Subcarrier wave quantum key distribution system with gaussian modulation

R Goncharov, E Samsonov and A D Kiselev
ITMO University, Saint-Petersburg 197101, Russia
E-mail: rgoncharov@itmo.ru

Abstract. The aim of the paper is to describe a well-known quantum key distribution GG02 protocol using multimode coherent states generated on subcarrier frequencies of the optical spectrum. In order to detect signal states, we use a method of coherent detection without the participation of a local oscillator directly but where power from a carrier wave is used as such. Within the framework of the modern GG02 protocol description and the security proof against collective attacks, we introduce the necessary amendments to reduce our model to a model of the common system.

1. Introduction
Quantum key distribution (QKD) is a method of sharing symmetric cryptographic keys between two parties (Alice and Bob) that is based on encoding information in the states of quantum objects and subsequent distillation of the key through a classical communication channel. Since QKD directly derives from the no-cloning theorem, an attacker (Eve) does not have the ability to intercept information without consequences. The first quantum cryptography protocols exploited the quantum system with a finite degrees of freedoms [1]. Such protocols are called discrete variable QKD (DV-QKD) protocols, and they are studied to a greater extent than those that will be discussed later. In experimental applications, DV-QKD requires single-photon detectors.

In turn, continuous-variable QKD (CV-QKD), which was proposed later, relies on methods of coherent detection for gaining information about the quantum states. The most famous and well-studied protocol in the framework of theoretical analysis is undoubtedly the GG02 protocol [2], which uses Gaussian modulated coherent states.

One of the notable techniques based on subcarrier wave (SCW) generation [3] can also be successfully applied in the context of the CV-QKD [4]. A defining property of SCW QKD is the method for quantum state encoding, where a strong monochromatic wave emitted by a laser is modulated in an electro-optic phase modulator to produce weak sidebands.

In SCW CV-QKD GG02 protocol described in this work, Alice prepares coherent multimode states where the first-order sidebands are Gaussian modulated, and Bob performs coherent detection to establish correlations with Alice.

Our aim in this work is to use a model of GG02 protocol to provide its analogy in the context of SCW and show the possibility of performing the performance analysis taking into account the peculiarities of the used approach.
2. SCW GG02 protocol
A simplified scheme of a SCW system based on the GG02 protocol is shown in Figure 1. An Alice’s laser generates pulses of constant duration at a specified rate. Next, the process of electro-optic phase modulation is carried out in which a small modulation index $m_A$ varies according to the Rayleigh distribution of the constant parameter $\sqrt{V_A}$, and the phase $\varphi_A$ is selected in accordance with the uniform distribution. It is easy to show that the output distribution of the first-order sidebands will correspond to a Gaussian distribution with zero mean and variance $V_A$ in the linear approximation of a small modulation index.

![Figure 1. Schematic diagram of SCW CV-QKD GG02 setup. PM is an electro-optic phase modulator; C is a circulator; SF is a spectral filter that cuts off the carrier; BD is a balanced detector. PD is a photodiode; MD is a measurement device. Diagrams in Alice’s block show the quadrature distributions.](image)

In most of the works, the described procedure is carried out using two (amplitude and phase) modulators [5, 6, 7]. The approach with a usage of only the phase modulation, in turn, was proposed earlier in [8]. Vacuum noise must be taken into account, so the resulting variance will be $V = V_A + 1$ in shot noise units (SNU).

Then the resultant signal passes through a Gaussian quantum channel with a transmittance $T$ and excess noise $\xi$ to the Bob’s module, which implements the coherent detection procedure described earlier in [9, 4]. That is, Bob uses a much larger modulation index ($m_B \approx 1.13$ in [9]), and randomly selects the phase $\varphi_B$ from the set $\{0, \pi/2\}$, thereby defining the measured quadrature (in Figure 1 $p$ and $q$, respectively). As a result of energy redistribution due to phase re-modulation, the sidebands power is greatly increased and information about the sent signal will be contained in the energy difference between the sidebands and the residual carrier wave. Further, by methods of spectral filtering, the separation of the carrier wave and side components and balanced detection are carried out. At the output of the balanced detector, Bob receives valid values correlated with those prepared by Alice. Next, the standard procedures of error correction and privacy amplification [10] are carried out.

3. Mathematical model
3.1. The efficiency of SCW coherent detection scheme
As a result of direct comparison of the schemes of classical homodyning and SCW coherent detection, it was calculated [9] that the latter is slightly less efficient. In this context, “classical homodyning” means that the amplitude of the signal is $\sqrt{1 - J_0^2(m_A)}$, and the amplitude of the local oscillator is $J_0(m_A)$. The results of comparison are shown in Figure 2.
3.2. Additional excess noise due to high-order sidebands

The excess noise itself can be detected through the Alice’s side, or through the Bob’s one. It turns out the following relation

\[ \xi := \xi_B = T\xi_A, \]

where \( \xi_A \) is an Alice’s excess noise, and \( \xi_B \) refers to Bob.

