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).

the information. An efficient way of encrypting the information is by the use of a key. The encryption key uses very complex algorithms that are very hard to break, but there is another problem: How does the sender send the key to the receiver? In early days, the key was transported to the receiver via physical medium such as paper, punch card, floppy disk, EEPROM or CDROM. There was no insurance of the interception of the key.

On a classical channel, used in the 1970-s, the answer was given in the form of RSA public keys[5], 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 or not an eavesdropper has entered the quantum channel.

2. Quantum Cryptography

Quantum cryptography solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of physics. This key can then be used with conventional cryptographic algorithms [5]. If one encodes the value of a digital bit on a single quantum object, its interception will necessarily translate into a perturbation, because the eavesdropper is forced to observe it. This perturbation causes errors in the sequence of bits exchanged by the sender and recipient. By checking for the presence of such errors, the two parties can verify whether their key was intercepted or not. It is important to stress that since this verification takes place after the exchange of bits, one finds out a posteriori whether the communication was eavesdropped or not. That is why this technology is used to exchange a key and not valuable information. Once the key is validated, it can be used to encrypt data. In telecommunication networks, light is routinely used to exchange information. For each bit of information, a pulse is emitted and sent down an optical fiber to the receiver, where it is registered and transformed back into an electronic signal. These pulses typically contain millions of photons [3, 14]. In quantum cryptography, one can follow the same approach, with the only difference that the pulses contain only a single photon. In particular a photon cannot be split into halves.[6].

3. The BB84 protocol

The first protocol for QC has been proposed in 1984 by Charles H. Bennett, from IBM New-York, and Gilles Brassard, from the University of Montreal, hence the name BB84 under which this protocol is recognized nowadays. They published their work in a conference in India, totally unknown to physicists.

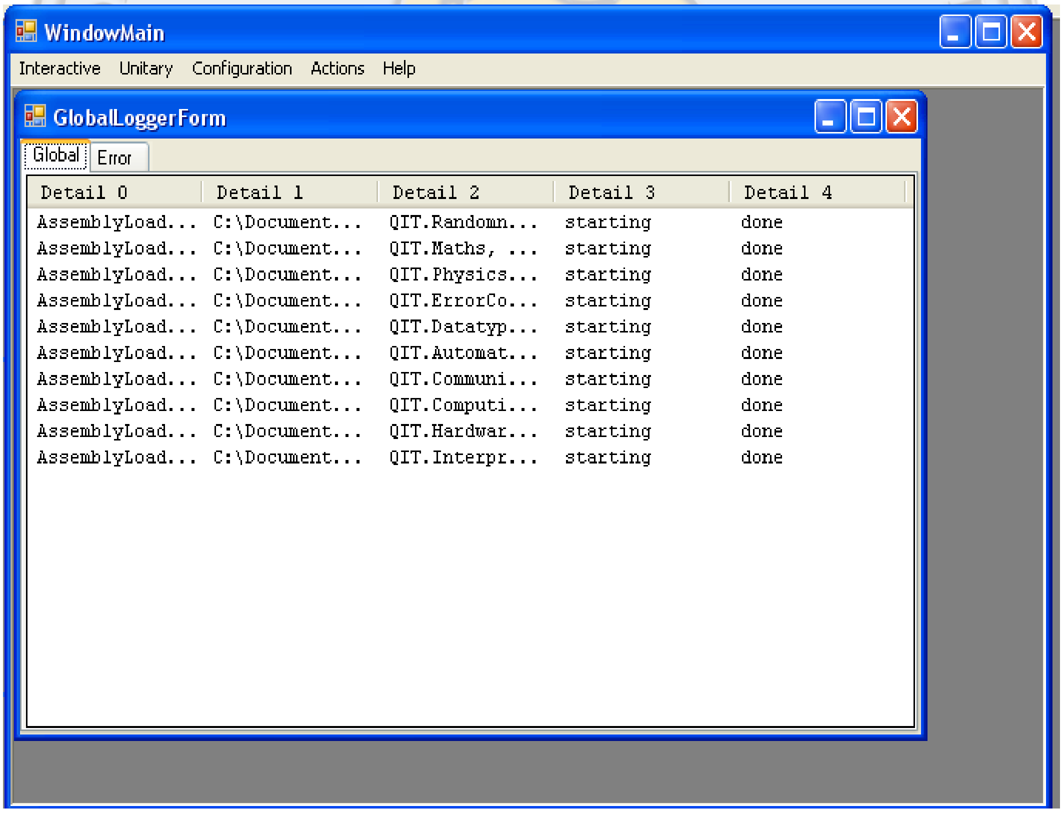
