Security of subcarrier wave quantum key distribution against the collective beam-splitting attack

A. V. Kozubov,1 A. A. Gaidash,1 A. V. Gleim,1 G. P. Miroshnichenko,1 and D. B. Horoshko2,3

1Department of Photonics and Optical Information Technology, ITMO University, Saint Petersburg, Russia
2Univ. Lille, CNRS, UMR 8523, Physique des Lasers Atomes et Molecules (PhLAM), F-59000 Lille, France
3B. I. Stepanov Institute of Physics, NASB, Nezavisimosti Avenue 68, Minsk 220072, Belarus

(Dated: July 16, 2018)

We consider a subcarrier wave quantum key distribution (QKD) system, where the quantum encoding is carried by weak sidebands generated to a coherent optical beam by means of an electro-optic phase modulation. We study the security of two protocols, B92 and BB84, against one of the most powerful attacks on the systems of this class: the collective beam splitting attack. We show that a subcarrier wave QKD system with realistic parameters is capable of distributing a cryptographic key over large distances. We show also that a modification of the BB84 protocol, with discrimination of only one state in each basis, performs not worse than the original BB84 protocol for this class of QKD systems, which brings a significant simplification to the development of cryptographic networks on the basis of considered technique.

PACS numbers: 03.67.Dd., 03.67.Hk

I. INTRODUCTION

Growing interest to the quantum key distribution (QKD) systems [1,2,3,4] in the last decades has led to emergence of a large number of experimental works dedicated to the development of reliable QKD setups suitable for everyday operation in existing telecommunication networks. Among them stand subcarrier wave (SCW) QKD systems, the most valuable feature of which is exceptionally efficient use of the quantum channel bandwidth and capability of signal multiplexing by adding independent sets of quantum subcarriers to the same carrier wave. It makes SCW QKD systems perfect candidates as backbone of multiuser quantum networks.

In the SCW QKD system a strong monochromatic wave, produced by a laser, is modulated to produce weak sidebands whose phase with respect to the strong coherent wave encodes the quantum information. Various protocols can be realized with this technique, the most popular ones being the BB84 protocol [4], using four phase values, and the B92 protocol [5], using just two phases. A realization of the B92 protocol with phase modulation has been demonstrated by Merolla group [6,7]. A realization of the BB84 protocol has been demonstrated by the same group with the help of amplitude rather than phase modulators [8]; the replacement of the phase modulation by a more technically complicated amplitude modulation being necessary for decoding all the states of the protocol at the side of receiver. The latter approach, combined with the employment of several microwave frequencies in the amplitude modulators by the technique of subcarrier multiplexing resulted recently in a significant increase of the key generation rate [9]. It was shown [10] that monitoring the intensity of the strong wave can provide additional security to the protocol, being a realization of the method of “strong reference” [5], suggested in the early days of quantum cryptography for fighting the most dangerous attacks, and proven recently to provide unconditional security for QKD with weak coherent states [11]. A variant of the BB84 protocol with phase modulation, allowing the receiver to decode only one of the two states in each basis, has been recently realized by some of us [12].

Notwithstanding the large experimental effort for building SCW QKD systems, the analysis of their security still requires special consideration. In this article we explore the security of the B92 and BB84 protocols against one but very powerful attack: the collective beam-splitting (CBS) attack. We analyse this attack and calculate the secure key generation rate for given protocols in its presence. The CBS attack is not limited by the employment of the strong reference, thus the obtained result is quite general and remains valid even for strong-reference-enhanced versions of the protocols. We show also that the secure key generation rate for the BB84 protocol with one state decoding (BB84-OSD) is the same as for BB84 with both states decoded, which allows the developers of the QKD networks to employ a relatively simple phase modulation in the future.

Our calculation of the secure key rate is based on the well-known Devetak-Winter bound [2,13], applicable to the case of collective attacks in one-way protocols of QKD with independent identically distributed information carriers, to which the considered protocols of SCW QKD belong. We employ the recently developed quantum model of electro-optical phase modulation [14], which allows us to deduce the states of sidebands in the quantum channel after the modulation, and their states after the demodulation before the detection. This model has an advantage of being applicable in the case of relatively high modulation index, where tens of sidebands contain non-negligible amount of photons.
This paper is organized as follows. Section II gives a description of the protocols implemented in SCW QKD device and builds the model of the quantum channel. In Section III we calculate the quantum bit error rate as function of loss in the quantum channel, which take into consideration the quantum efficiency and the dark count rate of the photodetector. In Section IV we consider the attacks on the protocols and in Section V we find the secure key rate dependence on the channel length for different sets of SCW QKD parameters. Section VI concludes the article.

