Iraqi Journal of Information and Communication Technology(**IJICT**)
Vol. 5, Issue 3, December 2022

www.ijict.edu.iq

ISSN:2222-758X
e-ISSN: 2789-7362

EVALUATION OF QUANTUM KEY DISTRIBUTION BY SIMULATION

Harith A. Qaisi [1], **M. F. Al-Gailani** [2]
[1,2] College of Information Engineering, Al-Nahrain University, Baghdad, Iraq
{harith.ahmed, m.falih}@coie-nahrain.edu.iq [1,2]

Received:5/12/2021, Accepted:22/2/2022
DOI:**10.31987/ijict.5.3.157**

***Abstract*- Cryptography is a scientific approach to transmitting information securely. While quantum cryptography relies on the physical rules to encrypt information. When the quantum computer debuted, the traditional cryptographic approach became less efficient. The quantum approach is frequently used to distribute keys across communication entities, which is known as quantum key distribution (QKD). The primary paradigm of QKD was initiated for a depolarization channel. Quantum key distribution is a secure method for exchanging keys across communication entities. The first QKD protocol, BB84, was introduced in 1984. The primary paradigm of QKD was initiated for a depolarizing channel. In traditional cryptography, secret keys are sent over a secure communication channel. The problem arises when both parties are unable to establish a secure channel for the first key exchange, so all their correspondence may be intercepted and decrypted by a third party that obtained the key during the initial key exchange. This paper demonstrates the ability to use MATLAB to simulate QKD. It has been found that the security of the QKD protocol depends on a variety of factors. It provides security tests, recommendations, and guidance on the lower and higher bounds of significant parameters such as the depolarizing channel parameter, number of input photons, and Eve's attack level for a target secret-key rate, as well as insightful outputs such as QBER, secret-key rates, the mutual information between Alice and Bob or Alice and Eve, and the expected number of bits to be leaked.**

***keywords:* Quantum cryptography, Simulation, QKD, Eve attack, Matlab.**

I. INTRODUCTION

Quantum cryptography seeks to provide information security by taking advantage of the fundamental characteristics of quantum physics [1] and [2]. In 1984, Charles Bennett and Gills Brassard invented the first technique for key distribution [1]. It is designated BB84. This is the first discovery of a quantum distribution system. The quantum system is built on the scattering of single particles or photons, with the photon polarization encoding the value of a classical bit [1], [2], [3], and [4]. Heisenberg's Uncertainty Principle and photon polarization are two fundamental principles of quantum physics in the twentieth century that form the basis for quantum cryptography. According to Heisenberg, certain pairs of physical properties are related in such a way that determining the value of one precludes the observer from determining the value of the other. [3], [4]. For instance, while measuring the polarization of a photon, the direction of measurement affects the subsequent measurements. This means that the polarization of a photon or any other particle of light can only be determined at the measurement site. This concept is critical to preventing eavesdropping attempts in the quantum cryptographic system. On the other hand, the photon polarization principle defines the process by which light photons can be polarized in a certain direction. Furthermore, as a result of an eavesdropper in 1982's discovery of the no-cloning theorem [4], [5], eavesdroppers cannot copy unknown qubits, i.e. unknown quantum states. Quantum cryptography enables two communication partners to agree on a bit of a string without physically meeting, and both parties may be confident that only the agreed bitstring will be exchanged between them. BB84 enables the creation of two secret shared key sequences, frequently "Alice" and "Bob," using polarized photons. The following are the contributions of this study: First, as controllable factors, the depolarizing channel effect, Individual Eve Intercept and-Resend assaults, and the number of input photons were studied. Second, it not only outputs figure-of-merit parameters like Quantum Bit Error Rate (QBER) and secret-key rates, but it also guides through the system settings he should employ to meet security and achieve his desired key rate. This eliminates the need for time-consuming experimentation. This resulted in a faster simulation time when compared to the work in [6]. This speedup is critical, especially when the number of input photons is hundreds of thousands.

