Decoy-State Quantum Key Distribution with Nonclassical Light Generated in a One-dimensional Waveguide

Huaixiu Zheng, Daniel J. Gauthier, and Harold U. Baranger

Department of Physics, Duke University, P. O. Box 90305, Durham, North Carolina 27708, USA

© 2014 Optical Society of America

OCIS codes: 270.5290, 270.5565, 270.5568

Quantum key distribution (QKD), which allows two distant users, Alice and Bob, to share a secret key with security guaranteed by principles of quantum physics, is the first commercially available application of quantum information science. The first QKD protocol, BB84 [1], proposes to use an ideal single-photon source, which is still beyond the current technology despite tremendous experimental effort worldwide. Hence, most QKD experiments use weak coherent states (WCS) from attenuated lasers as a photon source [2, 3]. Two drawbacks come with the WCS: the multiphoton and the vacuum components. The vacuum content limits Bob’s detection performance, and hence leads to a shorter maximal distance. The multiphoton component makes QKD vulnerable to the photon number splitting attack, where the eavesdropper (Eve) can suppress single-photon signals and split multiphoton signals, keeping one copy and sending one copy to Bob. This way, Eve obtains the full information without being detected, and the unconditional security breaks down. The decoy state method was proposed to beat such attacks [4–6]: Alice prepares additional decoy states, and learns about the eavesdropping from their transmission. Recently, alternative light sources, including spontaneous parametric down-conversion [7] and heralded single-photon [8], have been used in decoy-state QKD.

In this paper, we combine the decoy-state method with a sub-Poissonian single-photon source generated on demand by scattering a coherent state off a two-level system in a one-dimensional waveguide. We show that, compared to coherent state decoy-state QKD, there is a two-fold increase of the key generation rate. Furthermore, the performance is shown to be robust against both parameter variations and loss effects of the system.

We investigate a decoy-state quantum key distribution (QKD) scheme with a sub-Poissonian single-photon source, which is generated on demand by scattering a coherent state off a two-level system in a one-dimensional waveguide. We show that, compared to coherent state decoy-state QKD, there is a two-fold increase of the key generation rate. Furthermore, the performance is shown to be robust against both parameter variations and loss effects of the system.

Decoy-State Quantum Key Distribution with Nonclassical Light Generated in a One-dimensional Waveguide

Huaixiu Zheng*, Daniel J. Gauthier, and Harold U. Baranger†

Department of Physics, Duke University, P. O. Box 90305, Durham, North Carolina 27708, USA

*Corresponding author: hz33@duke.edu
†Corresponding author: baranger@phy.duke.edu

OCIS codes: 270.5290, 270.5565, 270.5568

Compiled May 10, 2014

We investigate a decoy-state quantum key distribution (QKD) scheme with a sub-Poissonian single-photon source, which is generated on demand by scattering a coherent state off a two-level system in a one-dimensional waveguide. We show that, compared to coherent state decoy-state QKD, there is a two-fold increase of the key generation rate. Furthermore, the performance is shown to be robust against both parameter variations and loss effects of the system. © 2014 Optical Society of America

We set the effective Purcell factor $P = \Gamma / \Gamma' = 20$ [12] for now, and return to the effect of loss later. For comparison, we also show $P_n$ (dashed line) of a coherent state with the same mean photon number as the reflected field.
It is remarkable that, for the full parameter range, the reflected field has higher single-photon and lower vacuum and multiphoton content than the coherent state. In the insert of Fig. 1, we show that the multiphoton content is strongly suppressed at $\sigma = \Gamma/2$. This is in agreement with the observed antibunching behavior of microwave photons [11], and is the key to increasing the key generation rate.