II. OPERATION PRINCIPLES OF SCW QKD

A. The setup and the protocols

We consider two protocols of SCW QKD sharing the same experimental setup, which is schematically shown in Fig. 1. The laser source produces a coherent monochromatic light beam with the optical frequency $\omega$, serving as the carrier wave of the setup. The sender Alice modulates this beam by means of a travelling-wave phase modulator, with the frequency of the microwave field $\Omega$ and its phase $\varphi_A$. As a result of phase modulation, the field at the output of the modulator acquires sidebands at frequencies $\omega_k = \omega + k\Omega$, where we limit ourselves to 25 sidebands and let the integer $k$ to run in the limits $-S \leq k \leq S$. The modulation index and the intensity of the carrier wave are chosen so that the total number of photons in the sidebands is less than unity, thus providing non-orthogonality of the used set of states, required by the no-cloning theorem, lying in the heart of the QKD security. The phase $\varphi_A$ is constant in a transmission window of duration $T$, but changes randomly within a predefined set in the next window. The value of this phase is written on the relative phase between the sidebands and the carrier wave, and thus encodes the bit, sent by Alice. In this article we consider two protocols, differing by the set of phases, used by Alice. The B92 [5] protocol employs only two non-orthogonal states and $\varphi_A \in \{0, \pi\}$, encoding the logical 0 and 1 respectively. The BB84 protocol [4] uses four states, split in two bases: $\varphi_A \in \{0, \pi\}$ corresponds to the basis 0, while $\varphi_A \in \{\pi/2, 3\pi/2\}$ corresponds to the basis 1, the first state of each basis encoding the logical 0, and the second one encoding the logical 1. In both protocols the carrier wave propagates together with the sidebands and can serve as “strong reference”, which was suggested for B92 protocol by its author Bennett [5], and can be extended to the BB84 protocol by analogy. Monitoring the power of the strong reference helps to fight the attacks employing measurement of the quantum carriers in the quantum channel and suppression of them in the case of unfavorable outcome, like the photon number splitting (PNS) attack and the unambiguous state discrimination (USD) attack. However, in the present article we do not consider the additional enhancement of security provided by the strong reference method, leaving it to a separate study.

The encoded states together with the carrier wave are sent to the receiver Bob, who applies a similar phase modulation to the received beam with the microwave phase $\varphi_B$ in each transmission window, and then directs all the sidebands to a single-photon detector (SPD). The set of phases used by Bob is the same as that of Alice in both protocols. The decoding is based on the fact, that each time Alice and Bob use different phases from the same set $\{0, \pi\}$ or $\{\pi/2, 3\pi/2\}$, so that $\varphi_A - \varphi_B = \pm \pi$, the sidebands after the Bob’s modulator are in the vacuum state and the SPD produces no click, except for dark counts. In the B92 protocol Bob decodes a bit value in the transmission windows where his SPD clicks, and this value corresponds to his phase $\varphi_B$. In the BB84-OSD protocol Bob waits while Alice announces the bases used for each bit by a public channel, and then decodes the bit value in the transmission windows where he used the same basis and where his SPD clicked, this value again corresponding to his phase $\varphi_B$. In this protocol Bob decodes only one state of the basis. For example, if Alice uses $\varphi_A = 0$, Bob decodes this bit only if he uses the phase $\varphi_B = 0$. The phase $\varphi_B = \pi$, however belonging to the same basis, does not result (in the ideal case) in a click of Bob’s detector. We show in Sec. V that this modification of the BB84 protocol does not affect the secure key generation rate.

B. The secure key generation rate

The described above protocols belong to the class of one-way protocols of QKD with independent identically distributed information carriers [2]. The secure key generation rate $K$ for the protocols of this class in the presence of collective attacks is lower bounded by the Devetak-Winter bound [2, 13]:

$$K = \nu_S P_B \left[ 1 - \text{leak}_{EC}(Q) - \max_E \chi(A : E) \right], \quad (1)$$
where $\nu_S$ is the repetition rate, in our case $\nu_S = T^{-1}$; $P_B$ is the probability of successful decoding and accepting a bit in one transmission window; $Q$ is the quantum bit error rate (QBER), the probability that a bit, accepted by Bob is erroneous; $\text{leak}_{EC}(Q)$ is the amount of information revealed by Alice by the public channel for the sake of the error correction, which depends on QBER and is limited by the Shannon bound: $\text{leak}_{EC}(Q) \geq h(Q)$, where $h(Q) = -Q \log_2 Q - (1 - Q) \log_2(1 - Q)$ is the binary Shannon entropy.

The quantity $\chi(A : E)$ in Eq. (1) is the Holevo information [13], giving the upper bound for the information accessible to the eavesdropper Eve in a given collective attack. In this class of attacks Eve realizes interaction of her ancilla with each information carrier in the quantum channel (light in one transmission window in our case), stores the ancillas for the entire transmitted block in a quantum memory, and waits while Alice and Bob finish the post-processing of their key. Afterwards Eve measures collectively all the ancillas of the block, taking into account all the information collected from the public channel. The best measurement cannot give her more information (per bit) than

$$\chi(A : E) = S(\rho) - \sum_k p_k S(\rho_k),$$

where the index $k$ enumerates the possible states in the quantum channel, $\rho_k$ is the state of the ancilla under condition that $k$th state was attacked, $p_k$ is the weight of the $k$th state, $\rho = \sum_k p_k \rho_k$ is the unconditional state of ancilla, and $S(\rho) = -\text{Tr}\{\rho \log_2 \rho\}$ is the von Neumann entropy. The accessible information in Eq. (1) is maximized over all possible attacks by Eve, which is almost impossible to realize by considering various attacks one by one. A different approach to finding the secure key rate is connected to considering an equivalent protocol of entanglement distillation [16], and proving thus the unconditional security of the given protocol. Unfortunately, such an approach has not been yet applied to the SCW QKD without strong reference. In Sec. IV we calculate the quantity, Eq. (2), for just one, but very powerful attack, the CBS attack.

