ERRATA

Erratum to: Are There Enough Decoy States to Ensure Key Secrecy in Quantum Cryptography?

S. N. Molotkov^{a,b,c,*}, K. S. Kravtsov^{d,e}, and M. I. Ryzhkin^a

^a*Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow oblast, 142432 Russia*

^b*Academy of Cryptography of the Russian Federation, Moscow, 121552 Russia*

^c*Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University, Moscow, 119899 Russia*

^d*Faculty of Physics, Moscow State University, Moscow, 119899 Russia*

^e*Prokhorov General Physics Institute, Russian Academy of Sciences, Moscow, 119991 Russia*

*e-mail: sergei.molotkov@gmail.com

Received April 29, 2019; revised April 29, 2019; accepted April 29, 2019

DOI: 10.1134/S1063776119080181

Initially, the decoy state method was proposed to detect a photon number splitting (PNS) attack. In brief, the idea of the method stems from the following premises. Since the phase of the coherent state itself is random in each message, not a pure state, but a statistical mixture of Fock states with different numbers of photons is present in a channel, and the number of photons obeys the Poisson statistics. It is assumed conservatively that the eavesdropper (Eve) can measure the number of photons directly at the transmitting station output. The probability of finding a state with number of photons $|k\rangle\langle k|$ depends on the average number of photons in state, $e^{-\mu}\mu^k/k!$, if a coherent state with average number μ of photons was sent. Having detected given number k of photons, the eavesdropper cannot in principle determine the coherent state from which state $|k\rangle\langle k|$ originates and with which average number of photons (μ , ν_1 , or ν_2). Then it is conservatively assumed that the length of the secret key is determined by the fraction of the single-photon component in the state. It is assumed that from all messages with number of photons $k \geq 2$, the eavesdropper obtains reliable information about the transmitted key bit. To estimate the observed fraction of the single-photon component, states with different average numbers of photons are sent. The fraction of the single-photon component and the error in it are estimated from the count rate of states with different numbers of photons.

The decoy state method was initially developed for detecting a change in the Poisson statistics of states. For certain attacks (e.g., a beam splitting (BS) attack), the Poisson statistics of states remains unchanged. Therefore, it is not obvious beforehand whether the decoy state overestimates the secret key length in such an attack.

This problem was considered in the article [JETP **128**, 544 (2019)]. However, the key length in the decoy

state method was overestimated as compared to a BS attack because of factor $e^{-\mu}$ omitted erroneously in formula (30). This formula must be written as follows:

$$R_{PNS} - R_{BS} = \left\{ \frac{e^{-\mu}\mu(p_d + \eta T(L))}{p_d + 1 - e^{-\mu\eta T(L)}} \right. \\ \times \left[1 - h\left(\frac{0.5p_d}{p_d + \eta T(L)}\right) \right] - h\left(\frac{0.5p_d}{p_d + 1 - e^{-\mu\eta T(L)}}\right) \Bigg\} \\ - \left\{ e^{-\mu(1-T(L))} - h\left(\frac{0.5p_d}{p_d + 1 - e^{-\mu\eta T(L)}}\right) \right\}.$$

It is worth noting in this connection that the lack of Eve's information about the key in the BS attack (term $e^{-\mu(1-T(L))}$) is not conservative for Eve. In a conservative estimate, it is necessary to perform substitution $e^{-\mu(1-T(L))} \rightarrow e^{-\mu}$. Quantity $e^{-\mu}$ is $1 - \chi(\mu) = e^{-\mu}$, $\chi(\mu)$ being a fundamental Holevo quantity having the meaning of the upper boundary of the amount of information that can be received from an ensemble of quantum states directly at the output of the source of quantum states. This boundary includes information from all components of the state (single-photon, two-photon, etc.). In contrast to decoy state estimates, this conservative estimate of Eve's information does not contain any model assumptions concerning the parameters of the channel and detectors (quantum efficiency η and dark noise probability p_d).

The dependences of the secret key length in conservative estimates based on the Holevo boundary in the case of a BS attack and in the decoy state method are shown in the figure. It can be seen that for certain communication line lengths, the conservative estimate based on the fundamental Holevo quantity is more rigorous.

It follows from the above arguments and the figure that different existing conservative estimates of

Fig. 1. (Color online) Secret key length recalculated to a registered message as a function of the communication line length. Curves 1 and R_{PNS} correspond to estimates based on the decoy state method; curves 2 and R_{BS} correspond to BS attack. Parameters: average number of photons $\mu = 0.5$ and detector quantum efficiency $\eta = 0.2$ are the same in (a–d). Dark noise probability is $p_d = 10^{-6}$ (a, b) and 10^{-7} (c, d).

the key length give close but still different results in different regions of the communication channel. In our opinion, the problem of obtaining of universal close estimates for the secret key length (especially for a combination of different attacks) without using

model assumptions has not been solved completely as yet.

The original article can be found online at <https://doi.org/10.1134/S1063776119030105>