Heterodyne-based subcarrier wave quantum cryptography under the chromatic dispersion impact

R. K. Goncharov[1], A. V. Zinovev[1], F. D. Kiselev[1,2], E. O. Samsonov[1,2]

[1]St. Petersburg National Research ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia
[2]Quanttelecom LLC, Vasilievsky island, 6 Line, 59, St. Petersburg, 199178, Russia

eosamsonov@itmo.ru, rkgoncharov@itmo.ru

In this paper, we investigate the effect of chromatic dispersion on a continuous variable quantum key distribution system with heterodyne detection, in which information is encoded in the sidebands of modulated laser radiation. We consider the system in which a balanced detector output is downconverted to an intermediate frequency and propose a non-standard methods of dispersion compensation using RF phase shifters.

Keywords: heterodyne detection, subcarrier wave, quantum key distribution, chromatic dispersion.

1. Introduction

Rapidly evolving quantum technologies bring a threat to most of the contemporary cryptography protocols, since quantum computers are able to solve several tasks such as factorization remarkably faster than classical ones [1]. This fact explains the emerging interest in the field of quantum key distribution (QKD), which is the only known method of transfer of cryptographic keys in real time with an unconditional security. It was established in 1984 by seminal work of Brassard and Bennett [2].

There exists two major approaches to quantum key distribution: discrete-variable (DV) QKD and continuous-variable (CV) QKD. The essence of CV-QKD is the detection of signal quadratures of a coherent state [3–11]. Such protocols are appealing since its practical implementations can be manufactured from off-the-shelf components [12–14].

This paper describes a CV-QKD protocol based on subcarrier wave (SCW) modulation method. In SCW QKD protocols [15–20] multimode weak coherent states are generated by electro-optic phase modulation. As a result, sideband spectrum is formed with its phase, relative to the initial carrier field, containing the quantum information [21–23] (detailed descriptions of SCW DV-QKD and CV-QKD protocols can be found in [15] and [20], respectively). The main advantages of SCW QKD are the simplification of the phase shift matching between Alice and Bob and lack of complex interference schemes and efficient usage of the channel's bandwidth. It was shown that such method is suitable both for DV-QKD and CV-QKD. Detection scheme extracts information from coherent multimode states in a way similar to classical heterodyning. Feasibility and advantages of such scheme is fully described in [24].

However, this method is extremely prone to the chromatic dispersion, since in this case each sideband in the channel undergoes a different phase shift depending on the frequency. Its influence on SCW DV-QKD and possible ways to reduce the negative impact were examined in [25].

In this paper, we investigate the dispersion influence on the proposed scheme. We suggest a numerical model that takes dispersion of the optical fiber channel into account. We demonstrate the main feature of introduced scheme, which is the ability to compensate the difference between phase shifts of different subcarrier modes.

This paper is organized as follows. In Section 2, we describe suggested scheme, using plain classical model. In Section 3 dispersion influence on the protocol is discussed. In this paper, we consider only a simple analytical dispersion model of the SCW QKD protocol.

2. Proposed scheme

Here, we describe a scheme for SCW QKD, based on the method of coherent detection [24]. The main advantage of the method lies in the simultaneous detection of two quadrature components without the need for two balanced detectors and double homodyning. It is worth noting that proposed scheme has not only the advantage of detecting both of the quadratures, but also has only passive optical components on the receiver's side. Hence, such scheme is both affordable and easy to adjust.

