Subcarrier wave continuous-variable quantum key distribution with Gaussian modulation: composable security analysis

R.K. Goncharov [1], A.D. Kiselev [1,2], E.O. Samsonov [1], V.I. Egorov [1]
[1] ITMO University, Leading Research Center "National Center of Quantum Internet",
199034, Saint Petersburg, Russia, Birzhevaya Line 16;
[2] ITMO University, Laboratory of Quantum Processes and Measurements,
199034, Saint Petersburg, Russia, Kadetskaya Line 3

Abstract

In this paper, we continue the study of the quantum cryptographic GG02 protocol, performed using the approach based on the subcarrier waves. We modify the scheme via heterodyne detection and perform security analysis for the full trusted hardware noise model in the presence of collective attacks with finite-key effects. It is shown that the system can potentially distribute the key even if the level of losses in the channel is above 9 dB. This result is consistent with the general technical level and comply with modern standards of practical CV-QKD systems. Finally, the system under consideration fully meets the criterion of composability.

Keywords: continuous variables, subcarrier waves, quantum key distribution.

Citation: Goncharov RK, Kiselev AD, Samsonov EO, Egorov VI. Subcarrier wave continuous-variable quantum key distribution with Gaussian modulation: composable security analysis. Computer Optics 2023; 47(3): 374-380. DOI: 10.18287/2412-6179-CO-1225.

Introduction

Quantum Key Distribution (QKD) [1] allows two (Alice and Bob) or more legitimate parties to exchange symmetric cryptographic (secure) keys. The essence of the method is to encode the classical information into quantum states and use an authentic classical communication channel for key processing.

Theoretically, owing to the laws of quantum mechanics, QKD can be regarded as a reliable tool for distribution of unconditionally secure keys that cannot be intercepted by a third party (Eve). In practice, of course, the necessary technical clarifications are required. Importantly, the latter includes imperfections of the hardware used, whereas the equipment employed by an adversary is assumed to be perfect.

All the QKD protocols can be divided into two groups: the protocols using discrete variables (DV) [2] and the protocols using continuous variables (CV) [3]. One of the key differences between these two groups is the detection system: the DV-QKD systems use single-photon detectors, whereas the CV-QKD ones employ coherent receivers. The latter are implemented with balanced detectors used in classical fiber-optic communication systems, not technically complex and expensive single photon detectors. It also means that due to the designated standardization of optical equipment, CV-QKD can be more successfully integrated into the telecommunications infrastructure.

Both approaches are quite diverse in the implementation and can be built on a variety of methods for encoding and decoding the information. One of these methods is the subcarrier wave method (SCW) where phase modulation is applied to encode information into the phases of subcarrier modes of weak multimode coherent states [4, 5]. This method has a number of advantages. In particular, it does not require an additional reference signal (the reference is provided by the carrier wave on the central frequency) and it provides a versatile means for multiplexing purposes [6, 7, 8]. This approach has been demonstrated to be effective in implementations of DV-QKD in the fiber communication lines [9, 10] and in the free-space QKD [11]. In this paper, we are primarily concerned with the SCW implementation of CV-QKD protocols introduced in our previous studies [12, 13, 14].

We are aimed to expand the framework of the SCW method in the context of Gaussian modulation (GG02) CV-QKD protocol [3]. This protocol is notable for the presence of a theoretical base in terms of security proof in exact analytical form. At the moment, it is also the only point-to-point CV-QKD protocol that has been proven to be secure against general attacks in the regime of finite keys [1]. For this purpose, it is essential to fill the gaps in the security model discussed in [14] by supplementing it with proof against collective attacks and taking in to account finite-key effects. Our key result is the finite secure key rate of the SCW CV-QKD protocol evaluated as a result of the security analysis that meets the criterion of composability. The composability criterion naturally came from classical cryptography to quantum key distribution [1]. The main idea of composable security is to define an ideal protocol and use it as a reference against which an existing realistic implementation can be compared. The problem can be formulated as a game played by a so-called "distinguisher" whose task is to guess whether Alice and Bob implement the real protocol or the ideal protocol. Thus, the criterion can be formed as follows: $D\left(\rho_{\mathrm{ABE}}, \tilde{\rho}_{\mathrm{ABE}}\right) \leq \varepsilon$, where $D(\cdot, \cdot)$ is a trace distance, ρ_{ABE} denotes the tripartite quantum state held by a distinguisher interacting with the real system and $\tilde{\rho}_{\mathrm{ABE}}$

is the ideal where the registers "A" and "B" keep the final messages, and the register "E" only holds the state ρ_E resulting from an attack and attempts to steal the key. In the ideal case, there is no correlation between the register "E" and the pair of legitimate users' registers "AB". It is also necessary to take in to account the finiteness of the samples and the finiteness of the output keys, which require appropriate corrections (finite-key effects mentioned above). In simpler, but unrealistic, asymptotic regime with infinite keys, such corrections are omitted.

