SCIENCE CHINA
Physics, Mechanics & Astronomy

• Article •

December 2021 Vol. 64 No. 12: 120311
https://doi.org/10.1007/s11433-021-1775-4

Practical decoy-state quantum secure direct communication

Xin Liu[1], Zijian Li[1], Di Luo[1], Chunfeng Huang[1], Di Ma[1], Minming Geng[2], Junwei Wang[3], Zhenrong Zhang[2], and Kejin Wei[1*]

[1] *Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning 530004, China;*
[2] *Guangxi Key Laboratory of Multimedia Communications and Network Technology, School of Computer, Electronics, and Information, Guangxi University, Nanning 530004, China;*
[3] *CAS Quantum Network Co., Ltd, Shanghai 201315, China*

Received July 2, 2021; accepted August 20, 2021; published online October 28, 2021

Quantum secure direct communication (QSDC) has been demonstrated in both fiber-based and free-space channels using attenuated lasers. Decoy-state QSDC by exploiting four decoy states has been proposed to address the problem of photon-number-splitting attacks caused by the use of attenuated lasers. In this study, we present an analysis of the practical aspects of decoy-state QSDC. First, we design a two-decoy-state protocol that only requires two decoy states, thereby significantly reducing experimental complexity. Second, we successfully perform full parameter optimization for a real-life QSDC system by introducing a genetic algorithm. Our simulation results show that the two-decoy-state protocol could be the best choice for developing a practical QSDC system. Furthermore, full optimization is crucial for a high-performance QSDC system. Our work serves as a major step toward the further development of practical decoy-state QSDC systems.

quantum secure direct communication, decoy-state method, full parameter optimization

PACS number(s): 03.67.Dd, 03.67.Hk, 03.67.Ac

Citation: X. Liu, Z. Li, D. Luo, C. Huang, D. Ma, M. Geng, J. Wang, Z. Zhang, and K. Wei, Practical decoy-state quantum secure direct communication, Sci. China-Phys. Mech. Astron. **64**, 120311 (2021), https://doi.org/10.1007/s11433-021-1775-4

1 Introduction

Secure communication is crucial for economic, political, and social applications in the current age of information. The goal of secure communication is to exchange a secret message between two remote legal users, such that an eavesdropper (Eve) cannot intercept such a message. Currently, secure communication is guaranteed through public-key cryptography [1], which is mainly based on the computational difficulty of a specific mathematical problem. However, the security of such cryptographic approaches is at risk of being compromised owing to the rapid advancements in algorithmic [2] and computational power, and most notably, in quantum computing [3-5].

Quantum secure direct communication (QSDC), which was first proposed by Long and Liu [6] in 2000, has been introduced to allow users to directly transmit secret messages without any restrictions brought on by the Eve's computing power. Through significant effort, QSDC has developed remarkably both in theory and experimentally [7]. So far, security of QSDC has been proven by using Wyner's wiretap channel theory [8]. Several theoretical QSDC protocols

*Corresponding author (email: kjwei@gxu.edu.cn)

have been proposed to resolve technical challenges [9-12] or enhance efficiency [13]. Recently, semi-device [14-18] and device-independent schemes [19] have been reported to close the loopholes caused by the imperfections of practical components [20, 21]. Despite the point-to-point protocols, multiuser QSDC schemes have been developed, and their performance has been verified [22-25]. Recently, numerous novel quantum resources [26-28], such as the superposition of a single photon [28], have been introduced to perform QSDC.

When it comes to experiments, Hu et al. [29] reported the first experimental demonstration of QSDC using frequency coding. Subsequently, the feasibility of the entanglement-based QSDC protocol was proven through the help of atomic quantum memory [30]. Then the transmission distance was extended to an adequate distance of 0.5-km fiber [31]. Qi et al. [32] developed a practical QSDC system and further extended the transmission distance to 1.5-km fiber. Recently, a fully operational system for free-space QSDC was reported, and a secure key rate (SKR) of 500 bits per second (bps) over a 10-m free space was achieved [33].

Generally, many exciting experiments mentioned above employed weak-coherent pulses (WCPs), which occasionally emit multiphoton signals, as the sources. This attribute opens the door for sophisticated eavesdropping attacks, such as photon-number-splitting (PNS) attacks, whereby the Eve blocks all the single-photon signals and splits the multiphoton signals, thereby keeping one copy for measuring and resending the remains to a receiver, Bob. Fortunately, this problem has recently been solved by introducing the so-called decoy-state method [34, 35], whereby different intensities of WCPs are used to estimate the contribution of single-photon signals [33].

However, to ensure the practical application of decoy-state QSDC, several challenges must be addressed. First, although the decoy-state protocol was studied in the work of the ref. [33], it required five different intensities (one signal state and four decoy states) for parameter estimation, which increased the complexity of the experimental settings and the cost of random numbers. Second, the parameter optimization, including the intensities of the signal and decoy states as well as the probability of sending them, was ignored in previous studies owing to non-trivial technical challenges. Note that full parameter optimization, which has been extensively exploited in other branches of quantum cryptography [36-40], has proven to be essential in obtaining a high-performance system.

