SIDaC'19

Under the auspices of Prof. DIBI Zohir
Rector of the University Larbi Ben M'hidi
Oum El Bouaghi, Algeria.

QUANTUM KEY DISTRIBUTION PROTOCOLs IN OPTICAL LINKS

*L. Bouchoucha, S. Berrah , M. Sellami**

Laboratoire de Maitrise des Énergies renouvelables (LMER) , Faculty of Technology, University of Bejaia , 6000 Bejaia, Algeria

* Center university of Tamanrasset, Algeria

ABSTRACT

The object of this article is to study the principles of quantum cryptography in the optical channel in order to compare the distribution protocols of single-photon quantum keys, in particular the BB84 protocol, theB92 protocol ,and the continuous variable protocols (direct and inverse); according to different criteria, such as the transmission distance of the key, the data rate and the amount of information intercepted by the spy on the quantum channel.

1. INTRODUCTION

The quantum cryptography called Quantum Key Distribution (QKD) converges towards the use of the fundamental laws of quantum physics and the laws of information theory to guarantee the security of the secret key exchanged . We first focus on the first type of QKD, in particular the BB84 protocol and the B92 protocol. Secondly, a simulation of direct and inverse continuous variable protocols will be carried out in order to estimate the characteristics of the optical channel (losses and noise) and to evaluate the information exchanged and intercepted by the intruder Eve [1-5].

2. THE BB84 PROTOCOL

The first quantum key distribution protocol was developed by Bennett and Brassard in which a secret key is constructed either by coding on the polarization of the photons or on their phase, which will be exchanged between two users Alice and Bob.

Bit	Base B_+		Base B_X	
	Qbit	State	Qbit	State
0	$\|0>$	$\|\rightarrow>$	$\|0_X>=\frac{1}{\sqrt{2}}(\|0>+\|1>)$	$\|\nearrow>$
1	$\|1>$	$\|\uparrow>$	$\|1_X>=\frac{1}{\sqrt{2}}(\|0>-\|1>)$	$\|\nwarrow>$

Table 1. The polarization states of Qbits

Simulation de l'influence des paramètres physique des composants optiques sur le protocole BB84

The simulation of the BB84 protocol under the Matlab programming environment offers the opportunity to study the influence of the physical parameters of optical components on the quantum key distribution protocol and the impact of Eve on its security.

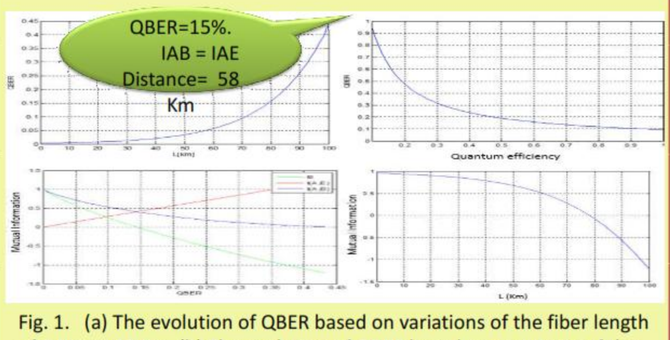

Fig. 1. (a) The evolution of QBER based on variations of the fiber length of 1 Km to 80 Km. (b) The evolution of QBER based on variations of the quantum efficiency of the detector. (c) Mutual information as function of the QBER variations. (d) Mutual information as function of the length variations

3. B92 PROTOCOL

The B92 protocol uses the photon phase to encode bits 0 and 1 on two non-orthogonal states of two conjugate bases.

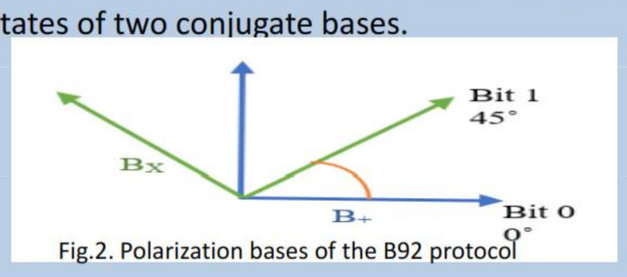

Fig.2. Polarization bases of the B92 protocol

Simulation of the BB92 protocol

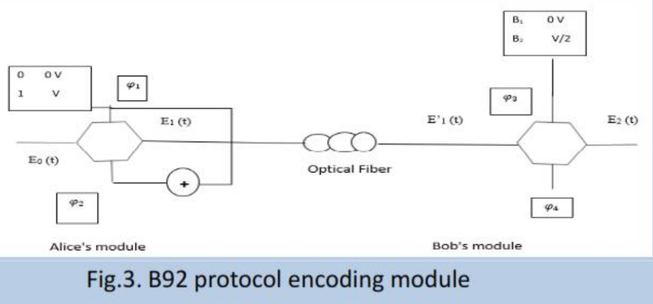

Fig.3. B92 protocol encoding module

The simulation of the B92 protocol is carried out under the MATLAB programming software and the experimental parameters