There are also several newly introduced effects. In particular, we show that in order to meet the symmetrization requirements of the described protocol [15] the detection scheme has to be changed homodyne to heterodyne. Another important point incorporated into our security analysis is that the trusted and untrusted noise and losses are explicitly separated. By trusted noise, we mean the noise that cannot be controlled by Eve. In turn, the so-called untrusted noise adjusted by Eve occurs exclusively in the quantum channel. The same applies to the losses: there are trusted losses that are set by the legitimate parties' equipment and remain outside the access of Eve, while losses in the channel (untrusted) Eve can completely simulate.

The paper is organized as follows. In section 1, we describe the GG02 protocol based on the SCW method and its modifications. In section 2, we provide the security analysis and evaluate the performance of the protocol. In section 3, we discuss our results and make concluding remarks.

1. Gaussian modulation and detection using SCW

1.1. CV-QKD protocol

Fig. 1 presents a scheme of our setup where the SCW system is used to implement the GG02 protocol. In this setup, the laser on the Alice side generates pulses of duration T with the power P and the frequency ω_0 at the specified rate. So, the input state is $\left|\sqrt{\mu_0}\right\rangle_0 \otimes \left|vac\right\rangle_{sb}$, where $|vac\rangle_{sb}$ indicates the vacuum state of the subcarrier modes and $\left|\sqrt{\mu_0}\right\rangle_0$ is the coherent state describing the radiation at the central frequency with the mean photon number $\mu_0 = |\alpha_0|^2 = PT/\hbar\omega_0$ ($\hbar$ is the Planck constant).

In order to perform Gaussian modulation of the input state as required by the GG02 protocol Alice utilizes the electro-optic phase modulator. In the phase modulation process, the modulation index m_A is assumed to be a small random variable governed by the Rayleigh probability distribution with the scale parameter $\sqrt{V_A}$, whereas the phase φ_A is uniformly distributed in the range from zero to 2π.

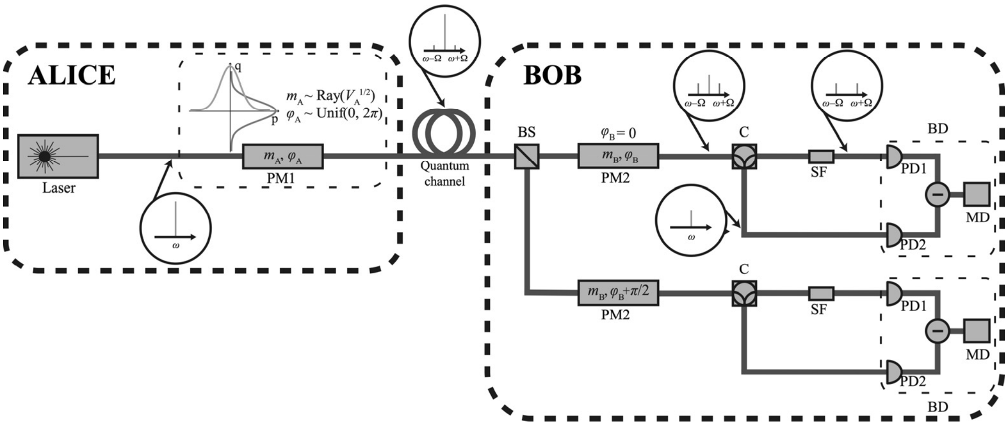

Fig. 1. Simplified scheme of SCW CV-QKD GG02 setup. PM is the electro-optic phase modulator; C is the circulator; SF is the spectral filter that cuts off the carrier; BD is the balanced detector; PD is the photodiode; MD is the measurement device. Diagrams in the Alice's block illustrate the quadrature distributions

An accurate theoretical treatment of this process requires using a quantum model of the phase modulator. There is a number of differently formulated models put forward in [16, 17, 18, 19]. Our subsequent calculations are based on the model developed in [18].

According to this model, there are $2S+1$ interacting frequency modes with frequencies $\omega_0 + k\Omega$, where k is the integer ranged from $-S$ to S, and the multimode coherent state

$$\left|\psi(\varphi)\right\rangle = \bigotimes_{k=-S}^{S} \left|\alpha_k(\varphi_A)\right\rangle_k, \tag{1}$$

with the amplitudes

$$\alpha_k(\varphi_A) = \sqrt{\mu_0}\, d_{0k}^S(\beta_A) \exp(-i\varphi_A k), \tag{2}$$

represents the modulated output state, where $d_{0k}^S(\beta_A)$ is the Wigner d-function [20]. In the limiting case with $S \to \infty$, the latter can be simplified as follows

$$d_{nk}^S(\beta_A) \underset{S\to\infty}{\to} J_{n-k}(m_A), \tag{3}$$

where $J_{n-k}(m_A)$ is the Bessel function of the first kind. This approximation is valid for the real SCW QKD systems [18, 10] in which standard fiber electro-optical modulators are used. It is generally accepted that standard fiber phase modulators (e.g. Thorlabs LN53S-FC) have sufficiently large values of output modes S [10] for the approximation to be valid.

