Device-independent quantum key distribution with generalized two-mode Schrödinger cat states

Curtis J. Broadbent,[1,2,3] Kevin Marshall,[4] Christian Weedbrook,[5] and John C. Howell[2,3]
[1]*Rochester Theory Center, University of Rochester, Rochester, New York 14627, USA*
[2]*Center for Coherence and Quantum Optics, University of Rochester, Rochester, New York 14627, USA*
[3]*Department of Physics and Astronomy, University of Rochester, Rochester, New York 14627, USA*
[4]*Department of Physics, University of Toronto, Toronto, Ontario M5S 1A7, Canada*
[5]*QKD Corp., 60 St. George St., Toronto, M5S 1A7, Canada*
(Received 27 February 2015; published 16 November 2015)

We show how weak nonlinearities can be used in a device-independent quantum key distribution (QKD) protocol using generalized two-mode Schrödinger cat states. The QKD protocol is therefore shown to be secure against collective attacks and for some coherent attacks. We derive analytical formulas for the optimal values of the Bell parameter, the quantum bit error rate, and the device-independent secret key rate in the noiseless lossy bosonic channel. Additionally, we give the filters and measurements which achieve these optimal values. We find that, over any distance in this channel, the quantum bit error rate is identically zero, in principle, and the states in the protocol are always able to violate a Bell inequality. The protocol is found to be superior in some regimes to a device-independent QKD protocol based on polarization entangled states in a depolarizing channel. Finally, we propose an implementation for the optimal filters and measurements.

DOI: 10.1103/PhysRevA.92.052318 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Dv, 89.70.Cf

The last two decades have seen a rise in the number and quality of quantum key distribution (QKD) protocols [1–3]. Some of these have been developed into successful commercial products currently deployed in telecommunications [4,5]. These systems are designed on the principle of provably secure communication in which, under certain assumptions, the security is guaranteed by the laws of physics, not the assumed difficulty of performing certain mathematical operations as in classical cryptography protocols. Unfortunately, practical implementations of QKD protocols have in many cases fallen short of their desired goal; due to rate ceilings, current QKD systems are used only to generate keys for use with standard cryptographic protocols. Additionally, in recent years both research and commercially developed QKD systems have been successfully hacked by using side-channel information [6–21].

In response to these limitations, there has been an effort to develop QKD protocols which are immune to the practical limitations of the devices in which they are implemented. These protocols are called device-independent QKD (DIQKD) protocols and are based on violation of Bell and Einstein–Podolsky–Rosen-steering (EPR-steering) inequalities [22–26]. If a particular physical implementation of the device-independent QKD protocol is able to violate a Bell inequality, then the resulting key can be considered to be secure, regardless of the details of the physical implementation. Device-independent QKD protocols have been shown to be secure under collective attacks and, in some instances, are secure under coherent attacks [23,24,27,28].

Although device-independence provides a way around the security limitations of previous QKD protocols, it further restricts the secret key generation rate which may be obtained. As a result, there is a growing interest in trying to implement DIQKD in diverse systems in an attempt to increase the secret key generation rate. With that in mind, in this paper we present an alternative implementation of DIQKD which makes use of highly non-Gaussian states: phase-entangled coherent states. We show here that, in certain bosonic channels, phase-entangled coherent states have secret key rates competitive with state-of-the-art DIQKD systems, including DIQKD systems based on discrete variables. Beyond being competitive with state-of-the-art systems, we also show that phase-entangled coherent states allow for a high degree of flexibility in the deployment of the QKD protocol. This could be helpful in situations where the properties of the channel, in particular, the total transmission rate, are variable over time. Additionally, although the phase-entangled coherent state is non-Gaussian, it is relatively easy to generate, requiring only a single photon source and a relatively weak Kerr nonlinearity [29].

