Practical high-dimensional quantum key distribution with decoy states

Darius Bunandar, Zheshen Zhang, Jeffrey H. Shapiro, and Dirk R. Englund

Phys. Rev. A **91**, 022336 — Published 27 February 2015

DOI: 10.1103/PhysRevA.91.022336

Practical high-dimensional quantum key distribution with decoy states

Darius Bunandar,[1,2,*] Zheshen Zhang,[1] Jeffrey H. Shapiro,[1] and Dirk R. Englund[1]

[1] *Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[2] *Department of Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

(Dated: January 7, 2015)

High-dimensional quantum key distribution (HD-QKD) allows two parties to generate multiple secure bits of information per detected photon. In this work, we show that decoy state protocols can be practically implemented for HD-QKD using only one or two decoy states. HD-QKD with two decoy states, under realistic experimental constraints, can generate multiple secure bits per coincidence at distances over 200 km and at rates similar to those achieved by a protocol with infinite decoy states. Furthermore, HD-QKD with only one decoy state is practical at short distances, where it is almost as secure as a protocol with two decoy states. HD-QKD with only one or two decoy states can therefore be implemented to optimize the rate of secure quantum communications.

PACS numbers: 03.67.Dd, 42.50.Ex, 42.65.Lm

I. INTRODUCTION

High-dimensional quantum key distribution (HD-QKD), using qudits of dimensions $d > 2$, enables its participants to optimize the secret-key capacity of a bosonic channel under technical constraints [1]; when the secret-key generation rate is limited by the rate at which Alice generates photons or by the rate at which Bob can detect photons due to the detector dead time, the secret-key generation rate can be improved by high-dimensional photon encoding where each photon can encode as much as $\log_2 d > 1$ bits of information. Moreover, HD-QKD protocols may tolerate more noise than two-level, or qubit [2–4], QKD protocols [5].

Discrete HD-QKD protocols have been proven to be secure against coherent attacks, in which Eve is allowed to interact with all signals simultaneously [6, 7]. Various photonic degrees of freedom have been investigated for HD-QKD, including position-momentum [1], time-energy [8–12], transverse momentum [13], and orbital angular momentum [14–17]. Among these, the time-energy basis is particularly attractive because time-energy correlations are compatible with wavelength-division multiplexing (WDM) systems and are robust in both free-space and fiber-based transmissions.

Recently, HD-QKD protocols employing time-energy entanglement have been proven to be secure against collective attacks, in which Eve's apparatus—which can include quantum memory—is restricted to interact with each signal separately [18, 19]. (The bounds for unconditional security for both coherent and collective attacks turn out to be identical for most protocols [20].) The proofs in [18, 19] use the time-frequency covariance matrix—similar to the one used in continuous-variable QKD protocols [21–23]—to derive a lower bound on the secure-key rate under collective attacks. The time-frequency covariance matrix can be measured using dispersive optics [18, 24] or Franson interferometers [19, 25]. The time-energy entanglement of photon pairs produced by spontaneous parametric down conversion (SPDC) has also been harnessed in several HD-QKD experiments [8, 11, 26].

All these experiments assume single-pair emissions from the SPDC source, whereas multi-pair emissions do occur. For a continuous-wave source, the signal and idler from each signal-idler mode pair are individually in identical thermal states with average photon numbers that are much smaller than one. Therefore, when the HD-QKD frame time does not greatly exceed the sources correlation time, multi-pair emissions occurring during a particular frame will tend to be correlated in timean effect known as photon bunching [27]. In such cases, when any of these HD-QKD protocols is performed via a lossy channel, it is vulnerable to the photon number splitting (PNS) attack. On the other hand, when the frame time is much greater than the correlation time, the number of photon pairs emitted in a frame will be Poisson distributed, hence no photon bunching is then expected. Nevertheless, a PNS attack can provide Eve with some information about Alice and Bobs measurements when they reconcile their results via classical communication that Eve can monitor.

In the PNS attack, Eve measures the photon number of each transmission and selectively suppresses single photon signals [28–31]. She then splits multiphoton signals—keeping one copy to herself and sending the other copy to Bob. Under the collective attack scheme, Eve stores her photons in a quantum memory and only measures them after Bob publishes his measurement bases over a public channel. She takes advantage of the timing correlations in the bunched photons to acquire information about Alice and Bob's key without being detected.

The decoy state protocol is designed to detect the PNS attack [32]. The central idea is to test the channel transmission properties by varying the source intensity. Decoy-state QKD has been discussed extensively in the context of BB84 protocol [33–36]. In addition, several experiments have demonstrated the generation of secure

* dariusb@mit.edu

bits over 144 km in free space [37] and over 107 km in optical fiber [38]. Furthermore, it has been shown that decoy states can also be generated passively by using a beam splitter or by monitoring the idler of an SPDC source [39–45]. Recently, decoy-state analysis was extended to HD-QKD protocols [19], but for an infinite number of decoy states, which is practically impossible.

Here, we analyze for the first time the security of HD-QKD protocols employing a practical number of decoy states. Unlike the BB84 decoy-state QKD protocol, we make use of the decrease in measurement correlations instead of the quantum bit error rate (QBER) to estimate the amount of information gained by Eve. As a consequence, we find that the two-decoy-state protocol with one vacuum decoy state, which provides the best secure-key rate for BB84 [35], is not optimal for HD-QKD.

The analysis presented here answers a pressing question for experimental implementations of HD-QKD: how many decoy states are necessary for HD-QKD protocols to be robust against the PNS attack? We show by numerical evaluations, assuming realistic experimental parameters, that the security of a protocol with two decoy states approaches that of a protocol with an infinite number of decoy states. HD-QKD with only two decoy states can therefore be used to maximize the rate of high-speed secure quantum communications under experimental constraints.

We shall focus our discussion on a specific HD-QKD scheme: the dispersive optics QKD (DO-QKD) protocol [18, 46, 47], which employs group velocity dispersion to transform between mutually unbiased time and frequency bases. Although we restrict our analysis to DO-QKD, the same arguments are also applicable to other HD-QKD protocols employing time-energy entanglement.

This work is organized as follows: Sec. II briefly reviews the DO-QKD protocol. Sec. III outlines the general decoy-state protocol. We discuss the relevant parameters that can be measured by Alice and Bob during quantum communication. In addition, we present a lower bound on the secure-key capacity when an infinite number of decoy states is available to Alice and Bob. Sec. IV derives a new lower bound on the secure-key capacity when only two decoy states are employed, and Sec. V considers the case of a single decoy state. Sec. VI presents a lower bound on the secure-key capacity when no decoy state is employed. The results of a numerical evaluation with realistic experimental contraints are presented in Sec. VII. We defer the calculation of mutual information between Alice and Bob and the calculation of Eve's Holevo information to Appendices A and B.