We shall explain the BB84 protocol using the language of spin 1/2 , any 2 level system being equivalent to it. The protocol uses two interlocutors, Alice, as the transmitter, and Bob, the receiver, as well as an eavesdropper, Eve. The photons of use are divided into 4 quantum states that constitute 2 bases, think of the states up | ↑i, down | ↓i, left | ←i and right | →i. Conventionally, one attributes the binary value 0 to states | ↑i and | →i and the value 1 to the other two states, and calls the states qubits (for quantum bits). In the first step, Alice sends individual spins to Bob in states chosen at random among the 4 basic states (the spin states | ↑i,| ↓i, | →i and | ←i are identified with the polarization states ”horizontal”, ”vertical”, ”+45 degrees” and ”-45 degrees”, respectively). How she ”chooses at random” is a delicate problem in practice, but in principle she could use her free will. The individual spins could be sent all at once, or one after the other (much more practical); the only restriction being that Alice and Bob can establish a one-to-one correspondence between the transmitted and the received spins[1]. Next, Bob measures the incoming spins in one of the two bases, chosen at random (using a random number generator independent from that of Alice). At this point, whenever they used the same basis, they get perfectly correlated results. However, whenever they used different basis, they get uncorrelated results. Hence, on average, Bob obtains a string of bits with 25% errors, called the raw key. This error rate is so large that standard error correction schemes would fail. But in this protocol Alice and Bob know which bits are perfectly correlated (the ones for which Alice and Bob used the same basis) and which ones are completely uncorrelated (all the other ones). Hence, a straightforward error correction scheme is possible: For each bit Bob announces publicly in which basis he measured the corresponding qubit (but he does not tell the result he obtained). Alice then only tells whether or not the state in which she encoded that qubit is compatible with the basis announced by Bob. If the state is compatible, they keep the bit, if not they disregard it. In this way about 50% of the bit string is discarded. This shorter key obtained after bases reconciliation is called the sifted key. The fact that Alice and Bob use a public channel at some stage of their protocol is very common in crypto-protocols. This channel does not have to be confidential, but has to be authentic. Hence, any adversary Eve can listen to it all the communication on the public channel, but she can’t modify it. In practice Alice and Bob may use the same optical fiber to implement both the quantum and the classical channels. Note that neither Alice nor Bob can decide which key results from the protocol. Indeed, it is the conjunction of both of their random choices which produces the key [4-6].