**C. The quantum channel**

The information channel between Alice and Bob, including quantum encoding, transmission via quantum channel, and quantum decoding, for each choice of basis has two input values, Alice’s bit $x = 0, 1$, and three output values, Bob’s bit $y = 0, 1, \text{and the inconclusive result } y = 2$ where Bob’s detector does not click. The absence of click is caused by the vacuum component in the state of the sidebands, and also by the possibility of destructive interference in the case Bob guesses the basis but not the state in BB84-OSD. The channel is completely determined by the matrix $P(y|x)$, the conditional probability of the Bob’s outcome $y$ when Alice sends $x$. We accept that Alice’s bit is random and its two values are equiprobable, which is known to maximize the channel capacity.

In the case where the probabilities of error and loss are independent of the input values, such a channel represents a binary symmetric error and erasure (BSEE) channel [17]. For such a channel we can write $E = P(0|1) = P(1|0), G = P(2|0) = P(2|1)$, and these two parameters determine completely the channel. The diagram of this channel is shown in Fig. 2a, and its capacity is given by

$$C = 1 - G - (1 - G) \log_2(1 - G) + E \log_2(E) + (1 - G - E) \log_2(1 - G - E).$$

FIG. 2. Diagrams of (a) the binary symmetric error and erasure channel and (b) the equivalent cascade of a symmetric binary channel and an erasure channel. The question mark denotes the inconclusive result.

It should be noted, that the “error probability” $E$ of BSEE channel is not the QBER value $Q$, entering Eq. (1), because the latter is the probability of error under condition of conclusive measurement outcome. To find the value of QBER, we represent BSEE channel as two cascaded channels [17]: a symmetric binary channel with error probability $Q$ and an erasure channel with the erasure probability $G'$, see Fig. 2b. It is easy to find that the two representations are equivalent, i.e, have the same matrix $P(y|x)$, if $G' = G$ and $Q(1 - G) = E$. It is easy to verify also that the capacity of the channel, given by Eq. (3), can be rewritten as $C = C_1 C_2$, where $C_1 = 1 - h(Q)$ is the capacity of the binary symmetric channel, and $C_2 = 1 - G$ is the capacity of the erasure channel. In the next section we calculate the values of $E$ and $G$, and as consequence, the QBER, from the explicit expressions for the quantum states, used in the SCW QKD system.

**III. QUANTUM BIT ERROR RATE**

The states of the multimode optical field at the entrance to the quantum channel can be found by the quantum model of electro-optical phase modulator developed in Ref. [14]. The model takes into consideration $2S + 1$ modes of the optical field with frequencies $\omega + k\Omega$, where the integer $k$ varies as $-S \leq k \leq S$. The input state of the Alice’s modulator is $|\sqrt{\nu_0}|_0 \otimes |\text{vac}\rangle_{SB}$, where $|\text{vac}\rangle_{SB}$ is the vacuum state of the sidebands and $|\sqrt{\nu_0}|_0$ is a coherent state of the carrier wave with the amplitude $\sqrt{\nu_0}$,
determined by the average number of photons in a transmission window: \( \mu_0 = PT/(\hbar \Omega) \), \( P \) being the power of the laser wave beam. The phase of the coherent state of the carrier wave is accepted to be zero and all other phases are calculated with respect to this phase. The state of the field at the output of the modulator is a multimode coherent state

\[
|\psi_0(\varphi_A)\rangle = \bigotimes_{k=-S}^S |\alpha_k(\varphi_A)\rangle_k,
\]

with the coherent amplitudes

\[
\alpha_k(\varphi_A) = \sqrt{\mu_0} d^{S}_{nk}(\beta) e^{-i(\theta_1 + \varphi_A)k},
\]

where \( \theta_1 \) is a constant phase and \( d^{S}_{nk}(\beta) \) is the Wigner d-function, appearing in the quantum theory of angular momentum [18]. The argument of the d-function \( \beta \) is determined by the modulation index \( m \), and disregarding the dispersion of the modulator medium this dependence can be written as [14]:

\[
\beta = \frac{2m}{2S + 1}.
\]

A remarkable property of the d-function is its asymptotic form [18]

\[
d^{S}_{nk}(m/S) \rightarrow J_{n-k}(m), \quad s \rightarrow \infty,
\]

where \( J_n(x) \) is the Bessel function of the first kind. This asymptotic form corresponds to a conventional description of the phase modulation with an infinite number of sidebands, leading in the quantum case to unphysical results because of appearance of negative frequencies, see discussion in Ref. [19].