Since the modulation index, m_A, is small, we have

$$J_{|k|}\left(m_{\mathrm{A}}\right) \approx \frac{1}{|k|!}\left(\frac{m_{\mathrm{A}}}{2}\right)^{|k|}, \qquad (4)$$

and the probability density function for the complex amplitudes of the first-order sidebands with $k \pm 1$ is given by the normal distribution with vanishing mean value and the variance V_{A}. Note that the vacuum noise must be taken in to account and the resulting variance that enter the covariance matrix will be $V = V_{\mathrm{A}} + 1$ in shot noise units (SNU).

In the bulk of previous studies, the above modulation procedure is carried out using two (amplitude and phase) modulators [21, 22, 23]. The subcarrier multiplexing technique with several phase modulators was also theoretically studied in [24] using the classical approach to phase modulation.

The modulated signal passes through the Gaussian quantum channel [25] with the transmittance T and the excess noise ξ to the Bob side. This side implements the coherent detection procedure described in [13, 12]. It implies that Bob uses two modulators with the modulation index optimized for detection tasks of the SCW method ($m_{\mathrm{B}} \approx 1.13$ in [13]). For the modulators in the first and second arms, he sets the values of the phase $\varphi_{\mathrm{B}} = 0$ and $\varphi_{\mathrm{B}} = \pi/2$, respectively, thereby detecting both quadratures (in Fig. 1 p and q, respectively). Phase remodulation results in redistribution of the energy leading to a significant increase in the sidebands power. Information encoded into the transmitted signal is determined by the energy difference between the sidebands and the carrier wave.

After the remodulation, the carrier wave and the sidebands are separated by spectral filtering and are collected by photodiodes placed in the arms of balanced detector. The photocurrents registered by the photodetectors are subtracted. At the output of the balanced detector, Bob receives valid values correlated with those prepared by Alice. The next involves the standard procedures of parameter estimation, error correction, and privacy amplification [1].

Considering that we use the trusted hardware noise model, it is necessary to divide the scheme into blocks in order to clarify which noises they contain:

- trusted preparation (Alice) noise ξ_{prep} (e.g., relative intensity noise and noise of digital-to-analog converter);
- untrusted quantum channel noise ξ_{ch} (e.g., Raman noise if the quantum channel is wavelength-multiplexed with a classical one);
- trusted receiver (Bob) noise ξ_{rec} (e.g., balanced detector noise).

It is usually assumed that various noise sources are independent of each other, so their variances are added to the total (separately trusted and untrusted) values. Various losses are distributed over the same blocks (Alice, channel, Bob).

It should be emphasized that, by contrast to the previous version of the method [14], the scheme is modified so as to utilize the heterodyne detection [26]. This modification is essential for subsequent security analysis as it allows us to incorporate the symmetry needed for discussing general attacks. The possibility to achieve a security against general attacks was shown using the recently proposed Gaussian de Finetti reduction approach to the GG02 protocol [15] that employs its invariance with respect the unitary group rather than the symmetric group. The matrix chosen from the unitary group describes the passive linear transformation through the transformation of the annihilation operators. In practice, this translates into applying a certain kind of permutation to classical data, given the quadrature pairs of Alice and Bob. A random choice of one quadrature per state (so-called "sifting") during homodyning leads to the information loss and breaks down the symmetry making impossible to apply the described analogy between classical data and quantum states. This means that, at the current state, it is impossible to analytically prove the security of CV-QKD protocol with homodyne detection against general attacks.

1.2. Peculiarities of SCW approach

There are two differences between the SCW approach and the standard method (see, e.g., [25, 27, 28]) that we need to take in to account [14]: a drop in the efficiency of the coherent detection scheme that results in reduction of the total trusted transmittance and the sideband-induced additional contributions to the channel excess noise.

The efficiency of the SCW coherent detection scheme is given by the following expression [13]

$$\eta_{\mathrm{SCW}} = \frac{1 - 4J_0^2\left(m\right) + 4J_0^4\left(m\right)}{4J_0^2\left(m_{\mathrm{A}}\right)\left(1 - J_0^2\left(m_{\mathrm{A}}\right)\right)}, \qquad (5)$$

where $m = m_{\mathrm{A}} + m_{\mathrm{B}}$. As is shown in [14], averaging over the Alice's modulation index m_{A} gives the expected value of the efficiency $\langle \eta_{\mathrm{SCW}} \rangle \approx 0.9$ that corresponds to the insertion loss of about 0.5 dB.

