CHIN. PHYS. LETT. Vol. 36, No. 4 (2019) 040301

Finite-Key Analysis for a Practical High-Dimensional Quantum Key Distribution System Based on Time-Phase States *

Ya-Hui Gan(甘亚辉)[1,2], Yang Wang(汪洋)[1,2**], Wan-Su Bao(鲍皖苏)[1,2**], Ru-Shi He(何如适)[1,2], Chun Zhou(周淳)[1,2], Mu-Sheng Jiang(江木生)[1,2]

[1]*Henan Key Laboratory of Quantum Information and Cryptography, Zhengzhou Information Science and Technology Institute, Zhengzhou 450001*

[2]*Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026*

(Received 19 December 2018)

High-dimensional quantum states key distribution (HD-QKD) can enable more than one bit per photon and tolerate more noise. Recently, a practical HD-QKD system based on time-phase states has provided a secret key at Mbps over metropolitan distances. For the purposes of further improving the secret key rate of a practical HD-QKD system, we make two main contributions in this work. Firstly, we present an improved parameter estimation for this system in the finite-key scenario based on the Chernoff bound and the improved Chernoff bound. Secondly, we analyze how the dimension d affects the performance of the practical HD-QKD system. We present numerical simulations about the secret key rate of the practical HD-QKD system based on different parameter estimation methods. It is found that using the improved Chernoff bound can improve the secret key rate and maximum channel loss of the practical HD-QKD system. In addition, a mixture of the 4-level and 8-level practical HD-QKD system can provide better performance in terms of the key generation rate over metropolitan distances.

PACS: 03.67.Dd, 03.67.Hk, 03.67.−a DOI: 10.1088/0256-307X/36/4/040301

Quantum key distribution (QKD)[1,2] can allow two distant authorized parties to share an identical secure key. The laws of quantum physics guarantee the unconditional security of QKD. However, the secret key rate is restrained by several practical factors which restrict the widespread application of QKD. For the purposes of improving the secret key rate, high-dimensional quantum states key distribution (HD-QKD)[3−7] has been proposed. High-dimensional quantum states qubits (dimension $d > 2$) are employed in HD-QKD, which can carry $\log_2 d$ bits of information. Therefore, HD-QKD can provide a higher photon information efficiency (PIE) than qubit-based QKD. When the secret key rate of the QKD system is limited by the saturation of single-photon detectors, it can be improved by high-dimensional photon encoding. Moreover, HD-QKD has a higher resistance to quantum channel noise as compared to qubit-based QKD.[5]

Recently, significant efforts have been made in HD-QKD. An attractive candidate for implementation is the time-energy HD-QKD protocol.[8−10] Rigorous security analyses[11−14] and experiments[15−17] have been presented. Another appealing candidate is the HD-QKD protocol with time-phase states.[18] Based on the HD-QKD system presented in Ref. [18], the secret key rate scales as Mbps can be achieved over metropolitan distances. Moreover, an HD-QKD system using fewer monitoring states[19] has been proposed, which can simplify the design of HD-QKD systems. However, the simplified HD-QKD system has lower secret key rate and resistance to noise than the one with the full setup.[18] In this work, we mainly focus on the security of this practical HD-QKD system based on time-phase states with full setup.

The security analysis in Ref. [18] ensures that the HD-QKD system is secure against coherent attacks, finite-key effects, and many other imperfections. To defeat a so-called photon number splitting (PNS) attack,[20] the decoy-state method[21] is used in the parameter estimation process. Moreover, the saturation of the single photon detector is also considered, which results in the rate-dependent detection efficiency. Specifically, the detection efficiency drops sharply as the rate increases beyond a few MHz.[18] Islam *et al.*[18] also proposed finite-key analysis based on Hoeffding's inequality.[22] However, for the purposes of improving the secret key rate, it is of importance to explore the improved method for parameter estimation in the finite-key analysis. Therefore, we present a rigorous finite-key analysis using the Chernoff bound[23] and the improved Chernoff bound[24] based on the security proof in Ref. [18].