II. Related Work

In recent years, QKD has emerged as a new development technique for protecting sensitive data during transmission in a new networking environment. Several scholars collaborated on QKD simulation to develop a secure file transfer using various simulator parameters. Qiao & Chen in 2009 [7], For the depolarization channel, the BB84 protocol was used as the base QKD model, which was simulated using a MATLAB simulator. The simulation results were agreed with the theoretical conclusions. Nevertheless, the results of their analysis were weak. Kalra & Poonia in 2018 [8], It has been concluded that QKD is a secure method for sending keys between communication entities. The first QKD protocol was BB84, which was created in 1984 and described the C++ simulation technique of the BB84 protocol as well as the protocol simulation provided by C++ using an object-focused approach. On the other end of the protocol, a bidirectional quantum channel and an additional beginning bit sequence are formed for polarization. Dehmani et al. in 2018 [9], The goal of the QKD BB84 protocol is to allow transmitters and receivers to exchange keys over a quantum channel while also detecting "eavesdropping attacks" . This study aimed to examine the outcomes of several interceptions, retransmission, and cloning attacks on eavesdroppers, in addition, to proposing several scenarios for the location and manner of the eavesdropping attack and calculating the reciprocal knowledge of each event. The explicit formulations of shared information and quantum error indisputably show that the number of eavesdroppers and their attack parameters in the quantum channel determine the security of the transmitted data. Kiktenko et al. in 2020 [10], QKD enables secure communication over a quantum channel and an authentic public channel between two parties. Reducing the number of secret keys generated by the quantum during authentication is essential to increase the performance of the QKD system. The authors introduce a lightweight authentication mechanism for QKD based on the ping-pong method for QKD authenticity checks. From the literature above, it may be deduced that a variety of technologies could be utilized to simulate quantum key distribution using various programming languages. Some of these studies have limits, such as the number of photons used and how the secret key rates are achieved. The proposed work, however, varies from previous work in that it would use a variable number of photons, ranging from one to thousands, while also providing security testing for QKD.

III. Basics of BB84 Protocol

IBM's Charles H. Bennett and Gilles Brassard at the University of Montreal developed the BB84 quantum cryptography protocol in 1984. Their findings were presented at the IEEE conference in India. Polarized single-photon light pulses were used in the BB84 procedure. Quantum channels, such as fiber, connect Alice and Bob, while regular public channels, such as phone lines or the Internet, connect them to the real world. They found that the connection between the two channels is often the same. This would be an optical fiber with light pulses of different intensities over the quantum and classical channels, assuming the use of polarized photons. Alice's non-orthogonal states allow for secure communication. In this system, there are two bases of a polarized photon:

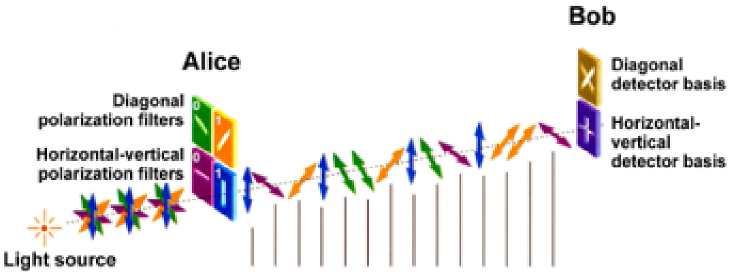
When one of the polarizations is selected randomly, it tells Bob about the current situation. It is vital to remember that putting "random selection" into practice is a difficult process. On one of the two bases, Bob is currently assessing the incoming situation. If Alice and Bob used the same method to conduct their research, their results would be entangled. Bob will not be able to obtain any information about the current state of the Photon if he chooses a different basis than Alice. In Fig. 1, suppose that Alice transmits a" horizontally polarized" photon $| \leftrightarrow >$ on a diagonal basis $\otimes$, and Bob "measures "on a diagonal basis $\otimes$, Bob will get either $+45 >$ polarized photon or $-45 >$, with a probability of 50 percent. Even if he later realizes that he made the wrong decision based on reasons, he will not be able to explain why.