II. DISPERSIVE OPTICS QUANTUM KEY DISTRIBUTION

In the DO-QKD protocol, illustrated in Fig. 1, Alice weakly pumps an SPDC source such that the time-energy entangled output state when only one pair is emitted can be approximated to have a Gaussian envelope [26]:

$$\psi(t_A, t_B) \propto e^{-(t_A - t_B)^2/4\sigma_{\rm cor}^2} e^{-(t_A + t_B)^2/16\sigma_{\rm coh}^2}. \quad (1)$$

Here, $\sigma_{\rm coh}$ is the coherence time of the pump field, and $\sigma_{\rm cor}$ is the correlation time between the two photons generated by the SPDC source. $\sigma_{\rm coh}$ typically can be longer than a microsecond for a diode laser, and $\sigma_{\rm cor}$ is typically on the order of picoseconds for typical SPDC sources [48]. The number of alphabet characters per photon pulse, $d = \sigma_{\rm coh}/\sigma_{\rm cor}$ (the Schmidt number), therefore can be large [11, 49].

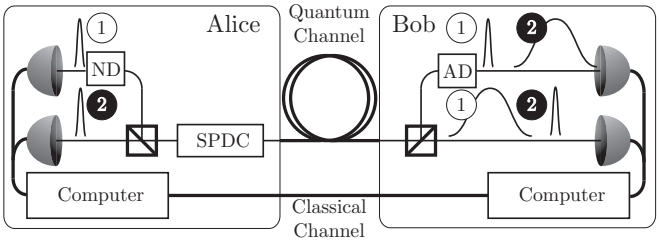

FIG. 1. Schematic diagram of the DO-QKD setup. Alice and Bob randomly choose to measure in either the arrival-time basis or the frequency basis. In case 1, Alice measures in the frequency basis by applying a normal dispersion (ND). Bob's measurement is only anti-correlated to Alice's if he also measures in the frequency basis by applying an anomalous dispersion (AD). In case 2, Alice measures in the arrival-time basis, and Bob's measurement is only correlated to Alice's if he also measures in the arrival-time basis.

Alice and Bob randomly choose to measure their photons in the conjugate bases of photon arrival time and photon frequency; the two bases are measured using a fast single-photon detector or a dispersive optical element followed by photodetection, respectively. We assume that Alice and Bob have complete control of their own setups, precluding tampering by any third party such as Eve. In a single measurement frame, if both Alice and Bob measure their photons in the arrival-time basis, their timing measurements will be correlated. Similarly, if both parties measure in the frequency basis, their measurements will be anti-correlated. On the other hand, if one party measures in the frequency basis while the other measures in the arrival-time basis, the timing correlation between their photons is severely diminished.

After the measurement stage, Alice and Bob sift for frames in which both of them registered at least one detection event. For any frame with more than one coincidence, Alice and Bob replace their detection events with a random variable whose probability distribution matches that of photons originating from single-pair emissions. Finally, they apply error correction and privacy amplification to establish identical secret keys.

The DO-QKD protocol is not prone to the PNS attack when it is performed using an on-demand single photon

source. When such a photon source is used, the bound on the secure-key capacity of a DO-QKD protocol, in terms of bits per photon-pair coincidence (bpc), is [23, 50]

$$\Delta I \geqslant \beta I(A;B) - \chi^{\mathrm{UB}}_{\xi_t,\xi_\omega}(A;E), \tag{2}$$

where β is the reconciliation efficiency and $I(A;B)$ is the mutual information between Alice and Bob. $\chi^{\mathrm{UB}}_{\xi_t,\xi_\omega}(A;E)$ is an upper bound on Eve's Holevo information under collective attacks, given the excess-noise factors ξ_t and ξ_ω for the timing and the frequency correlations, respectively.

Eve's attack on Alice's transmission degrades the correlations of Alice and Bob's measurements in a manner parameterized by the excess-noise factors. Explicitly, $\mathrm{Var}[T'_A - T'_B] = (1+\xi_t)\,\mathrm{Var}[T_A - T_B]$ and $\mathrm{Var}[\Omega'_A + \Omega'_B] = (1+\xi_\omega)\,\mathrm{Var}[\Omega_A + \Omega_B]$, where T_A (T_B) and Ω_A (Ω_B) are the random variables associated with Alice's (Bob's) time and frequency measurements without Eve's presence. The corresponding primed variables are the random variables after Eve's intrusion. The sign difference is a consequence of Alice and Bob's timing measurements being directly correlated while their frequency measurements are anti-correlated. These excess-noise factors allow us to place an upper bound on Eve's Holevo information.

III. GENERAL DECOY STATE PROTOCOL

A. Postselection probability

We consider the practical case of interest for SPDC-based HD-QKD systems, i.e., we assume a continuous-wave source operating at low brightness (signal and idler beams have average photon numbers per mode much less than one) with a frame time that greatly exceeds the correlation time. In this case, the photon-pair statistics are approximately Poissonian [51, 52]. Suppose that Alice's SPDC source emits an average of λ pairs per measurement frame, the probability Pr_n of emitting n-photon pairs in a single measurement frame is then

$$\mathrm{Pr}_n = \frac{\lambda^n}{n!} e^{-\lambda}. \tag{3}$$

Furthermore, the postselection probability, which is the probability of Alice and Bob registering at least one detection (due to a photon or a dark count) in a single measurement frame, can be written as

$$P_\lambda = \sum_{n=0}^{\infty} \mathrm{Pr}_n C_n = \sum_{n=0}^{\infty} \frac{\lambda^n}{n!} e^{-\lambda} C_n, \tag{4}$$

where C_n is the conditional probability of measuring at least one detection given n-photon pairs are emitted. Explicitly, in Eve's absence we have

$$\begin{aligned} C_n =& [1-(1-\eta_A)^n(1-p_d)] \\ &\times [1-(1-\eta_B\eta_P)^n(1-p_d)]\,. \end{aligned} \tag{5}$$

Here, η_A and η_B are Alice and Bob's detector efficiencies, η_P is the transmittance of the quantum channel linking Alice's source to Bob's terminal, and p_d is the probability of one dark count in a single measurement frame. We are neglecting the possibility of multiple dark counts occurring in a frame because the product of the frame duration and the dark count rate for a typical superconducting nanowire single-photon detectors is much smaller than one [53]. Eve, in principle, has the freedom to affect the C_n values. The goal of the decoy state protocol is to estimate the C_n values from the postselection probabilities of different choices of λ.

B. Excess noise

Alice and Bob cannot directly measure their timing and frequency correlations when there are multiphoton emissions and dark counts. They can only measure the averaged correlations:

$$\begin{aligned} \mathrm{Var}[T'_A - T'_B]_\lambda &= F_\lambda\,\mathrm{Var}[T'_A - T'_B] + (1-F_\lambda)\,\Delta\sigma_t^2, \\ \mathrm{Var}[\Omega'_A + \Omega'_B]_\lambda &= F_\lambda\,\mathrm{Var}[\Omega'_A + \Omega'_B] + (1-F_\lambda)\,\Delta\sigma_\omega^2, \end{aligned} \tag{6}$$

where $F_\lambda = \lambda e^{-\lambda} C_1 / P_\lambda$ is the fraction of postselected events that are due to single photon emissions, and $\Delta\sigma_t^2$ ($\Delta\sigma_\omega^2$) is the measured time (dispersed-time) correlations that are due to measurements of multiphoton emissions and dark counts.

