Annals of the Academy of Romanian Scientists
Series on Science and Technology of Information
ISSN 2066-8562 Volume **5**, Number **1**/**2012**

APPLICATIONS OF QUANTUM CRYPTOLOGY FOR DATA TRANSMISSIONS IMPLEMENTED IN A STUDENT LABORATORY

Bogdan-Adrian STEFANESCU[1], Dan ANGHEL[1], Octavian DANILA[1], Paul STERIAN[1], Andreea Rodica STERIAN[1]

Abstract. *Quantum cryptography based on the BB84 protocol is discussed in the following presentation, containing the concepts and the work that has been carried out in the field, with some developments suitable for student research. Although it has not been implemented on a commercial level, data transmissions based on quantum cryptology is a good alternative for integration in optical fibers communications, with a wide range of applications due to its' securing capabilities. Evolution in photon-study related fields, such as photon echo, contribute to the better understanding and further improvement of the quantum key distribution protocol. An efficient way of encrypting the information is by the use of a key. As it is well known, the encryption key uses very complex algorithms that are very hard to break but the problem of key transmission between the transmitter and receiver still remains. On a classical channel, the answer was given in the form of RSA public keys that were sent between the transmitter and receiver several times, and implied the use of randomizing algorithms by use of prime numbers. Quantum approach of this problem can be solved through the following principle: If a quantum system that resides in a defined state is observed, thus measured, the state of that system is irreparably changed. This has a direct application in detecting whether an eavesdropper has entered the quantum channel or not. A student-oriented experimental apparatus is presented, together with a virtual simulation of the protocol that implements the principles of quantum cryptography. Our optical channel can be improved using the photon echo effect. Excitement of superradiant states by irradiating a probe with a coherent optical impulse, with its duration and intensity conveniently chosen can be shown with the photon echo. We demonstrated that the photon echo can improve the code by adding either a controlled error on the channel or transforming the channel from a binary channel to a ternary channel.*

Keywords: Quantum cryptology, Data transmission, superradiant states, ternary channel

1. Introduction

The goal of this paper is to help students understand the application of quantum physics in information security.

Why is information security so important? In present days, a lot of information is exchanged via large networks, such as a LAN or the Internet [1-3, 11]. If sensitive information is exchanged, a way of guarding the information from unwanted eavesdroppers is needed [4-6]. A quite simple way of doing this is by encrypting

[1]Academic Center for Optical Engineering and Photonics, Faculty of Applied Sciences, University "Politehnica" Bucharest, Romania (sterian@physics.pub.ro).