Let us now consider the security of the above ideal protocol (ideal because so far we did not take into account unavoidable noise due to technical imperfections). Assume that some adversary Eve intercepts a qubit propagating from Alice to Bob. This is very easy, but if Bob does not receive an expected qubit, he will simply inform Alice to disregard it. Hence, in this way Eve only lowers the bit rate (possibly down to zero), but she does not gain any useful information. For real eavesdropping Eve must send a qubit to Bob. Ideally she would like to send this qubit in its original state, keeping a copy for herself.

4. Simple software simulation of the BB84 protocol

There are many software implementations used to simulate the BB84 protocol. Some are written in PHP code, Java ,C++, or native quantum simulation software. For this paper we have chosen a software written in Visual C++ called QIT designed by Fernando Lucas Rodriguez. This is a general public license (GPL) software and it can be found on the Internet for student training and research. The program has an interactive graphical user interface (GUI) that allows students to watch a step by step execution of the protocol. Students will use the program to find the different quantum keys.

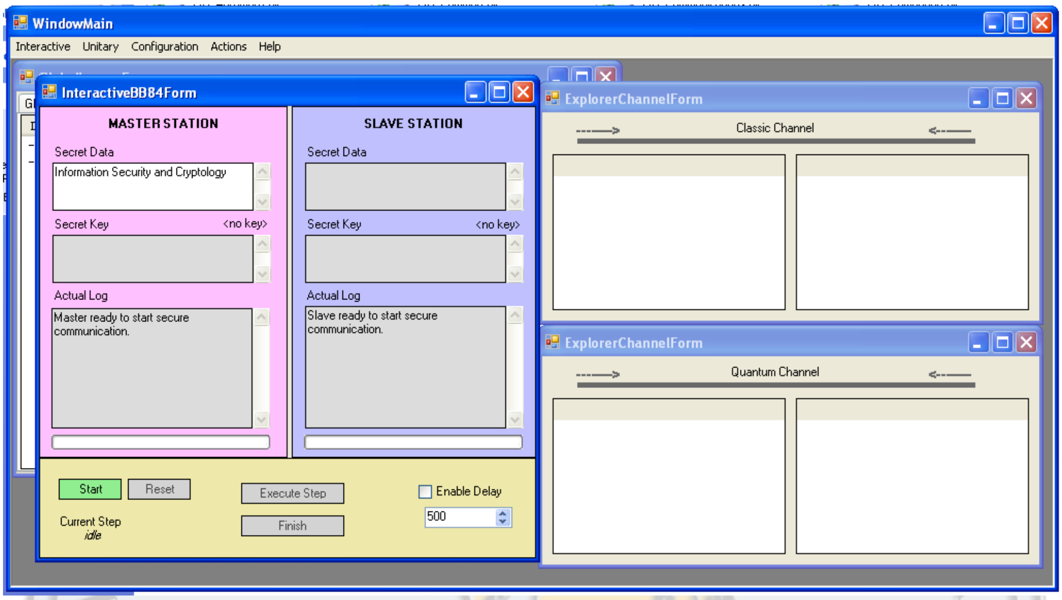
The program will run from one of the 2 computers on the lab table witch must run a Windows XP 2 operating system with .NET 2 installed. From the folder QIT13 the students must execute QIT IDE.exe [9]. After the execution the following window will appear (Fig. 1.):



```
Detail 0          Detail 1          Detail 2          Detail 3          Detail 4
AssemblyLoad...   C:\Document...    QIT.Randomn...    starting          done
AssemblyLoad...   C:\Document...    QIT.Maths, ...    starting          done
AssemblyLoad...   C:\Document...    QIT.Physics...    starting          done
AssemblyLoad...   C:\Document...    QIT.ErrorCo...    starting          done
AssemblyLoad...   C:\Document...    QIT.Datatyp...    starting          done
AssemblyLoad...   C:\Document...    QIT.Automat...    starting          done
AssemblyLoad...   C:\Document...    QIT.Communi...    starting          done
AssemblyLoad...   C:\Document...    QIT.Computi...    starting          done
AssemblyLoad...   C:\Document...    QIT.Hardwar...    starting          done
AssemblyLoad...   C:\Document...    QIT.Interpr...    starting          done
```

Fig. 1. Output window of QIT.exe

Then from the Interactive menu ->Communications->InteractiveBB84 Cryptosystem is selected. With this selection the interface for simulating the BB84 protocol will appear (Fig. 2.):



Information Security and Cryptology

Master ready to start secure communication.

Slave ready to start secure communication.

Current Step idle

500

Fig.2. GUI of QIT.exe

Example: The secret data to be sent is: "Information Security and Cryptology". Press Start, then Finish. The resulting binary secret key is:

1101010011011100110100001010100000000100111101111011011110010000 10
011000110101011110101111010000010101001001010011100100110111100000
000010010001100111101110110101011010001010111010100110010101110010
0101100000000001011000101101011100010111110001010000111000000111110
1100100111000100

A step by step execution of the protocol is available by pressing Start then Execute Step [9].

The figure 1 and 2 represent the main steps in the execution of the protocol.

Behind the software the steps are as follow: the (4+delta)·N qubits will be transmitted. For each bit, Master station selects a basis randomly (horizontal-vertical or diagonal), and also selects a random value (true or false). It sends the resulting quantum state after encoding the true or false value into the selected basis. It also stores the basis selected and the random value. The slave station measures values received into a random basis (horizontal-vertical or diagonal). It stores the basis used for measurement and the value measured. The master station sends the basis used for values encoding. The values are not transmitted, they are the secret.

The slave station stores the master's used basis for encoding. The master station stores coincidences. Slave station informs Master about which basis there was coincidence during qubit encoding and slave measurement. Values measured are not transmitted, only if there was coincidence.

The master and slave generates an intermediary 'secret private' key with the values of qubits of which where was coincidence on basis encoding and measurement and checks that intermediary key has at least the double of bits needed for chippering data.

The master select random intermediary-key bits indexes for public comparisons, and informs of those positions to the slave. The number of bits to compare will be the size of intermediary key minus the number of bits needed for chippering data. Slave stores the indexes of the positions that will be compared.

The master sends the values that tried to encode on quantum channel of the selected indexes. Slave stores the values that Master sends. The master stores the values that Slave sends. Slave sends the values that measured on quantum channel of the selected indexes.

Master calculates noise level (it knows what it tried to send, and what Slave received). If noise rate is too high (over 25%) with high probability there is an Eavesdropper and data transmission is aborted. Slave calculates noise level (it knows what Master tried to send and what it received). If noise rate is too high (over 25%) with high probability there is an Eavesdropper and data transmission is aborted. The data is sent using Vernam chippering with the BB84 key on a Classic public channel. The Slave Station stores and decodes the ciphered message with the BB84 secret, private & secure key (Fig. 2).