Following the reasoning presented in [14] additional excess noise originated from high-order ($k \geq 2$) sidebands can be written in the form

$$\xi_{\mathrm{SCW}} = 2\pi \sum_{k=2}^{\infty} \int_0^{\infty} dx \frac{1}{(2^k k!)^2} \left(\frac{x^{2k+1} \exp(-\dfrac{x^2}{2V_A^2})}{V_A} \right). \qquad (6)$$

Fig. 2 presents the dependence of the excess noise (6) on the scale parameter $V_{\mathrm{A}}^{1/2}$. It turned out that the values of ξ_{SCW} are of the same order as small contributions to the excess noise such as the relative intensity noise (RIN) and the noise of digital-to-analog-converter reported in Ref. [29].

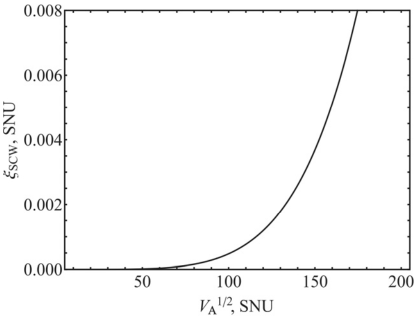

Fig. 2. Dependence of the excess noise ξ_{SCW} induced by the high-order sidebands on the scale parameter $\sqrt{V_A}$ set on the electro-optic modulator

2. Security analysis

2.1. Asymptotic security

In this section, we, following Refs. [30, 31], use the trusted noise scenario and obtain an accurate estimate of the Holevo bound [32] using an appropriately modified covariance matrix.

The theoretical study of the GG02 security, by analogy with some DV-QKD protocols, is based on the concept of the virtual entanglement [33]. According to this concept, the event of sending a single-mode coherent state to the Gaussian quantum channel by Alice and the subsequent detection by Bob is completely analogous to the event in which modes of the two-mode squeezed vacuum state (TMSVS) are distributed between the legitimate users. Both events are described by the same covariance matrix up to some constants. In the considered trusted noise scenario, Eve can manipulate only the state in the channel, and purify it there. This means that the state of the system must be considered through three separate subsystems [31]: Alice (sender), Eve (adversary that may control the parameters of the channel), and Bob (receiver).

In the SCW protocol, independent first-order sidebands are considered as separate single-mode states containing the same information [18, 24, 14].

The mutual information between Alice and Bob can be calculated as follows [29]

$$I_{\mathrm{AB}} = \frac{\mu}{2}\log_2(1+\mathrm{SNR}) = \frac{\mu}{2}\log_2\left(1+\frac{\frac{1}{\mu}TV_{\mathrm{A}}}{1+\frac{1}{\mu}\xi}\right), \tag{7}$$

where $\mu\in\{1,2\}$ is the homo-/heterodyning parameter, SNR is the signal-to-noise ratio, T is the total transmittance, and ξ is the amount of total excess noise.

Since the GG02 protocol uses Gaussian quantum channel and Gaussian modulated states, the optimal attack is known to be Gaussian [34, 35]. In this case, the Holevo bound can be estimated as follows

$$\chi_{\mathrm{EB}} \equiv S_{\mathrm{E}} - S_{\mathrm{E|B}}, \tag{8}$$

$$S = \sum_i \left(\frac{v_i+1}{2}\log_2\left(\frac{v_i+1}{2}\right) - \frac{v_i-1}{2}\log_2\left(\frac{v_i-1}{2}\right)\right), \tag{9}$$

where S is the von Neumann entropy and v_i is the symplectic eigenvalue of the corresponding covariance matrix. Subscripts show predestination: "A" stands for Alice, "B" stands for Bob, and "E" stands for Eve. Vertical bar determines the conditionality of entropy and sets the case after the measurement.

Assuming that the Bob side is fully trusted, T_{rec} and ξ_{rec} are out of Eve's reach. The symplectic eigenvalues of the covariance matrix before Bob's measurement (it is needed to calculate the von Neumann entropy S_{E}) are

$$\begin{aligned} v_{1,2} = \frac{1}{2}(&\sqrt{(V+T_{\mathrm{ch}}(V-1)+1+\xi_{\mathrm{ch}})^2-4T_{\mathrm{ch}}(V^2-1)} \pm \\ &\pm\left(T_{\mathrm{ch}}(V-1)+1+\xi_{\mathrm{ch}}-V\right)), \end{aligned} \tag{10}$$

where $V = V_{\mathrm{A}}+1$.

