Semiconductor Physics, Quantum Electronics & Optoelectronics, 2018. V. 21, N 1. P. 73-79.

Optoelectronics and optoelectronic devices

Influence of experimental parameters inherent to optical fibers on Quantum Key Distribution, the protocol BB84

L. Bouchoucha[1], S. Berrah[1], M. Sellami[2]

[1]*Department of Electrical Engineering, LMER laboratory, Faculty of Technology*
Abd Rahman MIRA University of Bejaia, Algeria
E-mail: bouchouchalydia.bl@gmail.com, Sm.berrah@gmail.com

[2]*Center university of Tamnrasset, Algeria*
E-mail: sellami_mohammed@yahoo.fr

Abstract. In this work, we represent the principle of quantum cryptography (QC) that is based on fundamental laws of quantum physics. QC or Quantum Key Distribution (QKD) uses various protocols to exchange a secret key between two communicating parties. This research paper focuses and examines the quantum key distribution by using the protocol BB84 in the case of encoding on the single-photon polarization and shows the influence of optical components parameters on the quantum key distribution. We also introduce Quantum Bit Error Rate (QBER) to better interpret our results and show its relationship with the intrusion of the eavesdropper called Eve on the optical channel to exploit these vulnerabilities.

Keywords: cryptography, quantum key distribution, BB84 protocol, Qbit, quantum bit error rate.

doi: https://doi.org/10.15407/spqeo21.01.073
PACS

Manuscript received 04.01.18; revised version received 22.02.18; accepted for publication 29.03.18; published online 29.03.18.

1. Introduction

Quantum cryptography is a solution to the weaknesses and flaws of classical cryptography that is based on digital signature, the electronic certificate and the classical cryptographic protocols (DES, RSA ...) [1] in the security of the secret key exchanged between two communicating parties.

Quantum Cryptography called Quantum Key Distribution (QKD) [1-3] converges to use the fundamental laws of quantum physics to guarantee the security of the exchanged key [2]. The QKD allows Alice and Bob to exchange a key by using two communication channels: the first is the quantum channel that can be the optical fiber or free space, and the second is the classical channel that is the public channel that can be Internet or a telephone line [2-4].

In the view of quantum cryptography, there are two types of Quantum Key Distribution, the first type is "prepare and measure" [2]. The protocol BB84 was published by Bennett and Brassard, it is the first protocol that has been operating in the first type of QKD, where Alice sends photons in four possible states by using two different polarization bases [5]. Then, there was an improvement of this protocol through polarization of photons in two non-orthogonal states using the protocol B92 [2, 6, 7]. Security of single photon with this protocol was proved by Tamaki *et al*. [8]. Then, another protocol was proposed by Pasquinucci and Gisin, which consists in adding another polarization base forming a protocol with six polarization states [5, 8-10]. The second type constituted a new approach of QKD by using quantum teleportation that is based on the quantum entanglement (calibration), when Ekret proposed the first protocol based on Bell's theorem, called the protocol E91 [2, 5, 11].

In our study, we focus on the first type of QKD, specifically BB84 protocol in the case of coding on the single-photon polarization [2, 12]. This distribution is influenced by intrusion of malicious hackers who exploit any loopholes that would allow them to be undetectable and unnoticed by Alice and Bob. These flaws are related to the influence of physical parameters of optical components that can be the optical channel (the optical fiber), single-photon source or photodetectors. The quantum bit error rate (QBER) is influenced by these parameters, that's why it will be the main landmark to interpret our results; it is that adds to its influence on mutual information between communicating parties.

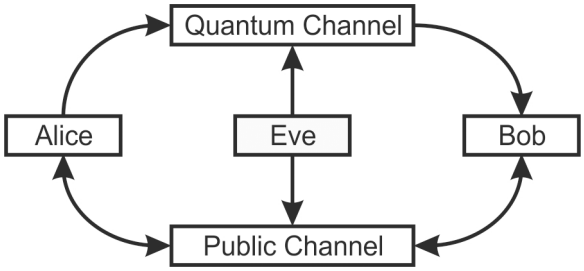

Fig. 1. Quantum cryptography communication.

2. BB84 protocol

The first quantum key distribution protocol was elaborated by Bennett and Brassard [6], when a secret key was exchanged between two users Alice and Bob by using a quantum channel (the optical fiber or free space) and a classical channel, it is presented in Fig. 1.