5. Implementing the BB84 protocol in a student oriented experimental apparatus

5.1. Background

The experimental setup will follow the initial idea that was used in the Optical Institute of Orsay, France. In that case, the photons were transmitted between two windows of two separate buildings. For coding the qubits the experiment used the four polarization states (horizontal, vertical, circular left and circular right). Physically, they were created by applying a voltage on an electro-optical modulator. The qubit sequence resulting from the coded polarization is generated by hardware means, by using two Fibonacci configured linear registries. Each registry has an output of $2^{20}-1$ bits, and the 4 states of the protocol suffer 2-bit coding, each of the bits being a part of a pseudo-random sequence. For minimizing diffraction effects, the radius of the photon beam is extended to 2 cm, by using a two-lens system, before being transmitted 30 m through open air. The photons are collected by Bob through the same system, at which 4 avalanche photo-diodes were added. Measurements of polarization were made by selecting the states, as the photons are either transmitted or reflected by a beam splitter at the incidence angle of 45°. Horizontal and vertical states were created by the beam splitter, while the circular left and right states were separated by a special splitter that converts circular polarization into linear polarization, and then discern them through the same splitting method.

5.2. The efficiency of the single photon source and the Poisson statistics

Primary characteristics of the single photon source quality made by Alice consist of measuring the single and multi-photon emission probabilities, compared with weak coherent pulses (WCP), with the same amount of photons per pulse. For a transmission sequence of 0.2 s and pulse frequency of 5.3 MHz, a total of 8.8×10^{4} photons are recorded by Alice. By correcting the efficiency of the photo-diodes (APD) $\eta_{APD}=0.6$ the global efficiency adds up to 2.8%. After passing through the modulator, characterized by $T_{EOM}=0.9$ and $T_{optic}=0.94$, the mean of the sent photons per pulse was $\mu=0.0235$. Reduction of the multi-photon emissions can be set in Alice's part of apparatus. Photon statistics can be counted precisely by Bob's measurements, thus resulting in the distribution of the photon numbers. Evaluations were carried out on 40×10^{6} pulses recorded by Bob [1]. For a time sample, detection probabilities for a photon or photon pair are $P_{1d}=7.6\times10^{-3}$ and $P_{2d}=2.7\times10^{-6}$. Configuration of the photo-diodes shows that the detection probability P_{2d} is 5/8 of the reception probability of the same pair, while the probability that a photon pair falls on the same photo-diode is of 3/8. The reduction factor is given by: $R=\frac{5}{8}\times\frac{P_{1d}^{2}}{2P_{2d}}=6.7$. This result is in accordance with the Poisson distribution, and thus can be used in further calculus. Information leak to an intruder connected to the quantum channel is $S^{(m)}$, which shows the probability that a photon leaves Alice's system. For an equivalent WCP we have $S_{WCP}^{(m)}=1-(1+\mu)e^{-\mu}=2.7\times10^{-4}$, while for the SPS $S_{SPS}^{(m)}=\frac{1}{6.7}[1-(1+\mu)e^{-\mu}]=4.1\times10^{-5}$ [4].

5.3. Detection probabilities of Bob's system

Detection probability of Bob's apparatus over a time threshold is $p_{\exp}\cong7.6\times10^{-3}$. Assuming that the absorption of the beam is negligible through the 30 m transmission, and taking into account that the mean $\mu=0.0235$, an estimate of the detection apparatus is $\eta_{Bob}\cong0.3$. While measuring photons, errors might appear, because of unpolarized light. This contributes to compromising the security of the transmission, and decrease the maximum transmission distance. By filtering and spectral insulation, the optical environment can be protected. Measurements were made at night time, the probability of recording an incorrect photon per time threshold is $p_{dark} = 3.8\times10^{-5} s^{-1}$ [4].

6. Our experimental proposal setup

The experiment will take place on a lab table, so there is no need to have complicated alignment system. A simple laser diode and the transmitter can be used for alignment, by moving the two supporting legs.

