Intercept-resend attack on passive side channel of the light source in BB84 decoy-state protocol

D Babukhin\textsuperscript{1,2,3}, D Sych\textsuperscript{3,4,5}
\textsuperscript{1}Dukhov Research Institute of Automatics (VNIIA), Moscow 127055, Russia
\textsuperscript{2}Russian Quantum Center (RQC), Moscow 143026, Russia
\textsuperscript{3}QRate LLC, Moscow 121353, Russia
\textsuperscript{4}Moscow State Pedagogical University, Moscow 119992, Russia
\textsuperscript{5}P.N. Lebedev Physical Institute, Moscow 119991, Russia

Abstract. Quantum key distribution (QKD) promises unconditionally secure communication based on fundamental laws of physics, though practical realizations of QKD may have loopholes and side channels, thus their security can be compromised. We analyze the intercept-resend attack on the BB84 decoy-state protocol under the presence of a passive side channel of the light source. We derive an upper bound for the secret key rate and show that it does not significantly deviate from the ideal side-channel-free case.

1. Introduction
Among the emerging quantum technologies, QKD is the most developed branch up to date. The security of QKD is based on the fundamental laws of quantum physics and the constraints imposed on the ability of an eavesdropper to obtain the exact copy of a quantum signal. The problem with the QKD security appears when the eavesdropper attacks the real-world QKD implementations. In practice, all devices differ from their ideal models. For example, quantum communication signals emitted by different lasers may have slightly different spectral, temporal, or spatial modes. These differences, called passive side channels of the light source, allow the adversary to obtain additional information about the quantum signals. The question of how to estimate and properly account for side channels is an active research subject [1]. Since the original proof of unconditional security of the BB84 protocol for ideal devices [2], there were a number of works on the QKD security with imperfect devices [3-5].

In this work, we take into account the overall photonic mode mismatch as a side channel, estimated via the Hong-Ou-Mandel (HOM) interference [1], and show an explicit intercept-resend attack on the BB84 decoy state protocol which makes use of this side channel. The obtained secret key rate serves as an upper bound on the possible secret key rate in the presence of passive side channel of the light source for an arbitrary attack.

2. Methods
We use auxiliary degrees of freedom of phase-randomized weak coherent states of light, employed as signal states in BB84 decoy-state protocol, as a model of the passive side channel. The degree of distinguishability of quantum states is estimated from the HOM interference visibility. We numerically calculate secret key rate under the intercept-resend attack on the BB84 protocol for different values of the HOM interference visibility.
For the intercept-resend attack, Eve tries to replace Bob in the communication channel. She chooses at random a measurement basis and makes a measurement followed by sending a new signal state corresponding to the measurement result. If she chose the right basis, she does not introduce disturbance to the signal state, but if she chose the wrong basis, Bob will see errors in some communication acts. Eve attacks with some probability $p$ and just makes a guess about the secret bit with probability $1-p$. As a result, Bob receives a mixed state 

$$\rho = (1-p)\rho_{Alice} + pI \quad (1)$$

where $\rho_{Alice}$ is one of the possible states that Alice sends to Bob 

$$|0\rangle\langle 0|, |1\rangle\langle 1|, \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|), \frac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|) \quad (2)$$

and $I$ is a qubit identity operator. The critical QBER for this attack is $Q_c=0.25$, when Eve intercepts every communication act (i.e., $p=1$). If Eve sometimes chooses to skip the state to Bob and just guess the encoded bit, then there is a nonzero secret key rate.