After passing the distance \( L \) in the quantum channel (optical fiber), the states of all spectral components are attenuated. The transmission coefficient of the quantum channel is \( \eta(L) = 10^{-\xi L/10} \), where \( \xi \) is the fibre loss per unit length. The state of the optical field in one transmission window at the entrance to the Bob’s module is

\[
|\psi_L(\varphi_A)\rangle = \bigotimes_{k=-S}^S \sqrt{\eta(L)} |\alpha_k(\varphi_A)\rangle_k.
\]

The microwave field in the Bob’s phase modulator has the same frequency \( \Omega \) as that of the Alice’s one, but a different phase \( \varphi \). Additional field is produced in this modulator on the same sideband frequencies \( \omega + k \Omega \), which interferes with the field already present on these frequencies. The resulting state of the field is a multimode coherent state [14]

\[
|\psi_B(\varphi_A, \varphi)\rangle = \bigotimes_{k=-S}^S |\alpha_k(\varphi_A, \varphi)\rangle_k,
\]

with the coherent amplitudes

\[
\alpha_k(\varphi_A, \varphi) = \sqrt{\mu_0} \eta(L) d^{S}_{nk}(\beta') e^{-i(\theta_2 + \varphi_A + \varphi)k},
\]

where the new argument of the d-function is determined by the relation

\[
\cos \theta_1 = \cos^2 \beta - \sin^2 \beta \cos (\varphi_A - \varphi).
\]

while \( \theta_2 \) and \( \varphi_0 \) are some constant phases determined by the construction of the phase modulator [14]. Equation (11) shows that to achieve constructive interference on the sidebands, Bob should use \( \varphi_0 \) as offset for his phase, and apply in his modulator the microwave phase \( \varphi = \varphi_0 + \varphi_B \). Then, for \( \varphi_A - \varphi_B = 0 \), the argument of the d-function doubles: \( \beta' = 2\beta \), while for \( \varphi_A - \varphi_B = \pm \pi \) it vanishes: \( \beta' = 0 \). Since \( d^{S}_{nk}(0) = \delta_{nk} \), a zero argument corresponds to the presence of photons only on the carrier frequency, all the sidebands being in the vacuum state.

The optical losses in the Bob’s module can be described by the transmittance coefficient \( \eta_B \). These losses can be taken into account by replacing the amplitudes determined by Eq. (10) with the following ones:

\[
\tilde{\alpha}_k(\varphi_A, \varphi_B) = \sqrt{\mu_0 \eta(L) \eta_B} d^{S}_{nk}(\beta') e^{-i(\theta_3 + \varphi_A + \varphi)k},
\]

where \( \theta_3 = \theta_2 + \varphi_0 \). It is unimportant if some of the optical losses took place before the phase modulation, during or after it, as soon as they are the same for all spectral components.

The spectral filtering in the Bob’s module aims at removing the relatively strong carrier wave. Unfortunately, in a practical QKD system this wave can be only attenuated by the factor \( \theta \ll 1 \), resulting in a replacement \( \tilde{\alpha}_0(\varphi_A, \varphi_B) = \sqrt{\theta} \alpha_0(\varphi_A, \varphi_B) \).

Thus, the average number of photons, arriving at the Bob’s detector in the transmission window \( T \) is given by the average total number of photons at all spectral components

\[
n_{ph}(\varphi_A, \varphi_B) = \theta |\tilde{\alpha}_0(\varphi_A, \varphi_B)|^2 + \sum_{k \neq 0} |\tilde{\alpha}_k(\varphi_A, \varphi_B)|^2
\]

\[
= \mu_0 \eta(L) \eta_B (1 - (1 - \theta)|d^{S}_{nk}(\beta')|^2),
\]

where we have used the property of the d-functions [18]

\[
\sum_{k=-S}^S d^{S}_{nk}(\beta) (d^{S}_{nk}(\beta))^* = \delta_{n_l},
\]

meaning that \( d^{S}_{nk}(\beta) \) is a unitary matrix with respect to its lower indices.

For the values \( n_{ph} \ll 1 \), typical for a long-distance QKD line, the probability for the SPD to produce a click in the window \( T \) is [20]

\[
P_{ph}(\varphi_A, \varphi_B) = \left( \eta_D n_{ph}(\varphi_A, \varphi_B) + \gamma_{dark} \right) \Delta t,
\]

where \( \eta_D \) is the detector quantum efficiency, \( \gamma_{dark} \) is the dark count rate, and \( \Delta t = T \) for the continuous operation.
of the detector, but if a gating time shorter than $T$ is used, then $\Delta t$ is equal to the gating time of the detector.

Now we can calculate the parameters of the BSEE channel between Alice and Bob. These parameters are the same for both protocols B92 and BB84-OSD, and are given by the following relations

$$P_{\text{det}}(0, \pi + \Delta \varphi) = E,$$

$$P_{\text{det}}(0, \Delta \varphi)) = 1 - E - G,$$

where the phase $\Delta \varphi$ describes slight phase instability, caused, for instance, by jitter or phase mismatch due to non-perfect synchronization.

The QBER $Q = E/(1 - G)$ can be calculated from Eqs. (13,15,16,17) as function of the distance $L$. The calculation can be simplified by considering a sufficiently high number of sidebands $S \gg 10$ and taking the limit, given by Eq. (7).