Moreover, one of the possible ways to improve the secret key rate is to increase the dimension.[16,25] As we know, the secret key rate is relevant to the PIE and the transmitted rate of quantum states. Obviously, the PIE increases as the dimension increases. However, in the time-bin encoding system, a trade-off is made between the dimension and the transmitted

*Supported by the National Basic Research Program of China under Grant No 2013CB338002, and the National Natural Science Foundation of China under Grant Nos 61505261, 61675235, 61605248 and 11304397.

**Corresponding author. Email: wy@qiclab.cn; bws@qiclab.cn

rate of qubits: an increase in the former directly corresponds to a decrease in the latter. Considering the rate-dependent efficiency of detectors, the dimension can influence the detection efficiency and further influence the key generation rate. Therefore, for the purposes of maximizing the secret key rate in a practical HD-QKD system over metropolitan distances, we present research on how the dimension affects the performance of this system.

Firstly, we introduce the HD-QKD protocol based on time-phase states. (1) Preparation: Alice choose bases randomly from $\{T, F\}$ with probabilities p_T and p_F, respectively, to prepare time states and phase states. The d-dimension time states $|t_n\rangle$ $(n = 0, \ldots, d-1)$ are prepared by emitting photonic wave packets of width Δt produced by a continuous laser, which are localized to a time bin of width τ within a frame of d contiguous time bins. The phase states are a linear superposition of all the time states, which are given by $|f_n\rangle = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} e^{\frac{2\pi i n m}{d}} |t_m\rangle$ $(n = 0, \ldots, d-1)$. She also randomly modulates the intensity $k \in \{\mu, \upsilon, \omega\}$ with probabilities p_μ, p_ν and p_ω, respectively. Then, photon states are sent to Bob.

(2) Measurement: Bob measures arrived photon states by selecting bases from $\{T, F\}$ randomly with probabilities p_T and p_F, respectively. He makes T basis measurements by means of a superconducting nanowire single-photon detector. Here F basis measurements are made by means of a cascaded interferometric tree. Then, the measurement outcomes are recorded by a time-to-digital converter.

(3) Basis reconciliation: They both announce the choices of bases and intensities in the public authorized channel. They record the number of detected events in the same basis, $n_{T,k}$ and $n_{F,k}$ for intensity $k \in \{\mu, \nu, \omega\}$.

(4) Parameter estimation: They both use all intensity levels for the key generation. They record $m_{F,k}$, the number of detected events with bit errors. Then, they calculate the lower bound of single-photon events $s_{T,1}$ $(s_{F,1})$, the lower bound of vacuum photon events $s_{T,0}$ and the upper bound of the errors $c_{F,1}$ for single-photon events. Finally, if $\phi := c_{F,1}/s_{F,1}$ is lower than the predetermined phase error rate $\bar{\phi}$, they will continue the protocol. If it is not satisfied, they will abandon the protocol.

(5) Postprocessing: They both carry out the error correction, in which leak_{EC} bits of information are consumed. Then, they carry out the error verification. Finally, privacy amplification is carried out to obtain the shared secret key length l.

Next, we will present the security analysis. Note that this study is based on the composable security definition.[26] For some small error parameters, $\varepsilon_{\text{cor}}, \varepsilon_{\text{sec}} > 0$, the HD-QKD protocol will be $\varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}$ secure if it is ε_{cor} correct and ε_{sec} secret. The quantum leftover-hash lemma[27] is used to bound the secret key length l when the dimension $d = 4$ in Ref. [18]. Without loss of generality, we can extend it to an arbitrary dimension d, which is given by

$$l = \max_{\beta>0} \lfloor s_{T,0} \log_2 d + s_{T,1}[\log_2 d - H(\phi^U)] - \text{leak}_{\text{EC}} - \log_2 \frac{32}{\beta^8 \varepsilon_{\text{cor}}} \rfloor, \quad (1)$$

where $s_{T,0}$ is the number of vacuum detections in the T basis, $s_{T,1}$ is the number of single-photon detections in the T basis, $H(x) = -x \log_2[x/(d-1)] - (1-x)\log_2(1-x)$ is the binary entropy for arbitrary dimension d, and $\text{leak}_{\text{EC}} = n_{T,\mu} f_{\text{EC}} H(e_{T,\mu})$ bits are consumed in the error correction, where f_{EC} is the error correction efficiency and $e_{T,\mu}$ is the bit error rate in the T basis.