Now, we discuss the decoy-state method with light sources, including weak coherent states, a heralded single-photon source (HSPS), and the 2LS source (2LSS). The secure key generation rate (per signal pulse emitted by Alice) is given by [20]

$$ R \geq q\{ -Q_s f(E_s) H_2(E_s) + Q_1[1 - H_2(e_1)] \}, \quad (1) $$

where the efficiency $q$ is 1/2 for the Bennett-Brassard 1984 (BB84) protocol, $f(E_s)$ is the error correction efficiency (we use $f = 1.22$ [21]), $Q_s$ and $E_s$ are the overall gain and error rate of signal states, respectively, $Q_1$ and $e_1$ are the gain and error rate of single-photon states, respectively, and $H_2(x)$ is the binary Shannon information function: $H_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$.

In Eq. (1), while $Q_s$ and $E_s$ are measurable quantities in experiments, $Q_1$ and $e_1$ are unknown variables. $Q_s$ and $E_s$ are given by

$$ Q_s = \sum_{n=0}^{\infty} p_n^s Y_n, \quad E_s = \frac{1}{Q_s} \sum_{n=0}^{\infty} p_n^s Y_n e_n, \quad (2) $$

where $p_n^s$ is the $n$-photon probability of signal states, $e_n$ is the error rate of an $n$-photon state, and $Y_n$ is the $n$-photon yield, i.e., the conditional probability of a click on Bob's side given that Alice has sent an $n$-photon state.

To generate a lower bound on the key generation rate, we have to estimate a lower bound of $Q_1$ (or equivalently $Y_1$ as $Q_1 = p_1^s Y_1$) and an upper bound of $e_1$. Estimating the lower bound $Y_1^d$ and the upper bound $e_1^d$ based solely on Eq. (2) unavoidably underestimates the secure key generation rate due to the lack of enough information about the transmission channel. The decoy-state idea [4–6] is a clever way to obtain additional channel information by sending in additional decoy states. The decoy states are used to detect eavesdropping, but not for key generation. By measuring the transmission of the decoy states, Alice and Bob have another set of constraints

$$ Q_d = \sum_{n=0}^{\infty} p_n^d Y_n, \quad E_d = \frac{1}{Q_d} \sum_{n=0}^{\infty} p_n^d Y_n e_n, \quad (3) $$

where $Q_d$ and $E_d$ are the measured overall gain and error rate of decoy states, respectively. Because Eve has no way to distinguish an $n$-photon decoy state from an $n$-photon signal state, the yield $Y_n$ and the error rate $e_n$ are the same for both the decoy and signal states.

For our numerical simulation, we use the channel model in Ref. 22 to calculate the experimental parameters $Q_s$, $E_s$, $Q_d$, and $E_d$. In this model, the yield is $Y_n = 1 - (1 - Y_0)(1 - \eta)^n$, where $Y_0$ is the background rate and $\eta$ is the overall transmittance given by $\eta = \eta_{AB} \eta_{Bob}$, where $\eta_{AB} = 10^{-\alpha\ell/10}$ is the channel transmittance and $\eta_{Bob}$ is the detection efficiency on Bob's side. Here, $\alpha$ is the loss coefficient and $\ell$ is the transmission distance. The error rate is given by $e_n = [e_0 Y_0 + e_d(Y_n - Y_0)]/Y_n$, where $e_d$ is the probability that a photon hits the wrong detector and $e_0$ is the error rate of the background. We use the experimental parameters in Ref. 23: $\alpha = 0.21$ dB/km, $e_d = 3.3\%$, $Y_0 = 1.7 \times 10^{-6}$, $e_0 = 0.5$, and $\eta_{Bob} = 0.045$.

We apply the linear programming method [24] to estimate $Y_1^d$ and $e_1^d$ from Eqs. (2) and (3). This method is applicable to light sources with general number statistics. We use two decoy states—the vacuum and a weak decoy state. For the weak coherent states, the key generation rate is optimized in terms of the mean photon number in both the signal and decoy states [22]. For the her-
that the maximal transmission distance ($\ell_{\text{max}}$ shown in Fig. 3(a), the key generation rate gradually converges with respect to the variation of system parameter $\Gamma / \sigma$ as shown in Fig. 1.

