Passive decoy-state quantum key distribution with imperfect source

A Gavrilovich\textsuperscript{1,2,3}, D Sych\textsuperscript{1,5,6} and Y Kurochkin\textsuperscript{1,2,6}

\textsuperscript{1} QRate, Skolkovo, 143026, Russia
\textsuperscript{2} Russian Quantum Center, Skolkovo, 143026, Russia
\textsuperscript{3} Moscow Institute of Physics and Technology, Dolgoprudny, 141700, Russia
\textsuperscript{4} P.N.Lebedev Physical Institute, Russian Academy of Sciences, Moscow, 119991, Russia
\textsuperscript{5} Department of Physics, Moscow State Pedagogical University, Moscow, 119992, Russia
\textsuperscript{6} National University of Science and Technology MISiS, Moscow, 119049, Russia
\textsuperscript{7} Sirius University of Science and Technology, Sochi, 354340, Russia

E-mail: gavrilovich.aa@phystech.edu

Abstract. Passive generation is a sophisticated way of state preparation in quantum key distribution (QKD) systems which is designed to exploit some internal physical process as a source of randomness. It can be profitable in a wide range of scenarios. However, the original analysis of the passive scheme implies an ideal interference which is almost impossible to assure in practice, therefore utilizing such method potentially compromises the security of the system. Here we develop a general technique to estimate decoy-state parameters for a passive protocol with an arbitrary experimental distribution of intensity. We compare this analysis with the original method and show that the proposed technique can provide higher key generation rates.

1. Introduction

QKD allows establishing a secret key between two distant users in the presence of an eavesdropper with unlimited computational power. Currently, there exist a lot of different QKD protocols \cite{1-8}. Many of them are similar in the sense that they imply performing a random choice of some quantity (intensity, phase, etc.) at the transmitter’s side. For the unconditional security of QKD it is crucial to make this choice using quantum randomness. Therefore, conventionally QKD schemes involve a fully-fledged quantum random number generator which alongside a modulator carries out the active state preparation. An alternative approach is a so-called passive generation. It allows exploiting internal physical process of the system to perform a random choice of the necessary quantity. Passive method is expected to be more robust against side-channel information leakage and may significantly simplify the experimental setup.

In general, there are many different ways to realize passive generation. One can, for example, make use of entanglement \cite{9,10} by operating a spontaneous parametric down-conversion source. However, existing devices are not capable of producing states on demand, therefore this implementation is not widely used. Another evident source of quantum randomness is the phase difference of the independently emitted laser pulses. By interfering them one can get pulses of random intensity and use the result as decoy states in BB84. Since the proposal of such scheme in \cite{11}, several works were dedicated to refining the original analyses, for example \cite{12} which
takes into account statistical fluctuations. However, recent research [13] shows that besides finite-
size effects there are also numerous imperfections of a laser source that significantly change the
shape of intensity probability density function (PDF). Any emerging mismatches may provide
additional information to an adversary, thus violating the security of the system. To bridge
the gap between the original model and a real-world setup one should take into account the
combined effect of chirp, jitter, and relaxation oscillations.

In this work, we consider phase-randomized coherent light and develop a method to estimate
BB84 decoy-state parameters for any experimental distribution of intensity. We explicitly derive
the lower and the upper bound of single-photon yield and error rate. Then we calculate the
secret key and show that it can provide higher secret key rates in comparison with the original
analysis.

2. Passive generation
The phase difference of the independently emitted laser pulses, being a fundamentally random
value, can be used to achieve different intensities via interference as shown in Fig.1. The scheme
allows not only to generate pulses of random intensity but also to read out the signal by detecting
half of it in the second arm of the interferometer. Assuming that interfering pulses have the
same polarization and each pulse shape exhibits a Gaussian temporal profile, the intensity of a
signal produced by a passive source can be written the following way:

\[ I = I_1 + I_2 + 2\eta\sqrt{I_1I_2}\cos\Delta\Phi \]

where \( I_1 \) and \( I_2 \) are the intensities of interfering pulses, \( \Delta\Phi \) is the phase difference and \( \eta \)
is the visibility. \( I \) depends on various real-life imperfections of apparatus, such as intensity
fluctuations, laser chirp, jitter, etc. For a detailed review, see [13]. As an illustration, three
different cases from [13] are presented in Fig.2