The **horizontal-vertical basis** $\oplus$

- Horizontally polarised $|\leftrightarrow\rangle$
- Vertically polarised $|\updownarrow\rangle$

and the **diagonal basis** $\otimes$

- $+45°$ polarised $|\nearrow\rangle$
- $-45°$ polarised $|\nwarrow\rangle$


Bob
Diagonal detector basis
Horizontal-vertical detector basis
Alice
Diagonal polarization filters
Horizontal-vertical polarization filters
Light source

Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob's detection basis	⊞	⊠	⊞	⊞	⊠	⊠	⊞	⊞	⊠	⊞	⊠	⊠	⊞	⊞
Bob's measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

Figure 1: BB84 protocol stages (from[11])

IV. Classifications of Quantum Key Distribution Protocols

Depending on the effects of quantum physics used, the key generation methods used, and the physical principles adopted for security, a QKD system can be built in a variety of ways. Listed below are some examples:

1) Bennett and Brassard's protocol, "BB84" is based on two observations that do not have the same correlation [1].

2) Bennett's "B92" protocol (Bennett, 1992), this is based on non-orthogonal states of two variables.
3) Brub's "Six-state" procedure (extension BB84) [12].
4) The "entanglement-based" approach proposed by Ekert [13].
5) The Spedalieri technique is based on "Orbital Angular Momentum" [14].
6) Coherent state protocols, such as [15] [16].

V. Implementation of Experiment

The simulation model was created using a computer with the following parameters: Windows 10, 8th generation Intel Core i7 processor, 12 GB RAM. This was accomplished using MATLAB (version 9.6). Alice sends a stream of pulses, one at a time, from the transmitter side. A Single-Photon Source (SPS) should be used to generate the pulse. Each pulse is polarized independently by one of two mutually non-orthogonal bases: rectilinear (+) or diagonal (x). If the (+) basis is chosen, key bit 0 is encoded as a horizontally polarized pulse with a state vector of $|0° >$ and key bit 1 as a vertically polarized $|90° >$. If the (x) basis is chosen, key bit 0 is encoded as a circular-right polarized pulse with a state vector of $|45° >$, and key bit 1 as a circular-left $|-45° >$. This is accomplished using a polarization modulator controlled by a bases selector and a key bits generator as shown in Fig. 2. Bob decodes the received pulses by measuring their polarization states at the receiver side. The bits that were measured with unmatched basis are then discarded after Alice and Bob reveal their base choices. A polarization modulator is used to achieve the measurement setup, which is then followed by a Polarizing Beam Splitter (PBS) followed by single-photon detector. The sifted key is the key that remains after removing the bits that correspond to unmatched bases. QBER is the error rate in the sifted key. Then, to maximize protection against the knowledge Eve has received from the bits that have been released during data reconciliation, privacy amplification is used, in which more crucial bits are deleted. The secret key is the only remaining key available to Alice/Bob. The secret-key bit rate k is defined as the ratio between the length of the sifting key and the length of the hidden key, which is of major importance. The "MATLAB" (rand) function was used to generate pseudorandom numbers with an equal distribution over time. Then the "MATLAB function" is used to round the integers to the nearest integer (round). As a result, the two generators produce equally distributed random binary bits. The former specifies the bases randomly, with 0 for (+) and 1 for (x), and the latter produces key bits to be passed. The basic collection bits and key bits are transmitted using four case-specific instances of "1, 2, 3, and 4" , which are $|0°, |90°, |45°$, and $|-45°$, respectively. The output states are also uniformly dispersed due to the even distribution of the inputs in the four scenarios.

