Practical decoy state measurement-device-independent quantum key distribution with coherent state

Shi-Hai Sun[1*], Ming Gao[2], Chun-Yan Li[1], Zhi Ma[2], and Lin-Mei Liang[†1,3]
[1] *Department of Physics, National University of Defense Technology, Changsha 410073, P.R.China*
[2] *Zhengzhou Information Science and Technology Institute, Zhengzhou 450001, P.R.China*
[3] *State Key Laboratory of High Performance Computing, National University of Defense Technology, Changsha 410073, P.R.China*

Although the measurement-device-independent quantum key distribution(MDI-QKD) [1–5] is immune to all the detection attacking, when the practical weak coherent source is used, he decoy state method must be used to defeat the photon-number-splitting (PNS) attack. Recently, the security of the decoy state MDI-QKD has been considered by many researchers [1, 4, 6–8]. However, there still exists some disadvantages for theirs results. In Ref.[1], infinitely many decoy states are needed, which is impractical due to the limited resource in practical situations. In Ref.[4, 6, 7], the authors considered the effect of the finite-size data and a finite number of decoy states, but they estimate the contribution of single-photon pulses by solving the nonlinear minimization problem, but not giving general formulas liking the regular decoy state QKD, furthermore, in their method, four states (vacuum+two-weak decoy state) are needed to close to the asymptotic limit of infinitely decoy states. Therefore, a more stringent security bound and the general theory of decoy state MDI-QKD is imperative.

In this paper, we discuss the decoy state MDI-QKD with vacuum+weak decoy state, in which both Alice and Bob use three kinds of state with different intensity (one signal state, one decoy state and one vacuum state). Then we derive general formulas to estimate the yield Y_{11} and error rate e_{11} for the fraction of signals in which both Alice and Bob send single photon pulse to Charlie. The numerical simulations show that our formulas are very tight, and our vacuum+weak decoy state method asymptotically approaches to the theoretical limit of the infinite decoy state method.

The definitions used in this paper are listed below:

(1)We assume the intensities of signal state, decoy state and vacuum for Alice (Bob) are μ_2, μ_1 and $\mu_0 \equiv 0$ (ν_2, ν_1 and $\nu_0 \equiv 0$). Here we assume $\mu_2 > \mu_1 > 0$ and $\nu_2 > \nu_1 > 0$.

(2)Alice and Bob randomly chooses her basis from $\omega = \{x, z\}$ and bit from $\{0, 1\}$.

(3)$Q^{\omega}_{\mu_i\nu_j}$ ($E^{\omega}_{\mu_i\nu_j}$) is the total gain (error rate) when Alice's intensity is μ_i, Bob's intensity is ν_j.

(4)Y^{ω}_{nm} (e^{ω}_{nm}) is the yield (error rate) when Alice (Bob) sends n-photon (m-photon) pulse.

With these parameters, Alice and Bob can estimate the final key rate, which is given by [1, 6]

$$R \geq \mu_2\nu_2 e^{-\mu_2-\nu_2} Y^z_{11}[1-H(e^x_{11})] - Q^z_{\mu_2\nu_2} f H(E^z_{\mu_2\nu_2}), \quad (1)$$

where f is the error correction inefficiency, $H(x)$ is the binary Shannon entropy function.

In the following, we give two tight formulas to bound Y^{ω}_{11} and e^{ω}_{11}, which are the main contributions of this paper.

Theorem 1: The lower bound of of Y^{ω}_{11} is given by

$$Y^{\omega}_{11} \geq \underline{Y^{\omega}_{11}} \equiv \frac{g^{\omega}_1 + g^{\omega}_2 + g^{\omega}_3 - e^{\mu_2+\nu_2} Q^{\omega}_{\mu_2\nu_2} + e^{\mu_1+\nu_1} Q^{\omega}_{\mu_1\nu_1}}{\mu_1\nu_1 - \mu_2\nu_2 + \alpha\mu_2\nu_1 + \alpha\mu_1\nu_2}. \quad (2)$$

where $\omega = z, x$, $\alpha = \min\{a, b, c\}$, $a = \frac{\mu_2\nu_2^2 - \mu_1\nu_1^2}{\mu_2\nu_1^2 + \mu_1\nu_2^2}$, $b = \frac{\mu_2^2\nu_2 - \mu_1^2\nu_1}{\mu_2^2\nu_1 + \mu_1^2\nu_2}$, $c = \frac{\mu_2^2\nu_2^2 - \mu_1^2\nu_1^2}{\mu_2^2\nu_1^2 + \mu_1^2\nu_2^2}$, and $g_1 = e^{\nu_2} Q_{0\nu_2} + e^{\mu_2} Q_{\mu_2 0} - e^{\nu_1} Q_{0\nu_1} - e^{\mu_1} Q_{\mu_1 0}$, $g_2 = \alpha(e^{\mu_2+\nu_1} Q_{\mu_2\nu_1} - e^{\nu_1} Q_{0\nu_1} - e^{\mu_2} Q_{\mu_2 0} + Q_{00})$, $g_3 = \alpha(e^{\mu_1+\nu_2} Q_{\mu_1\nu_2} - e^{\nu_2} Q_{0\nu_2} - e^{\mu_1} Q_{\mu_1 0} + Q_{00})$.