In this study, we provide solutions to address the implementation issues mentioned above. We design a practical decoy-state QSDC protocol, which only requires two decoy states, thereby significantly reducing experimental complexity. By simulating a real-life experiment, we find that our proposed two-decoy-state protocol always outperforms the four-decoy-state protocol, and the only exception occurs at significantly short distances. Furthermore, we use a genetic algorithm (GA) to successfully perform a full parameter optimization for QSDC. Through optimal parameters, both the secrecy capacity and the secure distance are significantly improved by more than two times compared with the non-optimization results.

The remainder of this paper is organized as follows: In sect. 2, we introduce the decoy-state protocol for QSDC. In sect. 3, we present the two-decoy-state QSDC scheme. In sect. 4, we perform full optimization on all experimental parameters. In sect. 5, we present the simulation results. Finally, we present the conclusion in sect. 6.

2 General decoy-state QSDC

Pan et al. [33] conducted a rigorous security analysis for a practical DL04-QSDC system under a general collective attack on a single photon and a PNS attack on multiple photons. Specifically, the work exploited the Wyner's wiretap channel theory and achieved a lower bound of the secrecy capacity of the QSDC system, which is expressed as follows:

$$\begin{aligned} C_{\mathrm{s}} =& Q_{\mu}^{BAB}\left[1-h\left(E_{\mu}^{BAB}\right)\right]-Q_{\mu,n=1}^{BAE}h\left(2e_{1}^{BA}\right) \\ &-Q_{\mu,n=2}^{BAE}\left[\frac{1}{2}h\left(2e_{2}^{BA}\right)+\frac{1}{2}\right]-Q_{\mu,n\geq 3}^{BAE}\cdot 1, \end{aligned} \tag{1}$$

where Q_{μ}^{BAB} and E_{μ}^{BAB} represent the overall gain and the overall (quantum bit error rate) QBER of signal state μ at Bob, e_1^{BA} (e_2^{BA}) represents the detection quantum bit error rate (DQBER) of a single (two) photon signal, $Q_{\mu,n}^{BAE}$ represents the n-photon signal gain at the Eve, and $h(x) = -x\log_2 x-(1-x)\log_2(1-x)$ represents the binary Shannon entropy.

Seven key variables are required in eq. (1). Q_{u}^{BAB} and E_{u}^{BAB} are directly measured from the experiment, whereas the remaining variables must be estimated using sophisticated techniques. Therefore, Pan et al. [33] introduced a well-established decoy-state method for QSDC to accurately estimate the remaining variables. In other words, besides the signal state μ, Bob randomly prepares m weak intensities states (decoy states, represented as ν_1, ν_2, ν_3, $\ldots$, ν_m) and sends them to Alice. Alice randomly chooses part of the received states to perform a decoy analysis to estimate the remaining variables. In other words, Bob publishes the pulses that are decoy states, and Alice receives their corresponding gain Q_x^{BA} and QBER E_x^{BA}, as follows:

$$Q_{x}^{BA}=\sum_{n=0}^{\infty}Y_{n}^{A}\frac{e^{-x}}{n!}x^{n}=Y_{0}^{A}+1-e^{-\eta^{BA}x},$$

$$E_x^{BA}Q_x^{BA} = \sum_{n=0}^{\infty} e_n^{BA}Y_n^A \frac{e^{-x}}{n!}x^n = e_0 Y_0^A + e_{\text{det}}^{BA}\left(1 - e^{-\eta^{BA}x}\right), \quad (2)$$

where Y_n denotes the yield of an n-photon signal, and $x \in \{\mu, \nu_1, \nu_2, \nu_3, \ldots, \nu_m\}$ represents the intensities for different states. In principle, when $m \to \infty$, we can mathematically deduce the exact values of $Q_{\mu,n\geq 1}^{BA}$ and $e_{n\geq 1}^{BA}$. Moreover, we can estimate $Q_{\mu,n}^{BAE}$ from the value of $Q_{\mu,n}^{BA}$, as presented in the work of Pan et al. [33], as follows:

$$Q_{\mu,n}^{BAE} = p(n,\mu)Y_n^E \leq \left[Q_{\mu,n}^{BA} - p(n,\mu)Y_n^A\right]\max\left\{1, \frac{\gamma^E}{\gamma^A}\right\}, \quad (3)$$

where γ^A represents the overall transmission for the photons received and measured by Alice, and γ^E represents the overall transmission of the Eve after Alice encodes her received photons.

For practical implementation, Pan et al. also proposed a four-decoy-state protocol because it is impossible to prepare infinite decoy states. Moreover, they demonstrated that a decoy QSDC can be secure over 5 dB channel attenuation for the free-space QSDC setup. Further details on the four-decoy-state protocol are summarized in Appendix A2. Nonetheless, we remark that the four-decoy-state protocol may still be practically inefficient because it would increase experimental complexity as well as random number consumption during state preparation.