The fundamental concept of this protocol is that Alice randomly selects a series of Qbits, then she sends them into a quantum channel in the form of photon to Bob in order to create a secret key. It will be encoding either on its polarization or phase [1, 3].

In the case of encoding on the polarization of single photon, BB84 protocol uses two polarization bases: the linear base and the diagonal one [2-4], to represent the four polarization states.

Fig. 2 shows that Qbit |0> is represented in the linear basis by a horizontal polarization state (0°) and in a diagonal basis – by a diagonal polarization (45°), but the Qbit |1> is represented in the linear basis by the horizontal polarization state (90°) and in a diagonal basis – by an anti-diagonal polarization. *i.e.* (135°).

The procedure of BB84 protocol is done according to the following steps [3, 4, 6]: the first step, Alice sends single photons into the optical channel according to the four polarization states. Using randomly two polarizers, the first polarizer allows representation of the vertical state (90°) or horizontal state (0°) on the linear base, and the second polarizer allows representing the diagonal state (45°) or anti-diagonal state (135°) on the diagonal basis. At the reception, Bob has two analyzers. These randomly select the base on which they will measure the state of photon received with 50% probability of choosing the right polarization.

The second step, after having exchanged photons constituting the sequence of Qbits sent by Alice. Bob has to sacrifice a large number of photons received by sending the bases chosen for measurements of polarization states on the public channel in order to compare with those chosen by Alice. The latter announces the results of comparison in three posts: no correspondence between bases, 50% correspondence, correspondence with the personal key [2].

In the third step, if there is a correspondence between the bases chosen between Alice and Bob; and there is not the intrusion of an eavesdropper Eve. So, they randomly select the secret key to share between them and send it on the public channel. BB84 protocol allows sharing a series of strongly correlated Qbits constituting the secret key [3]. In this case, it is checked if the distribution system is technologically perfect (components without loss) the keys of Alice and Bob are identical in the absence of any intervention of Eve.

A. The protocol BB84 without the presence of an eavesdropper

Ideally, BB84 protocol is perfectly secure [4], its implementation in practice is not easy because there are some effects of attenuation and noise in the quantum channel. In the case of the optical fiber, there are attenuation of the channel due to the Rayleigh effect, the effect of the dark count due to the photodetector and the single photon source. The noise and attenuation reduce the channel efficiency, and they affect the transmission distance and the rate of exchange photons.

1) The influence of the source

BB84 protocol requires the use of single photon sources [3, 4, 12] that allow for an optical pulse comprising single photon. It is for this fact use of laser sources strongly attenuated and obeys the Poisson distribution ($\mu = 0.1$) [14]:

$$p(n,\mu)=\frac{\mu^n \cdot e^{-\mu}}{n!}, \quad (1)$$

n and μ are a number of photons and a number of photons per pulse, respectively.

2) The influence of quantum channel

During transmission of photons, the latter are exposed to different effects, namely: effects of absorption, diffraction and attenuation per unit length due to the Rayleigh scattering [15]. These interactions and losses in the optical channel have a significant and major influence on the probability to detect photons emitted by Alice and received by Bob, because they modified their properties (polarization and phase). The used quantum channel is the single-mode optical fiber. The losses in this type of fibers in the case of the 1550 nm telecom window reach $\alpha = 0.22$ dB/km [3, 5]. The quantum efficiency of the fiber may thus be defined as follows:

$$\eta_{fiber}=10^{-\frac{\alpha L}{10}}, \quad (2)$$

where L is the length of optical fiber.

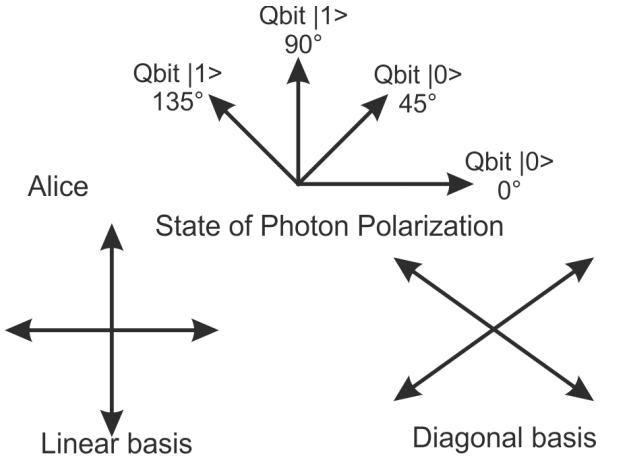

Fig. 2. Polarization basis of the protocol BB84.