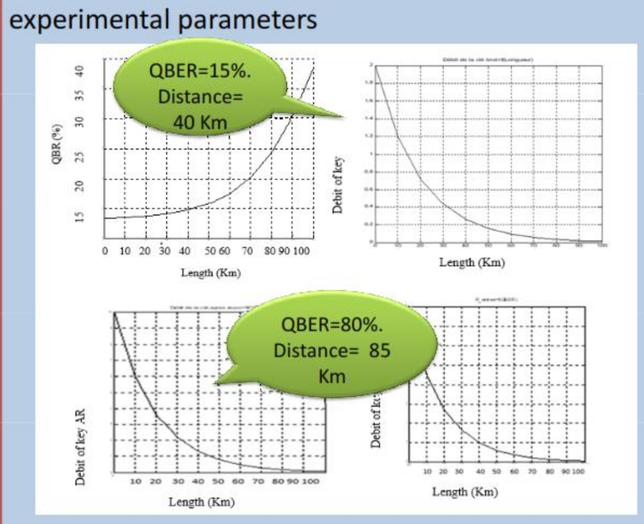

Fig.4. The evolution of QBER based on variations of the fiber length of 1 Km to 100 Km. (b) The evolution the debit of key based on variations of length of fiber . (c) The evolution the debit of key AR based on variations of length of fiber (d) The evolution the debit of key AR based on variations of length of fiber with new contrast

4. COUNTINUS VARIABLES PROTOCOLS

The continuous variables protocol is based on the measurement of the quadratures of the quantum states either on the compressed states which is the homodyne detection or on the coherent states which is defined by the heterodyne detection.

The procedure of these protocols, as follows:

- Alice draws two random numbers xA and pA of a Gaussian law and a variance VA.N0. It then sends Bob the coherent state | xA + i pA> through a quantum channel.
- Bob chooses at random to measure a quadrature either X or P and informs Alice of his choice of quadrature via a public channel.
- Alice and Bob compare the corresponding data (as in BB84), they can then estimate the characteristics of the transmission channel (losses and noise) and then evaluate the information exchanged and intercepted by Eve.
- For the reconciliation step, two choices are possible. If Alice's data serves as a basis for the development of the key, that is, Bob corrects his mistakes to find Alice's values, reconciliation is said to be direct; If it is the data of Bob which serve as reference, it is called inverse.

Simulation of the QKD-CV protocol

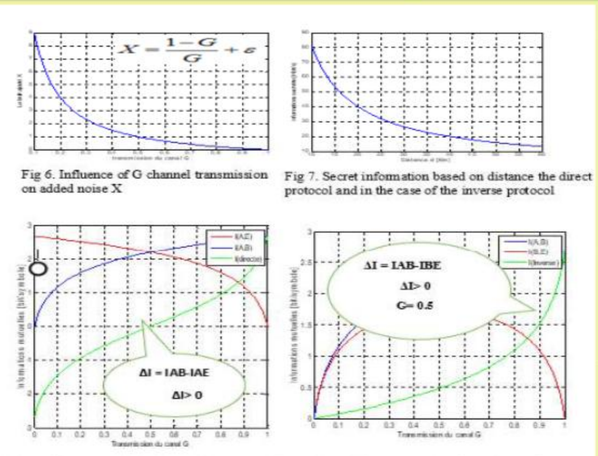

Fig 6. Influence of G channel transmission on added noise X

Fig 7. Secret information based on distance the direct protocol and in the case of the inverse protocol

Fig 8. The mutual information as a function of the transmission of the G-channel, (a) in the case of the direct protocol and (b) in the case of the inverse protocol

5. CONCLUSIONS

As a result, we have limited ourselves to the threshold of QBER = 15%, which allowed a transmission of a key using the BB84 protocol at a distance of 58 km and for a low rate.

On the other hand, the results obtained by the continuous variables are more efficient, precisely the inverse protocol, a makes it possible to construct a secret key that ensures optimal security. Where the bit rate of the secret key is considerable is of the order of Kbit/s at a distance that exceeds 62 km.

REFERENCES

1. A.J. Omer and A.Anas, The Goals of Parity Bits in Quantum Key Distribution System, International Journal of Computer Applications, Volume 56, No.18, October 2012.
2. K. Elampari and K. Ramakrishan, Study of BB84 protocol using QKD simulator,International, Journal of Engineering Science Invention Research Development; Vol,www.ijesird.com e-ISSN: 2349-6185,May 2015.
3. H. Zbinden, H. Bechmann , N. Gisin N and G. Ribordy ,Quantum cryptography, Appl.Phys,B 67, 1998.
[4] Raùl Garcıa, Patron and Nicolas J. Cerf1, Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels, Physical review letters, PRL 102, 130501, 2009.
5. Frédéric Grosshans et all,Quantum key distribution using gaussian modulated coherent states, letters to nature, VOL 421, 2003.

Contact Information

L. Bouchoucha

Laboratoire de Maitrise des Énergies renouvelables (LMER) , Faculty of Technology, University of Bejaia , 6000 Bejaia, Algeria

Tel: 0796847490

Email:bouchouchalydia.bl@gmail.com