The conditional von Neumann entropy $S_{\mathrm{E|B}}$ that determines Eve's information after the measurement on the Bob side is estimated via the following symplectic eigenvalues

$$v_{3,4} = \frac{\sqrt{(e_1+e_3)^2-4e_2^2} \pm (e_3-e_1)}{2(TV_A/\mu+1+\xi/\mu+1)}, \tag{11}$$

$$\begin{aligned} e_1 = &V\left(\left(1-T_{\mathrm{rec}}\right)W_{\mathrm{rec}}+T_{\mathrm{rec}}W_{\mathrm{ch}}+1\right)+ \\ &+T_{\mathrm{ch}}\left(W_{\mathrm{ch}}-V\right)\left(1+\left(1-T_{\mathrm{rec}}\right)W_{\mathrm{rec}}\right), \end{aligned} \tag{12}$$

$$e_2 = \sqrt{T_{\mathrm{ch}}\left(W_{\mathrm{ch}}^2-1\right)}\left(T_{\mathrm{rec}}V+\left(1-T_{\mathrm{rec}}\right)W_{\mathrm{rec}}+1\right), \tag{13}$$

$$e_3 = \left(1-T_{\mathrm{rec}}\right)W_{\mathrm{ch}}W_{\mathrm{rec}}+T_{\mathrm{rec}}T_{\mathrm{ch}}\left(VW_{\mathrm{ch}}-1\right)+T_{\mathrm{rec}}+W_{\mathrm{ch}}, \tag{14}$$

where $W_{\mathrm{ch}} = \xi_{\mathrm{ch}}/(1-T_{\mathrm{ch}})+1$, $W_{\mathrm{rec}} = \xi_{\mathrm{rec}}/(1-T_{\mathrm{rec}})+1$, and T_{det} is the transmittance responsible for losses and the detector's efficiency in the receiver module. For SCW coherent detection method, the parameter T_{det} that enter Eqs. (11–14) should be replaced by the rescaled value given by

$$T'_{\mathrm{det}} = T_{\mathrm{det}}\left\langle \eta_{\mathrm{SCW}} \right\rangle. \tag{15}$$

Note that it is possible to introduce the model of trusted sender's (Alice) noise can be introduced using substitution V with $V+\xi_{\mathrm{pr}}$, where ξ_{pr} is the preparation excess noise [31]. It is however, demonstrated in [29] that the value of such noise is negligibly small. Losses T_{pr} in Alice's block can be neglected, since she can always adjust the necessary attenuation.

According to the Devetak-Winter bound [36], the asymptotic secure key fraction is

$$r_{\mathrm{coll}}^{\mathrm{asympt}} \geq \left(1-\mathrm{FER}\right)\left(\beta I_{\mathrm{AB}}-\chi_{\mathrm{EB}}\right), \tag{16}$$

where FER is the frame error rate and β is the reverse reconciliation efficiency. Our next step is to consider the finite-key effects.

2.2. Finite-key effects and composable security

In order to take into account the finite-key effects and the composability criterion in the presence of collective attacks, we refine the secure key fraction bound using the result of Refs. [37, 38, 39, 40] that reads

$$r_{\text{coll}}^{\text{finite}} \geq \frac{n(1-\text{FER})}{n_{\text{states}}}\left(\beta I_{\text{AB}}(w)-\chi_{\text{EB}}(w)-\frac{\Delta_{AEP}}{\sqrt{n}}+\frac{\Theta}{n}\right), \quad (17)$$

$$\Delta_{\text{AEP}} = 4\log_2(2\sqrt{d}+1)\sqrt{\log_2\left(\frac{18}{(1-FER)^2\varepsilon_s^4}\right)}, \quad (18)$$

$$\Theta = \log_2\left[(1-\text{FER})(1-\varepsilon_{\text{s}}^2/3)\right]+2\log_2\sqrt{2}\varepsilon_{\text{h}}, \quad (19)$$

$$\varepsilon = 2(1-\text{FER})\varepsilon_{\text{pe}}+\varepsilon_{\text{cor}}+\varepsilon_{\text{s}}+\varepsilon_{\text{h}}, \quad (20)$$

where n is the number of symbols left to process the finite key, n_{states} is the number of states, Δ_{AEP} is the parameter according to the asymptotic equipartition property [41], Θ combines the hash mismatch accounting after the privacy amplification and the error correction leak [37, 38], d is the effective alphabet size. ε_j is the security parameter defining the tolerance for the security of the procedures being carried out and the composability of the QKD protocol: ε_{pe} is responsible for accuracy of the parameter estimation from a finite sample, ε_{cor} is an upper bound on the probability that strings are different after passing error correction procedure, ε_{S} shows the allowable fluctuation of errors in the channel, and ε_{S} is a parameter of the applied hash function. In real QKD systems ε-parameters are selected based on the security requirements set out in the relevant documents.