We deduced that the total transfer efficiency between Alice and the photodetector is related with the linear losses in the fiber and those in Bob's detector.

$$\eta_{total} = 10^{-\frac{\alpha L + \alpha_{Bob}}{10}}. \quad (3)$$

3) The influence of photodetector

As the power of detected photon is very even lower intrinsic to a photodiode (APD) that according to the counter mode allows detection of single photons. The major drawback of this type of photodetector is the effect of dark count, which introduces an error in the detection system. The probability of having the stroke of darkness per second is related with the detection time window $\Delta\tau$:

$$P_{dark} = n \cdot \Delta\tau. \quad (4)$$

3. Quantum bit error rate

QBER is defined as the ratio between the number of bit errors to the total number of bits detected by Bob:

$$QBER = \frac{N_{erroneous}}{N_{key} + N_{erroneous}}, \quad (5)$$

$$QBER = QBER_{opt} + QBER_{det}. \quad (6)$$

$QBER_{opt}$: It determines the error fraction in donation polarization or phase of photon committed by detector. Generally, P_{opt} is lower than 1% [3] and can be easily realized with any instalation; so the $QBER_{opt}$ may be neglected.

$QBER_{det}$: It depends on the probability of darkness rate and the probability of photon detection.

It is concluded that there are three factors that influence on QBER: dark count of the detector, the length of the transmission fiber and quantum efficiency of the detector.

So, we have:

$$QBER = QBER_{det} = \frac{n_{dark} \cdot \Delta\tau}{\mu \cdot \eta_{total} \cdot \eta_d}. \quad (7)$$

BB84 protocol with the presence of an eavesdropper

In this part, we are interested in the event when a spy (called Eve) intercepts the emitted photons in the quantum channel. Knowing that Eve leads a passive attack that is of the type to intercept and resend [4].

Eve randomly measures the states of photons intercepted by the analyzer according to the two bases. If Eve chooses the same polarization basis as Alice to measure the state of photon, so she returned it to the channel on the same basis, and Alice and Bob could not detect the intrusion of Eve. Then, the Qbit sent by Alice is received by Bob, but the eavesdropper Eve rubbed off some information from the key exchange between Alice and Bob. But if Eve chooses a different basis as Alice, it could be a 50% probability of choosing the right base. Then, it returns the photon to Bob according to the base where it makes its measurement.

At the reception, it measures the state of the photon randomly with the 50% probability of selecting the same basis as Alice; otherwise, it receives taint photons; so, the presence of Eve will be detected. After having sent the photon series on the quantum channel, Bob sent to Alice the polarization bases, in which he performed measurements on the classical channel. Alice, in turn, consults her given basis in what she recorded the polarization bases chosen to measure states of the emitted photons. Then, she meets three criteria as seen in the first case. Despite the step of reconciliation bases between Alice and Bob; Eve knows each polarization state used, so there may be a certain amount of information on the key exchange. The flow of the algorithm of key reconciliation was better explained and detailed by Omar and Anas in [1], where they defined the different phases of reconciliation from the raw key until the amplification of confidentiality and collection of the final key.

4. The relationship between the theory of information and QBER

The mutual information measures the security achieved between the parties on a system or between Alice and Bob, Alice and Eve and between Eve and Bob. If Eve is absent on the channel, we designate the mutual information between Alice and Bob by I_{AB}. On the other hand, if Eve is present on the channel, then she cuts the amount of information that Alice sent. It will be designated by the mutual information between Alice and Eve as I_{AE}. According to these equations, the condition of the central theorem can be applied, which is checked only if the information quantity exchanged between Alice and Bob is higher than that Eve has intercepted.

$$I_{AB} > I_{AE}. \quad (8)$$

We know that the quantum channel and the equipment have an error rate, which is expressed by QBER. The latter also has an influence on the amount of information exchanged for sharing the secret key. So, we can express mutual information based on previous QBER as follows where f is the pulse fraction of photons [3]:

$$I_{AB} = 1 + QBER \cdot \log_2(QBER) + \\ + (1 - QBER) \cdot \log_2(1 - QBER), \quad (9)$$

$$I_{AE} = \frac{4QBER}{\sqrt{2}} + \frac{1}{f + \frac{\mu}{2}}\left(\frac{\mu}{2} + \frac{f}{\sqrt{2}}\right). \quad (10)$$

From the condition $I_{AB} = I_{AE}$, we will bring $QBER = 15\%$. So, according to the central theorem, communication is a secured and the system can create a key to a value of a lower $QBER < 15\%$. Beyond this threshold, communication is not secure, and reconciliation is abandoned, because Eve intercepts more information than detained by Bob.

