An improved scheme on decoy-state method for measurement-device-independent quantum key distribution

Dong Wang1,2,3,4, Mo Li1,2,3,4, Guang-Can Guo1,2,3,4 & Qin Wang1,2,3

Quantum key distribution involving decoy-states is a significant application of quantum information. By using three-intensity decoy-states of single-photon-added coherent sources, we propose a practically realizable scheme on quantum key distribution which approaches very closely the ideal asymptotic case of an infinite number of decoy-states. We make a comparative study between this scheme and two other existing ones, i.e., two-intensity decoy-states with single-photon-added coherent sources, and three-intensity decoy-states with weak coherent sources. Through numerical analysis, we demonstrate the advantages of our scheme in secure transmission distance and the final key generation rate.

Quantum key distribution (QKD) entails two legitimate parties, Alice and Bob, to distribute secure keys in the presence of an eavesdropper, Eve1. The security of QKD has been established theoretically by virtue of the principle of quantum mechanics2–4. However, the security claims are based on theoretical and idealized assumptions, such as some convenient models on the photon sources or the detectors, which are not necessarily met by experimental implementations. In experiment, one usually adopts the weak coherent state (WCS) generated from attenuated lasers to replace the ideal single-photon source, which is unavailable at present. Nevertheless, there are non-negligible multi-photon components in WCS, which can be exploited by Eve via the photon-number-splitting (PNS) attack5–7.

To combat the PNS attack, the powerful decoy-state method is proposed8–17. Then more work about the decoy-state method with an arbitrary number of intensities and related security analysis for finite key length have been discussed18–20. The decoy-state method can be further combined with the newly proposed measurement-device-independent quantum key distribution (MDI-QKD) to fight all other potential detector side-channel attacks21–27. Through the decoy-state method, one can estimate the lower bound of the counting rate and the upper bound of the quantum-bit error-rate (QBER) caused by two-single-photon pulses, and thus obtain a lower bound for the secure key rate. In order to get more precise estimations, one can use better light sources with negligible vacuum component and multi-photon probabilities15,16, or use more intensities of decoy-states25. Large number of intensities of decoy-states will cause experimental difficulties and larger statistical fluctuations. In this report, by using single-photon-added coherent sources (SPACS)28,29, we propose a scheme involving only three intensities of decoy-states which nevertheless can approach very closely the asymptotic case involving infinite number of intensities.

1Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China. 2Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China. 3Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China. 4Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China. Correspondence and requests for materials should be addressed to Q.W. (email: qinw@njupt.edu.cn)
SPACS has a relatively high probability of single-photon and no vacuum component. In principle, the state \(|\alpha, 1\rangle\) of SPACS can be generated by the elementary one-photon excitation on a coherent state\(^{28-30}\), and is theoretically described by applying the photon creation operator \(\hat{a}^\dagger\) to a coherent state \(|\alpha\rangle\):

\[
|\alpha, 1\rangle := \frac{\hat{a}^\dagger|\alpha\rangle}{\sqrt{1 + |\alpha|^2}} = \frac{e^{-|\alpha|^2/2}}{\sqrt{1 + |\alpha|^2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \sqrt{n + 1} |n + 1\rangle.
\]

It is clear that there is no vacuum term contribution in the state of SPACS. The probability of finding \(n\) photons is

\[
P_n(\mu) = \frac{n}{\lambda + 1} e^{-\lambda} \frac{\lambda^n}{(n-1)!}, \quad n = 1, 2, \ldots
\]

where \(\lambda := \frac{1}{2} (\sqrt{\mu^2 - 2\mu + 5} + \mu - 3)\) and \(\mu\) is the mean photon number. SPACS has been experimentally created with high efficiency and fidelity\(^{29-34}\). In particular, Zavatta et al. prepared the SPACS by a conditional technique through parametric down-conversion process\(^{30,34}\), where a piece of LBO crystal is pumped with a Ti:sapphire laser working at 393 nm, and the generated SPACS is working at 786 nm, the overall efficiency obtained is 60%, and the corresponding state fidelity is up to 99.5%. In general, almost all the conditions required for QKD have been matched except for the signal wavelength. Nevertheless, we find no in-principle difficulty in generating the SPACS at telecommunications wavelength since what we need is only to change the phase-match conditions inside nonlinear crystals, e.g., replacing LBO with PPKTP. Therefore, it is feasible to apply SPACS to QKD under present technology.