3 Two-decoy-state QSDC

In this section, we propose a two-decoy-state protocol for QSDC. In other words, we use a vacuum state and a weak state to estimate variables. Before conducting our analysis, we provide a key theoretical observation on Wyner's wiretap secrecy capacity, which was achieved by Pan et al. As shown in eq. (1), it is necessary to estimate the DQBER of e_2^{BA} caused by two photons to ensure the rigorous bounding of the leaking information to the Eve. Therefore, four decoy states are required in Pan's four-decoy-state protocol. However, we note that for a weak coherent state, the proportion of two photons is far smaller than that of a single photon, indicating that the leaking information from two photons is negligible compared with that from a single photon. Therefore, for practical implementation, we propose using a weak version of Wyner's wiretap secrecy capacity result, which is expressed as follows:

$$C_{\text{s}} = Q_\mu^{BAB}\left[1 - h\left(E_\mu^{BAB}\right)\right] - Q_{\mu,n=1}^{BAE}h\left(2e_1^{BA}\right) - Q_{\mu,n\geq 2}^{BAE}\cdot 1, \quad (4)$$

where we simply assume that the Eve receives all the secret information of the multiple photons ($n \geq 2$). Such a formula does not require an evaluation of e_2^{BA}, and fewer decoy sates can be sufficient for variable estimation. To describe our two-decoy-state protocol, we must model a real-life QSDC system. In this study, we consider a practical QSDC system that is similar to that presented in ref. [33]. The system model is generalized from the work of Ma et al. [41], and it is presented in Appendix A1.

We assume that in a two-decoy-state protocol, the average photon numbers of the signal state and the two decoy states (weak and vacuum) are μ, and ν_1 and ν_2, respectively, which satisfies the following requirements:

$$\begin{aligned} &0 \leq \nu_2 \leq \nu_1, \\ &\nu_1 + \nu_2 < \mu. \end{aligned} \quad (5)$$

As shown in the work of ref. [41], the lower bound of Y_1^{BA} and the upper bound of e_1^{BA} can be estimated as follows:

$$\begin{aligned} Y_1^{BA} \geq Y_1^{BA,L,\nu_1,\nu_2} = &\frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \\ &\times\left(Q_{\nu_1}^{BA}e^{\nu_1} - Q_{\nu_2}^{BA}e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2}\left(Q_\mu^{BA}e^\mu - Y_0^A\right)\right), \end{aligned} \quad (6)$$

$$e_1^{BA} \leq e_1^{BA,U,\nu_1,\nu_2} = \frac{E_{\nu_1}^{BA}Q_{\nu_1}^{BA}e^{\nu_1} - E_{\nu_2}^{BA}Q_{\nu_2}^{BA}e^{\nu_2}}{(\nu_1 - \nu_2)\,Y_1^{BA,L,\nu_1,\nu_2}}. \quad (7)$$

In this study, Y_0^A denotes the background rate, and it can be estimated using the vacuum state, which is expressed as follows:

$$Y_0^A \geqslant Y_0^{A,L} = \max\left\{\frac{\nu_1 Q_{\nu_2}e^{\nu_2} - \nu_2 Q_{\nu_1}e^{\nu_1}}{\nu_1 - \nu_2}, 0\right\}. \quad (8)$$

Combined with eq. (3), a lower bound of $Q_{\mu,n=1}^{BAE}$ and $Q_{\mu,n=1}^{BAE,L}$ is obtained as follows:

$$\begin{aligned} Q_{\mu,n=1}^{BAE,L} &\leq \left[Q_{\mu,n=1}^{BA,L} - p(n=1,\mu)Y_0^A\right]\max\left\{1, \frac{\gamma^E}{\gamma^A}\right\} \\ &= p(n=1,\mu)\left(Y_1^{BA,L,\nu_1,\nu_2} - Y_0^A\right)\max\left\{1, \frac{\gamma^E}{\gamma^A}\right\}. \end{aligned} \quad (9)$$

4 Full parameter optimization

In practical QSDC implementations, when considering the decoy-state protocol, the intensity choices of the signal and decoy states as well as the probabilities of sending these states are crucial in achieving improved system performance. From eq. (4), we note that the secrecy capacity of QSDC has the same sense with the key rate formal of QKD. So, the physical meaning of the optimal intensities for decoy-state QSDC protocol are similar with that of QKD. That is the optimal value of signal state μ is maximize the gain of Q_μ^{BAB}, which is the only source for the final secrecy capacity. The optimal values of decoy states ν_1 and ν_2 is to be improving the estimation of Y_1^{BA} and e_1^{BA}.

To find the optimal values $\{\mu, \nu_1, \nu_2\}$ based on given experimental parameters, such as optical misalignment, data size, and channel attenuation, we can get optimal functions between optimal values and experimental parameters by solving

$$\frac{\partial C_{\mathrm{s}}}{\partial \mu} = 0, \ \frac{\partial C_{\mathrm{s}}}{\partial \nu_1} = 0, \ \frac{\partial C_{\mathrm{s}}}{\partial \nu_2} = 0, \tag{10}$$

which are rather complicatedly mathematical problems. Instead, we do it by using full numerical optimization.

Generally, such full optimization is completed using a brute-force global search, which is challenging owing to limited computational power. This might be a major reason why parameter optimization has been neglected in previous decoy-state QSDC. For example, for the four-decoy-state protocol [33], seven parameters must be optimized, i.e., the signal state intensity μ, the intensity of the three decoy states ν_1, ν_2, and ν_3, the probability of sending the signal state P, and that of the decoy states P_{ν_1}, P_{ν_2}, and P_{ν_3}. If we employ a brute-force global search using a standard desktop (Intel(R) Core(TM) i7-10700F CPU @2.90 GHz; GPU: NVIDIA GeForce GT 1030), simply searching over a significantly crude 10-sample resolution for each parameter would take over $\geq$ 400 h. Moreover, because the secrecy capacity function is nonconvex with respect to parameter space, some well-established optimization methods, such as local search algorithms, cannot execute parameter optimization for QSDC.