It is convenient to divide (6) by $\mathrm{Var}[T_A - T_B]$ or $\mathrm{Var}[\Omega_A + \Omega_B]$ so that the excess-noise factors ξ_t and ξ_ω are explicit:

$$\begin{aligned} \Xi_{t,\nu} &= F_\lambda(1+\xi_t) + (1-F_\lambda)\,\Delta\Xi_t, \\ \Xi_{\omega,\nu} &= F_\lambda(1+\xi_\omega) + (1-F_\lambda)\,\Delta\Xi_\omega. \end{aligned} \tag{7}$$

The quantity $\Xi_{x,\lambda}$ (for $x = t$ or ω) is the averaged excess-noise multiplier, which can be measured by Alice and Bob.

C. Infinite number of decoy states

Now suppose that Alice and Bob choose a signal state with an expected photon-pair number μ and decoy states with expected photon-pair numbers $\nu_1, \nu_2, \ldots, \nu_m$. Alice and Bob can then use the knowledge of the postselection probabilities $\mathcal{P} = \{P_\mu, P_{\nu_1}, \ldots, P_{\nu_m}\}$ and the multipliers $\mathcal{K} = \{\Xi_{x,\mu}, \Xi_{x,\nu_1}, \ldots, \Xi_{x,\nu_m}\}$ (for $x = t$ and ω) to estimate the values of C_n and ξ_x.

If we assume that $m \to \infty$, the key length is infinite, and the values of C_n are linearly independent of each other, then Alice and Bob can determine the C_n values to arbitrarily high confidence by measuring the set $\mathcal{P}$. Similarly, by measuring the set $\mathcal{K}$, they can determine ξ_x to arbitrarily high confidence. Therefore, Alice and Bob can detect any attack by Eve that affects the values of C_n and ξ_x [32–34].

The bound on the secure-key capacity with $m \to \infty$ decoy states is [19]

$$\Delta I \geqslant \beta I(A;B) - \chi', \tag{8}$$

where χ' is the amount of information assumed to be lost to Eve, defined as

$$\chi' = (1 - F_\mu)\, n_R + F_\mu\, \chi^{\mathrm{UB}}_{\xi_t,\xi_\omega}(A;E). \tag{9}$$

Here, $F_\mu = \mu e^{-\mu} C_1/P_\mu$, and n_R is the number of random bits shared between Alice and Bob when they use an error-correcting code employing an average of n_{ECC} syndrome bits, which are revealed over the public channel. $\beta = (n_R - n_{\mathrm{ECC}})/I(A;B)$ is the reconciliation efficiency. We have assumed that Alice and Bob can derive no security from multiphoton emissions. Note that when the photon source is an on-demand single photon source ($F_\mu = 1$), we recover (2).

IV. TWO DECOY STATES

When only a few decoy states are available, Alice and Bob cannot determine—to arbitrarily high confidence—the amount of information lost to Eve, χ'. They can, however, provide a reasonable upper bound to χ' by:

1. finding a lower bound on F_μ, which estimates how close their photon source is to an ideal one, and
2. finding upper bounds on ξ_t and ξ_ω, which estimate Eve's Holevo information $\chi(A;E)$.

We suppose that Alice and Bob choose fewer than three *weak* decoy states with mean photon-pair numbers ν_1 and ν_2 that satisfy

$$\begin{aligned} &0 \leqslant \nu_2 < \nu_1, \\ &\nu_1 + \nu_2 < \mu. \end{aligned} \tag{10}$$

A. Lower bound on F_μ

The postselection probabilities of the two different states are given by

$$P_{\nu_1} = \sum_{n=0}^{\infty} C_n \frac{\nu_1^n}{n!} e^{-\nu_1}, \tag{11}$$

and

$$P_{\nu_2} = \sum_{n=0}^{\infty} C_n \frac{\nu_2^n}{n!} e^{-\nu_2}. \tag{12}$$

As shown in [35], we can find a lower bound on C_1 from the difference of the two postselection probabilities:

$$\begin{aligned} C_1 \geqslant \frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \Bigg[& P_{\nu_1} e^{\nu_1} - P_{\nu_2} e^{\nu_2} \\ & - \frac{\nu_1^2 - \nu_2^2}{\mu^2} \left(P_\mu e^\mu - C_0 \right) \Bigg], \end{aligned} \tag{13}$$

where the inequality follows from the relation: $(\nu_1/\mu)^n - (\nu_2/\mu)^n \leqslant (\nu_1/\mu)^2 - (\nu_2/\mu)^2$ for $n \geqslant 2$ which is true given (10). The above relation tells us that a lower bound on C_0 is needed to make use of (13). One such bound is

$$C_0 \geqslant \frac{\nu_1 P_{\nu_2} e^{\nu_2} - \nu_2 P_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, \tag{14}$$

which follows from the assumption that $\nu_1 > \nu_2$.

Another lower bound on C_0 can be found using the assumption that Eve does not have access to both Alice and Bob's experimental setups. Since Alice owns the SPDC source, Eve cannot tamper with Alice's measurement of any output state generated by the source. When the source emits no photons, Alice's detector can only register a dark count, which occurs with probability p_d. Eve is allowed to do whatever she pleases with the vacuum state heading towards Bob, such as injecting photons into the channel. However, whatever she does cannot lower the probability of Bob registering a count to any value below p_d. Therefore, we conclude

$$C_0 \geqslant p_d^2. \tag{15}$$

Combining (14) and (15) then gives

$$C_0 \geqslant C_0^{\mathrm{LB},\{\nu_1,\nu_2\}} = \max\left\{ \frac{\nu_1 P_{\nu_2} e^{\nu_2} - \nu_2 P_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, p_d^2 \right\}. \tag{16}$$

By using (13) and (16), we find

$$\begin{aligned} F_\mu &= C_1 \frac{\mu e^{-\mu}}{P_\mu} \\ &\geqslant \frac{\mu^2}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \Bigg[\frac{P_{\nu_1}}{P_\mu} e^{\nu_1 - \mu} - \frac{P_{\nu_2}}{P_\mu} e^{\nu_2 - \mu} \\ &\quad - \frac{\nu_1^2 - \nu_2^2}{\mu^2} \left(1 - \frac{C_0^{\mathrm{LB},\{\nu_1,\nu_2\}} e^{-\mu}}{P_\mu} \right) \Bigg]. \end{aligned} \tag{17}$$