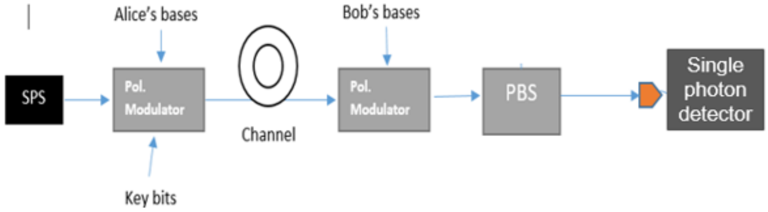
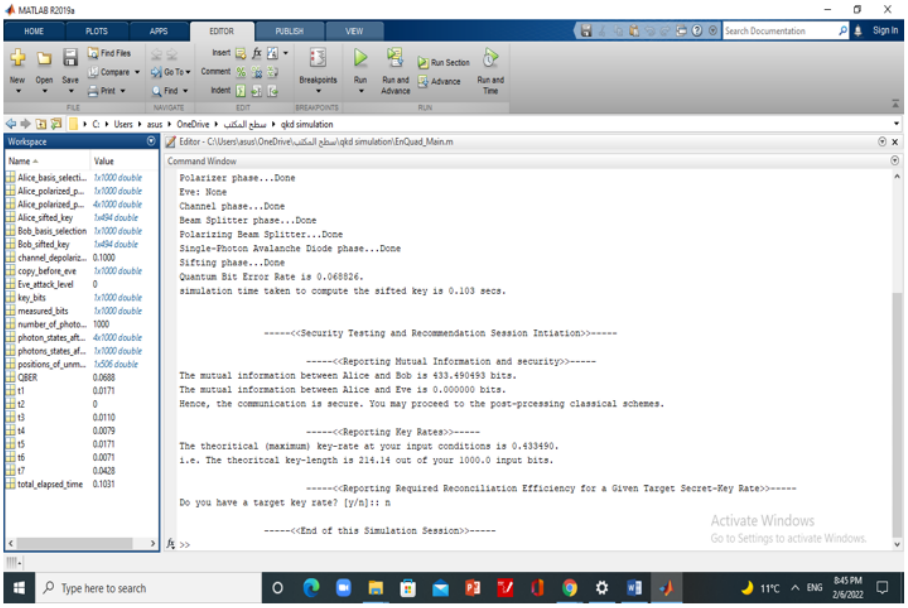


Figure 2: Diagram of BB84 experiment stages by matlab



Name ▲	Value
Alice_basis_selecti...	1x1000 double
Alice_polarized_p...	1x1000 double
Alice_polarized_p...	4x1000 double
Alice_sifted_key	1x494 double
Bob_basis_selection	1x1000 double
Bob_sifted_key	1x494 double
channel_depolariz...	0.1000
copy_before_eve	1x1000 double
Eve_attack_level	0
key_bits	1x1000 double
measured_bits	1x1000 double
number_of_photo...	1000
photon_states_aft...	4x1000 double
photons_states_af...	1x1000 double
positions_of_unm...	1x506 double
QBER	0.0688
t1	0.0171
t2	0
t3	0.0110
t4	0.0079
t5	0.0171
t6	0.0071
t7	0.0428
total_elapsed_time	0.1031

```
Polarizer phase...Done
Eve: None
Channel phase...Done
Beam Splitter phase...Done
Polarizing Beam Splitter...Done
Single-Photon Avalanche Diode phase...Done
Sifting phase...Done
Quantum Bit Error Rate is 0.068826.
simulation time taken to compute the sifted key is 0.103 secs.


          -----<<Security Testing and Recommendation Session Intiation>>-----

                -----<<Reporting Mutual Information and security>>-----
The mutual information between Alice and Bob is 433.490493 bits.
The mutual information between Alice and Eve is 0.000000 bits.
Hence, the communication is secure. You may proceed to the post-prcessing classical schemes.

                -----<<Reporting Key Rates>>-----
The theoritical (maximum) key-rate at your input conditions is 0.433490.
i.e. The theoritcal key-length is 214.14 out of your 1000.0 input bits.

                -----<<Reporting Required Reconciliation Efficiency for a Given Target Secret-Key Rate>>-----
Do you have a target key rate? [y/n]:: n

          -----<<End of this Simulation Session>>-----
>>
```

Figure 3: Screen shoot of matlab program

VI. Quantum Bit Error Rate

QBER is the ratio of errors with keys to provide information about the presence and knowledge of the eavesdropper. When Eve Intercept-Resend occurs, the probability that Bob will change sides is $\varepsilon/4$ [17]. This means that the attack level ε is defined as the pulse ratio over the pulse input when Eve Intercept-Resend occurs. The following equation calculates the total possibility of a bit passing from the source to the detector Bob through Eve if the channel is a binary symmetric (also known as the likelihood of error of the filtered key) [18].

