Passive BB84 decoy-state protocol with a flawed source

A Gavrilovich\textsuperscript{1,2,3}, D Sych\textsuperscript{4,5,6} and Y Kurochkin\textsuperscript{1,2,5}

\textsuperscript{1} QRate, Moscow, 121353, Russia
\textsuperscript{2} Russian Quantum Center, Moscow, 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} NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, 119049, Russia
\textsuperscript{6} Sirius University of Science and Technology, Sochi, 354340, Russia

E-mail: gavrilovich.aa@phystech.edu

Abstract. Passive generation of quantum states in quantum key distribution (QKD) is an elegant solution to utilise an internal source of quantum randomness of the transmitter’s scheme. It can be profitable, for example, in setups running at high repetition rates. However, the original analysis of passive protocol doesn’t consider real-life effects of a laser source, therefore possibly breaches the unconditional security of the scheme. Here we take into account the influence of various laser imperfections and make a refined comparison between active and passive setups. We show that the new bound on the secret key rate of the passive protocol stays similar to the one of an active scheme, thus proving passive generation to be a practical means of constructing QKD systems.

1. Introduction

QKD is a procedure enabling two distant parties to generate an identical sequence of random bits, a so-called secret key, in the presence of an eavesdropper. Since the original BB84 proposal [1], there were a number of other QKD protocols with better characteristics designed [2–8]. One of the common features of many QKD protocols is the use of random quantum signals at the transmitter side and a random choice of measurement on the receiving side. The random choice of measurement can be realized in a passive way via a proper set of beam splitters [9–11]. The conventional approach to random state preparation is the use of an active modulation controlled by an external quantum random number generator (QRNG). In some scenarios, for example, when the transmission rate is high, it is preferable to exploit an internal source of quantum randomness during the state preparation, i.e. to use passive quantum state generation.

There are many types of passive methods for quantum states generation, e.g. one can use entanglement [12,13]. A number of experimental realisations of QKD is based on the BB84 decoy-state protocol which can provide high secret key rate in the case of using phase-randomised weak coherent source and transmitting the quantum signal via a lossy channel. A readily available internal source of randomness is the phases of spontaneously emitted laser pulses. After interfering them via an unbalanced interferometer, one can get pulses of random intensity with a known probability density function (PDF). This method of passive generation was introduced
in [3]. However, the recent research [4] shows a significant dependence between probabilistic properties of such interference and different real-life effects such as chirp and jitter, therefore revealing the gap between theoretical model used in [3] and a real device. This mismatch can lead to inaccurate estimation of secret key rate, thus potentially compromising the security of the protocol.

In this work we carry out a refined comparison between the widely used vacuum+weak decoy active BB84 protocol and its passive counterpart. Our simulation shows that both setups (active and passive) provide comparable secret key rates.

2. Active and passive generation
The comparison between active and passive state preparation is shown in Fig.1. In the active scheme pulses are tuned by a QRNG-driven modulator so the intensity randomly takes a value from some pre-determined set. In the passive scheme the role of modulator and QRNG is performed by an unbalanced interferometer, which is designed in a way that the time difference between arms is equal to the period of laser generation. If the laser is modulated over the lasing threshold, the phase difference between pulses is a random value therefore the resulting intensity is random as well. At the end of the interferometer the signal is split into two arms to measure one half with a classical detector and to prepare the other one for the subsequent usage in key distribution (it is attenuated and then sifted by an intensity modulator to get rid of correlations between pulses).

![Conceptual schemes of active (top) and passive (bottom) state generation.](image)

The intensity distribution of passively prepared signals significantly depends on the combined effect of various real-life imperfections, several possible variants are shown in Fig.2. For a detailed review, see [14].

3. Decoy state BB84
A conventional active decoy-state BB84 implies using several different intensities with fixed probabilities of choosing each. The passive source, however, gives a continuous spectrum of intensity. The main idea of passive protocol is to set intervals of intensity values and assign them to different types of signals as shown in Fig. 3.