In this report, we apply SPACS to MDI-QKD by using three-intensity and combining the method proposed by Zhou et al.\(^{35}\). Due to the absence of vacuum component in SPACS, we need not take the contribution of vacuum pulses into account as in other schemes. Using only three non-zero intensities (two decoy-states and one signal state) of SPACS, we can get precise estimation of the counting rate and the contribution of vacuum pulses into account as in other schemes. Using only three non-zero intensities (two decoy-states and one signal state) of SPACS, we can get precise estimation of the counting rate and the quantum bit error rate (QBER) caused by single-photon pulses, which leads to significantly improved final key generation rate and secure transmission distance.

For our scheme, we will need the following results. First, when \(n \geq 2\) and \(1 \leq \mu_x < \mu_y\), the photon number distribution in a state of SPACS has the following property:

\[
\frac{P_{n-1}(\mu_y)}{P_n(\mu_x)} \geq \frac{P_{n-1}(\mu_y)}{P_{n}(\mu_y)} \geq \frac{P_{n}(\mu_y)}{P_{n}(\mu_x)} \geq \frac{P_{n}(\mu_y)}{P_{n}(\mu_x)}
\]

which follows from

\[
\frac{P_{n-1}(\mu_x)}{P_n(\mu_x)} = \frac{(n-1)!}{n} \left( \frac{1}{\lambda_x} \right)^{n-1} = \left( \frac{1}{\lambda_x} \right)^{n-1} \geq 0,
\]

where \(\lambda_x = \frac{1}{2} (\sqrt{\mu_x^2 - 2\mu_x + 5} + \mu_x - 3)\), \(\xi = x, y, z\). The last inequality is ensured by \(\lambda_x < \lambda_y\) since \(1 \leq \mu_x < \mu_y\).

Next, when \(i \leq j \leq k\) and \(\mu_x \leq \mu_y \leq \mu_z\), it holds that

\[
G(i, j, k) := [g_i(\mu_x) - g_j(\mu_x)] [g_j(\mu_y) - g_k(\mu_y)]
\]

\[
- [g_i(\mu_y) - g_j(\mu_y)] [g_j(\mu_x) - g_k(\mu_x)] \geq 0,
\]

where \(g_l(\mu) := \frac{P_l(\mu)}{P_l(\mu_x)}\), \(l \geq 1\), \(\xi = x, y, z\). To prove this, note that:

\[
g_l(\mu) = e^{(\lambda_x-\lambda_y)l} \left( \frac{1 + \lambda_x}{1 + \lambda_z} \right) \left( \frac{\lambda_x}{\lambda_z} \right)^{l-1}, \quad l = i, j, k; \xi = x, y, z,
\]

and \(G(i, j, k)\) can be rewritten as

\[
G(i, j, k) = \frac{1}{\lambda_x\lambda_y\lambda_z^{i+j+k-2}} \begin{vmatrix} \lambda_x^i & \lambda_y^i & \lambda_z^i \\ \lambda_x^j & \lambda_y^j & \lambda_z^j \\ \lambda_x^k & \lambda_y^k & \lambda_z^k \end{vmatrix}
\]

which is positive due to the property of generalized Vandermonde determinant and the conditions \(i \leq j \leq k, \lambda_x < \lambda_y < \lambda_z\).
In MDI-QKD, Alice and Bob simultaneously send signals to an untrusted third party (UTP, possibly controlled by an eavesdropper Eve). The UTP performs a partial BSM and announces whether the measurement result is successful. According to the UTP’s announcement, those successful events will be post-selected and further processed for the final key generation by Alice and Bob. A schematic setup of our three-intensity decoy-state MDI-QKD with SPACS is shown in Fig. 1. Alice and Bob need to randomly prepare the signals with intensities $\alpha$, $\beta$, respectively, where $\alpha, \beta \in \{\mu_x, \mu_y, \mu_z\}$. Here $\mu_x$ and $\mu_y$ are the intensities of the two decoy-states, while $\mu_z$ is the intensity of the signal state, $\mu_x < \mu_y < \mu_z$.

When Alice and Bob send signals with intensities $\alpha$ and $\beta$, respectively, the gain and QBER are given by

$$Q^{W}_{\alpha,\beta} = \sum_{n,m=1}^{\infty} P_n(\alpha) P_m(\beta) Y_{nm}^W, \quad E_{\alpha,\beta}^{W}Q^{W}_{\alpha,\beta} = \sum_{n,m=1}^{\infty} P_n(\alpha) P_m(\beta) e_{nm}^W Y_{nm}^W,$$

respectively. Here $W$ represents the Z- or X-basis, and $n, m$ denote the number of photons sent by Alice and Bob, respectively. $Y_{nm}^W$ denotes the yield, and $e_{nm}^W$ denotes the error rate, when Alice sends an $n$-photon pulse and Bob sends an $m$-photon pulse to the UTP. The decoy-states and signal-state are prepared in different bases. Hereafter we shall omit the superscript $W$ without causing any confusion.