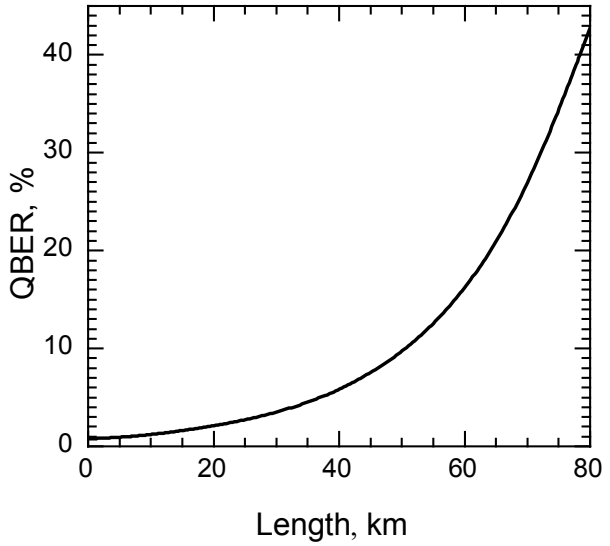

Fig. 3. Evolution of QBER based on variations of the fiber length within the range 1 up to 80 km.

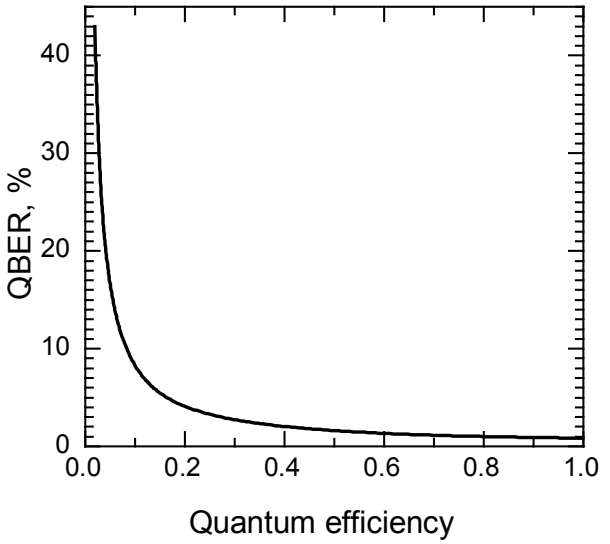

Fig. 4. Evolution of QBER based on variations of the detector quantum efficiency.

5. Simulation and results

Simulation of BB84 protocol by using Matlab offers the opportunity to perform a study on the influence of physical parameters on quantum key distribution and the impact of the spy on safety with this protocol.

Table represents the values of the physical parameters of the optical components necessary to implement this simulation.

Table. The physical parameters used in industry in the case of telecom window 1550 nm.

Number of photons per pulse (μ)	0.1
Losses in the fiber (dB/km)	0.22
Dark count rate (counts/s)	60
Time window (μs)	2
Detector efficiency (dB)	0.2

Fig. 3 shows the influence of variations of the optical fiber length on the rate QBER. It is obtained for variations in the optical fiber length within the range 1 to 80 km for the telecom wavelength 1550 nm, which fiber possesses the linear losses of 0.22 dB/km.

According to the curve, it is clear that the error rate increases with increasing the length of the optical fiber, and quality of the link decreases. Knowing that according to the central theorem; the maximum threshold for secure communication is performed to a value of less than 15% of QBER.

In this case, we note that the safety distance is achieved for the minimum value of 58 km; beyond this distance the security is breached. It is known that the linear losses are also related to changes in the length of the fiber, which plays an important role in the error rate on QBER.

As shown in Fig. 4, variations of the quantum efficiency also have their influence on QBER. It is clear that QBER decreases with increasing the η parameter, since quality of the optical connection is improved with increasing the latter. We also note that the value $\eta = 0.05$ ensures secure connection given that QBER is less than the threshold 15%.

