to determine the Bell's parameter (S)

$S = E(\Phi_1^a, \Phi_3^b) + E(\Phi_1^a, \Phi_2^b) + E(\Phi_2^a, \Phi_3^b) - E(\Phi_2^a, \Phi_2^b)$

The second group: contains the outcomes of Alice and Bob using identical measurement bases. It represented by a quantum transmission raw that is used in the error-reduction stage as shown in figure (2) below. Bell's parameter and quantum bit error rate (QBER)(e) ,(Guillermin and Dedeurwaerdere., 2013)are actually connected by the fact that a decrease in the latter (toward minimum or eavesdropping) corresponds to an increase in the former (toward Bell's inequality violation). In particular, the following relates the maximum violation of Bell's inequality to QBER(Gisin et al., 2002), (Guillermin and Dedeurwaerdere., 2013):

$$|S|_{\max} = \begin{cases} 2\sqrt{2}, Eveisabsent \\ (1-2e).2\sqrt{2}, Eveispresent \end{cases} \quad (24)$$

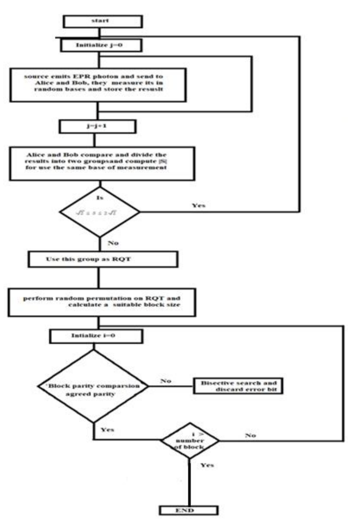

Figure 2: A simplified flowchart for the simulation

Results:

The system run from(500-10000) EPR photon pairs (500) in each step he relation between Number of EPR photon pairs &Number of coincidences is plot in figure(3)Number of EPR photon pairs & Bell parameter |S| is plot in figure (4)and Number of EPR photon pairs & innocent error E is plot in figure (5)respectively

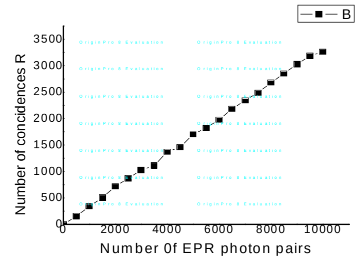

Figure (3): A plot diagram of number of total coincidences R versus number of EPR photon pairs.

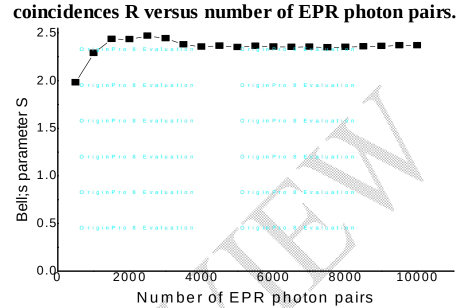

Figure (4): A plot diagram of Bell parameter, S, versus number of EPR photon

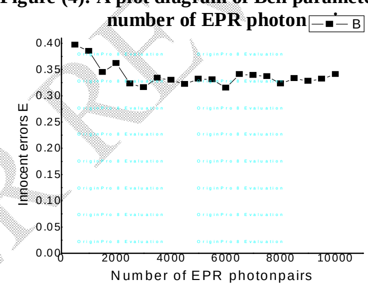

Figure (5): A plot diagram of innocent error E versus No. of EPR photon pairs.

Effect of point wise privacy amplification parameter

Discussions:

It given and explored how the number of EPR photons affected the number of coincidences and the values of the Bell's parameter. The sum of the coincidence counts for the Bell-CHSH analyzer orientation combinations at various reliable detection clicks is the total coincidences, or R. Figure (3) shown how the number of total coincidences consistently rises as the number of EPR pairs increases Taking the extremes for example, (R=156) in Run (1) for (PH.No=500 EPR pairs), while it reaches its higher value in the state (R=3263) in Run (20) for the high value of EPR pairs number (PH.No= 10000 EPR pairs).. In reality, after a quantum transmission has been completed, Alice and Bob begin their computations of the Bell parameter and count the total number of coincidences. The rise in EPR pairs figure (4) makes it easy to see the tiny alterations (stability) in the Bell parameter Taking the extremes for example, (S=2.435) in Run (3) for (PH.No=1500 EPR pairs), while it reaches (S=2.369) in Run (20) for the high value of number of EPR photon pairs (PH.No = 10000 EPR pairs). These results were obtained without Eve's presence. One can notice clearly the small mutations (stability) in innocent error with the increase in EPR pairs in figure (5) .Taking the extremes for example, (E=0.975) in Run (1) for

(PH.No=500 EPR pairs), while it reaches (S=0.341) in Run (20) for the high value of number of EPR pairs (PH.No= 10000 EPR pairs). These results were taken in absence of eavesdropper. From previous studies: (Ignatovich., 2015) said that ‘a final check of two versions of quantum mechanics with individual and entangled photons it is required an experiment with parallel aligned crystals and rare pulses of the photon pairs, where each pair is marked by the time of registration concerned with this study.