Also, given the finiteness of the available sample for parameter estimation, it is necessary to introduce additional corrections related to the confidence intervals. These corrections are given by [42, 37]

$$\text{Corr}_{\xi,j} = w\frac{\xi_j+\mu}{\sqrt{2\mu n_{pe}}}, \quad (21)$$

$$\text{Corr}_{T,j} = 2w\xi_j/V_{\text{A}}\sqrt{T_j/(\mu n_{\text{pe}})}, \quad (22)$$

where subscript j indicate the QKD block (Alice's preparation, Bob's receiver, channel), $w=\sqrt{2\ln(1/\varepsilon_{\text{pe}})}$ is the confidence [37], and n_{pe} is the number of states for parameter estimation.

According to Ref. [37], the above corrections are implemented into the trusted noise scenario through the following substitutions:

$$T_{\text{det}}^{'} \rightarrow T_{\text{det}}^{'}+\text{Corr}_{T,\text{full}}, \quad (23)$$

$$T_{\text{ch}} \rightarrow T_{\text{ch}}-\text{Corr}_{T,\text{ch}}, \quad (24)$$

$$\xi_{\text{ch}} \rightarrow \xi_{\text{ch}}+\text{Corr}_{\xi,\text{ch}}. \quad (25)$$

In our numerical calculations, we have used the following parameters: $\mu=2$; $V_{\text{A}}=6$; $T_{\text{ch}}=10^{-\zeta L}$, where L is the channel length and ζ is the attenuation in dB/km; $\xi_{\text{ch,standart}}=0.003T_{\text{ch}}$, $\xi_{\text{ch,SCW}}=0.0031T_{\text{ch}}$, $\xi_{\text{rec}}=0.1$, $T_{\text{det}}=10^{-0.725}$, $\text{FER}=0.03$, $\beta=0.95$, $n=2\cdot10^8$, $n_{\text{states}}=6\cdot10^8$, $d=2^4$, $\varepsilon_{\text{s}}=\varepsilon_{\text{h}}=10^{-10}$, $\varepsilon=5.6\cdot10^{-9}$, $n_{\text{pe}}=6\cdot10^7$, $w=6.34$. The parameters are taken in accordance with the general technical level and comply with modern trends of practical CV-QKD systems [1, 27, 28, 29, 31, 37, 38].

The results for the performance of both the SCW CV-QKD system and the standard GG02 protocol computed from Eq. (17) are presented in Fig. 3. It can be seen that the difference between the limiting channel losses (under which the secure key fraction is still positive) for the standard and the SCW based GG02 protocols is about 0.5 dB and its level cannot be regarded as critical.

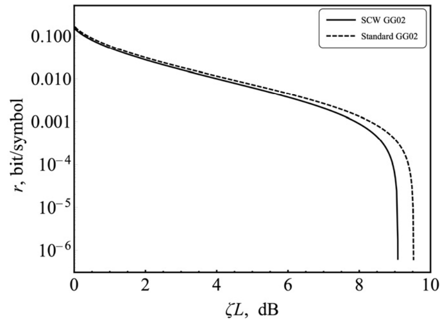

Fig. 3. Dependence of the secure key fraction on the losses in the fiber quantum channel

Another point is that the performance of SCW CV-QKD appears to be significantly improved as compared to the results reported in our previous study [14]. The latter is mainly due to the suitably modified trusted noise model in which the Holevo information decreases much faster than the mutual information with legitimate users' insertion losses.

Conclusion

We have analyzed the security and performance of the GG02 protocol in the implementation through the SCW approach. We have shown that the differences from the standard approach are insignificant and substantiated security against collective attacks with the composability criterion and the finite-key effects taken in to account. The enhanced detection system allows to subsequently generalize the given analysis to the case of general attacks using the available symmetrization. As far as the merits of the SCW method briefly mentioned in Introduction are concerned, our concluding remark is that they will potentially far outweigh a slight performance hit we have demonstrated.

Acknowledgements

The work was done by Leading Research Center "National Center for Quantum Internet" of ITMO University by order of JSCo Russian Railways.

References

[1] Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira JL, Razavi M, Shamsul Shaari J, Tomamichel M, Usenko VC, Vallone G, Villoresi P, Wallden P. Advances in quantum cryptography. Adv Opt Photonics 2020; 12(4): 1012. DOI: 10.1364/AOP.361502.

[2] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Theor Comput Sci 2014; 560: 7-11. DOI: 10.1016/j.tcs.2014.05.025.

[3] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using gaussian-modulated coherent states. Nature 2003; 421(6920): 238-241. DOI: 10.1038/nature01289.

[4] Merolla J-M, Mazurenko YT, Goedgebuer J-P, Duraffourg L, Porte H, Rhodes WT. Quantum cryptographic device using single-photon phase modulation. Physical Review A 1999; 60(3): 1899. DOI: 10.1103/PhysRevA.60.1899.

