Implementation of multiplexing in a subcarrier-wave quantum cryptography system

V V Chistyakov, A V Gleim, V I Egorov, Yu V Nazarov

St.Petersburg National Research University of Information Technologies, Mechanics and Optics, Kronverkskiy pr. 49, St.Petersburg 197101, Russian Federation

E-mail: pspuser@mail.ru

Abstract. Quantum cryptography allows distributing secure keys in a way that any eavesdropping in the channel is inevitably detected. This work is dedicated to introducing wavelength division multiplexing in a subcarrier-wave quantum cryptography system. Compared to other existing schemes, the resulting device is able to achieve higher bitrates (up to 2.26 Mbit/s at 20 km), is robust against external conditions and compatible with standard telecommunication fibres in multi-user environment.

1. Introduction

Quantum cryptography allows distributing secure keys in a way that any eavesdropping in the channel is inevitably detected [1]. Recent progress in the area has led to an increasing interest in combining this technology with telecommunication techniques, thus opening the door to a new generation of secure networks [2-5]. Subcarrier wave quantum key distribution (SCW QKD) technology [6] belongs to a group of QKD schemes most perspective for telecommunication applications. In particular, these systems are unidirectional, polarization insensitive and robust against natural conditions [7-8]. Another important advantage lies in ability to distribute several cryptographic keys using a wavelength division multiplexing technology (WDM). System with the several sidebands was developed using simultaneous phase-frequency modulation of a single central band [9]. Quality of this method is limited by losses of used modulators and complexity of the close spaced sidebands filtration system. In this work we present another principal scheme of a multichannel SCW QKD system operating at multiple bands, and experimental results that demonstrate its operation in the classical mode. This system allows distributing the keys with high speed or between more than two users, which can be useful for integrating it in telecommunication networks.

2. Theoretical analysis

In terms of SCW QKD multichannel system means that several intense carrier waves, each with its own pair of subcarriers acting as quantum channel, are transmitted through a single fiber from sender (Alice) to receiver (Bob), where they are splitted, filtered and detected. In the first part of work we estimated the impact of using WDM technique on raw key generation rate (bitrate) and quantum bit error rate (QBER) of the resulting system. It is known that bitrate is limited by detection frequency:

$$R_{\text{raw}} = \frac{1}{2} f_{\text{bit}} \mu_{\text{loss}} \eta,$$

where $f_{\text{bit}}$ is the bit frequency, $\mu_{\text{loss}}$ is the loss factor, and $\eta$ is the detection efficiency.
where ½ is multiplier that means possibility of modulators states matching in B92 protocol [1], $f_{bit}$ – phase-shifting frequency, $\mu$ – mean value of photon number per pulse, $\eta$ – quantum efficiency of a single photon detector, $a_{\text{loss}}$ means probability of photon arrival and defined through the value of total losses $A_{\text{all}}$ in the channel:

$$a_{\text{loss}} = 10^{-\frac{A_{\text{all}}}{10}}$$

Total losses include losses in the channel and element’s losses:

$$A_{\text{all}} = A_{\text{channel}} + A_{\text{elem}},$$

where $A_{\text{channel}} = L \cdot \alpha$, $L$ – length of the channel, $\alpha$ – attenuation coefficient, $\alpha = 0.2$ dB/km. To calculate $A_{\text{elem}}$ we should sum up losses in the Bob’s modulators, circulators, except demultiplexing system. In the single-channel SCW QKD systems this value is 10.47 dB. Losses at the sender unit shouldn’t be considered, because signal in the quantum channel is attenuated to $\mu = 0.2$ photon per pulse according to B92 protocol.

It is necessary to use SSPD as a photon counter with best combination of quantum efficiency and detection frequency. Our detector could achieve $f_{\text{bit}} = 500$ MHz and $\eta = 16\%$ [10].

We considered two methods of splitting the signal at the receiver unit: by using a cascade of circulators with optical filters (serial demultiplexing system) and a regular DWDM demultiplexer (parallel demultiplexing system). The first method is preferable for less than five channels because of the lower losses. Losses in the second configuration equal to 17.44 dB.

In the DWDM systems channel spacing is 0.8 nm (100 GHz). Because of that filtration becomes much easier than WDM SCW QKD with one carrier and several subcarriers. Also because of different wavelengths attenuation coefficient becomes different for an each channel. In our calculations we compared multichannel (up to 40) systems with the regular single channel setup and serial demultiplexing system with four channels (Figure 1 a,b).