$$\begin{aligned} QBER = qe(1-qch) + (1-qe)qch = \frac{\varepsilon}{4}\left[1-\frac{2p}{3}\right] + \left[1-\frac{\varepsilon}{3}\right] \\ = \frac{\varepsilon}{4} + \frac{2p}{3}(2-\varepsilon) \end{aligned} \tag{1}$$

VII. Testing Security of Quantum Key Distribution

As mentioned previously, when Alice-Bob mutual information I (A; B) surpasses Alice-Eve I (A; E) information, the QKD protocol is secure [19]. As a symmetric source analyzed without memory in alphabets $A = a0, a1 = 0, 1, p(a0) = p(a1) = 1/2$ and its maximum entropy is $H(A) = 1$. In addition, a binary symmetric channel was investigated with conditional probabilities $\rho(a0|a1) = \rho(a1|a0)$ and $\rho(a0|a0) = \rho(a1|a1)$ then the conditional entropies $H(A|B)$ and $H(A|B)$ are equal to $1-h(a)$, where $h(a)$ is the Shannon binary entropy with a transition probability a: $h(a) = -alog2a-(1-a)log2(1-a)$. For Eve attacking Alice, the term $(1/2-qe)$ is defined. In consequence of this, the lower bound protection in Eq. 2 might be reformulated as shown in Eq. 3. QBER is $< (1/2QE)$, where $h(QBER) < h(1/2QE)$ which is real in this case, as long as $QBER \leq 0.5$, and $(1/2QE) \leq 5$. If there is no assault on Eve, the maximum of $(1/2QE)$ is 0.5; QBER may not exceed 0.5 since the p parameter depolarization for available channels is restricted to 0.25 [20].

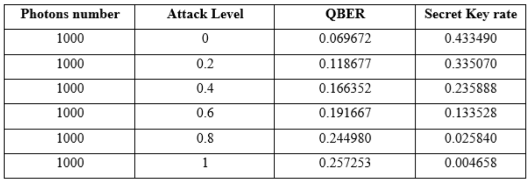
$$S:(1-h(QBER))>(1-h\left[\frac{1}{2}-qe\right]):h(QBER)<h\left[\frac{1}{2}-qe\right],$$
$$QBER<\left[\frac{1}{2}-qe\right]:\left[\frac{\varepsilon}{4}+\frac{2p}{3}(2-\varepsilon)\right]<\left[\frac{1}{2}-\frac{\varepsilon}{4}\right]:p<\frac{4(1-\varepsilon)}{3(2-\varepsilon)} \tag{2}$$

$$(I(A:B))=H(A)-H(A|B)>(I(A;E)=H(A)-H(A;E)) \tag{3}$$

VIII. Results of Experiment

The QBER ratio was calculated by comparing the filtered keys of Alice and Bob in the MATLAB simulation. The depolarization effect of the channel is turned off, and a limit of 1000 photons is set to keep QBER fluctuations to a minimum. As shown in Table I, the attack level was set between 0 and 1 and the number of photons was set at 1000. Eve's assault level was changed from 0 to 1 with a step of 0.2; indicating that Eve did not influence on Alice and Bob's communications. Nevertheless, this number was gradually increased by 0.2 to reach 1 indicating a full attack. The difference between $I(A;B)$ and $I(A;E)$ was the secret-key rate [18]. The number was considered as the Shannon minimum amount of information required by Bob from Alice to correct errors in the decoded bits caused by channel depolarization or eavesdropping. As shown in the chart below, the attack level has a direct impact on the QBER value.