Theorem 2: The upper bound of e^{ω}_{11} can be written as

$$e^{\omega}_{11} \leq \overline{e^{\omega}_{11}} \equiv \frac{e^{\mu_1+\nu_1} Q^{\omega}_{\mu_1\nu_1} E^{\omega}_{\mu_1\nu_1} - g^{\omega}_4}{\mu_1\nu_1 \underline{Y^{\omega}_{11}}}, \quad (3)$$

where $\omega = z, x$, and $g_4 = e^{\nu_1} Q_{0\nu_1} E_{0\nu_1} + e^{\mu_1} Q_{\mu_1 0} E_{\mu_1 0} - Q_{00} E_{00}$.

When Eve is absent, the total gains and error rates of Alice's intensity μ_i and Bob's intensity ν_j are given by [4, 6] $Q^x_{\mu_i\nu_j} = 2y^2[1 + 2y^2 - 4yI_0(s) + I_0(2s)]$, $Q^x_{\mu_i\nu_j} E^x_{\mu_i\nu_j} = e_0 Q^x_{\mu_i\nu_j} - 2(e_0 - e_d)y^2[I_0(2s) - 1]$, $Q^z_{\mu_i\nu_j} = Q_C + Q_E$, $Q^z_{\mu_i\nu_j} E^z_{\mu_i\nu_j} = e_d Q_C + (1 - e_d) Q_E$, where $Q_C = 2(1 - P_d)^2 e^{-\mu'/2}[1 - (1 - P_d)e^{-\eta_a\mu_i/2}] \times [1 - (1 - P_d)e^{-\eta_b\nu_j/2}]$, $Q_E = 2P_d(1 - P_d)^2 e^{-\mu'/2}[I_0(2x) - (1 - P_d)e^{-\mu'/2}]$. And $I_0(x)$ is the modified Bessel function of the first kind, e_d is the misalignment-error probability, $e_0 = 1/2$ is the error rate of background, P_d is the dark count of single photon detector, η_a (η_b) is the transmission of Alice (Bob), and $\mu' = \eta_a\mu_i + \eta_b\nu_j$, $s = \sqrt{\eta_a\mu_i\eta_b\nu_j}/2$, $y = (1 - P_d)e^{\mu'/4}$. Submitting these parameters into Eq.2 and Eq.3, we can estimate the lower bound of yield Y^z_{11} and upper bound of error rate e^x_{11}, which are shown in Fig.1(b) and (c) respectively, which clearly shows that our vacuum+weak decoy state method is very close to the asymptotic limit of the infinite decoy state method. Then, with these parameters, we can estimate the key rate, which is shown in Fig.1(a). It clearly shows that the key rate with our

*Email:shsun@nudt.edu.cn
†Email:nmliang@nudt.edu.cn

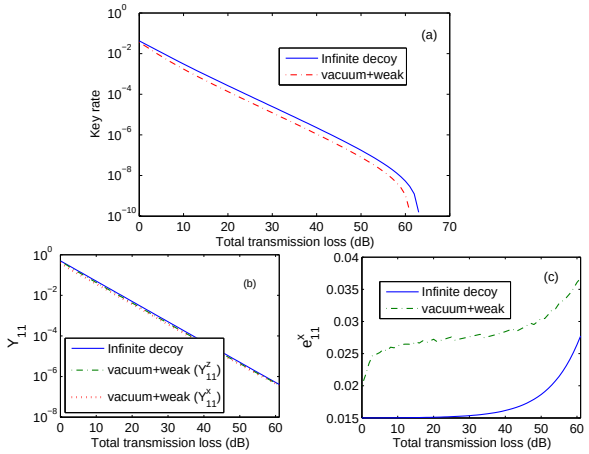

FIG. 1: (Color online) The key rate of decoy state MDI-QKD. The solid line is obtained for the infinite decoy state method, in which the exactly Y_{11}^z and e_{11}^x are known. The dot-dashed line is obtained for our vacuum+weak decoy state method. The key rate is maximized by optimizing the intensity of pulse. The same parameters as Ref.[6] are used in our simulations, which are $e_d = 1.5\%$, $P_d = 3 \times 10^{-6}$, $f = 1.16$.

method is also very close to the asymptotic limit of the infinite decoy state method.

In summary, we discuss the decoy state MDI-QKD with vacuum+weak decoy state. Then we derive general formulas to estimate the yield and error rate for the fraction of signals in which both Alice and Bob send single photon pulse to Charlie. The numerical simulations show that our formulas are very tight, and our method with vacuum+weak decoy state method asymptotically approaches to the theoretical limit of the general decoy state method (with an infinite number of decoy states).

[1] H. -K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[2] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, arXiv:1204.0738.

[3] Y. Liu, T. -Y. Chen, L. -J. Wang, H. Liang, G. -L. Shentu, J. Wang, *et al.*, arXiv:1209.6178.

[4] X. -F. Ma, and M. Razavi, Phys. Rev. A **86**, 062319 (2012).

[5] K. Tamaki, H. -K. Lo, C. -H. F. Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012).

[6] X. -F. Ma, C. -H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).

[7] T. -T. Song, Q. -Y. Wen, F. -Z. Guo, and X. Q. Tan, Phys. Rev. A **86**, 022332 (2012).

[8] X. -B. Wang, arXiv:1207.0392.