[5] Merolla J-M, Mazurenko Y, Goedgebuer J-P, Rhodes WT. Single-photon interference in sidebands of phase-modulated light for quantum cryptography. Phys Rev Lett 1999; 82(8): 1656. DOI: 10.1103/PhysRevLett.82.1656.

[6] Ortigosa-Blanch A, Capmany J. Subcarrier multiplexing optical quantum key distribution. Phys Rev A 2006; 73: 024305. DOI: 10.1103/PhysRevA.73.024305.

[7] Mora J, Ruiz-Alba A, Amaya W, Martínez A, García-Muñoz V, Calvo D, Capmany J. Experimental demonstration of subcarrier multiplexed quantum key distribution system. Opt Lett 2012; 37(11): 2031-2033. DOI: 10.1364/OL.37.002031.

[8] Mora J, Amaya W, Ruiz-Alba A, Martinez A, Calvo D, Muñoz VG, Capmany J. Simultaneous transmission of 20x2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON. Opt Express 2012; 20(15): 16358-16365. DOI: 10.1364/OE.20.016358.

[9] Gleim AV, Egorov VI, Nazarov YV, Smirnov SV, Chistyakov VV, Bannik OI, Anisimov AA, Kynev SM, Ivanova AE, Collins RJ, Kozlov SA, Buller GS. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. Opt Express 2016; 24(3): 2619-2633. DOI: 10.1364/OE.24.002619.

[10] Miroshnichenko GP, Kozubov AV, Gaidash AA, Gleim AV, Horoshko DB. Security of subcarrier wave quantum key distribution against the collective beam-splitting attack. Opt Express 2018; 26(9): 11292-11308. DOI: 10.1364/OE.26.011292.

[11] Kynev S, Chistyakov V, Smirnov S, Volkova K, Egorov V, Gleim A. Free-space subcarrier wave quantum communication. J Phys Conf Ser 2017; 917: 052003. DOI: 10.1088/1742-6596/917/5/052003.

[12] Samsonov E, Goncharov R, Gaidash A, Kozubov A, Egorov V, Gleim A. Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis. Sci Rep 2020; 10(1): 10034. DOI: 10.1038/s41598-020-66948-0.

[13] Samsonov E, Goncharov R, Fadeev M, Zinoviev A, Kirichenko D, Nasedkin B, Kiselev AD, Egorov V. Coherent detection schemes for subcarrier wave continuous variable quantum key distribution. J Opt Soc Am B 2021; 38(7): 2215-2222. DOI: 10.1364/JOSAB.424516.

[14] Goncharov R, Samsonov E, Kiselev AD. Subcarrier wave quantum key distribution system with gaussian modulation. J Phys Conf Ser 2021; 2103(1): 012169. DOI: 10.1088/1742-6596/2103/1/012169.

[15] Leverrier A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. Phys Rev Lett 2017; 118(20): 200501. DOI: 10.1103/PhysRevLett.118.200501.

[16] Kumar P, Prabhakar A. Evolution of quantum states in an electro-optic phase modulator. IEEE J Quantum Electron 2008; 45(2): 149-156. DOI: 10.1109/JQE.2008.2002673.

[17] Capmany J, Fernández-Pousa CR. Quantum model for electro-optical phase modulation. J Opt Soc Am B 2010; 27(6): A119-A129. DOI: 10.1364/JOSAB.27.00A119.

[18] Miroshnichenko GP, Kiselev AD, Trifanov AI, Gleim AV. Algebraic approach to electro-optic modulation of light: exactly solvable multimode quantum model. J Opt Soc Am B 2017; 34(6): 1177-1190. DOI: 10.1364/JOSAB.34.001177.

[19] Horoshko D, Eskandary M, Kilin SY. Quantum model for traveling-wave electro-optical phase modulator. J Opt Soc Am B 2018; 35(11): (2018) 2744-2753. DOI: 10.1364/JOSAB.35.002744.

[20] Varshalovich DA, Moskalev AN, Khersonskii VK. Quantum theory of angular momentum. World Scientific Publishing Co Pte Ltd; 1988.

[21] Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett 2002; 88(5): 057902. DOI: 10.1103/PhysRevLett.88.057902.

[22] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat Photonics 2013; 7(5): 378-381. DOI: 10.1038/nphoton.2013.63.

[23] Diamanti E, Leverrier A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. Entropy 2015; 17(9): 6072-6092. DOI: 10.3390/e17096072.

[24] Fang J, Huang P, Zeng G. Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation. Phys Rev A 2014; 89(2): 022315. DOI: 10.1103/PhysRevA.89.022315.