To solve this problem, we propose a method based on a GA, which is a well-known algorithm in the field of computer science. A GA is a general-purpose search algorithm, which can exploit the accumulated information regarding an initially unknown search space to guide subsequent searches into useful subspaces. This key feature enables the GA to efficiently find QSDC optima, even in cases involving complex, large, and poorly understood search spaces. As a result, the GA enables one to efficiently perform full optimization on all experimental parameters.

We apply the GA on QSDC and show the results compared with those of non-optimization, as shown in Figure 1. It can be observed that parameter optimization using the GA can significantly increase the secrecy capacity and extend the secure distance. Further details regarding this method are provided in Appendix A3.

5 Simulation

In all the simulations presented below, we used the experimental parameters that are mainly extracted from the free-space QSDC experiment provided in ref. [33], i.e., Alice and Bob use the superconducting single-photon detector with detection efficiency $\eta_{\mathrm{d}}^A = \eta_{\mathrm{d}}^B = \eta_{\mathrm{d}} = 70\%$ and background detection events $Y_0^A = Y_0^B = Y_0 = 8\times10^{-8}$, the intrinsic detector error rates are $e_0 = 1/2$, $e_{\mathrm{d}}^{BA} = 1.31\%$ and $e_{\mathrm{d}}^{BAB} = 0.26\%$.

5.1 Secrecy capacity comparison between full optimization and non-optimization

In previous studies on decoy-state QSDC [12, 33], researchers used empirical parameters without optimization. In this study, we compare our optimized secrecy capacity with those using typical parameters in ref. [33]. Figure 1 shows the comparison results. The orange-colored solid (purple dotted) curve represents the secrecy capacity using our two-decoy protocol with optimized (empirical) parameters. For comparison purposes, the yellow dotted curve shows the secrecy capacity, which results from using the parameters presented in the work of Pan et al. [33]. It can be observed that the optimized secrecy capacity using the GA for the two-decoy protocol is much higher than that of the non-optimized results, as well as that of the non-optimized results of the four-decoy protocol. Therefore, parameter optimization using the GA not only increases the secrecy capacity but also extends the secure distance. These results highlight the importance of parameter optimization in practical decoy-state QSDC.

5.2 Secrecy capacity comparison of the two-decoy-state and four-decoy-state protocols

Figure 2 shows the comparison results of the two-decoy-state

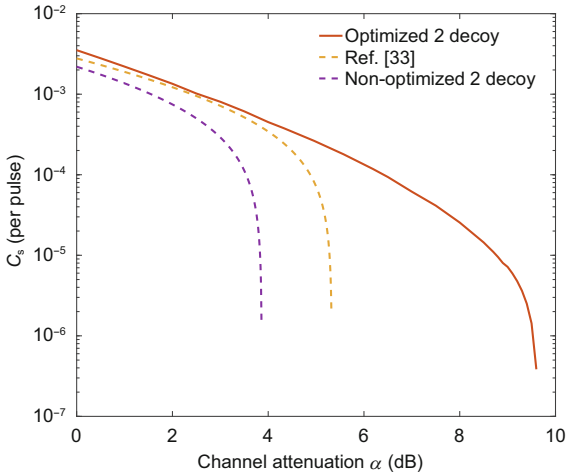

Figure 1 (Color online) Optimized and non-optimized secrecy capacity C_{s} for infinite data with different numbers of decoy states. The orange solid and purple dotted curves represent the secrecy capacity using our two-decoy protocol with optimized and empirical parameters ($\mu = 0.1$, $\nu_1 = 0.05$, and $\nu_2 = 0.02$). The yellow dotted curve shows the results of using the parameters ($\mu = 0.1$, $\nu_1 = 0.07$, $\nu_2 = 0.0445$, and $\nu_3 = 0.03$) presented in the work of ref. [33].

and the four-decoy-state in the case of infinite data. The secrecy capacity C_s and the optimized parameters for different channel attenuations α are listed in Table 1. At a low-attenuation regime (< 3 dB), the secrecy capacity of the four-decoy-state protocol is higher than that of the two-decoy-state protocol. However, the two-decoy-state protocol outperforms the four-decoy-state protocol over long distances. The improvement mainly results from the fewer constraints on the chosen parameters in the two-decoy-state protocol. Therefore, it is easy to find optimized parameters for obtaining improved performance in the two-decoy-state protocol. As shown in Table 1, the secrecy capacity using two decoy states is approximately 300% higher than that using four decoy states at a channel attenuation of 6 dB. Furthermore, at a channel attenuation of 9 dB, no secrecy capacity can be obtained using four decoy states. In contrast, the two-decoy-sate protocol produces a positive secrecy capacity.

Intuitively, the four-decoy-state protocol provides a higher secrecy capacity in quantum cryptography. On the other hand, in QSDC, the four-decoy-state protocol is only useful for significantly short distances, and the two-decoy-state protocol always outperforms the four-decoy-state protocol at long distances. In the first case, the four-decoy-state protocol can obtain a satisfactory estimation of e_2^{BA}, thereby providing a higher secrecy capacity. However, in the second case, the two-decoy-state protocol has relatively fewer constraints (this can be observed by comparing eq. (5) with eq. (a9)) on the choice of the signal and decoy intensities. Therefore, the two-decoy-state protocol obtains a higher secrecy capacity.