Thus, one can determine the key quantities of decoy state technique such as the gain $Q_i$, which is the probability that a pulse of $i$-th type is detected on Bob’s side. This quantity can be expressed in terms of yield $Y_j$ which is the conditional probability of photon detection by Bob.
given that Alice sends j-photon state. If i-th type of signal is characterized with $\rho_i$ and Alice uses phase-randomised coherent light with intensity $v$, one can write down a system of equations for gains:

$$Q_{vm} = \sum_{j=0}^{k-1} \rho_{m}v_{m}^{j}e^{-v_{m}}dv_{m} \frac{Y_{j}}{j!} + \sum_{j=k}^{\infty} \rho_{m}v_{m}^{j}Y_{j}e^{-v_{m}}dv_{m}, \quad m \in \{1,k\}$$

(1)

Similarly, defining $e_{i}$ to be the conditional probability of an error for a detected i-photon state, defining $E_{v_{m}}$ to be an overall quantum bit error rate for m-th type, one can formulate a system of equations for unconditional probabilities of having a flipped bit.

$$E_{v_{m}}Q_{vm} = \sum_{j=0}^{k-1} \rho_{m}v_{m}^{j}e^{-v_{m}}dv_{m} \frac{e_{j}Y_{j}}{j!} + \sum_{j=k}^{\infty} \rho_{m}v_{m}^{j}e_{j}Y_{j}e^{-v_{m}}dv_{m}, \quad m \in \{1,k\}$$

(2)

The key generation rate is

$$R = q \left\{ Y_{1}^{L}[1-h_{2}(e_{1}^{U})] \sum_{i=1}^{k} P_{v_{i}}[v_{i}e^{-v_{i}}] - f_{ec} \sum_{i=1}^{k} P_{v_{i}}Q_{v_{i}}^{U}h_{2}(E_{v_{i}}) \right\}$$
here $q \in (0,1]$ is a numerical factor characterizing the implementation of protocol, $f_{ec}$ is the error-correction efficiency, $h_2(x)$ is binary Shannon information function, $P_{vi}$ is the probability of picking $i$-th type of signal. $Q_{vi}$ and $E_{vi}$ are measured directly in the experiment, $Y_{L1}^{L}$ and $e_{U}^{L}$ are lower and upper bounds on the corresponding yield and error. To estimate them we interpret the emphasized factor in (1,2) as the element of a matrix which we call modified Vandermode’s matrix $\tilde{V}$, because it’s structure is very similar to the conventional Vandermode’s matrix. We show that the matrix $\tilde{V}$ is invertible and then derive the formula for $\tilde{V}^{-1}$. Combining the result with H. F. Chau’s technique [15] we obtain the following bounds:

$$Y_{L1}^{L} = \sum_{i=1}^{k} (\tilde{V}^{-1})_{2,i} Q_{vi}, \quad Y_{L1}^{U} = \sum_{i=1}^{k} (\tilde{V}^{-1})_{2,i} (E_{vi}Q_{vi})$$

4. Results and discussion

We simulate PDF of pulse interference in accordance with [14] and numerically calculate secret key rate to compare the refined bound on the performance of passive protocol with that of an active one. The calculated secret key rate for passive and active setups is shown in Fig. 4. From the results of the simulation one can see that both schemes provide similar secret key rates. Therefore, we demonstrate that the refined analysis confirm practicality of passive generation.

Figure 4. Comparison of the key rate as a function of communication distance for active and passive BB84 decoy state protocols.

Acknowledgments

Denis Sych acknowledges support from Russian Foundation for Basic Research grant 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] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 Phys. Rev. Lett. 93 170504
[10] Sych D and Leuchs G 2016 Phys. Rev. Lett. 117(20) 200501
[11] Shcherbatenko M L, Elezov M S, Goltsman G N and Sych D V 2020 Phys. Rev. A 101(3) 032306
[12] Sych D, Averchenko V and Leuchs G 2017 Phys. Rev. A 96(5) 053847
[13] Averchenko V, Sych D, Marquardt C and Leuchs G 2020 Phys. Rev. A 101(1) 013808
[14] Shakhovoy R, Sych D, Sharoglazova V, Udaltsov A, Fedorov A and Kurochkin Y 2020 Opt. Express 28 6209–6224
[15] Chau H F 2018 Phys. Rev. A 97(4) 040301