Device-independent quantum key distribution proceeds in the following manner: Two distant parties, Alice and Bob, receive entangled pairs from a distant third party, who is possibly under the control of an eavesdropper, Eve. We assume that the measurement device may not be trustworthy, having possibly been manufactured by Eve. Alice and Bob are able to set their devices to measure the operators $\{A_0, A_1, A_2\}$ and $\{B_1, B_2\}$ respectively; they record outcomes $\{a_i, b_j\}$ which take values in $\{-1, 1\}$. We assume that Alice and Bob are in secure locations; they are able to confirm that their devices do not transmit signals of any kind to Eve. Alice and Bob select their measurement settings at random for each photon they measure. After all measurements have been performed, Alice and Bob communicate the bases in which measurements where made. Measurements performed in the bases $\{A_0, B_1\}$ are used to generate a secret key and determine the quantum bit error rate (QBER) $Q = \text{prob}(a_0 \neq b_1)$. Measurements performed in the basis $\{A_i, B_j\}$ $(i, j \in \{1,2\})$ are used to determine whether a Bell inequality is violated. Measurements performed in the basis $\{A_0, B_2\}$ are assumed to be uncorrelated and are discarded.

We consider the phase-entangled coherent state which is created by the entangling interferometer described in Ref. [30],

$$|\psi\rangle = (|\alpha_+\rangle|\alpha_-\rangle - |\alpha_-\rangle|\alpha_+\rangle)/N, \tag{1}$$

where $|\alpha_\pm\rangle$ are coherent states with oppositely rotated phases $|\alpha_\pm\rangle = |\alpha e^{\pm i\phi}\rangle$ with $\alpha \geqslant 0$ where $N = [2(1-\gamma^2)]^{1/2}$ and

$\gamma = |\langle\alpha_+|\alpha_-\rangle|$. The phase-entangled coherent states are equivalent to displaced Schrödinger cat states,

$$|\psi\rangle = [\mathcal{D}(\alpha\cos\phi)\otimes\mathcal{D}(\alpha\cos\phi)] \times(|\beta\rangle|-\beta\rangle - |-\beta\rangle|\beta\rangle)/N, \quad (2)$$

where $\beta = i\alpha\sin\phi$. Additionally, we note that antisymmetric states of this type have a concurrence of 1, are relatively robust to photon loss, and are able to violate a Bell inequality after a distance 400 km by using state-discrimination techniques assuming a loss of 0.15 dB/km [29]. In the following, we show that, in principle, with optimal measurements, the phase-entangled coherent states can give rise to Bell-inequality violation at any distance. It is this property we leverage for our device-independent QKD protocol.

Once generated, the phase-entangled coherent states pass through an optical fiber to Alice and Bob. We model the loss incurred in the fiber as beam-splitter loss with transmission and reflection coefficients t and r, respectively, where $|t|^2 + |r|^2 = 1$, and where the other input mode of the beam-splitter is in the vacuum state. The resulting state is given by

$$|\psi'\rangle = (|t\alpha_+\rangle|t\alpha_-\rangle|r\alpha_+\rangle_L|r\alpha_-\rangle_L - |t\alpha_-\rangle|t\alpha_+\rangle|r\alpha_-\rangle_L|r\alpha_+\rangle_L)/N, \quad (3)$$

where we have assumed for simplicity that the loss coefficients for the fiber to Alice are equal to those for the fiber to Bob. The subscript L in Eq. (3) refers to the lossy modes of the optical fiber, where we establish the convention that, in products of the form $|\cdot\rangle_L|\cdot\rangle_L$, the first ket always refers to the lossy modes of Alice's fiber and the second to Bob's, and single kets of the form $|\cdot\rangle_L$ refer generally to the joint space of Alice and Bob's lossy modes.

We define the orthonormal states following the work of Ref. [31], which will be of use in tracing out the lossy modes and quantifying the entanglement of the remaining state,

$$|\pm\rangle = \frac{1}{N_\pm}(e^{i\delta_t/2}|t\alpha_+\rangle \pm e^{-i\delta_t/2}|t\alpha_-\rangle), \quad (4a)$$

$$|\pm\rangle_L = \frac{1}{M_\pm}(|r\alpha_+\rangle_L|r\alpha_-\rangle_L \pm |r\alpha_-\rangle_L|r\alpha_+\rangle_L), \quad (4b)$$

where $N_\pm = [2(1\pm\gamma_t)]^{1/2}$ and $M_\pm = [2(1\pm\gamma_r^2)]^{1/2}$, with $\gamma_q = |\langle q\alpha_+|q\alpha_-\rangle| = \gamma^{|q|^2}$ and $\delta_t = \arg\langle t\alpha_+|t\alpha_-\rangle$. It will also be helpful to write out the inverse relationships,

$$|t\alpha_\pm\rangle = \frac{e^{\mp i\delta_t/2}}{2}(N_+|+\rangle \pm N_-|-\rangle), \quad (5a)$$

$$|r\alpha_\pm\rangle_L|r\alpha_\mp\rangle_L = \tfrac{1}{2}(M_+|+\rangle_L \pm M_-|-\rangle_L). \quad (5b)$$