TABLE I
A comparison of photon inputs and intensity of Eve's assault with QBER



Photons number	Attack Level	QBER	Secret Key rate
1000	0	0.069672	0.433490
1000	0.2	0.118677	0.335070
1000	0.4	0.166352	0.235888
1000	0.6	0.191667	0.133528
1000	0.8	0.244980	0.025840
1000	1	0.257253	0.004658

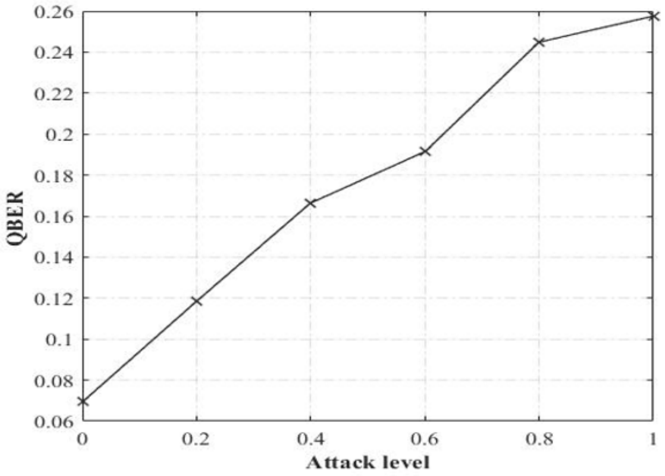


Figure 4: Plotting of QBER at various degrees of eve attack

The mutual information between Alice, Bob, and Eve was estimated after calculating the QBER, followed by security testing and reporting the lowest bound. For all possible combinations of the input settings, the number of photons received as input was set to 1000. ("p and e"). It is feasible to obtain security if "the mutual information between Alice and Bob $I(A;B)$ is greater than the mutual information between Alice and Eve $I(A;E)$." Increasing the attack level by 0.2 increased the mutual information between Alice and Eve while decreasing the mutual information between Alice and Bob, according to Table II. This means that the security target was not reached. As a result, the connection is no longer secure.

TABLE II
Comparison of alice with bob and alice with eve mutual information

Photons number	Attack Level	QBER	Secret Key rate
1000	0	0.069672	0.433490
1000	0.2	0.118677	0.335070
1000	0.4	0.166352	0.235888
1000	0.6	0.191667	0.133528
1000	0.8	0.244980	0.025840
1000	1	0.257253	0.004658

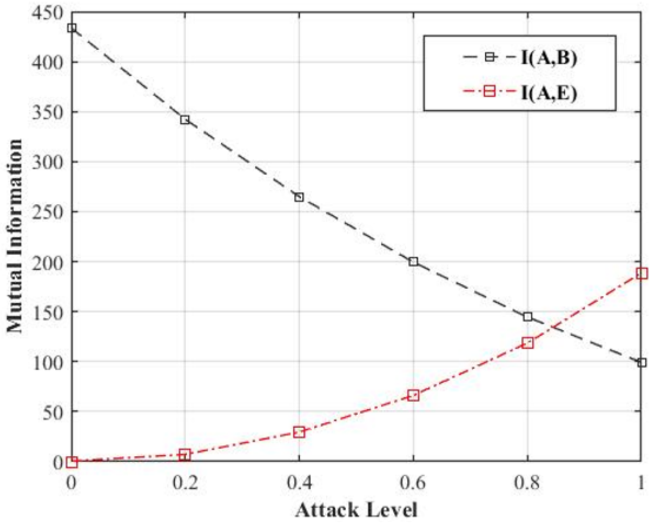


Figure 5: Mutual information between alice with bob and alice with eve various attack level

IX. Conclusion

Quantum cryptography is the most advanced quantum technology accessible today. It is the first fundamental quantum notion to move from theoretical computation to practical application. This paper examines the properties of BB84 and the parameters that affect the security of the protocol. It provides security tests, suggestions on the choice of compromise protocol, and advice on lower/upper bounds of critical parameters such as the depolarization channel parameter, the number of input photons, and the level of Eve attack for the desired secret-key rate. It also provides useful outputs such as QBER, theoretical secret-key rates, the mutual information between Alice and Bob or Alice and Eve, and the estimated number of bits to be leaked in post-processing techniques. The transmission's security was tested when the Eve assault was increased.