Due to the reduced vacuum and multiphoton contents, the HSPS scheme. Such a performance enhancement is increased as well. In addition, our scheme also outperforms the WCS method. The maximal transmission distance is increased of key generation rate compared to the same experimental parameters and estimation technique, our scheme using the 2LS source obtains a two-fold increasing of key generation rate compared to the useful for quantum key distribution.

Next, we investigate the robustness of our scheme with respect to the variation of system parameter $\Gamma / \sigma$. As shown in Fig. 3(a), the key generation rate gradually converges as $\Gamma / \sigma$ increases. In particular, the inset shows that the maximal transmission distance ($\ell_{\text{max}}$) has little change for $\Gamma / \sigma \geq 1$.

The effect of loss on the system performance is shown in Figure 3(b). We fix $\sigma = \Gamma / 2$ and choose different loss rates $\Gamma'$ of the 2LS. In Fig. 3(b), we observe that, as $P$ increases, the key generation rate increases and converges. It is evident that, for $P \geq 10$, the performance is very reliable against loss as shown in the insert. Given that values of $P$ as large as 20 have already been achieved in recent experiments [12,25], our scheme can be practically useful for quantum key distribution.

This work was supported by US NSF Grant No. PHY-10-68698. H.Z. is supported by a John T. Chambers Fellowship from the Fitzpatrick Institute for Photonics at Duke University.

References

1. C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, New York, 1984), pp. 175–179.
2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. 81, 1301 (2009).
3. H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
4. W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
5. H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
6. X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
7. Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. 99, 180503 (2007).
8. Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, Phys. Rev. Lett. 100, 090501 (2008).
9. J. Claudon, J. Bleuse, N. S. Malik, M. Bazin, P. Jaffrennou, N. Gregersen, C. Sauvan, P. Lalanne, and J.-M. Gérard, Nat. Photon. 4, 174 (2010).
10. O. Astafiev, A. M. Zagorskin, A. A. Abdumalikov, Y. A. Pashkin, T. Yamamoto, K. Inomata, Y. Nakamura, and J. S. Tsai, Science 327, 840 (2010).
11. I.-C. Hoi, T. Palomaki, J. Lindkvist, G. Johansson, P. Delsing, and C. M. Wilson, Phys. Rev. Lett. 108, 263601 (2012).
12. A. Laucht, S. Prütz, T. Günthner, N. Hauke, R. Saive, S. Frédérick, M. Bichler, M.-C. Amann, A. W. Holleitner, M. Kaniber, and J. J. Finley, Phys. Rev. X 2, 011014 (2012).
13. D. E. Chang, A. S. Sørensen, E. A. Demler, and M. D. Lukin, Nature Phys. 3, 807 (2007).
14. J.-T. Shen and S. Fan, Phys. Rev. Lett. 98, 153003 (2007).
15. E. Rephaeli, S. E. Kocabas, and S. Fan, Phys. Rev. A 84, 063832 (2011).
16. D. Roy, Phys. Rev. Lett. 106, 053601 (2011).
17. P. Kolchin, R. F. Oulton, and X. Zhang, Phys. Rev. Lett. 106, 113601 (2011).
18. H. Zheng, D. J. Gauthier, and H. U. Baranger, Phys. Rev. Lett. 107, 223601 (2011).
19. H. Zheng, D. J. Gauthier, and H. U. Baranger, Phys. Rev. A 82, 063816 (2010).
20. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).
21. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. 85, 1330 (2000).
22. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A 72, 012326 (2005).
23. G. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. 84, 3762 (2004).
24. T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Introduction to Algorithms (MIT Press and McGraw-Hill, New York, 2009), 3rd ed.
25. M. H. Mikkelsen, private communication (2012).
References