The study carried out in this part confirms that Eve can exploit loopholes due to physical parameters to intercept the photons carrying the Qbit and be undetectable by Alice and Bob.

Fig. 5 shows evolution of mutual information between Alice and Bob and between Alice and Eve based on QBER. We find that Eve did not intercept the photons sent by Alice, and it may chance to deduct the photon polarization states, if the QBER threshold is less than 15%. According to the central communication theorem, it

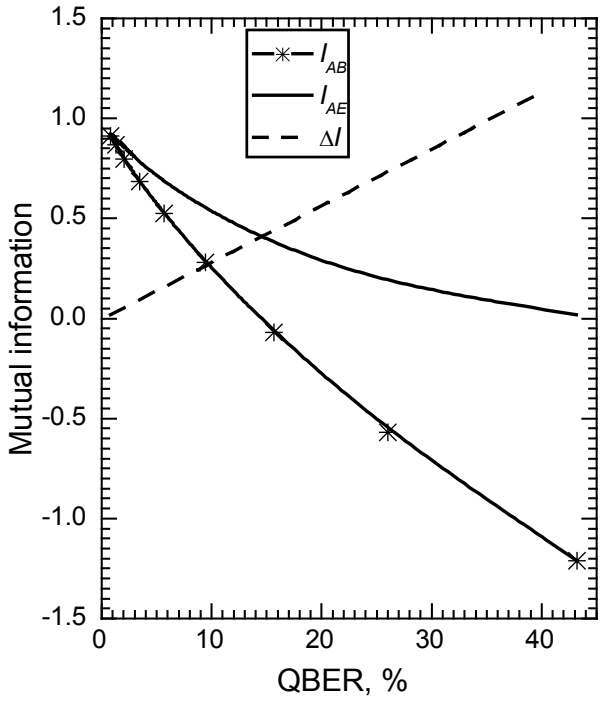

Fig. 5. Mutual information as a function of QBER variations.

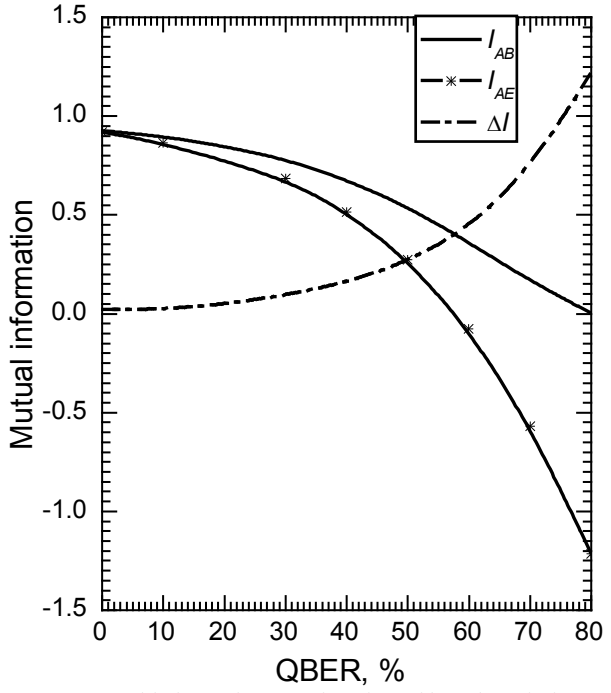

Fig. 6. Mutual information as a function of length variations.

is secure only if $IAB > IAE$. So, Alice and Bob are able to develop a secret key. On the other hand, from the threshold where QBER is above 15%, Eve will have more information than Bob has received, and the key will be abandoned. In this case, there will be $IAB < IAE$.

Visualizing Fig. 6 shows the influence of the optical fiber length on mutual information. We note that the distance, for which Eve will be able to capture more information, is 58 km. That meets the threshold required by QBER 15%. So, it confirms the results obtained in the latter section.

Fig. 7 allows us to visualize and monitor QBER based on variations of the fiber length (Fig. 7a), the quantum efficiency (Fig. 7b) and mutual information (Fig. 7c), this by taking the detector efficiency $\eta_{Bob} = 0.02$ and $P_{dark} = 10^{-5}$ (the value of probability of dark counts) [3]. We established that the safety distance is superior to that we obtained with our experimental parameters 66 km. However, the threshold limit by QBER for quantum efficiency is lower, and it is approximately 0.035. It is less as compared to the results achieved by us and affects quality of transmission.