Let us describe the BB84-like SCW CV-QKD protocol first (Fig. 1). Alice emits coherent pulses with a laser (1), then they get modulated with a phase modulator (2) and attenuated (3) in order to achieve a single-photon level of energy at the sidebands. Bob receives the signal and uses a low frequencies filter (5) to pass a half of central frequency and positive sidebands to the first arm of the balanced detector (6) and uses circulator (4) to send the second part of the central frequency and negative sidebands to the second arm of detector.
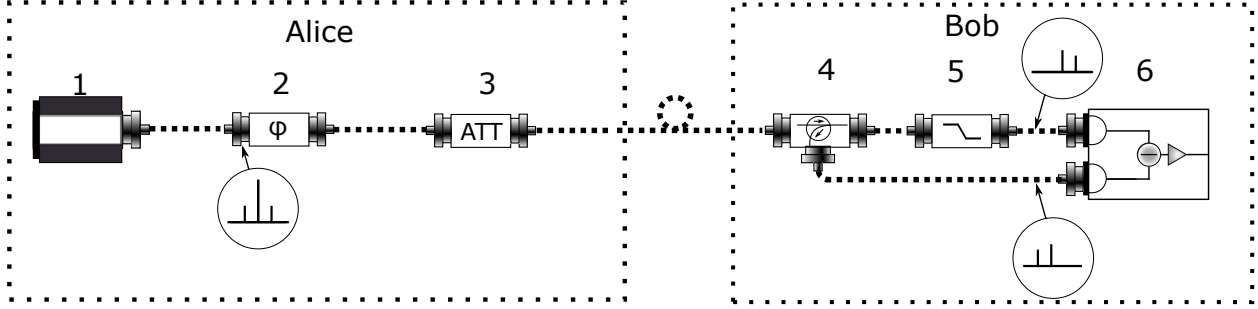

FIG. 1. Proposed SCW detection scheme. 1 – laser, 2 – phase modulator, 3 – attenuator, 4 – circulator, 5 – low frequency filter, 6 – balanced detector. Diagrams in circles show the simplified power spectrum.

We can obtain the expressions for the incident fields for both arms of the balanced detector before detection as:

$$E_1(t) = E_0 e^{i\omega t} \left(\sum_{k=1}^{\infty} i^k J_k(m_a) e^{ik(\Omega t + \phi_a)} + \sqrt{0.5} J_0(m_a) \right), \tag{1}$$

$$E_2(t) = E_0 e^{i\omega t} \left(\sum_{k=1}^{\infty} i^k J_k(m_a) e^{-ik(\Omega t + \phi_a)} + \sqrt{0.5} J_0(m_a) \right), \tag{2}$$

where J_k is the k-order Bessel function of the first kind, m_a is the modulation index, which is typically smaller than unity.

The output of the balanced detector can be written as [24]:

$$\begin{aligned} I(t) &= R(\lambda) G C \left(|E_1(t)|^2 - |E_2(t)|^2 \right) \\ &= R(\lambda) G C \left(2\sqrt{2} E_0^2 J_0(m_a) J_1(m_a) \sin(\Omega t + \phi_a) \right). \end{aligned} \tag{3}$$

where $R(\lambda)$ is the responsivity of photodiodes, G is the electronic gain of the photodetector and $C = S/2\xi$ is the ratio of the effective beam area S and the doubled impedance ξ of the medium.

Turns out that the resulting signal detected by Bob has exactly the same frequency as the modulating signal, while the phase is shifted by $90°$.

The resulting output, as one may see on Fig. 2, has the sinusoidal form. The most exiting feature of this oscillation is that it contains full information about the phase chosen by Alice. The possibility of extraction of this phase was experimentally proven in [24]. Hence, such detecting technique allows one to measure both quadratures simultaneously. However, a conflict between spectral filtering and the detector's bandwidth emerges here. To obtain the phase information correctly, the bandwidth of a balanced detector should be equal or more than Ω. Therefore, one may find themselves at the crossroads choosing the optimal Ω for practical implementation of the system. On the one hand, rise of modulation frequency causes the increase of required detector's bandwidth, which leads to additional electronic noises. Typical balanced detectors' bandwidth used for quantum measurements is less than 1 GHz. On the other hand, decrease of modulation frequency complicates the spectral filtering.