For calculations we use the experimental parameters from one of the regimes realized in Ref. [12]: $T = 10$ ns, $\mu_0 = 4$, $m = 0.319$, $\nu_S = 100$ MHz, $\Delta \varphi = 5^\circ$, $10 \log \eta_B = 6.4$ dB, $\theta = 10^{-3}$. Two different detectors are considered: a superconducting nanowire single-photon detector (SNSPD) with $\eta_{\text{PD}} = 0.2$, $\gamma_{\text{dark}} = 20$ Hz, operating in the continuous regime, and an avalanche photodiode (APD): $\eta_{\text{PD}} = 0.125$, $\gamma_{\text{dark}} = 400$ Hz, operating in the gated regime with the gating time $\Delta t = 4$ ns.

In Fig. 3 we show the dependence of QBER on the optical loss $\xi L$ for two considered detectors.

![FIG. 3. QBER dependence on the channel loss in SCW QKD system](image)

For relatively low loss, while the counting rate well surpasses the dark count rate, the QBER is mainly determined by the phase instability and imperfect filtering of the carrier wave. The loss at which the counting rate becomes comparable to $\gamma_{\text{dark}}$ is the maximal loss for a given QKD system, because above this value the QBER increases rapidly, reaching values, not suitable for the error correction.

### IV. ANALYSIS OF THE CBS ATTACK

#### A. The possible attacks

After Alice and Bob have successfully generated a block of shared bits of length $N$, containing some errors (the raw key), they perform error correction by disclosing $N \cdot \text{leak}_{EC}(Q)$ bits, this number depending on their error-correcting protocol, but lower limited by $N \cdot h(Q)$. After having corrected all the errors they do privacy amplification by shortening their block by means of a hash function, with the aim to eliminate almost totally the potential knowledge of Eve on the shorter block (the final key). The amount to which the block should be shortened is determined by Eq. (1), where the second term in the square brackets corresponds to the information disclosed during the error correction stage, while the third term in the squire brackets corresponds to the upper estimate of potential information of Eve on the key.

To obtain a good upper estimate of the Eve’s information, one needs to consider explicitly various attacks on the QKD line. The general scenario of the attack is as follows: Eve replaces the communication line characterized by the error rate $Q_0 \leq Q$ and the loss $\eta$ by a perfect errorless and lossless line and employs an eavesdropping procedure on the information carriers, introducing the same amount of error and loss as before the replacement, thus hiding her intrusion from the legitimate users, who monitor the error rate and the loss in the channel. The attacks suitable for modelling can be individual or collective, depending on the number of information carriers attacked at once. The most important individual attacks are the intercept-resend (IR) attack, introducing errors, but no loss [11], and three zero-error attacks, introducing only loss but no error [2]: the PNS attack, the USD attack, and the individual beam-splitting (IBS) attack. The most important collective attacks include the CBS attack, being a quantum-memory-enhanced version of the IBS attack, and the asymmetric cloning (AC) attack, consisting in entangling an ancillary system to the information carrier by means of an asymmetric cloning machine [21] or an asymmetric universal entangling machine [22]. The latter attack introduces errors but no loss.

The analysis of the previous section shows that in a SCW QKD system almost no error is caused by the transmission line, so that $Q_0 \approx 0$. In the “calibrated devices” approach to the security analysis [2] we accept that the Bob’s module is calibrated for errors and loss, and Eve has no access to its performance. Then the IR and AC attacks, introducing errors, can be rather easily detected by enhancement of the measured value of QBER. The zero-error PNS and USD attacks require a suppression of the signal and the carrier wave in the case of unsuccessful measurement outcome, and can be countered by monitoring the power of the carrier wave, which is the essence of the “strong reference” method [5, 11]. The CBS attack always outperforms the IBS attack, which is
its particular case, and therefore the CBS attack, in no way detectable, seems to be the most important for the security analysis of the SCW QKD system, serving the point of reference for all other attacks.

B. The CBS Attack

In the CBS attack Eve inserts a beam splitter with the transmission \( \eta(L) \) in the very beginning of the transmission line and sends the transmitted light to Bob via a lossless line, keeping the reflected light in a quantum memory, writing each window of duration \( T \) to a separate cell of memory. After the announcement of bases (in BB84-OSD) and error correction performed by the legitimate users for a block of bits, she discards (in BB84-OSD) the memory cells, corresponding to windows where the bases used by Alice and Bob do not coincide and makes a collective measurement of the rest of the cells. Below we calculate the Holevo information, Eq. (2), for the state of the information carrier in the quantum channel of an SCW QKD system.

As follows from the quantum consideration of the beam splitter [25], the state of the transmitted beam in the window \( T \) is given by Eq. (8) and is identical to one which should arrive at Bob’s module in the absence of eavesdropping, while the state of the reflected beam in the same window is

\[
|\psi_E(\varphi_A)\rangle = \bigotimes_{k=-S}^S |\sqrt{\tilde{\eta}(L)}\alpha_k(\varphi_A)\rangle_k, \tag{18}
\]

where \( \tilde{\eta}(L) = 1 - \eta(L) \) and the phase \( \varphi_A \) is a random member of the set, corresponding to the used protocol.