![Figure 1. Conceptual scheme of a passive source: LS — laser source, OA — optical
attenuator, D — classical detector, C — comparator(s).](image)

The resulting spectre of \( I \) can be used to define decoy states by assigning nonoverlapping
intervals of intensity to different types of signal as illustrated in Fig 3. After setting the boundary
values for each type of signal, one can distinguish them in practice by tuning a system of
comparators (see Fig.1).

3. Decoy state BB84
We use H.F. Chau’s idea of utilizing an arbitrary number of decoy intensities [14] and expand
this method to the passive setup.

Let yield \( Y_i \) be a conditional probability of detection event on Bob’s side given that Alice
sends \( i \) photons, then under the assumption that the light is coherent and phase-randomized
after summing the joint probability distribution over all values of \( i \in \{0, \infty\} \) one can get the
unconditional probability $Q_v$ of a click for a signal of intensity $v$. By averaging it with the posterior distribution $\rho_m(v)$ of intensity within $m$-th type of signal one can derive the unconditional probability for a pulse of $m$-th type to be detected. Applying this procedure to all $k$ types of signal gives a system of linear equations for $Y_i$:

$$
\begin{pmatrix}
Q_{v_1} \\
Q_{v_2} \\
\vdots \\
Q_{v_k}
\end{pmatrix} =
\begin{pmatrix}
\int \rho_1 e^{-v_1} dv_1 & \cdots & \int \rho_1 v_1^{k-1} e^{-v_1} dv_1 \\
\int \rho_2 e^{-v_2} dv_2 & \cdots & \int \rho_2 v_2^{k-1} e^{-v_2} dv_2 \\
\vdots & \cdots & \vdots \\
\int \rho_k e^{-v_k} dv_k & \cdots & \int \rho_k v_k^{k-1} e^{-v_k} dv_k \\
\end{pmatrix}
\begin{pmatrix}
Y_{0} \\
Y_{1} \\
\vdots \\
Y_{k-1}
\end{pmatrix} +
\begin{pmatrix}
\int_0^\infty \rho_1 v_1^{k} Y_{1} e^{-v_1} dv_1 \\
\int_0^\infty \rho_2 v_2^{k} Y_{2} e^{-v_2} dv_2 \\
\vdots \\
\int_0^\infty \rho_k v_k^{k} Y_{k-1} e^{-v_k} dv_k
\end{pmatrix}
$$

(1)

Analogically, if $e_i$ is a conditional probability of an error for a detected $i$-photon pulse, then one can write down a system of $k$ equations for unconditional probabilities of having an erroneous bit. Here $E_{vm}$ is an overall quantum bit error rate for $m$-th type of signal.

$$
E_{vm} Q_{vm} = \sum_{j=0}^{k-1} \hat{V}_{m,j} \frac{e_j Y_j}{j!} + \sum_{j=k}^{\infty} \int \rho_m v_m^j e_j Y_j e^{-v_m} dv_m
$$

It is secure to use only single photon pulses, therefore combining the GLLP approach with decoy state method one can derive formula for key generation rate:

$$
R = q \left\{ Y_1^L [1 - h_2(e_1^U)] \sum_{i=1}^{k} P_{v_i} [v_i e^{-v_i}] - f_{ec}(E_{v_i}) \sum_{i=1}^{k} P_{v_i} Q_{v_i} h_2(E_{v_i}) \right\}
$$

where $q$ depends on the implementation ($1/2$ for the original BB84, $1$ for the efficient BB84 protocol), $h_2(x)$ is binary Shannon information function, $f_{ec}$ is the error-correction efficiency function, $P_{v_i}$ is the probability of choosing $i$-th type of signal. $Q_{v_i}$ and $E_{v_i}$ are experimentally measured quantities, whereas $Y_1^U$ and $e_1^U$ (superscripts $L$ and $U$ denote a lower and an upper bound respectively) should be theoretically estimated. By introducing a modified Vandermode’s matrix $\hat{V}$ in (1) and deriving the explicit formula for it’s inverse we obtain that

**Figure 2.** Possible shapes of intensity probability density functions of passively prepared states: a) without fluctuations of interfering pulses b) with fluctuations of interfering pulses c) with fluctuations of interfering pulses and a linear chirp.