Another way of obtaining a lower bound on F_μ is immediately evident from the postselection probability of a single decoy state. Let $\lambda = \nu_1$ or ν_2 if $\nu_2 \neq 0$, and $\lambda = \nu_1$ if $\nu_2 = 0$. It then follows that

$$\begin{aligned} P_\lambda e^\lambda &= C_0 + C_1 \lambda + \sum_{n=2}^{\infty} \frac{\lambda^n}{n!} C_n \\ &< C_0 + C_1 \lambda + \frac{\lambda^2}{\mu^2} \sum_{n=2}^{\infty} \frac{\mu^n}{n!} C_n \\ &= C_0 + C_1 \lambda + \frac{\lambda^2}{\mu^2} \left(P_\mu e^\mu - C_0 - C_1 \mu \right), \end{aligned} \tag{18}$$

because $\lambda/\mu \leqslant 1$. Solving for C_1 we obtain

$$C_1 > \frac{\mu}{\mu\lambda - \lambda^2} \left[P_\lambda e^\lambda - \frac{\lambda^2}{\mu^2} P_\mu e^\mu - \frac{\mu^2 - \lambda^2}{\mu^2} C_0 \right], \tag{19}$$

which is similar to what is found in Ref. [35] using another method.

Now, we need to upper bound C_0 to find the lower bound of C_1. We again assume that Eve cannot intrude into Alice and Bob's experimental setups. This implies that, when Alice's source emits no photons, Alice and Bob's conditional coincidence probability C_0 cannot exceed the dark count probability of Alice's detectors:

$$C_0 \leqslant C_0^{\mathrm{UB},\{\nu_1,\nu_2\}} = p_d. \tag{20}$$

Therefore,

$$\begin{aligned} F_\mu &= C_1 \frac{\mu e^{-\mu}}{P_\mu} \\ &> \frac{\mu^2}{\mu\lambda - \lambda^2}\left[\frac{P_\lambda}{P_\mu}e^{\lambda-\mu} - \frac{\lambda^2}{\mu^2} - \frac{\mu^2-\lambda^2}{\mu^2}\frac{C_0^{\mathrm{UB},\{\nu_1,\nu_2\}}e^{-\mu}}{P_\mu}\right], \end{aligned} \tag{21}$$

where $\lambda = \nu_1$ or ν_2 if $\nu_2 \neq 0$, and $\lambda = \nu_1$ if $\nu_2 = 0$.

Combining (17) and (21), we get

$$\begin{aligned} F_\mu &\geqslant F_\mu^{\mathrm{LB},\{\nu_1,\nu_2\}} \\ &= \max\left\{\frac{\mu^2}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2}\left[\frac{P_{\nu_1}}{P_\mu}e^{\nu_1-\mu} - \frac{P_{\nu_2}}{P_\mu}e^{\nu_2-\mu}\right.\right. \\ &\quad \left. - \frac{\nu_1^2-\nu_2^2}{\mu^2}\left(1 - \frac{C_0^{\mathrm{LB},\{\nu_1,\nu_2\}}e^{-\mu}}{P_\mu}\right)\right], \\ &\quad \left.\frac{\mu^2}{\mu\lambda-\lambda^2}\left[\frac{P_\lambda}{P_\mu}e^{\lambda-\mu} - \frac{\lambda^2}{\mu^2} - \frac{\mu^2-\lambda^2}{\mu^2}\frac{C_0^{\mathrm{UB},\{\nu_1,\nu_2\}}e^{-\mu}}{P_\mu}\right]\right\}, \end{aligned} \tag{22}$$

where $\lambda = \nu_1$ or ν_2 if $\nu_2 \neq 0$, and $\lambda = \nu_1$ if $\nu_2 = 0$.

B. Upper bounds on ξ_t and ξ_ω

Let $(\lambda_1, \lambda_2) \in \mathcal{L} = \{(\mu,\nu_1),(\mu,\nu_2),(\nu_1,\nu_2)\}$. Each member of $\mathcal{L}$ is an ordered pair of two mean photon-pair numbers. The averaged excess-noise multipliers for the ordered pair (λ_1, λ_2) are

$$\begin{aligned} \Xi_{x,\lambda_1} &= F_{\lambda_1}(1+\xi_x) + \Delta\Xi_x\,(1-F_{\lambda_1}), \\ \Xi_{x,\lambda_2} &= F_{\lambda_2}(1+\xi_x) + \Delta\Xi_x\,(1-F_{\lambda_2}). \end{aligned} \tag{23}$$

Multiplying the above two equations by $P_{\lambda_1}e^{\lambda_1}$ and $P_{\lambda_2}e^{\lambda_2}$ respectively, we obtain

$$\begin{aligned} \Xi_{x,\lambda_1}P_{\lambda_1}e^{\lambda_1} &= \lambda_1 C_1(1+\xi_x) + \Delta\Xi_x\left(P_{\lambda_1}e^{\lambda_1} - \lambda_1 C_1\right), \\ \Xi_{x,\lambda_2}P_{\lambda_2}e^{\lambda_2} &= \lambda_2 C_1(1+\xi_x) + \Delta\Xi_x\left(P_{\lambda_2}e^{\lambda_2} - \lambda_2 C_1\right). \end{aligned} \tag{24}$$

To find upper bounds on ξ_t and ξ_ω, we take the difference between these two equations,

$$\begin{aligned} &\Xi_{x,\lambda_1}P_{\lambda_1}e^{\lambda_1} - \Xi_{x,\lambda_2}P_{\lambda_2}e^{\lambda_2} \\ &\quad = (\lambda_1-\lambda_2)C_1(1+\xi_x) \\ &\qquad + \Delta\Xi_x\left(P_{\lambda_1}e^{\lambda_1} - P_{\lambda_2}e^{\lambda_2} - (\lambda_1-\lambda_2)C_1\right) \\ &\quad \geqslant (\lambda_1-\lambda_2)C_1(1+\xi_x), \end{aligned} \tag{25}$$

where the inequality comes from

$$\begin{aligned} P_{\lambda_1}e^{\lambda_1} - P_{\lambda_2}e^{\lambda_2} &= \sum_{n=0}^{\infty}\frac{\lambda_1^n - \lambda_2^n}{n!}C_n \\ &\geqslant (\lambda_1-\lambda_2)C_1, \end{aligned} \tag{26}$$

since $\lambda_1 > \lambda_2$ for any ordered pair $(\lambda_1, \lambda_2) \in \mathcal{L}$. Thus,

$$\begin{aligned} (1+\xi_x) &\leqslant \frac{1}{(\lambda_1-\lambda_2)C_1}\left(\Xi_{x,\lambda_1}P_{\lambda_1}e^{\lambda_1} - \Xi_{x,\lambda_2}P_{\lambda_2}e^{\lambda_2}\right) \\ &\leqslant \frac{\mu e^{-\mu}}{(\lambda_1-\lambda_2)F_\mu^{\mathrm{LB},\{\nu_1,\nu_2\}}} \\ &\quad \times\left(\Xi_{x,\lambda_1}\frac{P_{\lambda_1}}{P_\mu}e^{\lambda_1} - \Xi_{x,\lambda_2}\frac{P_{\lambda_2}}{P_\mu}e^{\lambda_2}\right), \end{aligned} \tag{27}$$

for $x = t$ and ω.