In the B92 protocol for each cell Eve needs to distinguish only two states, \(|\psi_E(0)\rangle\) and \(|\psi_E(\pi)\rangle\). In the BB84-OSD protocol, for the cells corresponding to Alice’s choice of basis \( \{\pi/2, 3\pi/2\} \), Eve shifts the phase of the \( k \)th sideband by \( \pi k/2 \), which is realized by a unitary rotation of the state Eq. (18) with the evolution operator

\[
U = \exp\left(i\frac{\pi}{2} \sum_{k=-S}^S k \alpha_k^\dagger \alpha_k\right) \tag{19}
\]

where \( \alpha_k \) is the photon annihilation operator for the \( k \)th sideband. A unitary rotation does not change the accessible information, thus, Eve needs to distinguish the same two states as in the B92 protocol.

Since the two states to be distinguished are pure, the Holevo information, Eq. (2) is given by the von Neumann entropy of the mixed state

\[
\rho = \frac{1}{2} |\psi_E(0)\rangle\langle\psi_E(0)| + \frac{1}{2} |\psi_E(\pi)\rangle\langle\psi_E(\pi)|. \tag{20}
\]

The von Neumann entropy of a density operator is the Shannon entropy of its eigenvalues. The eigenvalues of operator \( \rho \) are

\[
\lambda_{1,2} = \frac{1}{2} (1 \pm |\psi(0, \pi)|) \tag{21}
\]

where the state overlap \( \psi(\varphi_1, \varphi_2) \) is calculated as

\[
\psi(\varphi_1, \varphi_2) = \langle \psi_E(\varphi_1) | \psi_E(\varphi_2) \rangle = \prod_{k=-S}^S k \sqrt{\tilde{\eta}(L)} \cdot \alpha_k(\varphi_1) | \sqrt{\tilde{\eta}(L)} \cdot \alpha_k(\varphi_2) \rangle_k \tag{22}
\]

Using the formula for the scalar product of two coherent states

\[
\langle \alpha | \beta \rangle = \exp \left( -\frac{1}{2} (|\alpha|^2 + |\beta|^2) + \alpha^\dagger \beta \right) \tag{23}
\]

we obtain

\[
\psi(\varphi_1, \varphi_2) = \exp \left( -\frac{\bar{\eta}(L)}{2} \sum_{k=-S}^S (|\alpha_k(\varphi_1)|^2 + |\alpha_k(\varphi_2)|^2 - 2\alpha_k^\dagger(\varphi_1) \alpha_k(\varphi_2)) \right) \tag{24}
\]

where we have employed Eq. (5). Using the properties of d-functions, we find

\[
\sum_{k=-S}^S |d_{0k}^S(\beta)|^2 \left( 1 - e^{i(\varphi_1 - \varphi_2)k} \right) = 1 - d_{00}^S(\beta_-), \tag{25}
\]

Finally,

\[
\psi(\varphi_1, \varphi_2) = \exp \left[ -\mu_0 \bar{\eta}(L) \left( 1 - d_{00}^S(\beta_-) \right) \right]. \tag{26}
\]

where for \( \varphi_1 - \varphi_2 = \pm \pi \) we need to substitute \( \beta_- = 2\beta \).

Thus, for both the B92 and the BB84-OSD protocols we obtain the Holevo information

\[
\chi(A : E) = h \left( \frac{1}{2} (1 - \exp \left[ -\mu_0 \bar{\eta}(L) \left( 1 - d_{00}^S(2\beta) \right) \right]) \right). \tag{27}
\]

V. THE SECURE KEY RATE

A. Rate dependence on the loss

Now we have all the necessary dependencies to calculate the secure key rate, determined by Eq. (1). The probability \( P_R \) for decoding and accepting a bit is given by \( P_R = (1 - G)f \), where \( f \) is the fraction of data where Bob guessed correctly the basis, equal to \( \frac{1}{4} \) for the BB84-OSD protocol and to \( 1 \) for the B92 protocol, and \( 1 - G \) is the probability of photodetection in the window \( T \) and is determined by Eqs. (10) and (11) [17]. As we have seen in the previous sections, all the functions, entering the right hand side of Eq. (1) are the same for the BB84-OSD and the
B92 protocols, except for \( f \). Thus, the secure key rate for the B92 protocol is always twice that for the BB84-OSD protocol, as far as we restrict our analysis to a CBS attack. For this reason we illustrate only the case of the latter protocol.

In Fig. 4 we show the dependence of the secure key rate on the channel loss \( \xi L \) for the same setting with two detectors as in Sec. III. The corresponding distance can be easily calculated using the value \( \xi = 0.18 \) dB/km typical for the telecommunication fibre.

![FIG. 4. Secure key rate dependence on channel loss in SCW QKD system](image)

We note that for rather low repetition rate, \( T^{-1} = 100 \) MHz, we can achieve high values of distances and secure key rates. In spite of low secure distances with APD it is still an effective solution for up to 100 km fiber lines due to its easier maintenance compared to SNSPD.

### B. Optimal modulation depth

The depth of the phase modulation in the Alice’s module determines the total number of photons in the sidebands of the field, entering the communication line and being the object of the Eve’s attack. The mean photon number in all the sidebands is an important parameter, commonly used for characterizing the regime of a QKD system [1,2] and it can be found as following:

\[
\mu = \sum_{k \neq 0} |\alpha_k(\varphi_A)|^2 = \mu_0 \cdot (1 - |d^{S}_{00}(\beta)|^2) \approx \mu_0 \cdot (1 - J_0(m)^2)
\]

(28)

where the last expression is the asymptotic form for a sufficiently large number of sidebands.