Calculation results show that in a 40 channel SCW QKD system bitrates up to 2.26 Mbit/s, 550 kbit/s, 53 kbit/s can be achieved at distances 20, 50, 100 km respectively. QBER is estimated to achieve the critical value of 11-12% at fiber length more than 200 km, therefore allowing key distribution to large distances.

![Figure 1 (a), (b). Dependence of raw key generation rate on the channel’s length with the different demultiplexing configurations.](image-url)
3. Experimental results

In the experimental part of work we developed a double-channel SCW QKD system prototype in two versions accordingly two stages: obtaining of the spectral characteristics (Figure 2) and oscillograms of constructive and destructive interference (Figure 3). In this setup optical carriers from two lasers (1550.12 nm and 1550.92 nm) are independently modulated at transmitter (Alice) side, combined and send to receiver (Bob). It is important that for subsequent modulation it is enough only one phase-frequency modulation system for all channels. After subsequent modulation and demultiplexing, the resulting spectrum passes through the optical filters in order to cut off the signal on subcarriers, which is then detected and analysed.

**Figure 2.** Principal scheme of multichannel subcarrier wave quantum cryptography system. L1, L2 – lasers, PM – phase modulator, BC – beam combiner, C – circulator, SF – spectral filter, D – detector. On the insets one can see signal spectra at different ports.

**Figure 3.** Demonstration of oscillograms. L1, L2 – lasers, PM – phase modulator, BC – beam combiner, C – circulator, SF – spectral filter, D – detector. On the insets one can see signal spectra at different ports.

Experiments have shown that weak signals at wavelengths as close as 0.881 nm that appear on side frequencies of the two carriers can be effectively extracted from signal spectrum in case of using π-shifted Bragg grating filters. For the first stage we constructed system in a way that sidebands were directed in the filter’s transmission spectra and observed by optical spectrum analyzer (Figure 4).
For the second stage we performed simulation of quantum key distribution in the classical mode with B92 protocol [1]: it was achieved by repeatedly changing the relative phase shift introduced by the modulators in a basis [0; π] at 1 kHz rate. The dependence of the light intensity on the sidebands looks like the same frequency meander (Figure 5). Signal contrast was measured to be 20 in both channels, which corresponds to visibility 90.4% in the quantum regime.

**Figure 4.** Spectra of constructive and destructive interference

**Figure 5.** Oscillograms of constructive and destructive interference

### 4. Conclusion
We developed a multichannel SCW QKD system and performed simulation of quantum key distribution in accordance to B92 protocol. The main motivation of this work lies in the necessity of integrating QKD devices into existing telecommunication environment. Due to quantum nature of information carriers, no amplifiers can be used in the communication link, therefore, wavelength division multiplexing is useful not only for implementing multiuser setups, but also for increasing raw key generation rates. Demultiplexing configuration’s selection depends on the number of channels: parallel splitting for five and higher channels or serial splitting for lower number. According to the calculations, the resulting bitrate may be as high as 2.26 Mbit/s. Combining our results with multiplexing at several subcarriers [9] would lead to even greater possibilities.

**Acknowledgements**
This work was financially supported by Government of Russian Federation, Grant 074-U01.
References
[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J et al 2009 Rev. Mod. Phys. 81, pp 1301-1350
[2] Townsend P D 1997 Electron. Lett. 33, pp 188-190
[3] Fernandez V, Collins R J, Gordon K J, Townsend P D and Buller G S 2007 IEEE J. Quantum. Electron. 43, 130
[4] Peev M, Pacher C, Alléaume R et al 2009 New Journal of Physics 11 075001
[5] Patel K A, Dynes J F, Choi I, Sharpe A W, Dixon A R, Yuan Z L, Penty R V and Shields A J 2012 Physical Review X 2, 041010
[6] Mérolla J-M, Mazurenko Yu T, Goedgebuer J-P, Porte H and Rhodes W T 1999 Optics Letters, Vol 24, Issue 2, pp 104-106
[7] Guerreau O, Mérolla J-M, Soujaeff A, Patois F, Goedgebuer J-P and Malassenet F J 2003 IEEE J. Sel. Top. Quantum Electron. 9, pp 1533-1540
[8] Gleim A V, Anisimov A A et al. 2014 Bulletin of the Russian Academy of Sciences. Physics, Vol 78, No 3, pp 171–175
[9] Mora J, Ruiz-Alba A, Amaya W, Martínez A, García-Muñoz V, Calvo D and Capmany J 2012 Optics Letters Vol 37, No 11
[10] G.N Gol’tsman, O. Okunev, et al. 2001 App. Phys. Lett., 79 (6), P. 705-707