Secure decoy-state quantum key distribution with calibration of unknown light sources

Masahiro Kumazawa,[1,2] Toshihiko Sasaki,[1] and Masato Koashi[1,2]

[1]*Photon Science Center, Graduate School of Engineering,*
The University of Tokyo, 7-3-1 Bunkyo-ku, Tokyo 113-8656, Japan
[2]*Department of Applied Physics, Graduate School of Engineering,*
The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan

The security of the decoy-state BB84 protocol, one of the most frequently demonstrated quantum key distribution (QKD) protocols, has usually been proved [1-4] under assumptions on the photon number statistics of the light source, such as a Poissonian distribution. Since these assumptions consist of infinite number of inequalities on the probability distribution of the photon number, it is impossible to verify them directly in a calibration experiment on the source. To bridge this gap, we propose a rigorous security proof of the decoy-state BB84 protocol by considering the calibration of the probability distribution of the photon number from a light source.

We first propose a method to calibrate the probability distribution of the photon number of phase-randomized state $\rho = \sum_{n=0}^{\infty} p_n |n\rangle\langle n|$ from a light source. The method is based on observing various rates of coincidence detections among D threshold detectors. It provides a lower bound p_n^L and an upper bound p_n^U on the probability p_n $(n = 0, \cdots, J)$. The number of J depends on the number of the detectors D. We have mathematically solved the optimization problem which has the constraint from the observed rates to derive the upper and lower bounds.

Next we explain the sketch of the security proof of decoy-state BB84 QKD protocols by using the result of the calibration method. We consider a decoy-state BB84 protocol using three states with different intensities, signal state $\rho_S = \sum_{n=0}^{\infty} a_n |n\rangle\langle n|$, decoy state $\rho_D = \sum_{n=0}^{\infty} a'_n |n\rangle\langle n|$, and vacuum state $\rho_V = |0\rangle\langle 0|$. We assume that the calibration method provides the bounds $a_n^L, a_n^U, a_n'^L, a_n'^U (n = 0, \cdots, J)$, and they satisfy $a_n^L/a_n'^U \geq a_2^U/a_2'^L$ and $a_n^L \geq a_n'^U$ $(n = 2, \cdots, J)$. We can then derive a lower bound on the yield of a 1-photon state, $Y_1^L = (a_2^L Q_D/p' - a_2'^U Q_S/p - (a_0'^U a_2^U - a_0^L a_2'^L)Y_0 - a_2^U(1 - \sum_{i=0}^{J} a_i'^L))/(a_1'^U a_2^U - a_1^L a_2'^L)$, and an upper bound on the error probability for a 1-photon state $e_1^U = (Q_S E_S/p - Q_D E_D/p' - (a_0^L - a_0'^U)e_0 Y_0 + (1 - \sum_{i=0}^{J} a_i'^L))/((a_1^L - a_1'^U)Y_1^L)$, where p and p' are the probabilities of the choice of signal state and decoy state, respectively; Q_S and Q_D ($Q_S E_S$ and $Q_D E_D$) the overall gains (the overall error rates) for signal state and decoy state, respectively. Then the asymptotic secure key rate can be calculated as $R = (pa_1^L + p'a_1'^L)Y_1^L(1 - H(e_1^U)) - (Q_S + Q_D)H((QE_S + QE_D)/(Q_S + Q_D))$. The calculated key rates are shown in FIG. 1, which shows that the calibration with four detectors achieves a rate close to that with Poissonian assumption ($J = \infty$).

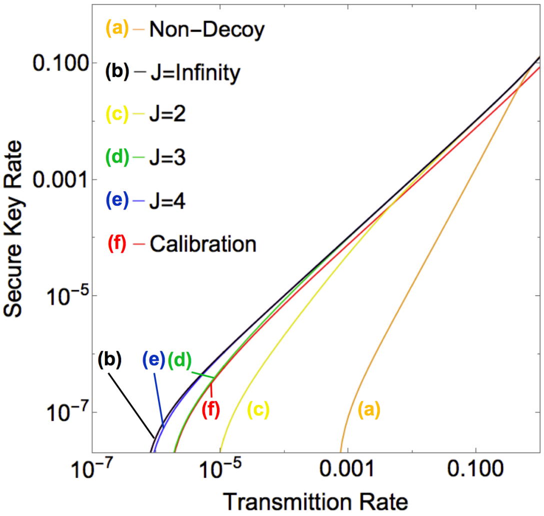

FIG. 1. Secure key rates per pulse for various protocols. The lowest curve (a) is for the BB84 protocol without decoy. The other curves (b)–(f) are for the decoy-state BB84 protocol with various levels of confidence on the light source. (b) An ideal Poissonian source with $a_n = e^{-\mu_S}\mu_S^n/n!$ and $a'_n = e^{-\mu_D}\mu_D^n/n!$ with $\mu_S = 0.5$ and $\mu_D = 0.05$. (c)–(e) The same source but only the values of a_n and a'_n $(n = 0, \cdots, J)$ are known. (f) Based on the calibration method with four detectors applied to the same source. The parameters: $p = 0.5$, $p' = 0.4$, and $Y_0 = 10^{-8}$. We assume a constant bit error rate of 1%.

[1] W. -Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[2] X. -B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[3] H.-K. Lo, et al., Phys. Rev. Lett. **94**, 230504 (2005).
[4] X. -B. Wang, et al., New Journal of Physics **11**, 075006 (2009).