Due to the finite-key effect, for the parameters used in the security analysis, there is a difference between the expected outcome and the measurement outcome. We should characterize the differences appropriately to obtain a rigorous security analysis. In Ref. [18], they use Hoeffding's inequality for the parameter estimation. Correspondingly, we adopt the Chernoff bound and the improved Chernoff bound, respectively, for the parameter estimation.

First of all, let us make some definitions as follows: (1) $s_{T,n}$: the number of detections observed by Bob when Alice emits n-photon time states; (2) n_T: the total number of detections on the assumption that Alice sends time states. Furthermore, we can obtain $n_T = \sum_{n=0}^{\infty} s_{T,n}$; (3) $n_{T,k}$: the observed number of detections on the assumption that Alice sends time states when the intensity is k; (4) $\bar{n}_{T,k}$: the expected number of detections on the assumption that Alice sends time states when the intensity is k; (5) $p_{k|n}$: the conditioned probability of choosing the intensity k on the assumption that Alice prepares an n-photon time state. Then, in the asymptotic case, we obtain

$$n_{T,k} \to \bar{n}_{T,k} = \sum_{n=0}^{\infty} p_{k|n} s_{T,n}.$$

In addition, we can obtain the calculated $p_{k|n}$ based on Bayes' rule,

$$p_{k|n} = \frac{p_k}{\tau_n} p_{n|k} = \frac{p_k}{\tau_n} \frac{e^{-k} k^n}{n!}$$

where $\tau_n := \sum p_k e^{-k} k^n / n!$ is the probability that Alice emits n-photon time states.

Using Hoeffding's inequality for parameter estimation, $n_{T,k}$ can be given by

$$|\bar{n}_{T,k} - n_{T,k}| \le \delta_{\text{H}}(n_T, \varepsilon_{\text{H}}), \quad (2)$$

with probability at least $1 - 2\varepsilon_{\text{H}}$, where $\delta_{\text{H}}(x, y) = \sqrt{x/2 \ln(1/y)}$.

Using the Chernoff bound for parameter estimation, $n_{T,k}$ can be given by

$$|\bar{n}_{T,k} - n_{T,k}| \le \delta_{\text{C}}(n_{T,k}, \varepsilon_{\text{C}}), \quad (3)$$

with probability at least $1-2\varepsilon_{\rm C}$, where $\delta_{\rm C} = \delta_{\rm C}(x,y) \in [-\delta,\hat{\delta}]$, $\delta = \sqrt{2x\ln(16y^{-4})}$ and $\hat{\delta} = \sqrt{2x\ln(y^{-3/2})}$.

Using the improved Chernoff bound for parameter estimation, $n_{T,k}$ can be given by

$$\begin{aligned}\bar{n}^L_{T,k} &= \frac{n_{T,k}}{1+\delta^L_{\rm IC}(n_{T,k},\varepsilon_{\rm IC})}\\ \bar{n}^U_{T,k} &= \frac{n_{T,k}}{1-\delta^U_{\rm IC}(n_{T,k},\varepsilon_{\rm IC})},\end{aligned} \tag{4}$$

with probability at least $1-2\varepsilon_{\rm IC}$. For $\delta^L_{\rm IC}(x,y)$ and $\delta^U_{\rm IC}(x,y)$, if $x > -6\ln(y/2)$ is satisfied, we can obtain a simplified analytical approximation

$$\begin{aligned}\delta^L_{\rm IC}(x,y) &= \delta^U_{\rm IC}(x,y)\\ &= \frac{-3\ln(y/2)+\sqrt{[\ln(y/2)]^2-8x\ln(y/2)}}{2x+2\ln(y/2)}.\end{aligned}$$