Substituting Eq. (5) into Eq. (3) and tracing over the lossy modes, we arrive at the following mixed state written in the basis of $\{|++\rangle,|+-\rangle,|-+\rangle,|--\rangle\}$:

$$\rho = \frac{M_-^2}{16N^2}(N_+^4+N_-^4)|\Psi\rangle\langle\Psi| + \frac{M_+^2}{16N^2}(2N_+^2N_-^2)|\Phi\rangle\langle\Phi|, \quad (6)$$

where $|\Psi\rangle = (N_+^2|++\rangle - N_-^2|--\rangle)(N_+^4+N_-^4)^{-1/2}$ and $|\Phi\rangle = (|+-\rangle - |-+\rangle)/\sqrt{2}$.

We use this form of ρ to determine the optimal filtering operations for single-copy entanglement distillation. The optimal filters $M_A\otimes M_B$ are those which result in a Bell-diagonal state, have maximum probability of success, and satisfy the requirements of being a valid filtering operation [32]. A Bell-diagonal state is one which can be expressed as a mixture of Bell states. The probability of success of the filtering operation is given by

$$p = \mathrm{Tr}\,(M_A\otimes M_B)\rho(M_A\otimes M_B)^\dagger. \quad (7)$$

Finally, a valid filtering operation M_i has the property that $(\mathbb{1} - M_i^\dagger M_i)$ is a positive operator. We introduce the state ϱ to simplify the algebra,

$$\varrho = \begin{pmatrix} a & 0 & 0 & -\sqrt{ad} \\ 0 & b & -b & 0 \\ 0 & -b & b & 0 \\ -\sqrt{ad} & 0 & 0 & d \end{pmatrix}, \quad (8)$$

where the quantities in ϱ are defined by the relation $\varrho = \rho$, i.e., $a = M_-^2N_+^4/(16N^2)$, $b = M_+^2N_+^2N_-^2/(16N^2)$, and $d = M_-^2N_-^4/(16N^2)$. Consequently, we note that $a \geqslant d$ since $N_+ \geqslant N_-$. By using the method described by Verstraete et al. [32] it can be shown that the optimal filtering operations are given by

$$M_A = M_B = \begin{pmatrix} (d/a)^{1/4} & 0 \\ 0 & 1 \end{pmatrix}, \quad (9)$$

also written as $M_A = M_B = (d/a)^{1/4}|+\rangle\langle+| + |-\rangle\langle-|$. The state after the filtering operation is given by

$$\varrho' = \frac{1}{2(b+\sqrt{ad})}\begin{pmatrix} \sqrt{ad} & 0 & 0 & -\sqrt{ad} \\ 0 & b & -b & 0 \\ 0 & -b & b & 0 \\ -\sqrt{ad} & 0 & 0 & \sqrt{ad} \end{pmatrix}, \quad (10)$$

which occurs with a probability of success of $p = 2\sqrt{d/a}(b+\sqrt{ad})$. Since a, b, and d are all positive, we see that the filtering operation always has a nonzero probability of success.