It is important to note that within last years there were several works dedicated to balanced detectors for quantum measurements with a bandwidth of several GHz. Kleis et al. [26] applied deep learning methods to adjust a CV-QKD system for the noises emerging from the expanding of the bandwidth. As the result, they have achieved a 9.2 Mbit/s key rate for a fiber line of 26 km. Huang and al. [27] reported about 1 Mbps secure key rate over 25 km of optical fiber. One major implementation that allowed us to achieve such results was the balanced detector with the bandwidth of 1 GHz. Hence, the development of wideband balanced detectors suitable for quantum measurements will remove the main obstacle for practical implementation of the scheme proposed in this paper.

Usage of these highly-sensitive and wideband balanced detectors in the scheme would allow us to successfully bring to life a system with several major advantages. First, the receiver's side has no active optical elements, which
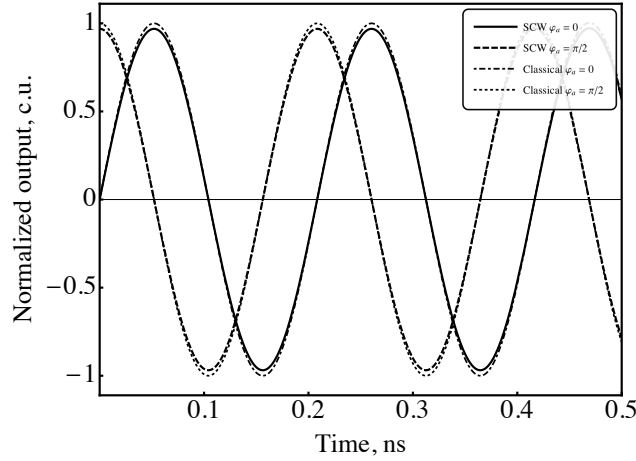
FIG. 2. Time dependence of the normalized heterodyne-derived signals for the SCW and the classical detection schemes. For the sake of thoroughness, two different phase shifts are depicted.

significantly enlarges the robustness and usability of the method. The lack of second phase modulator (which presence is fairly common for most of the SCW QKD schemes) also positively boosts the affordability of the system. Moreover, since the detector measure both quadratures, there is no need to shift the key. In addition, such system will be also resistant to the influence of chromatic dispersion, which is discussed in the next section.

3. Dispersion effects in the SCW CV-QKD

The influence of chromatic dispersion on the DV-SCW system was investigated in [25]. There was shown that SCW QKD systems are prone to the influence of the chromatic dispersion. The worst part of it is that for certain fiber lengths quantum key distribution is fundamentally impossible without any dispersion compensation.

One of the methods of mitigating the dispersion influence, proposed in [25], is to send only one half of the spectrum to the channel. In the case of QKD with coherent detection, one have to carry out classical heterodyning via spectral filter and beam splitter. Another method to reduce the dispersion effect is using a dispersion compensation module. Both methods increase the attenuation in optical channel, which is extremely undesirable for QKD system. Another downside is that such elements are expensive, what nullify affordability as one of the CV QKD system's major advantage.

Here we propose the system which is resistant to the chromatic dispersion influence. Let us begin from the description of the dispersion mathematical model for the system. Dependence of the propagation constant of the fundamental mode in single-mode optical fibers on wavelength can be represented as Taylor series within the vicinity of some wavelength [28]:

$$\beta(\omega) \approx \beta_0 + \beta_1 \Delta\omega + \frac{\beta_2}{2}\Delta\omega^2 + \frac{\beta_3}{6}\Delta\omega^3, \tag{4}$$

where $\delta\omega = \omega - \omega_0$.

Proposed protocol fits in the frame of such description since the both sidebands are situated spectrally close to the carrier band. Then, within the framework of the description, the central frequency ω is the frequency of the carrier mode. Taking into account the first two orders in the Eq. (4), the phase shift of the sidebands, depending on the fiber length L, can be calculated as follows:

$$\Phi_+ = \left(\beta_1 + \frac{\beta_2}{2}\Omega\right)\Omega L \tag{5}$$

for the "right" subcarrier and:

$$\Phi_- = -\left(\beta_1 - \frac{\beta_2}{2}\Omega\right)\Omega L \tag{6}$$

for the "left" subcarrier.