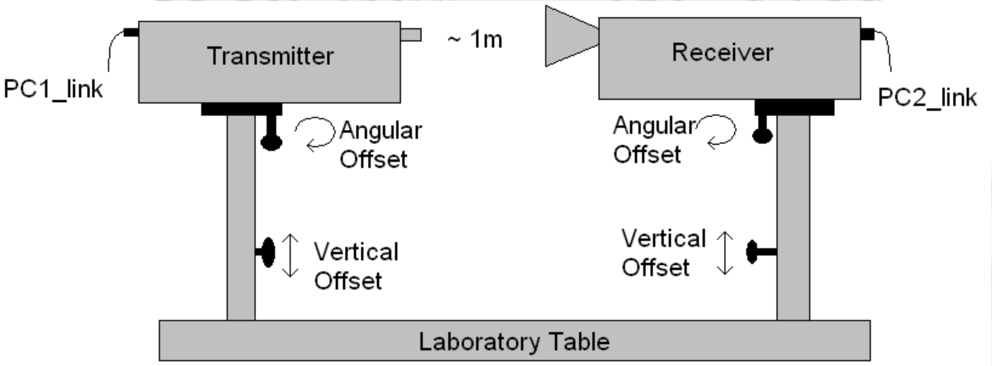


Fig. 2. Experimental proposal.

The experiment consists of two main modules: Alice and Bob, in our case, transmitting and receiving student, that communicate over open air, at the designated distance for laboratory of about 1 m.

The classical channel is a basic TCP/IP connection (coaxial or UTP cable). The experiments for optical fibers transmissions are also considered.

6.1. Transmitter Module

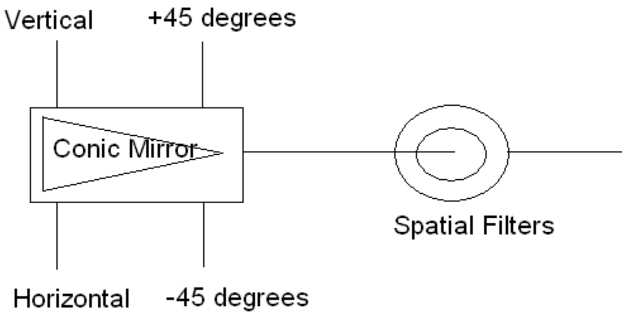


Fig. 3. The Alice module.

The module is designed to produce a stream of single polarized photons according to the choice of basis and bit value. Because no source can produce single photons, we use pulses that have the property of coherency. They are called weak coherent pulses (WCP), of Poisson distribution and mean photon number $\mu = 0.0235$. To produce the pulses, we will use four laser diodes, oriented around a conical mirror at the desired polarization angles. The polarization problem is solved by the laser diodes, that have intrinsic polarization. After the beams are reflected by the conical mirror, they pass a spatial filter, which consists of two $100\ \mu\text{m}$ at 0.9 cm apart. It serves a special purpose, that of making the pulse from the four diodes indistinguishable from the others, in spatial terms. This measure has to be taken because without the spatial filtering, the code can be broken quite easily. In order to get as much light as possible through the spatial filter, there is a lens with a focal length *f* = 2.75 mm between the conical mirror and the pinholes of the spatial filter. Because of the very strong spatial filtering, the alignment of the pinholes is crucial, otherwise the desired mean photon count will not be achieved for all polarizations. [4]

6.2. Receiver Module

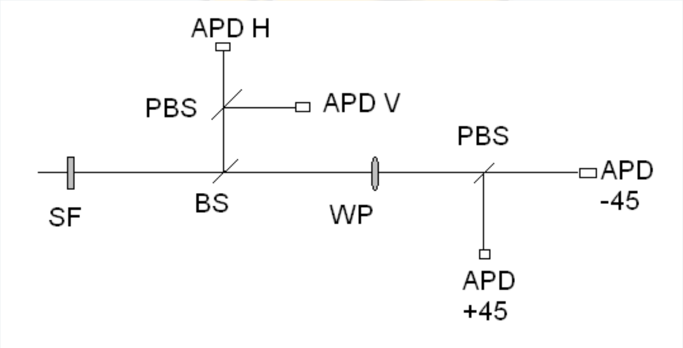


Fig. 4. Receiver module schematic.

The module is the heart of the receiver unit is connected directly to a receiver lens and a spatial filter (SF), that are positioned so that the transmitted beam is focused on the primary device of the module. The primary device is an interference filter with a red color glass filter. This is important to allow for daylight operation, because it rejects stray light, while permitting polarized light to pass. The remaining optical devices divide the photon beams into bases H/V and +/-, the construction being based on the idea by John Rarity and Paul Tapster. An incident photon sees the 50/50 beam splitter (BS). If it is reflected it will see the polarizing beam splitter(PBS) of the photon in the H/V basis, which in combination with the two silicon avalanche photo diodes (APD) H and V. If APD V detects a photon it is supposed to be in the V basis, whereas if APD H detects a photon, it is supposed to be in the H basis.