Following the work of Horodecki et al. [33], we can use the correlation matrix to determine the maximum possible Bell violation after the filtering operations. We briefly review how this is done. The correlation matrix C is defined to be $C_{ij} = \mathrm{Tr}\,(\sigma_i\otimes\sigma_j)\varrho'$, where σ_i and σ_j are the standard Pauli matrices in the basis $\{|+\rangle,|-\rangle\}$, with $i,j\in\{x,y,z\}$. A dichotomic measurement operator A with eigenvalues of ±1 can be represented by the unit vector $\mathbf{a} = (a_x,a_y,a_z)$ where $A = a_x\sigma_x + a_y\sigma_y + a_z\sigma_z$. It is straightforward to show that a joint dichotomic measurement $\langle A\otimes B\rangle$ can be calculated by using the correlation matrix as $\langle A\otimes B\rangle = \mathbf{a}\cdot C\cdot\mathbf{b}$, where we define $\mathbf{b}$ for operator B similar to $\mathbf{a}$. Consequently, the Bell parameter is given by

$$\langle S\rangle = (\mathbf{a}_1+\mathbf{a}_2)\cdot C\cdot\mathbf{b} + (\mathbf{a}_1-\mathbf{a}_2)\cdot C\cdot\mathbf{b}_2, \quad (11)$$

where $S = A_1\otimes B_1 + A_2\otimes B_1 + A_1\otimes B_2 - A_2\otimes B_2$. The form of the Bell parameter given in Eq. (11) lends itself easily to constrained maximization techniques, as shown by Horodecki et al. [33]. The maximum value of the Bell parameter is given by $S_{\max} = 2(s_1^2+s_2^2)^{1/2}$ where s_1 and s_2 are the largest two singular values of the correlation matrix. The left- and right-singular vectors $\mathbf{l}_i$ and $\mathbf{r}_i$ of the correlation matrix can be used to determine a set of measurements which achieves the maximum value of the Bell parameter.

Specifically,

$$\begin{aligned} \mathbf{a}_1 &= \cos\varphi\,\mathbf{l}_1 + \sin\varphi\,\mathbf{l}_2, \quad \mathbf{b}_1 = \mathbf{r}_1, \\ \mathbf{a}_2 &= \cos\varphi\,\mathbf{l}_1 - \sin\varphi\,\mathbf{l}_2, \quad \mathbf{b}_2 = \mathbf{r}_2, \end{aligned} \tag{12}$$

where $\cos\varphi = s_1(s_1^2 + s_2^2)^{-1/2}$ with $(0 \leqslant \varphi \leqslant \pi/4)$. Mapping the vectors in Eq. (12) back to operators in the two-qubit Hilbert spaces yields the appropriate measurements for achieving the maximum value of the Bell parameter experimentally.

In our specific case, i.e., for the state ϱ', the correlation matrix is diagonal with values $C_{xx} = -1$ and $C_{yy} = C_{zz} = -(b - \sqrt{ad})/(b + \sqrt{ad})$. Consequently, the maximum value of the Bell parameter is

$$S_{\max} = 2\sqrt{1 + \left(\frac{b - \sqrt{ad}}{b + \sqrt{ad}}\right)^2}. \tag{13}$$

Except for the case where $\sqrt{ad} = b$, the state ϱ' is always able to violate a Bell inequality. A set of measurements which give rise to the maximum value of the Bell parameter are

$$\begin{aligned} A_1 &= \cos\varphi\,\sigma_x + \sin\varphi\,\sigma_y, \quad B_1 = -\sigma_x, \\ A_2 &= \cos\varphi\,\sigma_x - \sin\varphi\,\sigma_y, \quad B_2 = -\sigma_y, \end{aligned} \tag{14}$$

where $\cos\varphi = 2/S_{\max}$ with $(0 \leqslant \varphi \leqslant \pi/4)$.

We now express the probability of success and the maximum value of the Bell parameter in terms of the initial overlap γ and the total transmission probability $T = |t|^2$:

$$p = \frac{(1 - \gamma^T)^2}{1 - \gamma^2}, \tag{15}$$

$$S_{\max} = 2\sqrt{1 + \gamma^{4(1-T)}}. \tag{16}$$

We see in Eq. (16) that, for a pure-loss channel, optimally filtered phase-entangled coherent states are able to violate a Bell inequality at any distance. Finally, as can be deduced from the value of C_{xx}, measurements made in the $\sigma_x \otimes \sigma_x$ basis are always perfectly anticorrelated regardless of the value of γ or T. If $A_0 = \sigma_x$ then, in principle, the QBER for the phase-entangled coherent states will be exactly zero: $Q_{\text{pecs}} = 0$. These two remarkable results, Bell inequality violation as well as zero QBER at any distance, are a result of the noiseless nature of the pure-loss channel considered here, and are not expected to extend to channel models which include noise.