According to [28] the β-parameters can be calculated as:

$$\beta_1 = 1/v_g, \tag{7}$$

$$\beta_2 = -\frac{D\lambda^2}{2\pi c}, \tag{8}$$

where v_g is a group velocity, D is a dispersion parameter, λ is a wavelength, and c is a velocity of light. For the SMF-28e fiber that was also used in [25], $\beta_1 = 4.8964 \cdot 10^{-6}$ s/km and $\beta_2 = -2.0407 \cdot 10^{-23}$ s^2/km.

While such model is an analytical simplification, taking into account only two sidebands, in [25] it was extensively investigated in the context of its application to SCW QKD; the results were also compared with the results obtained by numeric solution of the nonlinear Schrodinger equation.

Now let us write the simplified expressions for the electric fields considering the dispersion phase shifts:

$$E_1(t) \approx E_0 \left(iJ_1(m_a)e^{i((\omega+\Omega)t+\phi_a+\Phi_+)} + \sqrt{0.5}J_0(m_a)e^{i\omega t} \right), \tag{9}$$

$$E_2(t) \approx E_0 \left(iJ_1(m_a)e^{i((\omega-\Omega)t-\phi_a+\Phi_-)} + \sqrt{0.5}J_0(m_a)e^{i\omega t} \right). \tag{10}$$

Mimicking the way of obtaining the expression for the balanced detector output (3), we obtain:

$$I(t) \sim$$
$$\sqrt{2}J_1(m_a)J_0(m_a)\Big(\sin(\Omega t + \varphi_a + \Phi_+) + \sin(\Omega t + \varphi_a - \Phi_-) \Big)$$
$$= 2\sqrt{2}J_0(m_a)J_1(m_a) \sin\left(\Omega t + \varphi + \frac{\Phi_+ - \Phi_-}{2} \right) \cos\left(\frac{\Phi_+ + \Phi_-}{2} \right). \tag{11}$$

Obviously, for the observed sine function, the term $\dfrac{\Phi_+ - \Phi_-}{2} = \beta_1\Omega L$ introduces only an additional phase shift, which can be easily compensated. However, the external cosine factor affects the output's visibility which, disregarding chromatic dispersion, is equal to one in the considered lossless scenario. Therefore we express it as follows:

$$V = \left| \cos\left(\frac{\Phi_+ + \Phi_-}{2} \right) \right| = |\cos(\beta_2\Omega^2 L/2)|. \tag{12}$$

In case of the $L\beta_2\Omega^2/2 = \pi k/2$ with $k \in \mathbb{Z}$, visibility will always be zero, thus, it would be impossible to generate a secure key without any compensation of the dispersion effects. As is seen from Fig. 3 and Fig. 4, the visibility, as well as the detector output, drops to zero at the distance of 169.25 km, in case of SMF-28e fiber usage.
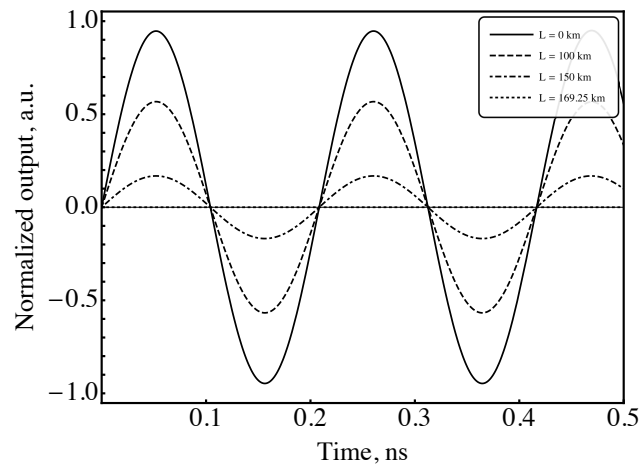

FIG. 3. Balanced detector output under the chromatic dispersion influence. The distance is fixed at certain values.