In general, excess noise includes the noise variances (in SNU) of all possible sources

\[ \xi = \xi_{\text{modul}} + \xi_{\text{Raman}} + \xi_{\text{quant}} + \xi_{\text{phase}} + \xi_{\text{det}} + \xi_{\text{RIN}} + \xi_{\text{CMRR}} + \cdots, \]

where \( \xi_{\text{modul}} \) is a modulation noise, \( \xi_{\text{Raman}} \) is a Raman noise, \( \xi_{\text{quant}} \) is a quantization noise, \( \xi_{\text{phase}} \) is a noise of phase fluctuation, \( \xi_{\text{det}} \) is a detection noise, \( \xi_{\text{RIN}} \) is a power fluctuation noise, and \( \xi_{\text{CMRR}} \) is a noise caused by imperfect common-mode rejection ratio of the balanced detector. The values of the above parameters are calculated in detail in [11]. Here, a new quantity is considered, which is fundamentally important for the system under consideration.

It is known from the general quantum model of the electro-optic modulator [12] that the output amplitudes of the sidebands are described by Wigner’s \( d \)-functions, or, in the asymptotic approximation, by Bessel functions. The main approximation used in the considered protocol is

\[ J_k(m) \approx \frac{1}{k!} \left( \frac{m}{2} \right)^k, \]
where $k$ is an integer mode index.

The relation above shows that the Rayleigh distribution (provided that $m_A$ corresponds to it) will only satisfy the sidebands with the index $k = \pm 1$. For this reason, high-order sidebands with unsatisfactory distributions should be taken into account in the excess noise term in Eq. (3). For this, it is necessary to calculate the SNU variances of the distributions of the high-order sidebands ($|k| \geq 2$). Thus, we can write

$$\xi_{SCW} = 2 \sum_{k=2}^{\infty} \left[ \int_{0}^{\infty} dx \frac{1}{(2^k k!)^2} \left( \frac{x^{2k+1} e^{-\frac{x^2}{2V_A^2}}}{V_A} \right) \int_{0}^{2\pi} d\varphi \cos^2 (k \varphi) - \left( \int_{0}^{\infty} dx \frac{1}{2^k k!} \left( \frac{x^{k+1} e^{-\frac{x^2}{2V_A^2}}}{V_A} \right) \int_{0}^{2\pi} d\varphi \cos (k \varphi) \right)^2 \right] = 2 \pi \sum_{k=2}^{\infty} \int_{0}^{\infty} dx \frac{1}{(2^k k!)^2} \left( \frac{x^{2k+1} e^{-\frac{x^2}{2V_A^2}}}{V_A} \right).$$

The integral can be taken numerically, and the series converges. From Figure 3 it can be seen that the dependence is nonlinear.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig3}
\caption{Dependence of the values of the excess noise caused by the high-order sidebands on the Rayleigh distribution parameter set on the electro-optic modulator.}
\end{figure}

4. Security analysis

The theoretical study of GG02 security, by analogy with some DV-QKD protocols, is based on the concept of virtual entanglement [13]. According to it, the event in which Alice sends a single-mode coherent state to the Gaussian quantum channel and 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, and both events are described by the same the same covariance matrix up to some constants.
In the considered SCW protocol, one should take into account the fact that in general only the tensor product over a finite number of modes \[12\] is considered without mode intersections, so, by analogy with \[8\], each sideband can be considered as a separate quantum channel. Considering that only the first-order \((k = \pm 1)\) sidebands are informative, and that upper and lower ones carry the same information, we can reduce the covariance matrices estimation to the single-mode case. Consideration of two matrices for each of the two sidebands separately will be also reduced to it. In this case, the security analysis against collective attacks in the asymptotic mode are already known \[11\] adjusted for for the fundamental lack of SCW detection scheme efficiency and additional noise from high-order sidebands.

In this paper, the so-called "trusted detector noise scenario" \[14\] is considered, that is, for example, the noise of a balanced detector, its efficiency (not to be confused with the \(\eta_{\text{hom}}\) above), etc. will not be taken into account in Holevo information estimation. So, the covariance matrix of TMSVS is then

\[
\Sigma_{AB} = \begin{pmatrix}
\sqrt{V_2} & \sqrt{T_{\text{ch}}(V^2 - 1)}
\end{pmatrix}
\begin{pmatrix}
\sigma_z \\
(T_{\text{ch}}[V - 1] + 1 + \xi_{\text{ch}})
\end{pmatrix}\begin{pmatrix}
\sqrt{V_2} \\
\sqrt{T_{\text{ch}}(V^2 - 1)}
\end{pmatrix},
\]

where \(T_{\text{ch}}\eta_{\text{hom}} = T\), \(1_2\) is an identity operator, \(\sigma_z\) is a Pauli z-matrix, and \(\xi_{\text{ch}} \equiv \xi\) is an excess noise without taking into account the noise on the receiver’s side.