We can use the probability of success, the maximum value of the Bell parameter, and the QBER to determine a secret key rate for a device-independent implementation of the protocol. This is done by noting that the Holevo information between Eve and Bob can be bounded by using the Bell violation,

$$\chi(B_1, E) \leqslant h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right), \tag{17}$$

where the Holevo information is equal to the quantum mutual information of the joint state shared by Bob and Eve after Bob's measurements have been performed [23]. In Eq. (17), h is the binary Shannon entropy. Noting that the mutual information between A_0 and B_1 is 1 and using the Holevo information in Eq. (17), we find that the Devetak–Winter rate for the optimally filtered state is given by

$$r_{\text{DW}} = 1 - h\left(\frac{1 + \gamma^{2(1-T)}}{2}\right). \tag{18}$$

Consequently, the raw secret key fraction K, under collective attacks and with one-way classical postprocessing from Bob to Alice is bounded by the probability of successful filtering times the Devetak–Winter rate,

$$K \geqslant p r_{\text{DW}} = \frac{(1 - \gamma^T)^2}{1 - \gamma^2}\left[1 - h\left(\frac{1 + \gamma^{2(1-T)}}{2}\right)\right]. \tag{19}$$

Since γ is a free parameter to be set by Alice and Bob given knowledge of the total transmission T, we may optimize the secret key fraction as a function of γ. We plot the resulting secret key fraction in Fig. 1. The total secret key rate is just the product of the secret key fraction, the $\{A_0, B_1\}$ sampling probability, and the raw repetition rate of the source.

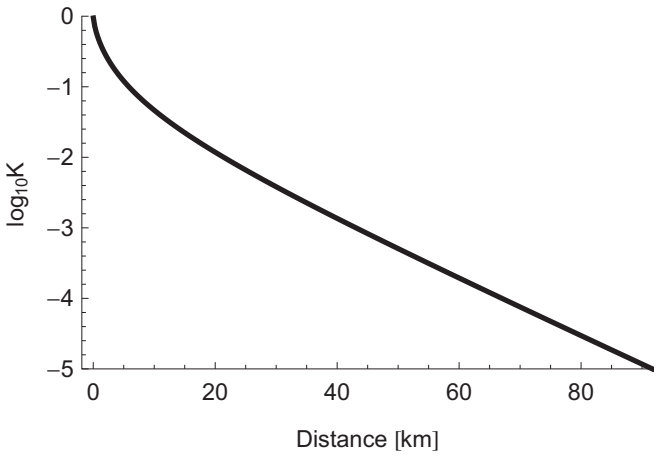

FIG. 1. The secret key fraction K as a function of the distance between Alice and Bob assuming a loss coefficient of 0.2 dB/km and the optimal γ for the specified distance. This plot gives the raw fraction; it does not include finite detection efficiencies, dark counts, thermal noise, or the relative sampling frequency of the $\{A_0, B_1\}$ measurement.

For large distances, to lowest order in the total transmission T, the optimal secret key fraction scales as T^2. The scaling coefficient is given by

$$\alpha = \frac{\log_{10}^2 \gamma}{1 - \gamma^2}\left[1 - h\left(\frac{1 + \gamma^2}{2}\right)\right], \tag{20}$$

which has a maximum of approximately 4.6% when $\gamma \simeq 0.74$. By comparison, due solely to loss, the secret key fraction for a biphoton entangled source scales no better than T^2 irrespective of the QKD protocol. This indicates that, compared against an error-free biphoton-based QKD protocol, our protocol can never have a secret key rate worse than 4.6% of that which can be achieved in a biphoton-based protocol. In the presence of noise, however, our protocol can drastically outperform some biphoton-based DIQKD protocols, as we now discuss.