Such signal degradation greatly reduces the potential of practical implementation. Since the key rate would decrease along with the visibility of the signal, a successful dispersion compensation is exceptionally important milestone on the way of implementation of this scheme.
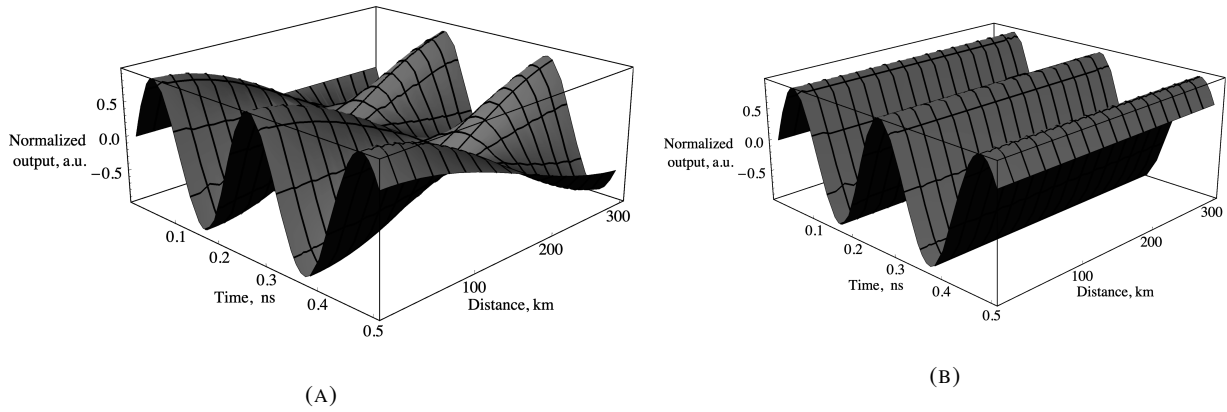
(A)   (B)

FIG. 4. Balanced detector output with a full dispersion compensation.

The best way to compensate dispersion effect for the proposed scheme is to install a RF phase shifter to one arm of the balanced detector, after photodiodes [29]. To completely mitigate the distorting influence of the chromatic dispersion, we propose to shift the phase in the upper arm by a known value $-(\Phi_- + \Phi_+)$ (or by $(\Phi_- + \Phi_+)$ in the lower arm) in order to achieve the same common phase in both arms that can be compensated afterwards [30]. This result can be represented graphically, as in Fig. 4b.

4. Conclusion

We have considered an analytical model of chromatic dispersion for the case of subcarrier wave quantum cryptography system with heterodyne detection. Due to the phase matching requirement in the proposed scheme, dispersion has a significant negative impact on the detector output. However, with a usage of RF electrical phase shifters and oscilloscope adjustment, one can fully compensate phase deviation between balanced detector arms. In future works, this can be implemented experimentally, as well as with a cohesive QKD security proof in terms of quantum model.

Acknowledgements

Conflict of interest

The authors declare no conflicts of interest.

References

[1] Pirandola S., Andersen U.L., et al. Advances in quantum cryptography. *Advances in Optics and Photonics*, 2020, **12** (4), P. 1012–1236.
[2] Bennett C., Brassard G. Quantum cryptography: public key distribution and coin tossing. *Proceedings of "IEEE International Conference on Computers, Systems and Signal"*, Bangalore, India, IEEE, 1984, P. 175–179.
[3] Lo H.-K., Curty M., Tamaki K. Secure quantum key distribution. *Nature Photonics*, 2014, **8** (8), P. 595–604.
[4] Ralph T.C. Continuous variable quantum cryptography. *Physical Review A*, 1999, **61** (1), 010303.
[5] Grosshans F., Van Assche G., et al. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 2003, **421** (6920), P. 238–241.
[6] Hirano T., Yamanaka H., et al. Quantum cryptography using pulsed homodyne detection. *Physical Review A*, 2003, **68** (4), 042331.
[7] Leverrier A., Grangier P. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Physical Review A*, 2011, **83** (4), 042312.
[8] Heid M., Lütkenhaus N. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Physical Review A*, 2006, **73** (5), 052316.
[9] Brádler K., Weedbrook C. Security proof of continuous-variable quantum key distribution using three coherent states. *Physical Review A*, 2018, **97** (2), 022310.
[10] Papanastasiou P., Lupo C. , Weedbrook C. , Pirandola S. Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels. *Physical Review A*, 2018, **98** (1), 012340.
[11] Lin J., Upadhyaya T., Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Physical Review X*, 2019, **9** (4), 041064.
[12] Comandar L.C., Brunner H.H., et al. A flexible continuous-variable QKD system using off-the-shelf components. *Quantum Information Science and Technology III*, 2018, **10442**, P. 37–43.
[13] Wang H., Pi Y., et al. High-speed gaussian-modulated continuous-variable quantum key distribution with a local oscillator based on pilot-tone-assisted phase compensation. *Optics Express*, 2020, **28** (22), P. 32882–32893.