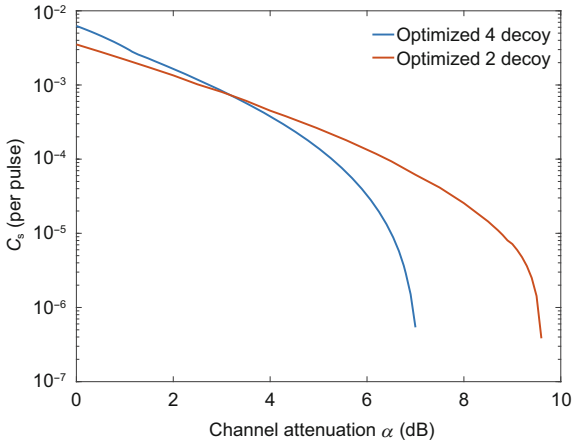

Figure 2 (Color online) Comparison results of the two decoy states and the four-decoy states in the case of infinite data. The orange-colored and the blue-colored solid curves represent the secrecy capacity with optimization using our proposed two-decoy protocol and the four-decoy protocol presented in the work of ref. [33].

Table 1 Secrecy capacity comparison and corresponding parameters at channel losses of 6 and 9 dB. The two-decoy-sate protocol involves only two decoy states, so ν_3 does not exist. When the channel attenuation is 9 dB, the secrecy capacity cannot be obtained using the four decoy states, and there is no optimal parameter

Parameters	Two decoy states		Ref. [33]	
	6 dB	9 dB	6 dB	9 dB
μ	0.0411	0.0119	0.0335	–
ν_1	0.0346	0.0078	0.0251	–
ν_2	0.0064	0.0040	0.0129	–
ν_3	–	–	2.49×10^{-8}	–
C_s	1.34×10^{-4}	7.22×10^{-6}	3.27×10^{-5}	–

6 Conclusion

In summary, in this study, we propose a practical decoy-state QSDC protocol that only uses two decoy states. Our simulation results show that our proposed decoy-state protocol outperforms previous four-decoy-state protocols in the high-loss regime. In addition, we introduce a GA to perform parameter optimization, and we prove that parameter optimization can significantly increase the secrecy capacity and extend the secure distance for decoy-state QSDC. Considering the simple components for two decoy states, the two-decoy-state protocol would be the best choice for developing a practical decoy-state QSDC system.

This study was supported by the National Natural Science Foundation of China (Grant Nos. 62171144, 62031024, and 11865004), and the Guangxi Science Foundation (Grant No. 2017GXNSFBA198231). We thank D. Pan, L. Yin and G.-L. Long for very helpful discussions.

1 R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).
2 P. W. Shor, in *Algorithms for quantum computation: discrete log and factoring: Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, 1994), p. 124.
3 F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrá, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Nature **574**, 505 (2019), arXiv: 1910.11333.
4 H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, Science **370**, 1460 (2020).
5 J. M. Arrazola, V. Bergholm, K. Brádler, T. R. Bromley, M. J. Collins, I. Dhand, A. Fumagalli, T. Gerrits, A. Goussev, L. G. Helt, J. Hundal,