We make a comparison to a DIQKD protocol based on polarization-entangled states subject to depolarizing noise [24]. In this case, depolarizing noise increases the probability of error and decreases the Bell violation. The

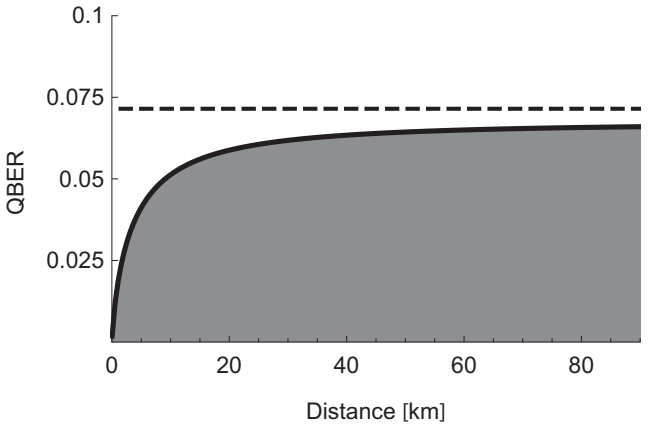

FIG. 2. Plot of the critical QBER Q_{crit} as a function of distance, see text for details. The biphoton approach is superior in the gray region, corresponding to $Q < Q_{\text{crit}}$. The phase-entangled coherent-state approach is superior in the white region, corresponding to $Q > Q_{\text{crit}}$. The discrete-variable DIQKD approach using biphotons cannot be used when the QBER exceeds the dashed black line.

resulting secret key fraction has been shown to be given by

$$K_{\text{biphoton}} = T^2\left(1 - h(Q) - h\left[\frac{1+\sqrt{(S/2)^2-1}}{2}\right]\right), \quad (21)$$

where $S = 2\sqrt{2}(1-2Q)$ [24]. To permit a comparison to known results, we would like to determine values of the QBER and the propagation distance for which the phase-entangled coherent-state-based protocol gives an improved secret key fraction as compared to biphoton-based QKD protocols, i.e., $K \geqslant K_{\text{biphoton}}$. We calculate numerically the critical QBER Q_{crit} such that $K_{\text{biphoton}} = K$ at a given distance. When the QBER exceeds Q_{crit}, the protocol based on the phase-entangled coherent state will have a higher secret key rate than the biphoton-based protocol, i.e., for $Q > Q_{\text{crit}}$ we find that $K > K_{\text{biphoton}}$. We plot this critical QBER as a function of distance in Fig. 2. We find that our approach using Schrödinger cat states is superior whenever the QBER for the depolarizing channel exceeds the black line in Fig. 2. For example, we find that, at a distance of 11 km, if the quantum bit error rate is 6.6%, our protocol has a secret key rate roughly twice that of the biphoton-based protocol. It can be seen that, at large distances, our approach is superior when the QBER of the depolarizing channel exceeds 6.7%. Furthermore, it is clear that there are QBERs for which the depolarizing channel cannot be used at all ($Q \geqslant 0.715$), whereas the phase-entangled coherent-state approach is viable over any distance. This analysis, which is valid only for a pure-loss channel for the phase-entangled DIQKD protocol, suggests that there may be physical channels in which the coherent-state approach is superior to alternative protocols, even in the presence of noise.

Examination of Figs. 1 and 2 reveals another advantage of the Schrödinger cat implementation of DIQKD: by tuning γ to the transmission distance, the secret key fraction can be improved dramatically for short distances relative to the long-term scaling. This sort of dynamical control is not typically present in standard implementations of DIQKD in discrete systems.

We now discuss the feasibility of performing the measurements required to implement the optimal filtering and to violate the Bell inequality. The primary requirement is the ability to make projective measurements in a superposition of the $|+\rangle$ and $|-\rangle$ states. Techniques for making such a measurement are the subject of ongoing investigations, but recent theoretical results for Gaussian states as well as advances in detectors suggest that these types of measurements are becoming easier to implement experimentally.