Another way to place upper bounds on ξ_t and ξ_ω is immediately evident from (7):

$$\begin{aligned} \Xi_{x,\lambda} &= F_\lambda\,(1+\xi_x) + (1-F_\lambda)\;\Delta\Xi_x \\ &\geqslant F_\lambda(1+\xi_x) \\ &= \frac{\lambda P_\mu}{\mu P_\lambda}e^{\mu-\lambda}F_\mu\,(1+\xi_x) \\ &\geqslant \frac{\lambda P_\mu}{\mu P_\lambda}e^{\mu-\lambda}F_\mu^{\mathrm{LB},\{\nu_1,\nu_2\}}\,(1+\xi_x), \end{aligned} \tag{28}$$

for $\lambda \in \{\mu, \nu_1, \nu_2\}$. The inequality above implies that

$$(1+\xi_x) \leqslant \min_{\lambda\in\{\mu,\nu_1,\nu_2\}}\left\{e^{\lambda-\mu}\frac{\mu P_\lambda}{\lambda P_\mu}\frac{\Xi_{x,\lambda}}{F_\mu^{\mathrm{LB},\{\nu_1,\nu_2\}}}\right\}. \tag{29}$$

Combining (27) and (29) gives us

$$\begin{aligned} \xi_x &\leqslant \xi_x^{\mathrm{UB},\{\nu_1,\nu_2\}} \\ &= \min\left\{\min_{(\lambda_1,\lambda_2)\in\mathcal{L}}\left\{\frac{\mu e^{-\mu}}{(\lambda_1-\lambda_2)F_\mu^{\mathrm{LB},\{\nu_1,\nu_2\}}}\right.\right. \\ &\quad \left.\times\left(\Xi_{x,\lambda_1}\frac{P_{\lambda_1}}{P_\mu}e^{\lambda_1} - \Xi_{x,\lambda_2}\frac{P_{\lambda_2}}{P_\mu}e^{\lambda_2}\right)\right\}, \\ &\quad \left.\min_{\lambda\in\{\mu,\nu_1,\nu_2\}}\left\{e^{\lambda-\mu}\frac{\mu P_\lambda}{\lambda P_\mu}\frac{\Xi_{x,\lambda}}{F_\mu^{\mathrm{LB},\{\nu_1,\nu_2\}}}\right\}\right\} - 1. \end{aligned} \tag{30}$$

Using (17) and (30), we obtain a bound on the secure-key capacity of HD-QKD using only two decoy states:

$$\begin{aligned} \Delta I \geqslant &\beta I(A;B)_\mu - (1-F_\mu^{\mathrm{LB},\{\nu_1,\nu_2\}})n_R \\ &- F_\mu^{\mathrm{LB},\{\nu_1,\nu_2\}}\chi^{\mathrm{UB}}_{\xi_t^{\mathrm{UB},\{\nu_1,\nu_2\}},\xi_\omega^{\mathrm{UB},\{\nu_1,\nu_2\}}}(A;E), \end{aligned} \tag{31}$$

where the subscript μ on $I(A;B)$ indicates that Alice and Bob's mutual information is calculated using the signal state.

V. ONE DECOY STATE

When Alice only uses one decoy state, whose mean photon-pair number ν is smaller than that of the signal state μ, we can find a lower bound on F_μ by using (21) with $\lambda = \nu$. The argument used to upper bound C_0 still applies because it only depends on the assumption that Eve cannot intrude into Alice and Bob's experimental setups. Therefore,

$$\begin{aligned} F_\mu &\geqslant F_\mu^{\mathrm{LB},\{\nu\}} \\ &= \frac{\mu^2}{\mu\nu - \nu^2}\left[\frac{P_\nu}{P_\mu}e^{\nu-\mu} - \frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2}\frac{C_0^{\mathrm{UB},\{\nu\}}e^{-\mu}}{P_\mu}\right], \end{aligned} \tag{32}$$

with $C_0 \leqslant C_0^{\mathrm{UB},\{\nu\}} = p_d$.

Similarly, upper bounds on ξ_t and ξ_ω can be found by using (30) with $(\lambda_1, \lambda_2) = (\mu, \nu)$ and $\lambda \in \{\mu, \nu\}$:

$$\begin{aligned} \xi_x &\leqslant \xi_x^{\mathrm{UB},\{\nu\}} \\ &= \min\left\{\frac{\mu}{(\mu-\nu)F_\mu^{\mathrm{LB},\{\nu\}}}\left(\Xi_{x,\mu} - \frac{P_\nu}{P_\mu}\Xi_{x,\nu}e^{\nu-\mu}\right),\right. \\ &\qquad \left.\min_{\lambda\in\{\mu,\nu\}}\left\{e^{\lambda-\mu}\frac{\mu P_\lambda}{\lambda P_\mu}\frac{\Xi_{x,\lambda}}{F_\mu^{\mathrm{LB},\{\nu\}}}\right\}\right\} - 1, \end{aligned} \tag{33}$$

for $x = t$ and ω.

VI. NO DECOY STATES

When decoy states are not employed, Alice and Bob must use a fraction of their signal frames to estimate the transmission parameters. To find a lower bound on F_μ, consider

$$\begin{aligned} P_\mu e^\mu &= C_0 + C_1\mu + \sum_{n=2}^{\infty}\frac{\mu^n}{n!}C_n \\ &\leqslant C_0^{\mathrm{UB},\emptyset} + C_1\mu + \sum_{n=2}^{\infty}\frac{\mu^n}{n!}C_n^{\mathrm{UB},\emptyset}, \end{aligned} \tag{34}$$

where

$$C_n \leqslant C_n^{\mathrm{UB},\emptyset} = 1 - (1-\eta_A)^n(1-p_d), \tag{35}$$

is a consequence of Eve's inability to affect Alice's detection probability.

Using the relations above, we have

$$C_1 \geqslant C_1^{\mathrm{LB},\emptyset} = \frac{1}{\mu}\left[P_\mu e^\mu - C_0^{\mathrm{UB},\emptyset} - \sum_{n=2}^{\infty}\frac{\mu^n}{n!}C_n^{\mathrm{UB},\emptyset}\right], \tag{36}$$

and hence

$$\begin{aligned} F_\mu &\geqslant F_\mu^{\mathrm{LB},\emptyset} \\ &= C_1^{\mathrm{LB},\emptyset}\frac{\mu e^{-\mu}}{P_\mu} \\ &= 1 - \frac{C_0^{\mathrm{UB},\emptyset}e^{-\mu}}{P_\mu} - \sum_{n=2}^{\infty}\frac{\mu^n}{n!}\frac{C_n^{\mathrm{UB},\emptyset}e^{-\mu}}{P_\mu}. \end{aligned} \tag{37}$$

Because $\Xi_{x,\mu}$ is the only available excess-noise multiplier, the upper bounds on ξ_t and ξ_ω are found by using (29) with $\lambda = \mu$:

$$\xi_x \leqslant \xi_x^{\mathrm{UB},\emptyset} = \frac{\Xi_{x,\mu}}{F_\mu^{\mathrm{LB},\emptyset}} - 1, \tag{38}$$

for $x = t$ and ω.