Higher values of \( \mu \) correspond to higher counting rate of the Bob’s detector and are very attractive from the practical point of view. However, the information available to Eve is also growing with \( \mu \), reaching 100 % in the limit where \( \mu \gg 1 \) and the states of the sidebands corresponding to different values of \( \varphi_A \) become almost orthogonal.

The optimal value of the modulation depth \( m \) and therefore \( \mu \) can be found by considering the key generation rate as function \( K(\mu, L) \) and finding the value \( \mu(L) \) which maximizes this function for a given \( L \). The numerically found dependence is presented in Fig. 5. According to it given value of \( \mu \) was chosen.

![FIG. 5. Mean photon number dependence on losses in the channel providing the maximum value of the secret key rate](image)

We see that the practical value for a long-distance QKD with SNSPD is \( \mu = 0.2 \), and higher values of the mean photon number, considered in the literature [10, 24], are not secure against the CBS attack.

### C. Secure key rate of BB84 versus BB84-OSD

Let us divide all the sidebands of the field in a SCW QKD system into the upper sidebands with frequencies \( \omega + k\Omega, k \in [1, S] \) and the lower sidebands with frequencies \( \omega + k\Omega, k \in [-S, -1] \).

The demodulation process in the Bob’s module, can be described by a demodulation operator \( D(\varphi_B) \), mapping the state arriving to his module, Eq. (8), to the state given by Eq. (9). In the case \( \varphi_B = 0 \) and if the basis is guessed correctly, this mapping is

\[
D(0)|\psi_L(0)\rangle = |\mu_+\rangle \otimes |\mu_-\rangle \otimes |\bar{\mu}\rangle_0,
\]

\[
D(0)|\psi_L(\pi)\rangle = |\text{vac}_+\rangle \otimes |\text{vac}_-\rangle \otimes |\bar{\mu}\rangle_0,
\]

(29)

(30)

where \( |\mu_+\rangle \) and \( |\mu_-\rangle \) are multimode coherent states of upper and lower sidebands respectively with the same
mean photon number $\mu_s$ each, defined as

\[ |\mu_s\rangle_+ = \bigotimes_{k=1}^{S} |\alpha_k'(0, \varphi_0)\rangle_k, \quad (31) \]

\[ |\mu_s\rangle_- = \bigotimes_{k=-S}^{-1} |\alpha_k'(0, \varphi_0)\rangle_k, \quad (32) \]

while $|\mu_c\rangle_0$ and $|\bar{\mu}\rangle_0$ are coherent states of the carrier wave with the mean photon numbers $\mu_c = |\alpha_0(0, \varphi_0)|^2$ and $\bar{\mu} = |\alpha_0'(\pi, \varphi_0)|^2$ respectively. It can be obtained from Eq. (10) that $\bar{\mu} = \mu_c + 2\mu_s$, which has a simple physical meaning: the demodulation process preserves the total number of photons in the field.

Let us consider a modification of the protocol BB84-OSD, where Bob has two detectors: one for the upper sidebands and one for the lower ones, and applies a demodulation operator $D'(\varphi_B)$ to the state of the field arriving to his module, Eq. (8), directing the photons either to the upper sidebands or to the lower ones depending on the phase $\varphi_B$ (under condition he uses the same basis as Alice). Here we consider only operators resulting in a linear transformation of the field, and therefore mapping coherent states onto coherent ones. In the case $\varphi_B = 0$ the mapping provided by the demodulation should be as follows:

\[ D'(0)|\psi_L(0)\rangle = |\mu'_s\rangle_+ \otimes |\text{vac}\rangle - |\mu'_c\rangle_0, \quad (33) \]

\[ D'(0)|\psi_L(\pi)\rangle = |\text{vac}\rangle_+ \otimes |\mu'_s\rangle_- - |\mu'_c\rangle_0, \quad (34) \]

where all the states are coherent and the mean numbers of photons are determined by their arguments. In this case Bob can distinguish the cases of $\varphi_a = 0$ and $\varphi_a = \pi$ by observing a click on the corresponding detector, which would correspond to a realization of the BB84 protocol. Let us calculate the corresponding counting rate.

From the unitarity of the operators $D(\varphi_B)$ and $D'(\varphi_B)$ we have

\[ \langle \psi_L(\pi)|D^\dagger(0)D(0)|\psi_L(0)\rangle = \langle \psi_L(\pi)|D^\dagger(0)D'(0)|\psi_L(0)\rangle, \quad (35) \]

wherefrom, with the help of Eqs. (29, 30, 33, 34), we obtain

\[ \exp\left\{-\mu_s - \frac{1}{2}\left(\sqrt{\mu} - \sqrt{\bar{\mu}}\right)^2\right\} = \exp\left\{-\mu'_s\right\} \quad (36) \]

or

\[ \mu'_s = \mu_s + \frac{1}{2}\left(\sqrt{\mu} - \sqrt{\bar{\mu}} - 2\mu_s\right)^2 \approx \mu_s + \frac{\mu^2}{2\bar{\mu}}. \quad (37) \]

We see, that in the case of low modulation index, where $\mu_s/\bar{\mu} \ll 1$, the average number of photons in the sidebands for the BB84 protocol is almost the same as for BB84-OSD, $\mu'_s \approx \mu_s$. It means that the Bob’s detectors in BB84 click with the rate $n_{BB84}$ each, while in the BB84-OSD protocol (with a perfect suppression of the carrier wave) the only detector clicks with the rate $2n_{BB84}$, the total count rate being the same for two protocols.