In the considered case, Holevo information is assessed as

\[
\chi_{EB} = S_E - S_{E|B} = S_{AB} - S_{A|B},
\]

where \(S\) is a von Neumann entropy.

That is, the evaluation is carried out directly from the described "Alice-Bob" covariance matrix. The von Neumann entropy of Gaussian state is described in terms of a symplectic eigenvalues of the covariance matrix \(\Sigma\), which are the absolute values of the eigenvalues of 
\[
\tilde{\Sigma} = i\Omega \Sigma \ [15].
\]

The secure key generation rate of is estimated from the signal-to-noise ratio (mutual information) and Holevo information with corrections for the efficiency of post-processing \[11\]. That is, in terms of key fraction we have

\[
r = (1 - \text{FER})(1 - v)(\beta I_{AB} - \chi_{EB}) = (1 - \text{FER})(1 - v) \left( \frac{\beta \mu}{2} \log_2 \left( 1 + \frac{1}{\mu} T V_A \right) + \frac{1}{\mu} \frac{\xi}{\xi_T} \right) - \chi_{EB},
\]

where FER is a frame-error rate, \(\beta\) is a post-processing efficiency, \(v\) is the key fraction disclosed for parameter estimation, \(\mu \in \{1, 2\}\) is a parameter of homo/heterodyne detection.

For a simplified representation, we set FER = 0, \(v = 0\). In this case, the plot of the key fraction \(r\) is shown in the Figure \[1\]. Other parameters are as follows: \(\beta = 0.96, V_A = 6, T_{\text{ch}} = 10^{-0.02L}, \xi = 0.02 T_{\text{ch}}\).

5. Conclusion

We have provided the analogy of the well-known GG02 protocol using SCW method, took into account the losses caused by the method, analyzed the additional noise and calculated the secure key rate against collective attacks in the asymptotic regime. Our calculation shows that the SCW QKD system allows to provide a secret key for channel losses up to 30 km. We hope that the foundation has been created from which further, more comprehensive security proofs will come as well as experiment implementations.
Figure 4. Dependence of the key fraction on the length of a fiber channel with specified losses.

Acknowledgments
This work was financially supported by Government of Russian Federation (grant MK-777.2020.8).

References
[1] Bennett C H and Brassard G 2014 Theor. Comput. Sci. 560 7
[2] Grosshans F, Van Assche G, Wenger J, Brouil R, Cerf N J and Grangier P 2003 Nature 421 238
[3] Gleim A V, Egorov V I, Nazarov Y V, Smirnov S V, Chistyakov V V, Bannik O I, Anisimov A A, Kynev S M, Ivanova A E, Collins R J, Kozlov S A and Buller G S 2016 Opt. Express 24 2619
[4] Samsonov E, Goncharov R, Gaidash A, Kozubov A, Egorov V and Gleim A 2020 Sci. Rep. 10 10034
[5] Grosshans F and Grangier P 2002 Phys. Rev. Lett. 88 057902
[6] Jouguet P, Kunz-Jacques S and Diamanti E 2013 Phys. Rev. A 87 062313
[7] Diamanti E and Leverrier A 2015 Entropy 17 6072
[8] Fang J, Huang P and Zeng G 2014 Phys. Rev. A 89 022315
[9] Samsonov E, Goncharov R, Fadeev M, Zinoviev A, Kirichenko D, Nasedkin B, Kiselev A D and Egorov V 2021 J. Opt. Soc. Am. B 38 2215
[10] Pirandola S, Andersen U, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira J, Razavi M, Shamsul Shaari J, Tomamichel M, Usenko V, Vallone G, Villoresi P and Wallden P 2020 Adv. Opt. Photon. 12 1012
[11] Laidenbach F, Pacher C, Fung C H F, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P and Hubel H 2018 Adv. Quantum Technol. 1 1800011
[12] Miroshnichenko G P, Kiselev A D, Trifanov A I and Gleim A V 2017 J. Opt. Soc. Am. B 34 1177
[13] Grosshans F, Cerf N J, Weng J, Tualle-Brouil R and Grangier P 2003 Quantum. Inf. Comput. 3 535–552
[14] Usenko V C and Filip R 2016 Entropy 18 20
[15] Serafini A 2017 Quantum continuous variables: A primer of theoretical methods (Boca Raton, FL: CRC Press, Taylor & Francis Group)