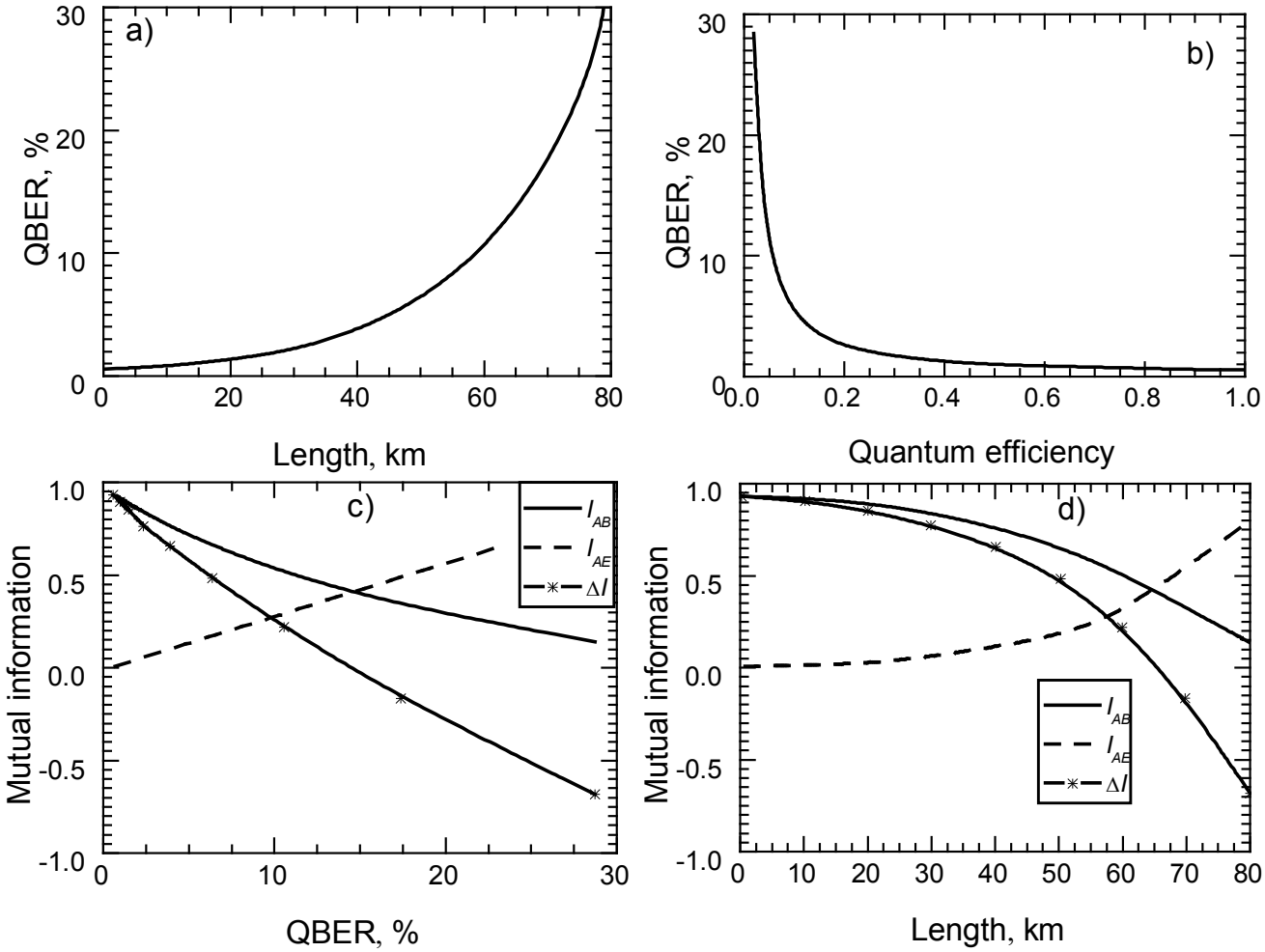

Fig. 7. (a) Evolution of QBER based on variations of the fiber length within the range 1 up to 80 km. (b) Evolution of QBER based on variations of the detector quantum efficiency. (c) Mutual information as a function of QBER variations. (d) Mutual information as a function of length variations. $\eta_{Bob} = 0.02$, $P_{dark} = 10^{-5}$.