1. C. H. Bennett and G. Brassard, “Proceedings of Ieee International Conference on Computers, Systems, and Signal Processing,” (IEEE, New York, 1984), pp. 175–179.
2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Rev. Mod. Phys. 81, 1301 (2009).
3. H.-K. Lo, M. Curty, and B. Qi, “Measurement-Device-Independent Quantum Key Distribution,” Phys. Rev. Lett. 108, 130503 (2012).
4. W.-Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” Phys. Rev. Lett. 91, 057901 (2003).
5. H.-K. Lo, X. Ma, and K. Chen, “Decoy State Quantum Key Distribution,” Phys. Rev. Lett. 94, 230503 (2005).
6. E.-B. Wang, “Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography,” Phys. Rev. Lett. 94, 230503 (2005).
7. Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, “Simple and efficient quantum key distribution with parametric down-conversion,” Phys. Rev. Lett. 99, 180503 (2007).
8. Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, “Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source,” Phys. Rev. Lett. 100, 090501 (2008).
9. J. Claudon, J. Bleuse, N. S. Malik, M. Bazin, P. Jaffrennou, N. Gregersen, C. Sauvan, P. Lalanne, and J.-M. Gérard, “A highly efficient single-photon source based on a quantum dot in a photonic nanowire,” Nat. Photon. 4, 174 (2010).
10. O. Astafiev, A. M. Zagoskin, A. A. Abdumalikov, Y. A. Pashkin, T. Yamamoto, K. Inomata, Y. Nakamura, and J. S. Tsai, “Resonance Fluorescence of a Single Artificial Atom,” Science 327, 840–843 (2010).
11. I.-C. Hoi, T. Palomaki, J. Lindkvist, G. Johansson, P. Delsing, and C. M. Wilson “Generation of Nonclassical Microwave States Using an Artificial Atom in 1D Open Space,” Phys. Rev. Lett. 108, 263601 (2012).
12. A. Laucht, S. Pütz, T. Günthner, N. Hauke, R. Saive, S. Frédérick, M. Bichler, M.-C. Amann, A. W. Holleitner, M. Kaniber, and J. J. Finley, “A waveguide-coupled on-chip single-photon source,” Phys. Rev. X 2, 011014 (2012).
13. D. E. Chang, A. S. Sørensen, E. A. Demler, and M. D. Lukin, “A single-photon transistor using nanoscale surface plasmons,” Nature Phys. 3, 807–812 (2007).
14. J.-T. Shen and S. Fan, “Strongly correlated two-photon transport in a one-dimensional waveguide coupled to a two-level system,” Phys. Rev. Lett. 98, 153003 (2007).
15. E. Rephaeli, S. E. Kocabas, and S. Fan, “Few-photon transport in a waveguide coupled to a pair of colocated two-level atoms,” Phys. Rev. A 84, 063832 (2011).
16. D. Roy, “Two-photon scattering by a driven three-level emitter in a one-dimensional waveguide and electromagnetically induced transparency,” Phys. Rev. Lett. 106, 053601 (2011).
17. P. Kolchin, R. F. Oulton, and X. Zhang, “Nonlinear quantum optics in a waveguide: Distinct single photons strongly interacting at the single atom level,” Phys. Rev. Lett. 106, 113601 (2011).
18. H. Zheng, D. J. Gauthier, and H. U. Baranger, “Cavity-free photon blockade induced by many-body bound states,” Phys. Rev. Lett. 107, 223601 (2011).
19. H. Zheng, D. J. Gauthier, and H. U. Baranger, “Waveguide qed: Many-body bound-state effects in coherent and fock-state scattering from a two-level system,” Phys. Rev. A 82, 063816 (2010).
20. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” Quantum Inf. Comput. 4, 325 (2004).
21. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on practical quantum cryptography,” Phys. Rev. Lett. 85, 1330–1333 (2000).
22. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” Phys. Rev. A 72, 012326 (2005).
23. G. Gobby, Z. L. Yuan, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber,” Appl. Phys. Lett. 84, 3762–3764 (2004).
24. T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Introduction to Algorithms (MIT Press and McGraw-Hill, New York, 2009), 3rd ed.
25. M. H. Mikkelsen, private communication (2012).