**Figure 3.** Example of a passive BB84 decoy-state protocol with three types of signals.
\[
Y^L_1 = \sum_{i=1}^{k} (\tilde{V}^{-1})_{2,i} Q_v, \quad e^U_1 = \sum_{i=1}^{k} (\tilde{V}^{-1})_{2,i} (E_v Q_v)/Y^L_1
\]

\[
(\tilde{V}^{-1})_{ij} = (-1)^{i+j} \int \prod_{t=1, t \neq j}^{k} \rho t e^{-\sum_{t=1, t \neq j}^{k} v_i S_{k-i,j} \prod_{l=m, (l \neq j)}^{k} (v_m - v_l) d^{k-1} v}
\]

where \(S_{m,i}^k\) is defined as the sum of all possible power products of \(m\) (where \(1 \leq m \leq k - 1\)) different intensity values \(v_j\) out of \(k\) used in the protocol such that \(1 \leq t_1 \leq \ldots \leq t_m \leq m, t_j \neq i\) (where \(1 \leq i \leq k\)).

4. Simulations
We compare the proposed technique with the original method by simulating the performance of a simple passive source in which the intensity spectre is split into two parts with a threshold value \(I_{th} = I_{max}/2\).

![Figure 4. Comparison of the key rate as a function of communication distance for original and refined analysis of a passive BB84 decoy-state protocol with two types of signals.](image)

From the results of the simulation, one can see that the developed method allows to significantly refine a secret key rate.

5. Conclusion
In this paper we developed a straightforward approach for decoy state estimation of a passive setup with an arbitrary distribution of intensity. Simulation results show that the refined analysis provides higher key generation rate, thus demonstrating the practical interest in the proposed analysis.

Acknowledgments
Denis Sych acknowledges funding by RFBR, Sirius University of Science and Technology, JSC Russian Railways and Educational Fund “Talent and success” project number 20-32-51004, Yury Kurochkin acknowledges support from Russian Science Foundation grant 17-71-20146 and Arina Gavrilovich acknowledges support from FASIE.
References
[1] Bennett C H and Brassard G 1984 Quantum cryptography: Public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems ad Signal Processing (New York: IEEE) p 175
[2] Bruß D 1998 Phys. Rev. Lett. 81 3018 – 3021
[3] Bechmann-Pasquinucci H and Tittel W 2000 Phys. Rev. A 61(6) 062308
[4] Sych D V, Grishanin B A and Zadkov V N 2004 Phys. Rev. A 70(5) 052331
[5] Sych D, Grishanin B and Zadkov V 2004 Laser Physics 14 1314–1321
[6] Sych D V, Grishanin B A and Zadkov V N 2005 Quantum Electronics 35 80–84
[7] Sych D and Leuchs G 2010 New Journal of Physics 12 053019
[8] Sych D and Leuchs G 2010 Optics and Spectroscopy 108 326–330
[9] Sych D, Averchenko V and Leuchs G 2017 Phys. Rev. A 96(5) 053847
[10] Averchenko V, Sych D, Marquardt C and Leuchs G 2020 Phys. Rev. A 101(1) 013808
[11] Curty M, Ma X, Qi B and Moroder T 2010 Phys. Rev. A 81(2) 022310
[12] Shao-Jie T and Rong-Zhen J 2010 Communications in Theoretical Physics 54 443–446
[13] Shakhovoy R, Sych D, Sharoglazova V, Udaltsov A, Fedorov A and Kurochkin Y 2020 Opt. Express 28 6209–6224
[14] Chau H F 2018 Phys. Rev. A 97(4) 040301