According to results in Ref. [18], the decoy-state estimates for T and F bases are given by

$$s^L_{T,0} = \frac{\tau_0}{(\nu-\omega)}\Big(\frac{\nu e^{\omega}n^L_{T,\omega}}{p_\omega} - \frac{\omega e^{\nu}n^U_{T,\nu}}{p_\nu}\Big), \tag{5}$$

$$s^L_{F,0} = \frac{\tau_0}{(\nu-\omega)}\Big(\frac{\nu e^{\omega}n^L_{F,\omega}}{p_\omega} - \frac{\omega e^{\nu}n^U_{F,\nu}}{p_\nu}\Big), \tag{6}$$

$$\begin{aligned}s^L_{T,1} = \frac{\mu\tau_1}{(\nu-\omega)(\mu-\nu-\omega)}\Big[&\frac{e^{\nu}n^L_{T,\nu}}{p_\nu} - \frac{e^{\omega}n^U_{T,\omega}}{p_\omega}\\ &- \frac{\nu^2-\omega^2}{\mu^2}\Big(\frac{e^{\mu}n^U_{T,\mu}}{p_\mu} - \frac{s^L_{T,0}}{\tau_0}\Big)\Big],\end{aligned} \tag{7}$$

$$\begin{aligned}s^L_{F,1} = \frac{\mu\tau_1}{(\nu-\omega)(\mu-\nu-\omega)}\Big[&\frac{e^{\nu}n^L_{F,\nu}}{p_\nu} - \frac{e^{\omega}n^U_{F,\omega}}{p_\omega}\\ &- \frac{\nu^2-\omega^2}{\mu^2}\Big(\frac{e^{\mu}n^U_{F,\mu}}{p_\mu} - \frac{s^L_{F,0}}{\tau_0}\Big)\Big],\end{aligned} \tag{8}$$

$$c^U_{F,1} = \frac{\tau_1}{\nu-\omega}\Big(\frac{e^{\nu}m^U_{F,\nu}}{p_\nu} - \frac{e^{\omega}m^L_{F,\omega}}{p_\omega}\Big). \tag{9}$$

Moreover, the upper bound of the phase error rate of the single-photon events in the T basis is given by

$$\phi^U = \frac{c^U_{F,1}}{s^L_{F,1}} + \xi, \tag{10}$$

where

$$\xi = \sqrt{\frac{(s^L_{T,1}+s^L_{F,1})(s^L_{F,1}+1)}{s^L_{T,1}(s^L_{F,1})^2}\ln\frac{2}{\beta}}.$$

Considering the finite-key case, the dimension has a great impact on the performance of HD-QKD, which can be described qualitatively as follows: first of all, we introduce the saturation model of the single-photon detector. The property of saturation often arises from the dead time of the detector, which refers to a period over which a single-photon detector resets from a previous detection event and remains unresponsive to an incident photon. Due to this property, we can infer that the detection efficiency is rate-dependent. To characterize this property, a heuristic model was proposed in Ref. [18], which can be given as

$$\eta_d = a\tanh(r\_x/b),$$

where $\eta_{\rm d}$ is the detection efficiency, r_x is the expected photon rate, a and b are the fit parameters obtained from calibration. When the detector is not saturated, the secret key rate scales as $(\log_2 d)/d$. When the detector is saturated, the secret key rate scales as $\log_2 d$.

Moreover, we note that the rate of Alice's preparing of photon states is relevant to the dimension. For arbitrary d, the rate is $r = 1/\tau d$. That is to say, for a fixed duration communication session, the number of photon states will decrease corresponding to the increase of the dimension. Therefore, the finite-key effect will be more obvious for the HD-QKD system in a larger dimension.