References

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Con Tos5" , 1984.
[2] S. Pirandola et al. , "Advances in Quantum Cryptography" , Adv. Opt. photonics, Vol. 12, No. 4, pp. 1012-1236, 2020.
[3] D. Hrg, L. Budin, and M. Golub, "Quantum Cryptography and Security of Information Systems" , in IEEE Proceedings of the 15th Conference on Information and Intelligent System, pp. 63-70, 2004.
[4] N. Papanikolaou, "An Introduction to Quantum Cryptography" , XRDS Crossroads, ACM Mag. Students, Vol. 11, No. 3, p. 3, 2005.
[5] E. C. Vagenas, A. Farag Ali, and H. Alshal, "GUP and The No-Cloning Theorem" , Eur. Phys. J. C, Vol. 79, No. 3, pp. 1-5, 2019.
[6] Arash Atashpendar, "Simulation and Analysis of QKD (BB84) " , Interdisciplinary Center for Security, University of Luxembourg,. https://www.qkdsimulator.com/.
[7] H. Qiao and X. Chen, "Simulation of BB84 Quantum Key Distribution in Depolarizing Channel" , 2009.
[8] M. Kalra and R. C. Poonia, "Simulation of BB84 and Proposed Protocol for Quantum Key Distribution" , J. Stat. Manag. Syst. , Vol. 21, No. 4, pp. 661-666, 2018.
[9] M. Dehmani, E. M. Salmani, H. Ez-Zahraouy, and A. Benyoussef, "BB84 with Both Several Cloning and Intercept-Resend Attacks" , Int. J. Electr. Comput. Eng. , Vol. 8, 2018.
[10] E. O. Kiktenko et al. , "Lightweight Authentication for Quantum Key Distribution" , IEEE Trans. Inf. Theory, 2020.
[11] W. Tittel, G. Ribordy, and N. Gisin, "Quantum Cryptography" , Phys. World, Vol. 11, No. 3, p. 41, 1998.
[12] D. Brub, "Optimal Eavesdropping in Quantum Cryptography with Six States" , Phys. Rev. Lett. , Vol. 81, No. 14, p. 3018, 1998.
[13] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem" , Phys. Rev. Lett. , Vol. 67, No. 6, p. 661, 1991.
[14] F. M. Spedalieri, "Quantum Key Distribution without Reference Frame Alignment: Exploiting Photon Orbital Angular Momentum" , Opt. Commun. , Vol. 260, No. 1, pp. 340-346, 2006.
[15] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum Key Distribution Using Qaussian-Modulated Coherent States" , Nature, Vol. 421, No. 6920, pp. 238-241, 2003.
[16] K. Inoue and Y. Iwai, "Differential-Quadrature-Phase-Shift Quantum Key Distribution" , Phys. Rev. A, Vol. 79, No. 2, p. 22319, 2009.
[17] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust Against Photon Number Splitting Attacks for Weak laser Pulse Implementations" , Phys. Rev. Lett. , Vol. 92, No. 5, p. 57901, 2004.
[18] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography" , Rev. Mod. Phys. , Vol. 74, No. 1, p. 145, 2002.
[19] A. Niederberger, V. Scarani, and N. Gisin, "Photon-Number-Splitting Versus Cloning Attacks in Practical Implementations of The Bennett-Brassard 1984 Protocol for Quantum Cryptography" , Phys. Rev. A, Vol. 71, No. 4, p. 42316, 2005.
[20] G. Smith and J. A. Smolin, "Additive Extensions of A Quantum Channel" , in 2008 IEEE Information Theory Workshop, ITW, pp. 368-372, 2008, doi: 10.1109/ITW.2008.4578688.
[21] L. Hanschke et al. , "Quantum Dot Single-Photon Sources with Ultra-Low Multi-Photon Probability" , NPJ Quantum Inf. , Vol. 4, No. 1, pp. 1-6, 2018.
[22] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum Random Number Generators" , Rev. Mod. Phys. , Vol. 89, No. 1, p. 15004, 2017.
[23] Z. Cao, H. Zhou, X. Yuan, and X. Ma, "Source-Independent Quantum Random Number Generation" , Phys. Rev. X, Vol. 6, No. 1, p. 11020, 2016.