Thus, in the regime of low modulation index there is no reason to install the second detector and employ sophisticated modulation/demodulation techniques for decoding both states of the same basis. The protocol BB84-OSD performs not worse than BB84 and is technically significantly simpler. For the same reasons an increase of the number of bases or the number of phases in each basis is not expected to increase the secure key rate [25].

VI. CONCLUSIONS

In this work we have calculated the secure key generation rate for two protocols of SCW QKD in the presence of the CBS attack in the quantum channel and have shown that a SCW QKD system allows a secure distribution of cryptographic key over large distances. It was shown that the optimal mean photon number value in the system is $\mu \approx 0.2$. We have found that the main limiting factors for a long distance communication are the dark counts of photodetector and the fraction of photons remaining at the carrier frequency that reach the detector. It should be noted that for a more accurate QBER estimations a more advanced model of the quantum channel can be considered, for instance, including the partial loss of coherence between the sidebands propagating in the fibre.

We have shown also that the version of the BB84 protocol with detection of just one of the states in each basis has a performance not worse than that of the full BB84 protocol. Also, the key generation rate of the B92 protocol is double that of the BB84 protocol, as long as the analysis of attacks is limited to the CBS attack. It is possible, that other attacks, like USD attack, may be more successful against B92, which uses lesser number of states, than against BB84. Individual attacks on SCW QKD system will be a subject of a separate study.

The obtained results are important for constructing long-distance QKD links and multiuser quantum networks using SCW QKD instrumentation: the possibility of harnessing the ultra-high bandwidth for QKD is compatible with the existing fibre optical infrastructures.

ACKNOWLEDGMENTS

This work was financially supported by the Government of Russian Federation, Grant 074-U01, by the Ministry of Education and Science of Russian Federation (project 14.578.21.0112, and contract 02.G25.31.0229) and by the Belarusian Republican Foundation for Fundamental Research.
[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys, 74, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, M. Peev, Rev. Mod. Phys, 81, 1301 (2009).
[3] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, A. Zeilinger, Theoretical Computer Science, 560, 62 (2014).
[4] C. H. Bennett, F. Bessette, G. Brassard, and L. Savail, J. Cryptology 5, 3 (1992).
[5] C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).
[6] J.-M. Merolla, Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes, Phys. Rev. Lett. 82, 1656 (1999).
[7] J.-M. Merolla, Y. Mazurenko, J.-P. Goedgebuer, L. Duraffourg, H. Porte, and W. T. Rhodes, Phys. Rev. A 60, 1899 (1999).
[8] J.-M. Merolla, L. Duraffourg, J.-P. Goedgebuer, A. Soujaeff, F. Patois, and W. T. Rhodes, Eur. Phys. J. D 18, 141 (2002).
[9] J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. Garcia Munoz, and J. Capmany, Opt. Expr. 20, 16358 (2012).
[10] O. Guerreau, F. J. Malassenet, S. W. McLaughlin, and J.-M. Merolla, IEEE Photon. Technol. Lett. 17, 1755 (2005).
[11] M. Koashi, Phys. Rev. Lett. 93, 120501 (2004).
[12] A. V. Gleim, V. I. Egorov, Yu. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, and G. S. Buller, Opt. Expr. 24, 2619 (2016).
[13] I. Devetak and A. Winter, Proc. R. Soc. Lond. A 461, 207 (2005).
[14] G. P. Miroshnichenko, A. D. Kiselev, A. I. Trifanov, A. V. Gleim, JOSA B, 34, 1177 (2017).
[15] A. S. Holevo, Probabilistic and Statistical Aspects of Quantum Theory (North-Holland, Amsterdam, 1982).
[16] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
[17] T. M. Cover, J. A. Thomas, Elements of information theory (Wiley, New-York, 1991).
[18] D. A. Varshalovich, A. N. Moskalev, V.K. Khersonsky, Quantum Theory of Angular Momentum (World Scientific, Singapore, 1988).
[19] J. Capmany and C. R. Fernandez-Pousa, J. Opt. Soc. Am. 27, 119 (2010).
[20] L. Mandel, E. Wolf, Optical coherence and quantum optics (Cambridge University Press, 1995).
[21] N. J. Cerf, J. Mod. Opt. 47, 187 (2000).
[22] D. Horoshko, S. Kilin, and M. Kolobov, Opt. Spectr. 103, 153 (2007).
[23] M. O. Scully and M. S. Zubairy, Quantum Optics (Cambridge University Press, 1997).
[24] A. N. Klimov, S. P. Kulik, S. N. Molotkov, and T. A. Potapova, Laser Phys. Lett. 14, 035201 (2017).
[25] D. B. Horoshko and S. Ya. Kilin, Opt. Spectr. 94, 691 (2003).