In addition, the phase-state measurement device[25,28] is presented for $d=4$ in Ref. [18]. Three interferometers are required to realize the discrimination of the phase states, which is divided into two levels of cascaded interferometer trees. The insertion loss of each level is $\eta_{\rm i}$. For arbitrary d, we need to use $d-1$ interferometers, which is divided into $\lceil\log_2 d\rceil$ levels of cascaded interferometer trees, to discriminate the phase states. Therefore, the total insertion loss is $\eta_{\rm tot} = \eta_i\lceil\log_2 d\rceil$. That is to say, the channel loss will increase, corresponding to the increase of the dimension.

In this study, we apply the HD-QKD system model[18] to simulate the secret key rate. Specifically, we assume that the intensity of the signal state and two decoy states are set to be μ, ν, ω, respectively. The probabilities of choosing the three intensities are $p_\mu = 0.8$, $p_\nu = 0.1$ and $p_\omega = 0.1$, respectively.

For parameter estimation, we can obtain the parameters in the experiment. To simulate the secret key rate, we evaluate them.[18] Specifically, the overall system transmittance is given as

$$\eta = \eta_{\rm d}\eta_{\rm qc}, \tag{11}$$

where $\eta_{\rm qc}$ is the loss of the quantum channel. The total number of detection events observed by Bob in the T basis for a given μ_k is given by

$$n_{T,k} = p_{\mu_k}{p_T}^2 N(1-e^{-\eta\mu_k}+p_{\rm d}), \tag{12}$$

where N is the total number of signals transmitted by Alice during a communication session. Similarly, the number of detection events observed by Bob in the F basis for a given μ_k is given by

$$n_{T,k} = p_{\mu_k}{p_F}^2 N(1-e^{-\eta\eta_{\rm tot}\mu_k}+p_{\rm d}). \tag{13}$$

The total number of error events in the T basis for a given μ_k is given by

$$m_{T,k} = p_{\mu_k}{p_T}^2 N(e_{\rm d}(1-e^{-\eta\mu_k})+0.75p_{\rm d}), \tag{14}$$

where $e_{\rm d}$ is the intrinsic error rate of detectors. Similarly, the total number of error events in the F basis for a given μ_k is given by

$$m_{F,k} = p_{\mu_k} {p_F}^2 N(e_{\rm d}(1 - e^{-\eta\eta_{\rm tot}\mu_k}) + 0.75 p_{\rm d}). \quad (15)$$

We assume that the dark count rate of the detector is $p_{\rm d} = 10^{-8}$, and the intrinsic error rates in the T and F bases are set to be 0.01 and 0.02, respectively. Moreover, we set the intensity $\omega = 0$, $\varepsilon_{\rm cor} = 10^{-12}$, $\varepsilon_{\rm sec} = 10^{-15}$ and $\beta = \varepsilon_C = \varepsilon_{\rm IC} = 1.72 \times 10^{-10}$.

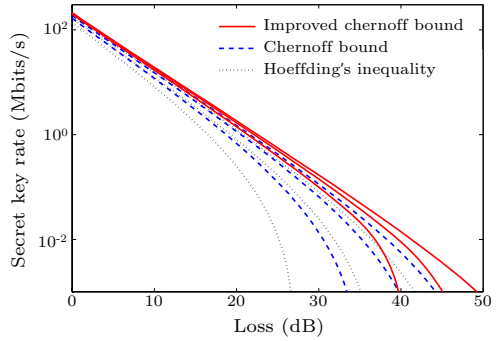

Fig. 1. Optimized secret key rate as a function of channel loss for $N = 6.25 \times 10^x$ with $x = 9, 10, 11$ (curves from left to right) based on the 4-level HD-QKD system. The solid, dashed and dotted lines represent the secret-key rate based on the improved Chernoff bound, the Chernoff bound and Hoeffding's inequality, respectively.