T. Isacsson, R. B. Israel, J. Izaac, S. Jahangiri, R. Janik, N. Killoran, S. P. Kumar, J. Lavoie, A. E. Lita, D. H. Mahler, M. Menotti, B. Morrison, S. W. Nam, L. Neuhaus, H. Y. Qi, N. Quesada, A. Repingon, K. K. Sabapathy, M. Schuld, D. Su, J. Swinarton, A. Száva, K. Tan, P. Tan, V. D. Vaidya, Z. Vernon, Z. Zabaneh, and Y. Zhang, Nature **591**, 54 (2021), arXiv: 2103.02109.
6 G. L. Long, and X. S. Liu, Phys. Rev. A **65**, 032302 (2002), arXiv: quant-ph/0012056.
7 C. Wang, Fundam. Res. **1**, 91 (2021).
8 J. Wu, Z. Lin, L. Yin, and G.-L. Long, Quantum Eng. **1**, e26 (2019).
9 F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003), arXiv: quant-ph/0308173.
10 F. G. Deng, and G. L. Long, Phys. Rev. A **69**, 052319 (2004), arXiv: quant-ph/0405177.
11 S. S. Chen, L. Zhou, W. Zhong, and Y. B. Sheng, Sci. China-Phys. Mech. Astron. **61**, 90312 (2018).
12 L. Yang, J. W. Wu, Z. S. Lin, L. G. Yin, and G. L. Long, Sci. China-Phys. Mech. Astron. **63**, 110311 (2020).
13 C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Phys. Rev. A **71**, 044305 (2005).
14 P. H. Niu, Z. R. Zhou, Z. S. Lin, Y. B. Sheng, L. G. Yin, and G. L. Long, Sci. Bull. **63**, 1345 (2018).
15 Z. R. Zhou, Y. B. Sheng, P. H. Niu, L. G. Yin, G. L. Long, and L. Hanzo, Sci. China-Phys. Mech. Astron. **63**, 230362 (2020), arXiv: 1805.07228.
16 Z. Gao, T. Li, and Z. Li, Europhys. Lett. **125**, 40004 (2019).
17 Z. K. Zou, L. Zhou, W. Zhong, and Y. B. Sheng, Europhys. Lett. **131**, 40005 (2020).
18 T. Li, and G. L. Long, New J. Phys. **22**, 063017 (2020).
19 L. Zhou, Y. B. Sheng, and G. L. Long, Sci. Bull. **65**, 12 (2020).
20 K. Wei, W. Zhang, Y. L. Tang, L. You, and F. Xu, Phys. Rev. A **100**, 022325 (2019), arXiv: 1909.05509.
21 F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, Rev. Mod. Phys. **92**, 025002 (2020), arXiv: 1903.09051.
22 F. G. Deng, H. Y. Zhou, and G. L. Long, J. Phys. A-Math. Gen. **39**, 14089 (2006), arXiv: quant-ph/0612018.
23 F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou, Chin. Phys. **16**, 3553 (2007), arXiv: quant-ph/0606008.
24 K. J. Wei, H. Q. Ma, and J. H. Yang, Opt. Express **21**, 16663 (2013).
25 Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, arXiv: 2106.13509.
26 J. H. Shapiro, D. M. Boroson, P. B. Dixon, M. E. Grein, and S. A. Hamilton, J. Opt. Soc. Am. B **36**, B41 (2019).
27 J. H. Shapiro, Z. Zhang, and F. N. C. Wong, Quantum Inf. Process. **13**, 2171 (2014).
28 F. Del Santo, and B. Dakić, Phys. Rev. Lett. **120**, 060503 (2018), arXiv: 1706.08144.
29 J. Y. Hu, B. Yu, M. Y. Jing, L. T. Xiao, S. T. Jia, G. Q. Qin, and G. L. Long, Light Sci. Appl. **5**, e16144 (2016), arXiv: 1503.00451.
30 W. Zhang, D. S. Ding, Y. B. Sheng, L. Zhou, B. S. Shi, and G. C. Guo, Phys. Rev. Lett. **118**, 220501 (2017), arXiv: 1609.09184.
31 F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, Sci. Bull. **62**, 1519 (2017), arXiv: 1710.07951.
32 R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G. L. Long, Light Sci. Appl. **8**, 22 (2019), arXiv: 1810.11806.
33 D. Pan, Z. Lin, J. Wu, H. Zhang, Z. Sun, D. Ruan, L. Yin, and G. L. Long, Photon. Res. **8**, 1522 (2020).
34 H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005), arXiv: quant-ph/0411004.
35 X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005), arXiv: quant-ph/0410075.
36 Y. F. Jiang, K. Wei, L. Huang, K. Xu, Q. C. Sun, Y. Z. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H. K. Lo, F. Xu, Q. Zhang, and J. W. Pan, Phys. Rev. Lett. **123**, 100503 (2019), arXiv: 1903.07862.
37 F. Y. Lu, Z. Q. Yin, C. Wang, C. H. Cui, J. Teng, S. Wang, W. Chen, W. Huang, B. J. Xu, G. C. Guo, and Z. F. Han, J. Opt. Soc. Am. B **36**, B92 (2019), arXiv: 1812.08388.
38 W. Wang, and H. K. Lo, Phys. Rev. A **100**, 062334 (2019), arXiv: 1812.07724.
39 H. J. Ding, J. Y. Liu, C. M. Zhang, and Q. Wang, Quantum Inf. Process. **19**, 60 (2020).
40 D. Ma, Y. Wang, and K. Wei, Quantum Inf. Process. **19**, 384 (2020).
41 X. Ma, B. Qi, Y. Zhao, and H. K. Lo, Phys. Rev. A **72**, 012326 (2005), arXiv: quant-ph/0503005.

Appendix

A1 System model

In this study, we considering a free-space system as ref. [33]. In this system, Bob sends different intensities of light pulses to Alice using a laser source. The light pulses transmits over a forward quantum channel *BA* to Alice. One part of pulses are directly measured by Alice to check Eve and the other part are encoded and reflected to Bob over a backward quantum channel *BAB*. The forward quantum channel and back ward quantum channel are the same. In order to analyze performance of a real-life QSDC experimental system, we must first model the source, channel and detection.

A1.1 Source

The laser source can adopt the weak coherent light model. Assuming that the phase of each pulse is completely random and the average photon number μ of each pulse follows the Poisson distribution, then the probability of the weakly coherent light source generating n-photon signal is given by

$$P_\mu(n) = \frac{e^{-\mu}}{n!}\mu^n. \tag{a1}$$

A1.2 Channel

In QSDC, there are two quantum channel, a forward channel *BA* and a backward channel *BAB*. We defines the loss of quantum channel as α_i, where $i \in \{BA, BAB\}$. Hence, the channel transmittance is expressed as follows:

$$t_i = 10^{-\frac{\alpha_i}{10}}. \tag{a2}$$

A1.3 Detection

The overall transmission are expressed as η_i, which represent the probability of a single-photon signal being successfully detected by Alice and Bob,

$$\eta^i = t_i \eta^i_{\rm opt} \eta^j_{\rm d}, \tag{a3}$$

where $\eta^j_{\rm d}$ represents the detection efficiency at $j \in \{A, B\}$ station. The subscript A and B denotes Alice and Bob, respectively. $\eta^i_{\rm opt}$ is the intrinsic optical loss of the device.