VII. NUMERICAL RESULTS AND DISCUSSION

Figure 2 plots the secure-key capacity of decoy-state HD-QKD with an SPDC source of mean photon-pair numbers per frame $\mu = 0.01, 0.10$, and 0.25. The top panels show the case in which the Schmidt number $d = 8$ while the bottom panels show the case in which $d = 32$. Three different decoy state protocols are plotted in each panel: the one-decoy-state protocol, the two-decoy-state protocol, and the infinite-decoy-state protocol. For comparison, we also plot the security of HD-QKD protocol without decoy states.

In particular, we consider the case $\nu = \mu/2$ for the one-decoy-state protocol. For the two-decoy-state protocol, we similarly assume $\nu_1 = \mu/2$, but we optimize ν_2 such that, for any particular transmission distance, the lower bound on the secure-key capacity ΔI is maximized. Figure 3 plots the optimal values of ν_2 as a function of transmission distance at 10 km increments.

For the cases of $\mu = 0.10$ and 0.25, (21) gives a better lower bound on F_μ at short distances. The sharp drop in the optimal values of ν_2 (at ∼50 km for $\mu = 0.10$ and at ∼100 km for $\mu = 0.25$) indicates where (17) starts to provide a better lower bound on F_μ than (21). On the other hand, for the cases of $\mu = 0.01$, (17) provides a better lower bound on F_μ at all distances. Moreover, the optimal values of ν_2 are small compared to μ—but non-zero. This result is in contrast to the two-decoy-state BB84 protocol whose lower bound on secure-key capacity is always maximized when $\nu_2 \to 0$ [35].

We take $\sigma_{\mathrm{cor}} = 30$ ps for both d values, and $\sigma_{\mathrm{coh}} = d\sigma_{\mathrm{cor}}$. The frame duration T_f is chosen to be $T_f = 2\sqrt{2\ln 2}\,\sigma_{\mathrm{coh}}$. Experimentally, when a larger d is wanted, it is easier to increase the coherence time σ_{coh} than to decrease the correlation time σ_{cor}. This is because the σ_{coh} can be increased by modulating the pulse duration of the laser pump field. On the other hand, σ_{cor} is determined by the phase-matching bandwidth of the SPDC source and is characteristic to the parametric down-conversion process.

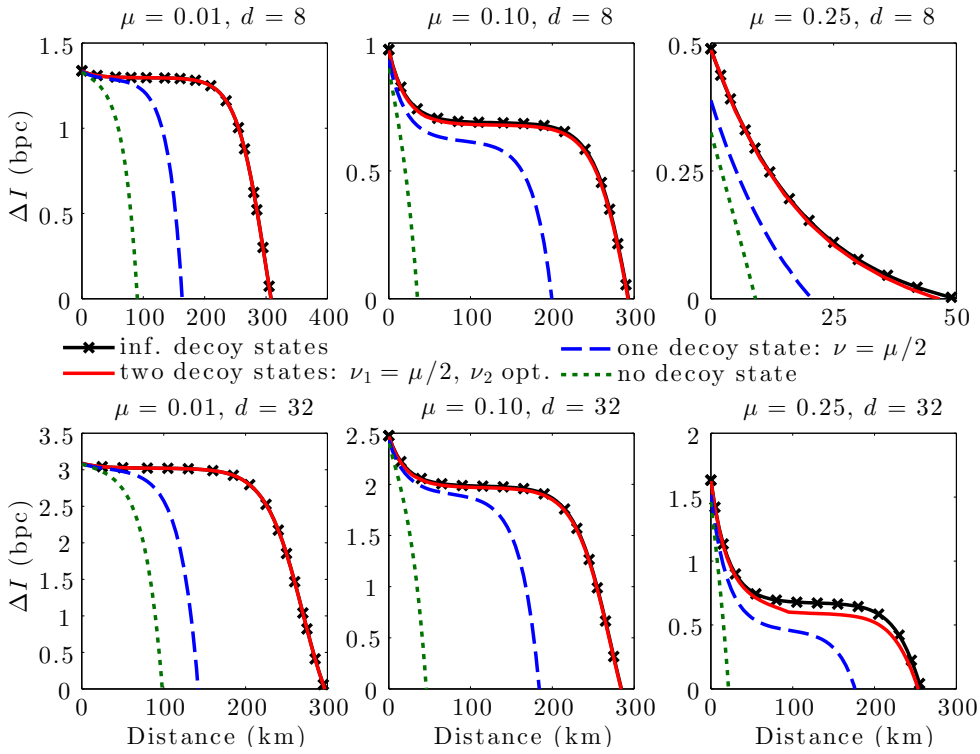

FIG. 2. Lower bounds on the secure-key capacity (in bits per coincidence) of decoy-state HD-QKD as a function of transmission distance. Top panels show the case $d = 8$ and bottom panels show the case $d = 32$. Solid lines with crosses (black) correspond to HD-QKD with infinite decoy states; solid lines (red) correspond to HD-QKD with two weak decoy states of $\nu_1 = \mu/2$ and an optimized ν_2; dashed lines (blue) correspond to HD-QKD with only one decoy state of $\nu = \mu/2$; and dotted lines (green) show the performance of HD-QKD without decoy states. For $\mu = 0.01$ and 0.10 ($d = 8$ and 32), lines for the infinite-decoy-state and the two-decoy-state protocols are indistinguishable at the plots' scales.

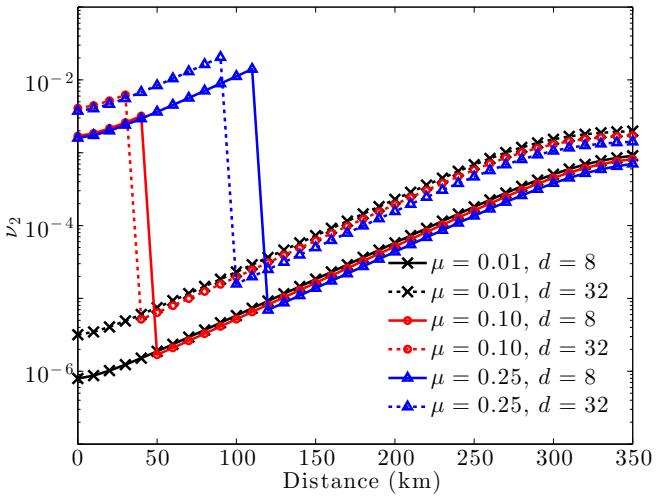

FIG. 3. Optimal values of ν_2 at different transmission distances for two-decoy-state protocols with $\mu = \{0.01, 0.10, 0.25\}$ and $\nu_1 = \mu/2$.