Let us reformulate Eve interception and measurement in a slightly different manner. Assume that Eve knows a set of states Alice can send to Bob. Eve tries to optimally discriminate what state was sent in every single transmission act with a properly tuned measurement. In other words, Eve makes an optimal state discrimination for a particular set of quantum states. For BB84 there is a set of four states $\{\rho_i\}_{i=1}^4$, and Eve knows there is one of these states in the quantum channel with probabilities $\{q_i\}_{i=1}^4$. The overall quantum state Eve sees in the quantum channel is 

$$\rho = \sum q_i \rho_i, \sum q_i = 1. \quad (3)$$

Eve has a measurement device with 4 outcomes $M = \{|M_k\}_{k=1}^4, M_k \geq 0, \sum M_k = I$. With this device, Eve can measure each of the ensemble states with probability: 

$$p(k|i) = \text{Tr}[M_k \rho_i] \text{ for } k = 1, \ldots, 4 \text{ and } i = 1, \ldots, 4. \quad (4)$$

Eve wants to tune her measurement device to optimally guess which one of the four possible states she received in a particular act of communication. There are different ways to define the optimality of discrimination depending on a figure of merit to be optimized (see Refs. [6,7]). If one wants to discriminate with minimal error, the POVM $M$ must satisfy the requirement: 

$$1 - p_{\text{error}} = p_{\text{guess}} = \max_M \sum q_k p(k|k), \quad (5)$$

subject to $\sum M_k = I \forall M_k \geq 0. \quad (6)$

To find a POVM with constraints to minimal error of states discrimination, one can use semi-definite programming method [8].

Applying this approach to BB84 will lead to a critical error $Q_c=0.25$. But if states, used for transmission, have additional distinguishability, the resulting critical error will be lower. These distinguishability (gathered under the name passive side channels) comes from physical properties of secret bit carriers, which are not used in the QKD protocol, but can be exploited by an adversary. An intuitive way to model these side channels is to augment signal states with an additional degree of freedom, which parametrically controls orthogonality of states. This leads to grow of the overall dimension of signal states, and Eve is supposed to use this growth for her purposes. Consequently, POVMs of the optimal discrimination in the intercept-resend attack will have higher than qubit dimension.
3. Decoy state BB84

In practice, to generate signal states for the BB84 protocol, one usually uses attenuated laser pulses. These sources produce phase-randomized weak coherent pulses (PRWCP) of the form

$$\rho_x^\mu = \sum e^{-\mu} \frac{\mu^2}{k!} |k;x\rangle \langle k;x|,$$  \hspace{1cm} (7)

where $\mu$ is the intensity of the signal coherent state and $x$ is the encoded secret bit. These signal states are vulnerable to a photon number splitting (PNS) attack. Eve can non-destructively measure the number of photons, and if there is one photon in the pulse, she blocks this pulse, in another case she sends one photon to Bob and holds other photons. This allows her to obtain a photon, which state is the same as Bob's photon, without introducing state disturbance to the latter. If there is a loss in the quantum channel (which is true for practice channels), legitimate users will not discover Eve's presence and hence their communication will no longer be secure.

Measuring the number of photons in the signal pulse does not give Eve information about the whole coherent state, and thus she does not know it's intensity. This means, that she will attack different coherent state, sent in the quantum channel, in a similar way, because she cannot distinguish one from another. One can use this lack of knowledge to close the loophole of the PNS attack by sending coherent states with different intensities and using their observable values to calculate the outcome of the single-photon component, which cannot be eavesdropped without state disturbance, and the single-photon error rate. This is the essence of a decoy-state method ([9,10,11]). Let us review the main steps of this protocol.

Suppose Alice chose a basis and a secret bit value and sent a PRWCP state (16) into the quantum channel. Bob receives a photon from this state and measures it in one of two bases. He does not know, how many photons were in the state where is received photon from. This means, that, taking into account all possible Alice bit choices, Bob can receive a photon from the $k$-photon state. For a $k$-photon component, the photon detection yield is

$$Y_k = \sum \sum P_A(a) P_B(b | A = a),$$ \hspace{1cm} (8)

where $A$ is a value of Alice's random bit, and $B$ is a value of Bob's bit, obtained from measurement. Bob does not know how many photons were in the pulse, and his observable values are averaged over all possible photon numbers. The full probability of having a detection count, when a coherent state with intensity $\mu$ was received from the quantum channel, is

$$Q_\mu = \sum e^{-\mu} \frac{\mu^2}{k!} Y_k,$$ \hspace{1cm} (9)