From (Mafu., 2016) We have demonstrated the principle of operation of QKD. We have shown how one can use the properties of the laws of quantum mechanics to allow the legitimate parties to share a secret key. In particular, we have shown that the eavesdropper cannot guess the output or outcome from the legitimate parties and gain more than half of the information being transmitted. This means that the key generated by quantum cryptography is always secure, thus showing the power of quantum mechanics in securing information that agreed with present study (Singh et al., 2014) Quantum key distribution is clearly an unconditionally secure means of establishing secret keys. Combined with unconditionally secure authentication, and an unconditionally secure cryptosystem. The major difference of quantum key distribution is the ability to detect any interception of the key, whereas with courier the key security cannot be proven or tested. QKD system has the advantage of being automatic, with greater reliability and lower operating costs than a secure human courier network

Conclusions:

From the results of the simulation weconcluded:

Total coincidences of the Bell – CHSH analyzer angle combinations increase with increasing of EPR pairs, Bell’s parameter $|S| \le 2\sqrt{2}$ was verified in case of no eavesdropping. It was clear from the results that $|S|$ values were stable when EPR pairs were increased;there was a small random change in the expected error rate (estimated by Alice and Bob after quantum transmission stage before beginning the error elimination stage) in case of no eavesdropping when EPR pairs were increased.

Data Availability Statement

All data underlying the results are available as part of the article and no additional source data are required.

References:

A. K. Ekert. Quantum cryptography based on Bell’s theorem: Phys. Rev. 1991 ; 67: 661–663

A. Einstein, B. Podolsky, N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete: Physical Review.1935; 47(10): 777-780.

A. M. Maki. Simulation of Quantum Key Distribution Based on Entangled Pairs of Photons Using the Basic Ekert Protocol. M.Sc. Thesis University of Baghdad.2004

A.I. Nurhaci and N. R. Syambas. Quantum Key Distribution (QKD) Protocols: A Survey," 2018 4th International Conference on Wireless and Telematics (ICWT). 2018.

Abud hahir Buhari and Zuriati Ahmad Zukarnain, S. K. Subramaniam, Hishamuddin Zainuddin, Suhairi Saharudin. An efficient modeling and simulation of quantum key distribution protocols using Opti System: IEEE Symposium on Industrial Electronics and Applications. 2012 :84-89.

Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani. Device-independent security of quantum cryptography against collective attacks: Phys. Rev. 2007; 98:230501

Bennett CH. Quantum cryptography using any two nonorthogonal states: Physical review letters. 1992 May 25;68(21):3121.

F. Flamini, N. Spagnolo, F. Sciarrino. Photonic quantum information processing: A review. Rep. Prog. Phys. 2018; 82. 016001

Fritz W. Bopp. Causal Classical Physics in Time Symmetric Quantum Mechanics :4th International Electronic Conference on Entropy and Its Applications, Basel, Switzerland.2017; http://sciforum.net/conference/ecea-4.

Gerardo Iovane. Computational quantum key distribution (CQKD) on decentralized ledger and blockchain. Journal of Discrete Mathematical Sciences and Cryptography2021 24:4, pages 1021-1042.

Hitesh Singh, D.L. Gupta, A.K Singh. Quantum Key Distribution Protocols: A Review: IOSR Journal of Computer Engineering (IOSR) 2014; 16(2) 1-9

J. S. Bell. On the Einstein Podolosky Rosen Paradox. Physics. 1964;1: 195-200

J. S. Bell. On the Einstein Podolsky Rosen Paradox: Physics. 1964;1: 195-200.

Kalra, M, Poonia, R.C. Design a New Protocol and Compare with BB84 Protocol for Quantum Key Distribution. In: Bansal, J., Das, K., Nagar, A., Deep, K., Ojha, A. (eds) Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing: Springer. 2019; 817: 978-981, Singapore.

Mafu, M. A Simple Security Proof for Entanglement-Based Quantum Key Distribution: Journal of Quantum Information Science.2016;6: 296-303.doi: 10.4236/jqis.2016.64018.

Mathieu Guillermin and Tom Dedeurwaerdere. Epistemic Values, Bell's Inequalities and Realism: The Case of Contemporary Approaches to Quantum Mechanics. SSRN .2013;10(2139):2284104

M. O. Scully and M. S. Zubairy (1997). Quantum Optics, Combridge University Press. UK

Minal Lopes and Nisha Sarwade. Cryptography from Quantum Mechanical Viewpoint: International Journal on Cryptography and Information Security (IJCIS). 2014;4(2).

Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, Hugo Zbinden. Quantum cryptography: Rev. Mod. Phys. 2002; 74: 145

M. Rau, T. Heindel, S. Unsleber, T. Braun, J. Fischer, S. Frick, S. Nauerth, C. Schneider, G. Vest, S. Reitzenstein, M. Kamp, A. Forchel, S. Höfling, H. Weinfurter. (2014). Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources—A proof of principle experiment. New J. Phys. 16: 043003

S. Naik, C. G. Peterson, A. G. White, A.J. Bergland, and P.G. Kwiat. (1999). Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol. : Physical Review Letters. 84. 20: 4733-4736

S.T. Faraj. Quantum Cryptography Key Distribution in Optical Communication Networks. PhD Thesis Submitted to The Collage of Engineering of The Former Sadam University, Electronic and Communication Engineering1999.

Vladimir K. Ignatovich. Closer Look at EPR Paradox and Bell's Inequality: American Journal of Modern Physics and Application. 2015;2(2) :16-20.

Weier H. Experimental quantum cryptography. Diploma Dissertation, Technical University of Munich. 2003 Dec.

X. Ma, C.-H. F. Fung, H.-K. Lo. Quantum key distribution with entangled photon sources: Phys. Rev. 2007 ;76: 012307

Zeilinger (Eds). (1998). The Physics of Quantum Information.springer Inc. ISBN-13: 978-3540667780