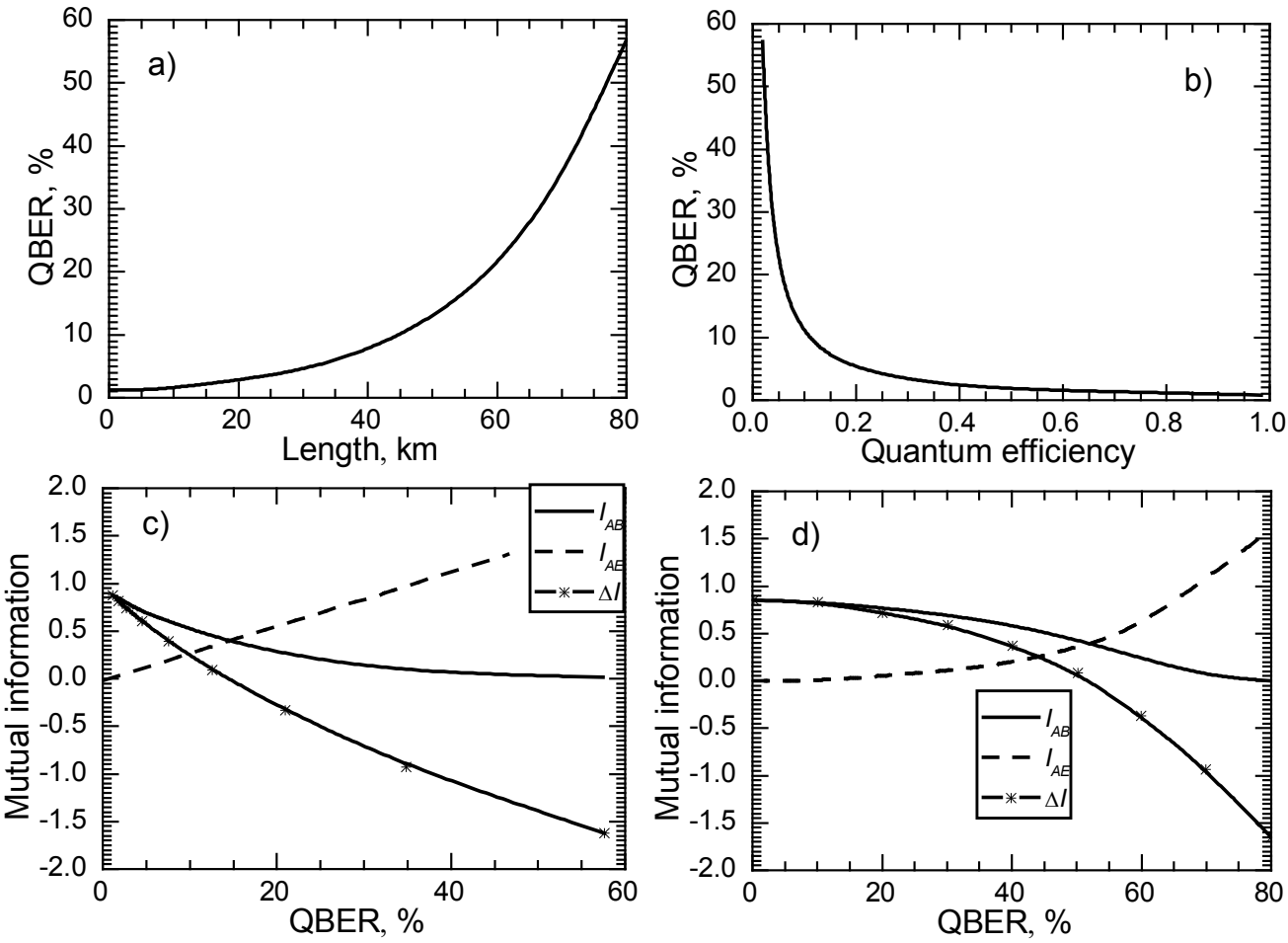

Fig. 8. (a) Evolution of QBER based on variations of the fiber length within the range 1 up to 80 km. (b) Evolution of QBER based on variations of the detector quantum efficiency. (c) Mutual information as a function of QBER variations. (d) Mutual information as a function of length variations. $\eta_{Bob} = 0.01$, $P_{dark} = 10^{-5}$.