Any photon that is transmitted through the beam splitter passes through a half-wave plate, set at an angle of 22.5, so that it rotates the linear polarization by 45 degrees. Afterwards, a +45 degrees polarized photon is detected by APD 1 and converted into the horizontal basis H, while a - 45 degrees polarized photon is detected by APD 3 and converted into the vertical basis V. Whenever a photon is measured in the wrong basis, the measurement outcome is completely random. The APD-s have to be cooled in order to reduce dark counts, at a temperature between - 25 and - 10 degrees. To reach these temperatures, the photo-diodes are put into an aluminum block which is cooled by a Peltier element glued to it from below [4]. The bit error rate (BER) [6] for each channel was estimated from data taken during key exchange. It is given by the expression: $BER = \frac{N_{wrong}}{N_{total}}$, where N_{wrong} is the number of bits in error and N_{total} is the number of bits received in total. This gives a measure of the likelihood of receiving a zero when a one was sent from the transmitter. All but one of the BER values in table 1 are sufficiently low showing that optical imperfections from the equipment will contribute little to the error in the sifted key. The system will operate in natural light and artificial light in the lab, thus the background error rate must be considered. This is a factor that could limit the entire experimental setup. We start from the signal count for this rig [8]: $S = \frac{RMT\eta}{4}$, where R is the repetition rate, M is the average number of photons per pulse, T is the lumped transmission and η is the detection efficiency of Bob's APDs. The product is divided by 4 because there are 4 detectors (or 4 polarization states). The background rate is given by $P_b = Bt$, where B is the background the background count rate per APD and t is the time synchronization gate. Half the counts induce errors and half of there are thrown away. The error rate is: $E = E_{base} + \frac{P_b}{S}$. E must be less the 0.07 therefore the maximum acceptable background rate is: $B < \frac{MT\eta}{75.5t}$. In considering the system presented here, estimates can be made for the following values [8]:

1. $M \sim 0.3$, an accepted value for guaranteed security of low loss systems.
2. $T \sim 1$ since the source can be imaged on to the receiver and the system is short range and thus atmospheric loss is negligible.
3. $\eta \sim 0.045$ taking into account the quantum efficiency of the detectors and the presence of the narrow band filter and polarizers.
4. $t = 5$ ns gate synchronization time.

Thus the maximum background count rate per detector can be given as roughly B ≪ 36000 counts/s. In this system, the data is recorded first during the quantum transmission and processed afterwards in a few seconds. The start of the transmission is determined approximately by searching for a jump in the frequency of time tags as Bob starts measuring before Alice begins her transmission. Alice transmits sub-5 ns pulses every 200 ns, therefore a time synchronization gate of 5 ns reduces the probability of registering a background event within the gate by a factor of 40 [8]. The clock at the receiver is thus synchronized with the clock at the transmitter by searching for time tags that sit at separations of 200 ns and adjusting the time separation slightly every ~100 ms to compensate for clock drift. The advantage of this set-up is that no timing reference signal is needed. To determine the exact start time of the data, the receiver reveals a random subset of his measured bit values and the basis he used to the transmitter. The transmitter then finds the data start by performing a sparse correlation against her stored data. This random subset can also be reused to estimate the error rate.

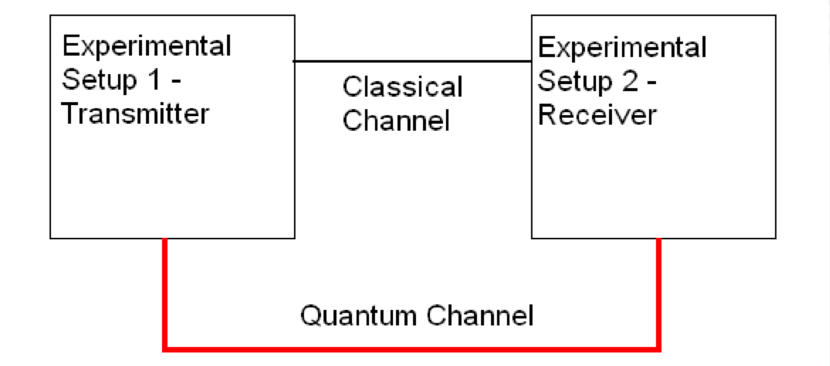

Experimental Setup 1 - Transmitter
Classical Channel
Experimental Setup 2 - Receiver
Quantum Channel

Fig. 5. Full experimental rig.