We assume the following experimental parameters: propagation loss $\alpha = 0.2$ dB/km; detector timing jitter $\sigma_J = 20$ ps; dark count rate $r_D = 1000\ \mathrm{s}^{-1}$; reconciliation efficiency $\beta = 0.9$; $n_R = \log_2 d$. The transmittance $\eta_P = 10^{-\alpha L/10}$, where L is the length of the quantum channel in km. We also assume that Alice and Bob have the same detector efficiencies: $\eta_A = \eta_B = 0.93$ [53].

For simplicity, we assume equal excess-noise factors for both the arrival-time and the frequency measurements, $\xi_t = \xi_\omega = \xi$. The change in correlation time due to Eve's interaction is assumed to be $\sigma_\Delta = \left(\sqrt{1+\xi} - 1\right) \times \sigma_{\mathrm{cor}} = 10$ ps. When Alice and Bob do not use an infinite number of decoy states, they can only measure Ξ_μ. For the calculations, we assume that $\Delta\Xi = 1 + \xi$. Details on calculating Alice and Bob's mutual information, as well as Eve's Holevo information, are outlined in Appendices A and B.

Using decoy states improves the security of the HD-QKD protocol. For example, while the case of $\mu = 0.25$ and $d = 32$ is insecure beyond 25 km without decoy states, the one-decoy-state protocol is able to generate 0.45 secure bpc at a distance of 100 km. Furthermore, when two weak decoy states are used, the protocol can generate more than 0.52 secure bpc up to a distance of 200 km.

Even though the probability of multiphoton emissions is low for $\mu = 0.01$, we only obtain secure bits up to a distance of ∼100 km without decoy states. However,

the presence of one decoy state allows us to obtain 1.22 secure bpc for $d = 8$ and 2.57 secure bpc for $d = 32$ at the 100 km distance. The two-decoy-state protocols generate more than 1.26 secure bpc for $d = 8$ and more than 2.83 secure bpc for $d = 32$ up to a distance of 200 km.

In Fig. 2, we also see that protocols with two decoy states perform almost as well as protocols with infinite decoy states. Intuitively, a protocol with an infinite number of decoy states should perform the best because an infinite number of decoy states allows us to estimate the values of all C_n precisely. Nevertheless, the two-decoy-state protocols asymptotes to the infinite-decoy-state protocols—performing only slightly worse in the generation of secure-bit capacities at similar transmission distances. When two decoy states are employed, Alice and Bob can find useful lower bounds on C_1 and C_0 (and hence F_μ). High-dimensional QKD protocols with two decoy states therefore appear practical as they offer multiple secure bits per coincidence at distances and at rates similar to those achieved by a protocol with infinite decoy states.

The two-decoy-state protocol can reach a longer secure distance than the one-decoy-state protocol. To see why, consider (4) and (5). Notice that at short distances, where the transmittance $\eta_P \sim 1$, the postselection probability is dominated by C_n with small values of n. However, at large distances, where the transmittance $\eta_P \ll 1$, the postselection probability is dominated by C_n with large values of n. Therefore, referring to (32), the lower bound on F_μ in the one-decoy-state protocol—calculated by taking the difference between $P_\nu e^\nu$ and C_0—decreases quickly as the channel transmittance η_P decreases. On the other hand, the lower bound of F_μ in (17) for the two-decoy-state protocol is calculated by taking the difference between $P_{\nu_1} e^{\nu_1}$ and $P_{\nu_2} e^{\nu_2}$, which are of comparable values at both short and long distances. The one-decoy-state protocol is nevertheless easy to implement. Moreover, the one-decoy-state protocol offers boosts to the lower bound on secure-key capacity—increasing the secure distance and the generation rate—of a protocol without decoy states.

It is also interesting that, independent of the number of decoy states employed, the photon efficiency of HD-QKD (in bpc) decreases rapidly with increasing μ. The case of $\mu = 0.25$ and $d = 8$ is insecure at only 50 km—even when infinite decoy states are used. This implies that the μ value employed in HD-QKD should be chosen to ensure that the probability of multiphoton emissions is low.

VIII. CONCLUSION

We have analyzed the practicality of HD-QKD protocols with decoy states. In particular, we considered the case of HD-QKD with two decoy states and with one decoy state. For completeness, we have also studied how the HD-QKD would perform without decoy states.

Through simple numerical examples, we have shown that HD-QKD with two decoy states is practical: it can achieve multiple secure bits per coincidence at distances over 200 km and at rates similar to those achieved by a protocol with infinite decoy states. The HD-QKD protocol with only one decoy state is also practical at short distances, in which case it is almost as secure as the two-decoy-state protocol at short distances.

While we have only considered the DO-QKD protocol, the arguments presented in this work can be generalized to other HD-QKD protocols [12, 19]. Decoy-state HD-QKD protocols that are robust against collective PNS attacks can therefore be used to maximize the rate of high-speed secure quantum communications.

IX. ACKNOWLEDGMENTS

The authors would like to thank Jacob Mower, Catherine Lee, and Gregory Steinbrecher for their helpful discussions. This work was supported by the DARPA Quiness Program through U.S. Army Research Office Grant No. W31P4Q-12-1-0019. DB acknowledges the support of Bruno Rossi Graduate Fellowship in Physics at MIT.

Appendix A: Eve's Holevo information

The output state from an SPDC source in the low-flux limit is Gaussian, and Gaussian attacks are optimal for a given covariance matrix [22, 23]. Alice and Bob's time-frequency covariance matrix is therefore crucial in estimating Eve's Holevo information [54]. Before any interaction with Eve, it is

$$\Gamma = \begin{pmatrix} \gamma_{AA} & \gamma_{AB} \\ \gamma_{BA} & \gamma_{BB} \end{pmatrix}, \tag{A1}$$

where the submatrices γ_{JK} for $J, K = A, B$ are given by

$$\begin{aligned} \gamma_{AA} &= \begin{pmatrix} \frac{u+v}{16} & -\frac{u+v}{8k} \\ -\frac{u+v}{8k} & \frac{(u+v)(4k^2+uv)}{4k^2uv} \end{pmatrix}, \\ \gamma_{AB} = \gamma_{BA}^T &= \begin{pmatrix} \frac{u-v}{16} & \frac{u-v}{8k} \\ -\frac{u-v}{8k} & -\frac{(u-v)(4k^2+uv)}{4k^2uv} \end{pmatrix}, \\ \gamma_{BB} &= \begin{pmatrix} \frac{u+v}{16} & \frac{u+v}{8k} \\ \frac{u+v}{8k} & \frac{(u+v)(4k^2+uv)}{4k^2uv} \end{pmatrix}, \end{aligned} \tag{A2}$$

with $u = 16\sigma_{\text{coh}}^2$ and $v = 4\sigma_{\text{cor}}^2$ [18]. Note that every entry in the covariance matrix is measured in units of time. After Eve's interaction, the new covariance matrix is

$$\Gamma' = \begin{pmatrix} \gamma'_{AA} & \gamma'_{AB} \\ \gamma'_{BA} & \gamma'_{BB} \end{pmatrix}, \tag{A3}$$

where the new submatrices are

$$\begin{aligned}\gamma'_{AA} &= \gamma_{AA},\\ \gamma'_{AB} &= (\gamma'_{BA})^T = \begin{pmatrix} 1-\eta_t & 0 \\ 0 & 1-\eta_\omega \end{pmatrix} \gamma_{AB},\\ \gamma'_{BB} &= \begin{pmatrix} 1-\epsilon_t & 0 \\ 0 & 1-\epsilon_\omega \end{pmatrix} \gamma_{BB}.\end{aligned} \tag{A4}$$

Here, η_t and η_ω represent the decrease in correlations, while ϵ_t and ϵ_ω represent the excess noise—all due to Eve's interactions.

