

Setup for quantum cryptography with floating basis protocol in frequency coding.

*Kurochkin Yury^{1,2}, Donnet Stéphane¹, Cussey Johann¹,
Kurochkin Vladimir², Merolla Jean-Marc¹.*

PhD student

¹University of Franche-Comté, Besancon, France

²Institute of Semiconductor Physics, SB RAS, Novosibirsk, Russia

E-mail: y.kurochkin@gmail.com

Introduction

Quantum information science allows solving tasks which is usually impossible in classical ways. The brightest examples are the quantum computer and quantum cryptography (or quantum key distribution) [1]. Quantum cryptography (QC) is the first commercial application of the quantum information science [2]. It allows two parties to establish absolutely secure communication which secrecy will be based not on the computation complexity but on the quantum laws [3].

The first quantum cryptography protocol is BB84 it was developed by Bennet and Brassard in 1984 [4]. It contains two non-orthogonal bases which should be chosen randomly. Now there are a lot of new quantum cryptography protocols. Its aim is to increase an efficiency and transmission speed. In this work we present the setup which will be suitable for a broad number of protocols such as BB84, Yuen protocol (Y00) [5], our floating basis protocol [6, 7] and some other.

There is a number of coding methods. Information can be encoded on the phase, polarization and other parameters of the photons. There is also the so called frequency coding [8]. In this coding amplitude of laser pulse is modulated and information is encoded on the sidebands with $\omega_0 - \Omega$ and $\omega_0 + \Omega$ frequency see (fig 1). In this type of coding the depth of modulation is chosen so that the power at the sidebands appears to be at the single photon level. Receiver modulates the signal in the same way and if the phase difference between the modulation frequencies is equal to 0 or π then the photon can be detected at $\omega_0 - \Omega$ or $\omega_0 + \Omega$ frequency.

Fig 1. In frequency coding information is carried by the quantum states of the sideband photons.

Protocol

In the floating basis protocol [6, 7] the basis of the transmission is defined by the pre-distributed secret key. The idea of this protocol arises from the idea of enlarging the number of bases to the incredibly large but without of the reduction of the transmission speed. It is possible because the basis position is not chosen randomly. Basis of each qubit is strictly defined by the secret information. This secret information (auxiliary key) was prepared by some other way. The aim of this protocol is the strong enlargement of the secret information amount. Auxiliary should be rearranged after some number of transmitted bits. Number of secure transmissions depends on the quantum channel losses. This protocol appeared to be tolerant against attacks with quantum memory and quantum computer.

Setup

In order to realize some high speed protocol with pre-distributed key it should be some confident but not obligatory fast secure channel. It can be BB84 protocol realized in the same setup. BB84 protocol has rather strong restrictions on the mean photon number per pulse and high key suppressing privacy amplification mechanism [3]. To achieve the high efficiency the quantum cryptography setup should be able both to generate the auxiliary key with the use of the BB84 protocol and use this key to establish the high speed quantum key distribution.

The structure of the setup is following (fig 2). First laser with the frequency ω_s generates strong synchronization pulses which are modulated by the Mach – Zehnder interferometer MZI. The 2 GHz frequency of the modulation Ω is generated by VCO. Second laser diode with central frequency ω_0 generates weak pulses which are modulated by another Mach – Zehnder interferometer. The electrical phase modulator MIQ shifts the phase of the ω_0 pulse amplitude modulation. The phase shift is chosen according to the protocol. Then these two pulses are coupled and propagate through the same fiber to the receiver. At the receivers side this two pulses are decoupled. The ω_s pulse propagates to the analog detector D_2 which retrieves the reference 2 GHz frequency. Then the phase of the reference frequency is shifted by the receivers MIQ and modulates the weak pulse ω_0 . If the phase shift has been chosen properly then the constructive and destructive interference can be seen (see fig 1 central and right picture). Then the Filter (Fabry-Perot) filters one sideband and it is detected by the single photon detector D_1 . All the process are controlled by the computer.

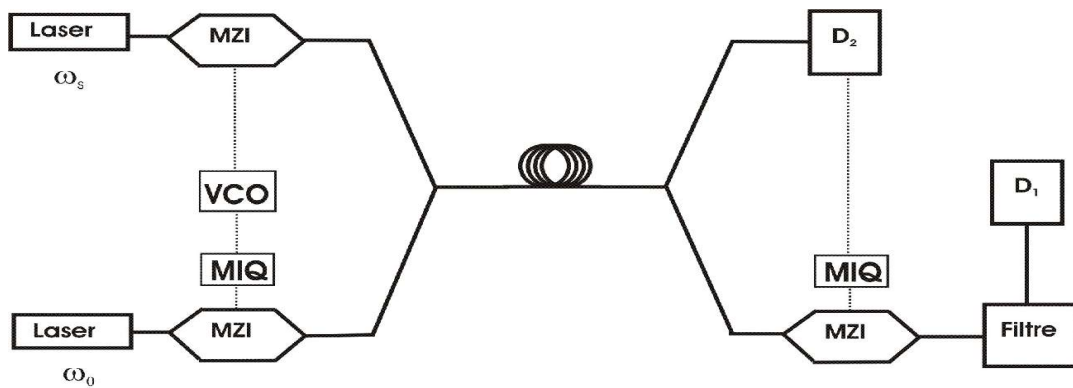


Fig 2. The quantum cryptography setup.

References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys 74, 145 (2002).
2. MagiQ Technologies, Inc. website: <http://www.magiqtech.com/> and id Quantique website: <http://www.idquantique.com/>.
3. D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill (2004), arXiv:quant-ph/0212066.
4. C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India pp. 175 {179 (1984).
5. H. P. Yuen (2004), arXiv:quant-ph/0311061 v6.
6. Y. V. Kurochkin and V. L. Kurochkin, Digest IV International Symposium on Modern Problem of Laser Physics, Novosibirsk, Russia. pp. 265 - 266 (2004).
7. Y. Kurochkin, Proceedings SPIE Quantum Informatics 2004 5833, 213 (2005).
8. Merolla J.-M., Mazurenko Y., Goedgebuer J.P. and Rhodes W.T. Phys. Rev. Lett. 1999, vol. 82, pp. 1656-1659.