For the 4-level HD-QKD system, we present a finite-key analysis based on different parameter estimation methods in Fig. 1. To compare with the performance in Ref. [18], we set the detector efficiency to be $\eta_{\rm d} = 0.8$ and optimize the secret key rate over the probability of selecting the time basis p_T, the signal and decoy intensities, $\{\mu, \nu\}$. Moreover, we present the calculated secret key rate for different block sizes, $N = 6.25 \times 10^x$ with $x = 9, 10, 11$, respectively. As shown in Fig. 1, we find that for the same block size, the HD-QKD system using the improved Chernoff bound outperforms those using the Chernoff bound or Hoeffding's inequality in both secret key rate and maximum channel loss. Moreover, the HD-QKD system using the Chernoff bound outperforms that using Hoeffding's inequality in both secret key rate and maximum channel loss. In addition, we find that for the smaller block size, the positive effect of using the improved Chernoff bound in the HD-QKD system is more obvious.

For an arbitrary d-level HD-QKD system, we present a finite-key analysis based on the improved Chernoff bound, which is proved to achieve a better performance than those based on the Chernoff bound and Hoeffding's inequality. In this analysis, we apply the rate-dependent model to characterize the detection efficiency. For simplicity, we set $p_T = 0.9$, $\mu = 0.6$ and $\nu = 0.2$. Then, we calculate the secret key rate as a function of loss for the d-level HD-QKD system in Fig. 2. Specifically, we set the dimensions of the HD-QKD system to be 2, 4, 8 and 16, respectively, so that the phase-state measurement setup can be fully used. As shown in Fig. 2, the HD-QKD system in a larger dimension provides a higher secret key rate at the low loss channel. However, at the high loss channel, the HD-QKD system in a larger dimension provides a lower secret key rate. Moreover, we find that the increase of dimension corresponds to the decrease of the maximum channel loss. In particular, the HD-QKD systems in $d = 2, 4, 8, 16$ have their own advantages in terms of secret key rate over different losses. In detail, in terms of secret key rate, the 16-level HD-QKD system performs better than the 8-level system within the loss of 4 dB. The 8-level HD-QKD system performs better than the 4-level one within the loss of 4–10 dB. The 4-level HD-QKD system performs better than the 2-level HD-QKD system within the loss of 10–33 dB. The 2-level HD-QKD system performs better than the others when the channel loss exceeds 33 dB. Considering metropolitan distances, we mainly focus on the transmission distance of 20–80 km, which is equivalent to a loss of 4–16 dB. Therefore, we mainly focus on the 4-level and 8-level HD-QKD systems, which perform better than others within metropolitan distances. As discussed above, to achieve a higher secret key rate, we should choose the appropriate dimension corresponding to the channel loss. That is to say, considering metropolitan distances, we should use the 4-level HD-QKD system within the loss of 4–10 dB. In contrast, within the loss of 10–16 dB, we should use the 8-level HD-QKD system.

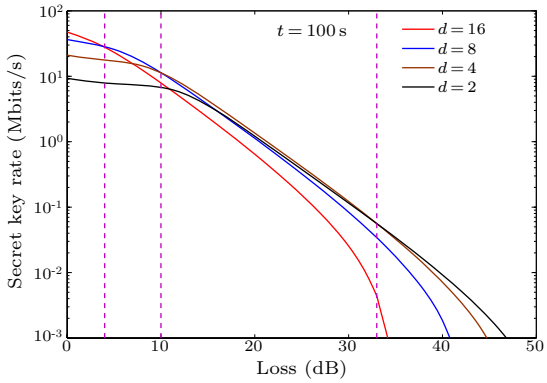

Fig. 2. Secret key rate as a function of channel loss for $d = 2, 4, 8, 16$. The transmitted signals are prepared in different dimensions during 100-s-duration communication session.