As demonstrated in ref. 25, as long as inequalities (1) and (2) are satisfied, we can get the lower bound of $Y_{11}$ by using the lowest two intensities ($\mu_x$ and $\mu_y$) for Alice and Bob such that

$$Y_{11} \geq Y_{11}^L = \frac{[P_1(\mu_x)P_2(\mu_y) + P_1(\mu_y)P_2(\mu_x)]Q_{\mu_x,\mu_y}}{P_1^2(\mu_x)[P_1(\mu_x)P_2(\mu_y) - P_1(\mu_y)P_2(\mu_x)]} - \frac{P_2(\mu_y)(Q_{\mu_x,\mu_y} + Q_{\mu_y,\mu_z})}{P_1(\mu_x)[P_1(\mu_x)P_2(\mu_y) - P_1(\mu_y)P_2(\mu_x)]}.$$

Moreover, we can get an upper bound of $e_{11}$ by inequalities (1) and (2) as

$$e_{11} \leq e_{11}^U := \frac{1}{\gamma Y_{11}^L} \left| \begin{array}{ccc} T_x & T_y & T_z \\ P_2(\mu_x) & P_2(\mu_y) & P_2(\mu_z) \\ P_3(\mu_x) & P_3(\mu_y) & P_3(\mu_z) \end{array} \right|,$$

where $\gamma = P_1(\mu_x)P_2(\mu_y)P_3(\mu_z)G(1,2,3)$, and for $\xi \in (x,y,z)$,

$$T_\xi = [g_2(\mu_y) + g_3(\mu_z) - g_3(\mu_x)] E_{\mu_x,\mu_y} Q_{\mu_x,\mu_z} - [g_2(\mu_x) + g_3(\mu_z) - g_3(\mu_y)] E_{\mu_y,\mu_z} Q_{\mu_x,\mu_y} + [g_3(\mu_x)g_2(\mu_y) - g_3(\mu_y)g_2(\mu_x)] E_{\mu_x,\mu_y} Q_{\mu_x,\mu_y}.$$

In our protocol, the Z-basis is used as the key generation basis, and the X-basis is for error testing only. Then by inequalities (3) and (4), one can obtain the lower bound of the successful single-photon yield $Y_{11}^{ZL}$ in the Z-basis and the upper bound of the single-photon error rate $e_{11}^{ZU}$ in the X-basis. The final secure key rate can be calculated with the observed total gains and error rates as

$$R \geq P_1^2(\mu_x) Y_{11}^{ZL} [1 - H(\epsilon_{11}^{XU})] - Q_{\mu_x,\mu_x}^Z f H \left( E_{\mu_x,\mu_x}^Z \right),$$

where $f$ is a function of $\epsilon_{11}^{XU}$.
with \( f \) being the error correction efficiency and \( H(p) = -p \log_2(p) - (1-p) \log_2(1-p) \) is the binary Shannon entropy function.

### Numerical Simulation

With inequalities (3–5) we can perform corresponding numerical simulation for our three-intensity MDI-QKD with SPACS. We further compare our scheme with the two-intensity MDI-QKD involving SPACS and the conventional three-intensity MDI-QKD involving WCS. For the total gains and error rates, which can be directly measured from the experiment, we use the channel model and method as in to estimate these values. The relevant parameters are listed in Table 1. During the simulation, for the two-intensity or our three-intensity decoy-states with SPACS, we set reasonable intensities with \( \mu_x = 1.05, \mu_y = 1.06 \) for the decoy-states, and \( \mu_z = 1.10 \) for the signal-state. For the three-intensity decoy-states with WCS, we set \( \mu_x = 0, \mu_y = 0.1 \) for decoy-states, and optimize the intensity for the signal-state \( (\mu_z) \) in each instance. Corresponding simulation results are shown in Figs 2 and 3.

In Fig. 2, we compare the estimation value of \( e_{11} \) between our three-intensity decoy-state method and the conventional two-intensity decoy-state method when both using SPACS. Obviously, by using our three-intensity decoy-state method, we can get significant improvement in the estimation of \( e_{11} \) over the conventional two-intensity decoy-states method.