It should be noted that our implementation of error correction requires that the two parties both generate the same random factor graph. Once both of them know the number of message bits they are error correcting over, and the measured error rate, they seed a pseudo-random number generator from their OTP and use this to generate an appropriate factor graph.

The eavesdropper, is assumed not to know which of the 2^{256}, say, different factor graphs the communicating parties are using [8].

For implementing this type of encryption we also can use fiber optics, as used in "Clavis" [9, 10] devices for BB84 code implementation.

Fiber optics may provide a much longer distance for light propagation, thus facilitating the wide area implementation for this type of secured data transmissions.

7. Improving BB84 by using photon echo

Our optical channel can be improved using the photon echo effect [3]. The code encrypting can be made by introducing a supplementary key if we use the photon echo. We have three states associated to the 1 and 0 qubits that are available for encrypting. That correspond to the possibility of associating to the two input impulses two or three output impulses, the third one corresponding to the photon echo, generated after an algorithm or by our own will. Excitement of super radiant states by irradiating a probe with an coherent optical impulse, with its duration and intensity conveniently chosen can be shown with the photon echo [3]. In principle, we consider the exciting of a ruby crystal, for example, with two coherent, identical optical impulses A and B (emitted by a ruby laser), having a duration of Δ*t* (ns), the delay of B impulse when passing through the probe, will be $\Delta T \gg \Delta t$, showing in the figure 6 [12, 13].

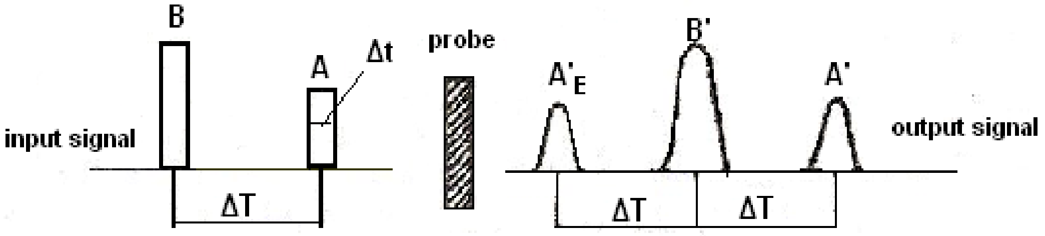


Fig. 6. Principle of photon echo.

We can see at the exit, beside the two impulses A' and B', which correspond to the emitted impulses A and B, a third impulse A", symmetrical positioned to A' and B', named photon echo [3]. For explaining the photon echo, we use the precession equation, for a circular polarized radiation field, in a reference system which rotates round the z axis with the frequency ω: $\frac{d}{dt}\langle P\rangle = \chi\langle P\rangle \times (E_i + \frac{\omega-\omega_0}{\chi}\bar{k}$.

Due to the unequal width of the transition frequency for ruby atoms, and due to the local field, variation, *P* and ω_0 will be affected by index *k* , which defines the *k* atom.

If before applying impulse A, the atoms were all in the fundamental state, the vector $\langle P\rangle = \sum_{k=1}^{N}\langle P_k\rangle$ is oriented in the negative direction of z axis. Applying the A impulse, of E_a amplitude, between *t* = 0 and *t* = Δ*t*, a precession movement of *P* around the pseudo field appears. If $E_A >> |\omega-\omega_0| / X$, the procession is made around the *x* axis with an $X E_a \Delta t$ angle so for an intensity of the impulse that satisfies the condition $X E_a \Delta t = \pi/2$ (π/2 impulse), $\langle P\rangle$ will be orientated after *y* axis in *t* = Δ*t*, the system being in a superradiant state Δ.

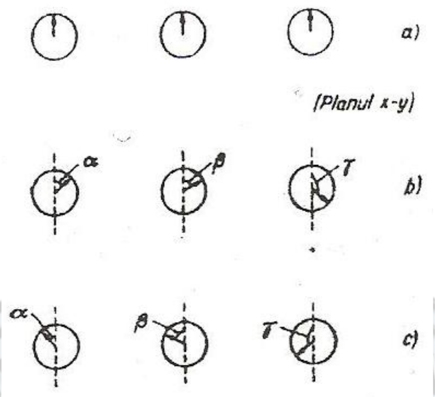


Fig. 7. Superradiance states.