and the full probability of bit error in the outcome

$$E_\mu = \frac{1}{Q_\mu} \sum e^{-\mu} \frac{\mu^2}{k!} Y_k e_k,$$ \hspace{1cm} (10)

where $k = 0$ corresponds to dark counts of photodetectors. Using such observables for signal state and decoy states, Bob can estimate the vacuum yield $Y_0$, the single-photon component yield $Y_1$, and single-photon error rate $e_1$. On practice, a decoy-state setup with two decoy-state intensities $\nu_1$ and $\nu_2$ is usually used, because this is asymptotically equivalent to the case of infinitely many decoy states protocol [12].

To calculate the secret key rate for a BB84 protocol with two decoy states, a slightly reorganized formula from [12] can used to incorporate the adversary attacks on the single-photon source protocol:

$$R(e_1) = \frac{1}{2} \left( Q_1 I_{AB}(e_1) - fQ_\mu \max \{ I_{AE}(E_\mu), I_{BE}(E_\mu) \} \right),$$ \hspace{1cm} (11)
where \( f \) is a post-processing efficiency factor and \( e_1 \) is bit error in one-photon component outcomes.

4. Results and discussion

The calculated secret key rate for several values of HOM interference visibility \( (0.2, 0.3, 0.4, 0.5) \) is shown in figure 1. For simulation we used error correction coefficient \( f = 1.22 \), fiber attenuation \( \alpha = 0.2 \) dB/km, Bob detector efficiency \( \eta_{Bob} = 0.01 \), background yield \( Y_0 = 10^5 \), background error rate \( e_0 \) is 0.5 and mean photon number in a pulse \( \mu = 0.5 \). To calculate the critical length of the transmission line, we used the formula

\[
L(e_1) = -\frac{10}{\alpha} \log_{10} \left( \frac{Y_0 (e_0 - e_1)}{\eta_{Bob} (e_1 - e_{det})} \right),
\]

(12)

where \( e_1 \) is single-photon component error rate and \( e_{det} \) is detector error rate.

\[\text{Figure 1. Secret key rate } R \text{ as a function of fiber-optic communication distance } L \text{ for different values of Hong-Ou-Mandel interference visibility } V, \text{ under the intercept-resend attack on the BB84 decoy-state protocol. We assume the standard single-mode optical fiber loss of } 0.2 \text{ dB/km.}\]

From the results, provided in figure 1, we conclude, that the photon mode mismatch does not completely compromise the security of the BB84 protocol with decoy states and causes only a slight decrease in critical transmission line length. Even for pessimistic values of the HOM visibility (which can serve as a measure of the source reliability), we see reasonable critical transmission line length values. We note that the modern laser sources used in QKD typically have HOM interference visibility values above 0.45. Thus we can say that there is almost no influence of realistic laser source imperfections on the upper bound of the secret key rate. The study of tighter bounds on the secret key rate requires analysis of more advanced eavesdropping strategies, which is currently in progress.
References
[1] Duplinskiy A and Sych D V Preprint arXiv:1908.04703 [quant-ph]
[2] Shor P W and Preskill J 2000 Phys. Rev. Lett. 85 441-444
[3] Gottesman D, Lo H-K, Lutkenhaus N and Preskill J 2004 Quant. Inf. Comput. 5 325-360
[4] Koashi M and Preskill J 2003 Phys. Rev. Lett. 90 057902
[5] Koashi M 2009 New J. Phys. 11 045018
[6] Bergou J A 2010 J. Mod. Opt. 57 160-180
[7] Bae J and Kwek L-C 2015 J. Phys. A: Math. Theor. 48 083001
[8] Eldar Y C, Megretski A and Verghese G C 2004 IEEE Trans. Inf Theor. 50 1198-1207
[9] Hwang W-Y 2003 Phys. Rev. Lett. 91 057901
[10] Lo H-K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
[11] Lo H-K 2004 Proc. IEEE ISIT (IEEE Press) p 137
[12] Ma X, Qi B, Zhao Y and Lo H-K 2005 Phys. Rev. A 72 012326