Generally, threshold detectors are placed in Bob and Alice. A threshold detector can only report click or non-click

events. That is to say, it cannot distinguish the photon number of received signal. Therefore, the transmittance of the n-photon state η_n^i is given by

$$\eta_n^i = 1-(1-\eta_i)^n, \tag{a4}$$

for $n = 1, 2, 3, \cdots$.

A1.4 Yield

Let Y_n^j and denote as the yield of n-photon signal at station j. In other word, it represents the conditional probability of the detection event at Alice's (Bob's) detector when sending n-photon state. Y_n^j can be expressed by

$$Y_n^j = Y_0^j + \eta_n^i - Y_0^j\eta_i^n \approx Y_0^j + \eta_n^i. \tag{a5}$$

The overall gains are the product of the probability that produces n-photon signal and the conditional probability that n-photon signal (and background count) cause detection event,

$$Q_x^i = \sum_{n=0}^{\infty} P_x(n)Y_n^j = Y_0^j + 1 - e^{-\eta^i x}. \tag{a6}$$

where $x \in \{\mu,\ \nu_1,\ \nu_2,\ \nu_3, \ldots, \nu_m\}$ represents the intensities for different states.

A1.5 Error rates

The quantum bit error rates (QBER) are given by

$$E_x^i = \frac{e_0 Y_0^j + e_{\mathrm{d}}^i\left(1-e^{-\eta^i x}\right)}{Q_x^i}, \tag{a7}$$

where $x \in \{\mu,\ \nu_1,\ \nu_2,\ \nu_3, \ldots, \nu_m\}$ represents the intensities for different states.

The error rate of the n-photon signal is

$$e_n^i = \frac{\left(e_0 Y_0^j + e_{\mathrm{d}}^i\eta_n^i\right)}{Y_n^j}, \tag{a8}$$

where $e_0 = \frac{1}{2}$ is the background error rate of detector dark count and other background contribution, e_{d}^i represent the error rates characterizing the alignment and stability of the optical system, which is generally assumed to be a constant.

A2 Four-decoy-state

Ref. [33] used a four-decoy-state protocol (one vacuum state and three weak decoy states (ν_1, ν_2, ν_3)) to estimate e_2^{BA} in eq. (1). The mean photon numbers μ, ν_1, ν_2 and ν_3 need to satisfy the following requirements:

$$\begin{aligned}
&0 < \nu_3 < \nu_2 \le \frac{2}{3}\mu < \nu_1 \le \frac{3}{4}\mu,\\
&\nu_1 + \nu_2 > \mu,\\
&\nu_2 + \nu_3 < \mu,\\
&\nu_1 - \nu_2 - \frac{\nu_1^3 - \nu_2^3}{\mu^2} = 0.
\end{aligned} \tag{a9}$$

The dark number of the system can be estimated by the vacuum decoy state, $Q_{\mathrm{vac}}^{BA} = Y_0$ and $E_{\mathrm{vac}}^{BA} = e_0 = \frac{1}{2}$. The upper bound of single-photon DBER and two-photon DBER are given by

$$e_1^{BA,U} = \frac{E_{\nu_3}^{BA}Q_{\nu_3}^{BA}e^{\nu_3} - e_0 Y_0^A}{Y_1^{BA,L}\nu_3}, \tag{a10}$$

$$e_2^{BA,U} = \frac{2\left(E_{\nu_2}^{BA}Q_{\nu_2}^{BA}e^{\nu_2} - \frac{\nu_2}{\nu_3}E_{\nu_3}^{BA}Q_{\nu_3}^{BA}e^{\nu_3} + \frac{\nu_2-\nu_3}{\nu_3}e_0 Y_0^A\right)}{Y_2^{BA,L}\nu_2\left(\nu_2-\nu_3\right)}, \tag{a11}$$

where

$$Y_1^{BA,L} = \frac{\mu^2\left(Q_{\nu_2}^{BA}e^{\nu_2} - Q_{\nu_3}^{BA}e^{\nu_3}\right) - \left(\nu_2^2-\nu_3^2\right)\left(Q_{\mu}^{BA}e^{\mu} - Y_0^A\right)}{\mu\left(\nu_2-\nu_3\right)\left(\mu-\nu_2-\nu_3\right)}, \tag{a12}$$

$$Y_2^{BA,L} = \frac{2\mu\left(Q_{\nu_1}^{BA}e^{\nu_1} - Q_{\nu_2}^{BA}e^{\nu_2}\right) - 2\left(\nu_1-\nu_2\right)\left(Q_{\mu}^{BA}e^{\mu} - Y_0^A\right)}{\mu\left(\nu_1-\nu_2\right)\left(\nu_1+\nu_2-\mu\right)}. \tag{a13}$$

A3 Genetic algorithm

Our full-parameter optimization method is primarily based on a GA, which uses a population of candidate solutions and then through four biological genetic steps: parent selection, crossover, mutation and replacement, so that the population evolves to explore the search space. A GA is capable of exploiting the information accumulated about an initially unknown search space to guide subsequent searches into useful subspaces without any restriction on the target function. This key feature, inherited from the GA, enables our method to overcome the limitations of LSAs and efficiently find QSDC optima.