In conclusion, we have presented a finite-key analysis for a practical HD-QKD system based on improved parameter estimation methods. Moreover, we study how the dimension affects the performance of the HD-QKD system. Also, we highlight the significance of developing an improved parameter estimation method and flexibly choosing the dimension of the HD-QKD system corresponding to the channel loss.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Comput. Syst. Signal Process. Bangalore India IEEE* p 175

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Tittel W, Brendel J, Zbinden H and Gisin N 2000 *Phys. Rev. Lett.* **84** 4737
[4] Bechmann-Pasquinucci H and Tittel W 2000 *Phys. Rev. A* **61** 062308
[5] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902
[6] Ali-Khan I, Broadbent C J and Howell J C 2007 *Phys. Rev. Lett.* **98** 060503
[7] Mohammad M, Omar S M L, Malcolm N O S, Brandon R, Mehul M, Martin P J L, Miles J P, Daniel J G and Robert W B 2015 *New J. Phys.* **17** 033033
[8] Mower J, Zhang Z, Desjardins P, Lee C, Shapiro J H and Englund D 2013 *Phys. Rev. A* **87** 062322
[9] Wang Y, Bao W S, Bao H Z, Zhou C, Jiang M S and Li H W 2017 *Phys. Lett. A* **381** 1393
[10] Bao H Z, Bao W S, Wang Y, Chen R K, Ma H X, Zhou C and Li H W 2017 *Chin. Phys. B* **26** 050302
[11] Zhang Z, Mower J, Englund D, Wong F N C and Shapiro J H 2014 *Phys. Rev. Lett.* **112** 120506
[12] Bunandar D, Zhang Z, Shapiro J H and Englund D 2015 *Phys. Rev. A* **91** 022336
[13] Bao H Z, Bao W S, Wang Y, Zhou C and Chen R K 2016 *J. Phys. A* **49** 205301
[14] Niu M Y, Xu F, Shapiro J H and Furrer F 2016 *Phys. Rev. A* **94** 052323
[15] Lee C, Zhang Z, Steinbrecher G R, Zhou H, Mower J, Zhong T, Wang L, Hu X, Horansky R D, Verma V B, Lita A E, Mirin R P, Marsili F, Shaw M D, Nam S W, Wornell G W, Wong F N C, Shapiro J H and Englund D 2014 *Phys. Rev. A* **90** 062331
[16] Lee C, Bunandar D, Zhang Z, Steinbrecher G R, Dixon P B, Wong F N C, Shapiro J H, Hamilton S A and Englund D 2016 arXiv:1611.01139v1[quant-ph]
[17] Zhong T, Zhou H, Horansky R D, Lee C, Verma V B, Lita A E, Restelli A, Bienfang J C, Mirin R P, Gerrits T, Nam S W, Marsili F, Shaw M D, Zhang Z, Wang L, Englund D, Wornell G W, Shapiro J H and Wong F N C 2015 *New J. Phys.* **17** 022002
[18] Islam N T, Lim C C W, Cahall C, Kim J S and Gauthier D J 2017 *Sci. Adv.* **3** e1701491
[19] Islam N T, Lim C C W, Cahall C, Kim J S and Gauthier D J 2018 *Phys. Rev. A* **97** 042347
[20] Brassard G, Lutkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[21] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[22] Hoeffding W 1963 *J. Am. Stat. Assoc.* **58** 13
[23] Chernoff H 1952 *Ann. Math. Stat.* **23** 493
[24] Zhang Z, Zhao Q, Razavi M and Ma X F 2017 *Phys. Rev. A* **95** 012333
[25] Brougham T, Barnett S M, McCusker K T, Kwiat P G and Gauthier D J 2013 *J. Phys. B: At. Mol. Opt. Phys.* **46** 104010
[26] Muller-Quade J and Renner R 2009 *New J. Phys.* **11** 085006
[27] Tomamichel M and Hayashi M 2013 *IEEE Trans. Inf. Theory* **59** 7693
[28] Islam N T, Cahall C, Aragoneses A, Lezama A, Kim J and Gauthier D J 2017 *Phys. Rev. Appl.* **7** 044010