In Fig. 3(a), we give the comparison of the key generation rates by using different methods, i.e., our three-intensity decoy-state with SPACS, the conventional two-intensity decoy-state with SPACS, and the three-intensity decoy-state with WCS. In each case the key generation rate has been normalized by the corresponding value of using an infinite number of intensities of decoy-states. Moreover, our method approaches very closely the ideal value by using an infinite number of intensities of decoy-states.

In Fig. 3(a), we give the comparison of the key generation rates by using different methods, i.e., our three-intensity decoy-state with SPACS, the conventional two-intensity decoy-state with SPACS, and the three-intensity decoy-state with WCS. In each case the key generation rate has been normalized by the corresponding value of using an infinite number of intensities of decoy-states. We find from Fig. 3(a) that our scheme performs much better than the other two methods: Longer secure transmission distance and much higher key generation rate. Moreover, our scheme shows excellent behavior even at rather long distance (>200 km). It exhibits tens of times or even hundreds of times of enhancement in the key generation rate than the three-intensity decoy-state method with WCS at long distances (>150 km), see the left axis of Fig. 3(b). When compared with the conventional two-intensity decoy-state method with SPACS, our scheme gains even more double enhancement in the key generation rate at very long distances (>200 km), see the right axis of Fig. 3(b).

### Table 1. Parameters values for simulations.

| \( \eta_d \) | \( Y_0 \) | \( e_d \) | \( e_0 \) | \( \alpha \) | \( f \) |
|---|---|---|---|---|---|
| 14.5% | \( 3.0 \times 10^{-4} \) | 1.5% | 0.5 | 0.2 dB/km | 1.16 |

\( \eta_d \) and \( Y_0 \) are the transmittance and dark count rate; \( e_d \) is the probability that the survived photon hits a wrong detector, which is independent of the transmission distance, and \( e_0 \) is the error rate of dark count; \( \alpha \) is the transmission fiber loss constant; \( f \) is the error correction efficiency. The UTP is located midway between Alice and Bob, and all detectors are identical.

![Figure 2. Comparison of the estimated values of e_{11} for MDI-QKD with SPACS by using different number of decoy states.](image-url)

The dashed curve represents the result of our three-intensity decoy-state method, the solid curve represents the result of using an infinite number of decoy-states, and the dotted curve corresponds to the result of two-intensity decoy-states method.
Conclusion
We have introduced an improved scheme on MDI-QKD involving three-intensity decoy-state with SPACS, and have compared its performance with two existing methods. Through numerical simulation, we have demonstrated that our scheme shows excellent behavior in both the secure transmission distance and the final key generation rate. For example, when compared with the conventional two-intensity MDI-QKD with SPACS, the key generation rate is enhanced by several times. Compared with the three-intensity MDI-QKD with WCS, our scheme not only presents almost one hundred kilometers increasing in the secure transmission distance, but also shows tens of times enhancement in the final key generation rate. We emphasize that our scheme depends on SPACS which can be generated with current technology, although its present setup is relatively bulky and has higher technical requirements compared with the WCS system. We can expect that with the development of technology, the emergence of miniaturization and maturing of SPACS system will cause it to replace other sources and launches a wide implementation in quantum key distributions in the near future.

References
1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing [175–179] (IEEE, New York, 1984).
2. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances, Science 283, 2050–2056 (1999).
3. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. 85, 441–444 (2000).
4. Mayers D. Unconditional security in quantum cryptography, J. ACM 48, 351–406 (2001).
5. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography, Phys. Rev. Lett. 85, 1330–1333 (2000).
6. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution, Phys. Rev. A 61, 052304 (2000).

Figure 3. The relative key generation rates of different decoy-state MDI-QKD protocols, either with SPACS or WCS. $S_0$, $S_1$, or $S_2$ represents the key generation rate for MDI-QKD involving three-intensity, two-intensity or infinite decoy-state, with SPACS. $W_3$ and $W_0$ are the corresponding key generation rates with WCS. (a) Comparison of the normalized key generation rate for different methods, i.e., two- or three-intensity decoy-state SPACS, or the three-intensity decoy-state WCS. (b) The ratio of the key generation rates between our scheme and the conventional two-intensity decoy-state with SPACS or the three-intensity decoy-state with WCS.
An improved scheme on decoy-state method of measurement-device-independent quantum key distribution.

How to cite this article
Wang, D. et al. An improved scheme on decoy-state method of measurement-device-independent quantum key distribution. Sci. Rep. 5, 15130; doi: 10.1038/srep15130 (2015).

This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article’s Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/