Fig. 8 allows us to visualize and monitor QBER based on variations of the fiber length (Fig. 8a), the quantum efficiency (Fig. 8b) and mutual information (Fig. 8c) by taking the detector efficiency $\eta_{Bob} = 0.01$ and $P_{dark} = 10^{-5}$ (the value of probability of dark counts) [9]. It shows that the safety limit distance for threshold QBER = 15% is less than the two previous results. However, achieving quantum efficiency for this threshold is 0.07 superior as compared to the results achieved, and quality of transmission will be improved, but attenuation and losses due to the optical fiber will influence transmission of the key.

From these three comparisons, one can find that the optical fiber length affects the photodetector, and this reflects on the safety distance, and therefore, on evolution of QBER.

6. Conclusion

The protocol BB84 is a required solution to quantum key distribution and remedying the intentional attacks of the eavesdropper.

This paper focuses on the influence of the physical parameters of optical components on the key distribution protocol. If these physical parameters allow Eve to recover a certain amount of information on the exchanged key, this is the fault of the protocol. As shown by the results obtained from simulation, the length of the optical fiber used and the quantum efficiency of the photodetector have a great influence on the amount of information exchanged between the communicating parties and, thus, on the shared key. It was visualized by variations of QBER and its influence on these parameters. Therefore, we fixed the lower QBER threshold at the level 15%; it allows us to have a secure communication and exchange of secure key, but the threshold beyond the exchange will not secure, and the key will be abandoned.

References

1. Omer A.J. and Anas A. The goals of parity bits in quantum key distribution system. *Intern. J. Comput. Applications*. 2012. **56**, No.18. P. 1–9.
2. Elampari K. and Ramakrishnan K. Study of BB84 protocol using QKD simulator. *Intern. J. Eng. Sci. Invent. Res. Development*. 2015. Vol. I, Issue XI; www.ijesird.com.

3. Zbinden H., Bechmann H., Gisin N. and Ribordy G. Quantum cryptography. *Appl. Phys. B*. 1998. **67**. P. 743–748.
4. Benletaief N., Rezig H., and Bouallegue A. Reconciliation for Practical Quantum Key Distribution with BB84 Protocol. *Mediterranean Microwave Symposium* (MMS), September 2011, DOI: 10.1109/MMS.2011.6068566.
5. Bennett C. and Brassard G. Quantum cryptography, Public key distribution and coin tossing. *Proc. Int. Conf. Comp. Syst. and Signal Proc.,* Bangalore, 1984. P. 175.
6. Hitesh S., Gupta D.L. and Singh A.K. Quantum key distribution protocols: a review. IOSR *J. Comput. Eng*. 2014. **16**, Issue 2, Ver. XI. P. 01–09.
7. Bennett C. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* 1992. **68**, No. 21. P. 3121–3124.
8. Tamaki K., Koashi M., and Imoto N. *Phys. Rev. Lett.* 2003. **90**. P. 167904.
9. Gisin N. and Bruss D. Talk presented at the workshop on Quantum Computation. Torino. *Phys. Rev. Lett.* 1998. **81**.
10. Bechmann H. and Gisin N. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. Lett.* 1999. **A59**. P. 4238–4248.
11. Artur E. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* 1991. **67**. P. 661–663.
12. Musharraf M. and Ishtiaq K. Protocols for secure quantum transmission: A review of recent developments. *Pakistan Journal of Information and Technology*. 2003. **2**. P. 265–276.

Authors and CV

Lydia BOUCHOUCHA: was born in 1991, she received the master degrees from university of Bejaia, in 2015, Algeria, currently, she is a PhD student at the university of Bejaia, Algeria, in the quantum cryptography subject.

Department of Electrical Engineering
LMER laboratory,Faculty of Technology
University of Bejaia, Algeria
E-mail: bouchouchalydia.bl@gmail.com

Smail BERRAH received his PhD of Sciences from the university of Sidi bel Abbes in 2006. He is currently a research professor in the Electrical Engineering Department at the University of Bejaia, Algeria. His research interests include microelectronics, optical link telecommunication and security.

Department of Electrical Engineering
LMER laboratory,Faculty of Technology
University of Bejaia, Algeria
E-mail: sm.berrah@gmail.com

Mohammed SELLAMI was born in 1967, he received his PhD degrees of sciences from the university of Constantine, Algeria, in 2008 currently. He is a research professor in the university center of Tamanrasset, Algeria. His research interests are computing and electrical engineering.

Center university of Tamnrasset, Algeria
E-mail: sellami_mohammed@yahoo.fr