[25] Weedbrook C, Pirandola S, García-Patrón R, Cerf NJ, Ralph TC, Shapiro JH, Lloyd S. Gaussian quantum information. Rev Mod Phys 2012; 84(2): 621-669. DOI: 10.1103/RevModPhys.84.621.

[26] Weedbrook C, Lance AM, Bowen WP, Symul T, Ralph TC, Lam PK. Quantum cryptography without switching, Phys Rev Lett 2004; 93(17): 170504. DOI: 10.1103/PhysRevLett.93.170504.

[27] Jouguet P, Kunz-Jacques S, Leverrier A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. Phys Rev A 2011; 84(6): 062317. DOI: 10.1103/PhysRevA.84.

[28] Jain N, Chin H-M, Mani H, et al. Practical continuous-variable quantum key distribution with composable security. Nat Commun 2022; 13(1): 4740. DOI: 10.1038/s41467-022-32161-y.

[29] Laudenbach F, Pacher C, Fung C-HF, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P, Hübel H. Continuous-variable quantum key distribution with gaussian modulation–The theory of practical implementations. Adv Quantum Technol 2018; 1(1): 1800011. DOI: 10.1002/qute.201800011.

[30] Usenko V, Filip R. Trusted noise in continuous-variable quantum key distribution: A threat and a defense. Entropy 2016; 18(1): 20. DOI: 10.3390/e18010020.

[31] Laudenbach F, Pacher C. Analysis of the trusted-device scenario in continuous-variable quantum key distribution. Adv Quantum Technol 2019; 2(11): 1900055. DOI: 10.1002/qute.201900055.

[32] Holevo AS. Bounds for the quantity of information transmitted by a quantum communication channel. Problemy Peredachi Informatsii 1973; 9(3): 3-11.

[33] Grosshans F, Cerf NJ, Wenger J, Tualle-Brouri R, Grangier P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quantum Inf Comput 2003; 3(7): 535-552. DOI: 10.5555/2011564.2011570.

[34] Navascués M, Grosshans F, Acín A. Optimality of Gaussian attacks in continuous-variable quantum

cryptography. Phys Rev Lett 2006; 97(19): 190502. DOI: 10.1103/PhysRevLett.97.190502.

[35] García-Patrón R, Cerf NJ. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys Rev Lett 2006; 97(19): 190503. DOI: 10.1103/PhysRevLett.97.190503.

[36] Devetak I, Winter A. Distillation of secret key and entanglement from quantum states. Proc Math Phys Eng Sci 2005; 461(2053): 207-235. DOI: 10.1098/rspa.2004.1372.

[37] Pirandola S. Limits and security of free-space quantum communications. Phys Rev Res 2021; 3(1): 013279. DOI: 10.1103/PhysRevResearch.3.013279.

[38] Pirandola S. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. Phys Rev Res 2021; 3(4): 043014. DOI: 10.1103/PhysRevResearch.3.043014.

[39] Leverrier A. Composable security proof for continuous-variable quantum key distribution with coherent states. Phys Rev Lett 2015; 114(7): 070501. DOI: 10.1103/PhysRevLett.114.070501.

[40] Leverrier A, Grosshans F, Grangier P. Finite-size analysis of a continuous-variable quantum key distribution. Phys Rev A 2010; 81(6): 062343. DOI: 10.1103/PhysRevA.81.062343.

[41] Tomamichel M, Colbeck R, Renner R. A fully quantum asymptotic equipartition property. IEEE Trans Inf Theory 2009; 55(12): 5840-5847. DOI: 10.1109/TIT.2009.2032797.

[42] Goncharov RK, Kiselev AD, Samsonov EO, Egorov VI. Continuous-variable quantum key distribution: security analysis with trusted hardware noise against general attacks. Nanosystems: Physics, Chemistry, Mathematics 2022; 13(4): 372-391. DOI: 10.17586/2220-8054-2022-13-4-372-391.

Authors' information

Roman Konstantinovich Goncharov, Bachelor of Science, Engineer at ITMO University. Research interests are quantum cryptography, quantum optics, and quantum computing. E-mail: *rkgoncharov@itmo.ru* .

Alexei Donislavovich Kiselev, DSc, PhD, Professor at ITMO University. Research interests are theoretical physics, mathematical physics, optical physics, optics and photonics. E-mail: *alexei.d.kiselev@gmail.com* .

Eduard Olegovich Samsonov, PhD, Leading Researcher at ITMO University. Research interests are quantum cryptography, quantum optics, and quantum computing. E-mail: *eosamsonov@itmo.ru* .

Vladimir Ilyich Egorov, PhD, Deputy Director of National Center for Quantum Internet at ITMO University. Research interests are quantum cryptography and quantum networks. E-mail: *viegorov@itmo.ru* .

Code of State Categories Scientific and Technical Information: 29.31.01.
Received September 14, 2022. The final version – December 14, 2022.