Here, we take the our two-decoy-state protocol as an example, where we search for the optimal decoy intensities μ and ν_1. The optimization was conducted using the built-in GA of MATLAB R2016b. The procedure is illustrated in Figure a1 and is summarized as follows.

(1) **Initialization** The algorithm starts with a random population of candidate solutions (called individuals). For the three-intensity protocol, we set the population size to 100 and used a range of common values for $\mu \in (0, 1)$, $\nu_1 \in (0, 1)$,

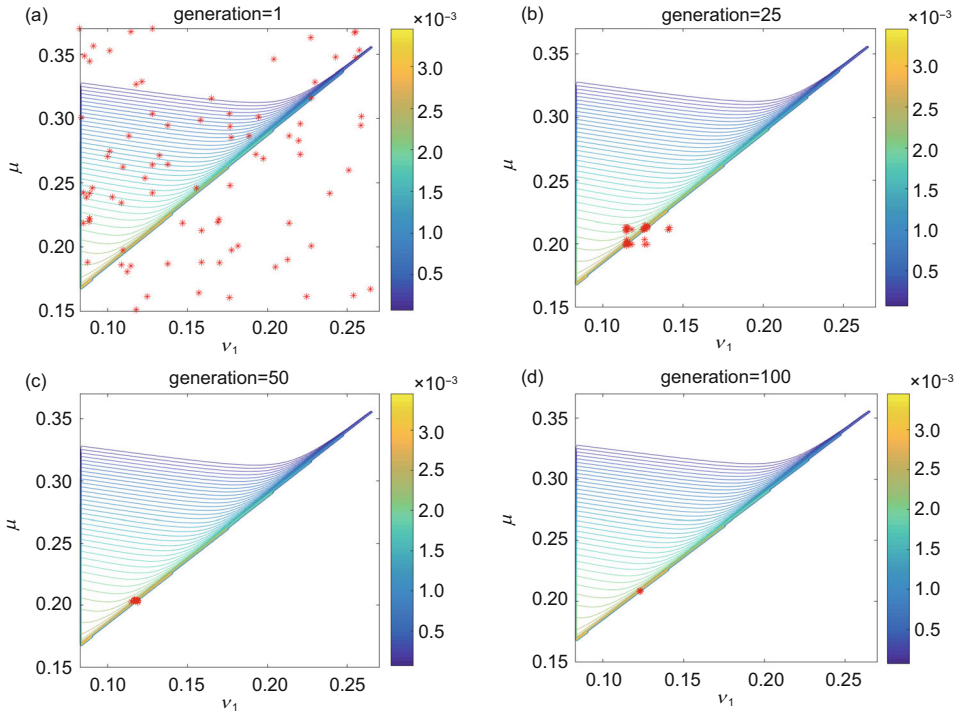

Figure a1 (Color online) Illustration of the proposed method for optimization in decoy-state QSDC protocol. The target is to search for the optimal μ and ν_1. The red points denote successive solutions in each generation. (a) In the 1st generation, the possible solutions are covered over all search spaces. (b), (c) Fitter solutions are selected through steps of selection and genetic operators. (d) After 100 generations, the algorithm is terminated at a point very close to the optimal one.

$P \in (0, 1)$. As shown in Figure a1(a), the entire range of possible solutions (the search space) is allowed in the 1st generation, and the solutions may occasionally be "seeded" in areas where optimal solutions are likely to be found despite the function being discontinuous.

(2) **Selection** In each iteration (or successive generation), a portion of the existing population (called the parents) is selected to breed a new population through a fitness-based process, which is determined by a fitness function. Here, we use the roulette selection method to select individuals, which uses the fitness function value of the parent individual to determine the probability of the individual being selected. In general, individuals with high fitness function values are more likely to be selected for the next step (i.e., crossover and mutation).

(3) **Genetic operators** The next step is to generate second-generation solutions to the population from those selected through a combination of genetic operators: crossover and mutation. For each new solution to be generated, a pair of "parent" solutions is chosen for breeding from the previously selected pool. By using crossover and mutation to generate a "child" solution, a new solution that usually has many of the characteristics of the "parent" is created. New parents are selected for each new child, and the process continues until a new population of solutions of appropriate size (we chose 100) is generated. The crossover and mutation operations are performed with a certain probability; we set the crossover and mutation probabilities to 0.8 and 0.02, respectively. For the crossover operation, a multipoint crossover method is used, where the parent exchanges genes at several randomly selected gene points. For the mutation operation, a random mutation method is adopted, where each gene of an individual has a probability of mutation.

The average fitness of the population will generally be increased by this procedure because only the best organisms from the first generation are selected for breeding, as shown in Figure a1(b). After several generations, a fitter population of solutions is obtained, as shown in Figure a1(c).

(4) **Stopping** Repeat the above process until one of the stopping criteria is reached. We used two stop criteria: (1) the number of iterations being greater than 1000, (2) the average value of the maximum function value difference between 100 successive generations is less than the function tolerance $\epsilon = 10^{-20}$. Once one of the two stopping criteria is reached, the algorithm is terminated. Usually, well-optimized parameters will be obtained by the time one of these criteria is reached, as shown in Figure a1(d).