[14] Fossier S., Diamanti E., et al. Field test of a continuous-variable quantum key distribution prototype. *New Journal of Physics*, 2009, **11** (4), 045023.

[15] Gleim A.V., Egorov V.I., et al. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. *Optics Express*, 2016, **24** (3), P. 2619–2619.

[16] Miroshnichenko G.P., Kozubov A.V., et al. Security of subcarrier wave quantum key distribution against the collective beam-splitting attack. *Optics Express*, 2018, **26** (9), P. 11292–11308.

[17] Kynev S.M., Chistyakov V.V., et al. Free-space subcarrier wave quantum communication. *Journal of Physics: Conference Series*, 2017, **917**, 052003.

[18] Merolla J.-M., Mazurenko Y., et al. Phase-modulation transmission system for quantum cryptography. *Optics Letters*, 1999, **24** (2), P. 104–106.

[19] Chistiakov V., Kozubov A., et al. Feasibility of twin-field quantum key distribution based on multi-mode coherent phase-coded states. *Optics Express*, 2019, **27** (25), P. 36551–36561.

[20] Samsonov E., Goncharov R., et al. Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis. *Scientific Reports*, 2020, **10** (1), P. 1–9.

[21] Miroshnichenko G.P., Kiselev A.D., Trifanov A.I., Gleim A.V. Algebraic approach to electro-optic modulation of light: exactly solvable multimode quantum model. *Journal of the Optical Society of America B*, 2017, **34** (6), P. 1177–1190.

[22] Capmany J., Fernández-Pousa C.R. Quantum model for electro-optical phase modulation. *Journal of the Optical Society of America B*, 2010, **27** (6), A119–A129.

[23] Kumar P., Prabhakar A. Evolution of quantum states in an electro-optic phase modulator. *IEEE journal of quantum electronics*, 2008, **45** (2), P. 149–156.

[24] Samsonov E., Goncharov R., et al. Coherent detection schemes for subcarrier wave continuous variable quantum key distribution. ArXiv:2006.16543, 2020.

[25] Kiselev F., Samsonov E., et al. Analysis of the chromatic dispersion effect on the subcarrier wave QKD system. *Optics Express*, 2020, **28** (19), P. 28696–28712.

[26] Kleis S., Rueckmann M., Schaeffer C.G. Continuous-variable quantum key distribution with a real local oscillator and without auxiliary signals. ArXiv:1908.03625, 2019.

[27] Huang D., Lin D.,et al. Continuous-variable quantum key distribution with 1 Mbps secure key rate. *Optics Express*, 2015, **23** (13), P. 17511–17519.

[28] Agrawal G.P. *Fiber-optic communication systems*. John Wiley & Sons, Hoboken, 2012, 626 p.

[29] Horowitz P., Hill W. *The art of electronics*. Cambridge University Press, Cambridge, 1989, 1220 p.

[30] Xinyi T. Broadband phase shifter design for phased array radar systems. PhD Thesis, National University of Singapore, 2011.