We briefly describe one possible approach which could be used to perform the required measurements by using presently available equipment. The primary difficulty is to measure in an arbitrary superposition of the basis states, $|\pm\rangle$. Without loss of generality, let us try to find a way to measure in the basis $\{|\phi\rangle,|\overline{\phi}\rangle\}$ where $|\phi\rangle = c|+\rangle + d|-\rangle$ and $|\overline{\phi}\rangle = d^*|+\rangle - c^*|-\rangle$. By using the following rotation, we can rotate the state to the $|\pm\rangle$ basis,

$$U = \begin{pmatrix} c^* & d^* \\ d & -c \end{pmatrix}. \quad (22)$$

The result of the rotation is $U|\phi\rangle = |+\rangle$ and $U|\overline{\phi}\rangle = |-\rangle$. $|+\rangle$ and $|-\rangle$ are standard Schrödinger cat states, albeit with an additional phase, and can be distinguished by using phase rotations and parity measurements.

To implement the rotation U one can use the approach of Ralph *et al.* [34] in which U is decomposed into Euler rotations which can be implemented nearly deterministically. The rotation above can be decomposed into

$$U(\theta,\lambda,\sigma) = iR_z(q)\hat{H}R_z(r)\hat{H}R_z(s), \quad (23)$$

where $\hat{H}$ is the Hadamard matrix, and $R_z(2\theta) = \mathbb{1}\cos\theta - i\sigma_z \sin\theta$ is the phase rotation gate [35]. The phase rotation gate can be accomplished by using a displacement operation and teleportation and the Hadamard matrix can be accomplished by using a teleportation-like setup [34]. The values of q, r, and s in Eq. (23) are given by

$$q = \frac{\pi}{2} + \xi + \eta, \quad r = 2\theta, \quad s = \frac{\pi}{2} + \xi - \eta, \quad (24)$$

where $\xi = \arg c$, $\eta = \arg d$, and $\tan\theta = |d/c|$. It is easy to see that this approach, involving five nondeterministic operations, will surely cause a reduction in the overall secret key fraction. Regardless, it is possible that an improved measurement approach may alleviate this problem.

We have shown an approach to implementing a device-independent quantum key distribution in which phase-entangled coherent states are used as the information carriers. We show how a judicious choice of initial states relative to the overall transmission rate of the channel can, in principle, lead to improved key-generation rates relative to depolarizing channels in device-independent quantum key distribution systems based on polarization entanglement. We have shown that, for QBERs exceeding ~6.7%, phase-entangled states can be superior to polarization-entangled states, and we have given the explicit form of the states and measurements which achieve this result. We reiterate that, apart from being secure against collective attacks and, in some instances, coherent attacks, our system is also flexible to time-varying loss in the quantum channel; for example, in ground-to-satellite schemes. This means, for example, that if the transmission loss suddenly

decreases, the input states and measurements may be adapted to optimally make use of the updated channel. Finally, we note that our implementation does not require the eavesdropper to be restricted to Gaussian measurements.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[3] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).

[4] http://www.idquantique.com/network-encryption/products/cerberis-quantum-key-distribution.html.

[5] http://quintessencelabs.com/qopticatm/.

[6] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).

[7] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **78**, 019905(E) (2008).

[8] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).

[9] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[10] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 801 (2010).

[13] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photonics **4**, 800 (2010).

[14] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).

[15] H. Weier, H. Krauss, M. Rau, M. Furst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).

[16] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).

[17] S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Phys. Rev. A **83**, 062331 (2011).

[18] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).

[19] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).

[20] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **87**, 062329 (2013).

[21] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **89**, 032304 (2014).

[22] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).

[23] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[24] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[25] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301 (2012).

[26] K. Marshall and C. Weedbrook, Phys. Rev. A **90**, 042311 (2014).

[27] M. McKague, New J. Phys. **11**, 103037 (2009).

[28] L. Masanes, A. Pironio, and A. Acín, Nat. Commun. **2**, 238 (2011).

[29] B. T. Kirby and J. D. Franson, Phys. Rev. A **89**, 033861 (2014).

[30] B. T. Kirby and J. D. Franson, Phys. Rev. A **87**, 053822 (2013).

[31] F. Lastra, G. Romero, C. E. López, N. Zagury, and J. C. Retamal, Opt. Commun. **283**, 3825 (2010).

[32] F. Verstraete, J. Dehaene, and B. DeMoor, Phys. Rev. A **64**, 010101 (2001).

[33] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **200**, 340 (1995).

[34] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, Phys. Rev. A **68**, 042319 (2003).

[35] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).