When the E_a field stops, the atoms will execute precession movement with different speeds around the pseudo-field $\frac{\Delta\omega}{X}\bar{k}$ where $\Delta\omega = \omega - \omega_{0k}$. During these movements in $t = \Delta t$ and $t = \Delta t + \Delta T$ interval, $\langle P_k \rangle$ components will be dephased so $\langle P \rangle$ diminishes [3]. *B* impulse which applies in the moment $t = \Delta t + \Delta T$ must reflect the $\langle P_k \rangle$ vectors in the *x–y* plane, reported to the *x* axis. To obtain this effect the following condition must apply: $\eta\, E_b \Delta t = \pi$ (π impulse), meaning that $I_B = 4I_A$, I_A and I_B specifying the two impulses intensities. In the interval $t = 2\,\Delta t + \Delta T$ and $t = 2\,(\Delta t + \Delta T)$ the vectors $\langle P_k \rangle$ are moving like in the dephase interval, getting in phase after another interval equal to ΔT. The corresponding state of the vectors $\langle P_k \rangle$ in rephasing is a superradiant state, highlighted by echo impulse emission A'_E [3]. We can use the photon echo to improve the code by adding either a controlled error on the channel or transforming the channel from a binary channel to a ternary channel. A ternary channel is more efficient in transmitting coded information but in this form the ternary channel will be created on a binary one, using the echo to create the third channel of communication. We also can improve a channel transmission width using the photon echo to create a bit of data when we want, thus changing the information meaning and receiving more information that was initially sent.

8. Conclusions

Quantum cryptography implemented with the BB84 protocol offers a high level of security for data communications. Although it has not been implemented on a commercial level, it is suitable for integration in optical fibers communications, with a wide range of applications. Our experimental proposal offers a good student insight into quantum cryptography, combining the already known and designed modules Alice and Bob with the potential of the photon echo.

REFERENCES

[1] Paul Sterian, Dan Alexandru Iordache, Viorica Iordache, *"Study of the Present Problems of the Scientific Information Processing and Transmission"*, Annals of the Academy of Romanian Scientists, Series on Science and Technology of Information, **vol. 3**, no. 1, 2010, pp. 101-112.

[2] Dan-Alexandru Iordache, Daniela Radu, Octavian Radu, *"Complexity Approach of Optical Communications Systems"*, Annals of the Academy of Romanian Scientists, Series on Science and Technology of Information, **vol. 2,** no. 1, 2009, pp. 9-16.

[3] Paul Sterian, "Fotonica", Editura Printech, Bucuresti 2000, ISBN 973-652-161-3.

[4] Harald Weinfurter and Alfred Laubereau, "Experimental Quantum Cryptography", 2003, http://xqp.physik.uni-muenchen.de/publ/henning-diplom.pdf.

[5] Id Quantique, Switzerland, "Securing Networks with the Vectis Link Encryptor", www.idquantique.com.

[6] Thomas Daniel Jennewein, Anton Zeilinger, "Quantum Communication and Teleportation using Entangled Photon Pairs", June 2002, http://www.quantum.univie.ac.at.

[7] Fernando Lucas Rodriguez, QIT IDE.exe, http://www.fernandolucas.info/QCS, fernandolucas@ieee.org.

[8] J. L. Duligall, M S Godfrey, K A Harrison, W J Munro and J G Rarity, "Low Cost and Compact Quantum key distribution", 2006, http://www.iop.org/EJ/abstract/1367-2630/8/10/249.

[9] D.Stucki, N. Gisin, O. Guinnard, G. Ribordy, H. Zbinden, "New Journal of Physics 4", www.njp.org.

[10] Id 3000 Datasheet v2.1, www.idquantique.com.

[11] Cornel Cobianu, Cazimir Bostan, s.al., "*From 2D Microelectronics to 3D Microsystems"*, Annals of the Academy of Romanian Scientists, Series on Science and Technology of Information, **vol. 3,** no. 1, 2010, pp. 31-46.

[12] Ion Apostol, Dan-Alexandru Iordache, Pier Paolo Delsanto, Viorica Iordache, "*Study of some Numerical Artifacts Intervening in the Finite Differences Simulations of KDV Solitons Propagation*", Annals of the Academy of Romanian Scientists, Series on Science and Technology of Information, **vol. 4,** no. 1, 2011, pp. 7-22.

[13] Dana Georgeta Popescu, Paul Sterian, "*Nonlinear Interaction Modeling in Photonic Crystals*", Annals of the Academy of Romanian Scientists, Series on Science and Technology of Information, **vol. 4**, no. 2, 2011, pp. 105-124.

[14] Sterian Andreea Rodica, "*Coherent Radiation Generation and Amplification in Erbium Doped Systems*", *Advances in Optical Amplifiers*, Paul Urquhart (Ed.), ISBN: 978-953-307-186-2, InTech, VIENNA, 2011.