Once Alice and Bob have estimated the covariance matrix Γ', we can then assume that Alice, Bob, and Eve share a pure Gaussian state ρ_{ABE} in evaluating Eve's Holevo information. If Alice and Bob only generate secure bits from their arrival-time measurements, Eve's Holevo information can then be calculated from

$$\chi_{\xi_t,\xi_\omega}(A;E) = S(\rho_{AB}) - S(\rho_{\,B|T_A}), \tag{A5}$$

where $S(\rho) = -\operatorname{Tr}[\rho \log_2 \rho]$ is the von Neumann entropy of the quantum state ρ. $S(\rho_{AB})$ can then be evaluated from $S(\rho_{AB}) = f(d_+) + f(d_-)$ where

$$f(x) = \left(x+\frac{1}{2}\right)\log_2\left(x+\frac{1}{2}\right) - \left(x-\frac{1}{2}\right)\log_2\left(x-\frac{1}{2}\right), \tag{A6}$$

and

$$\begin{aligned} d_\pm &= \frac{1}{\sqrt{2}}\sqrt{I_1 \pm \sqrt{I_1^2 - 4I_2}},\\ I_1 &= \det[\gamma'_{AA}] + \det[\gamma'_{BB}] + 2\det[\gamma'_{AB}],\\ I_2 &= \det\Gamma'. \end{aligned} \tag{A7}$$

Furthermore, $S(\rho_{\,B|T_A})$ can be computed from

$$S(\rho_{\,B|T_A}) = f\left(\sqrt{\det[\gamma'_{B|T_A}]}\right), \tag{A8}$$

where

$$\gamma'_{B|T_A} = \gamma'_{BB} - \gamma'_{BA}\left(X_t\gamma'_{AA}X_t\right)^{-1}\gamma'_{AB}, \tag{A9}$$

Here, $X_t = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, and the inverse is done carried out using the Moore-Penrose pseudoinverse.

As done in Ref. [18], we shall assume that the excess-noise factors in the arrival-time and frequency measurements to be equal, i.e. $\xi_t = \xi_\omega = \xi$. With this assumption, we can make the simplification: $\eta_t = \eta_\omega = \eta$ and $\epsilon_t = \epsilon_\omega = \epsilon$. Thus, we can write Alice and Bob's covariance matrix after Eve's interaction as

$$\Gamma' = \begin{pmatrix} \gamma_{AA} & (1-\eta)\gamma_{AB} \\ (1-\eta)\gamma_{BA} & (1+\epsilon)\gamma_{BB} \end{pmatrix}. \tag{A10}$$

The relationship between the three noise parameters η, ϵ, and ξ is

$$\epsilon = \frac{-2\eta(d^2 - 1/4) + \xi}{d^2 + 1/4}, \tag{A11}$$

where $d = \sigma_{\rm coh}/\sigma_{\rm cor}$ is the Schmidt number. After Alice and Bob estimate the value of ξ from their data, they should then choose the values of η and ϵ that maximize Eve's Holevo information. The range of possible η and ϵ satisfy not only the relationship given above but also the following additional constraints: (a) Eve cannot increase Alice and Bob's mutual information by interacting with only Bob's photons due to the data processing inequality; (b) the symplectic eigenvalues of the covariance matrix are greater than 1/2; and (c) Eve can only degrade Alice and Bob's arrival-time correlations, i.e. $\operatorname{Var}[T'_A - T'_B] \geqslant \operatorname{Var}[T_A - T_B]$.

Appendix B: Alice and Bob's mutual information

We assume that Alice and Bob only generate secure bits from their arrival-time measurements. During the reconciliation stage, Alice and Bob postselect frames in which each of them has at least one coincidence—either due to dark count or due to an actual photon. The probability for their postselecting a frame is given by (4). In some of these postselected frames, either Alice or Bob may have registered more than one coincidence. To prevent Eve from exploiting multiple-coincidence frames, Alice and Bob replace such data with single coincidences chosen randomly from a Gaussian distribution whose variance equals the corresponding entry in the covariance matrix Γ' plus the timing-jitter variance. Alice and Bob's arrival-time measurements therefore will derive from five different probability distributions: [19]

1. Bivariate Gaussian probability distribution with covariance matrix

$$\Lambda = \begin{pmatrix} \sigma_A^2 & \operatorname{Cov}[T'_A, T'_B] \\ \operatorname{Cov}[T'_A, T'_B] & \sigma_B^2 \end{pmatrix}, \tag{B1}$$

where $\operatorname{Cov}[T'_A, T'_B]$ means the covariance between T'_A and T'_B, i.e. the top-left entry of the submatrix γ'_{AB}, $\sigma_A^2 = \operatorname{Var}[T'_A] + \sigma_J^2$, and $\sigma_B^2 = \operatorname{Var}[T'_B] + \sigma_J^2$. This case is a postselected frame in which Alice's source emitted one photon-pair and neither party had a dark count.

2. Independent Gaussian probability distributions with variances σ_A^2 and σ_B^2. This case is a postselected frame in which one of two situations occurred: (a) Alice's source emitted multiple photon-pairs, and Alice and Bob registered at least one coincidence; or (b) Alice's source emitted one photon-pair, and Alice and Bob registered a single coincidence with at least one of them also having a dark count. (There could be some correlations between Alice and Bob's measurements, but—being conservative—we are neglecting this possibility.)

3. Alice's arrival time is a Gaussian random variable with variance σ_A^2, and Bob's arrival time is uniformly distributed over the measurement frame.

This case is a postselected frame in which Alice detected at least one photon and Bob had a dark count without detecting photons.

4. Bob's arrival time is a Gaussian random variable with variance σ_B^2, and Alice's arrival time is uniformly distributed over the measurement frame. This case is a postselected frame in which Bob detected at least one photon and Alice had a dark count without detecting photons.

5. Both Alice and Bob's arrival times are uniformly distributed over the measurement frame. This is a postselected frame in which both Alice and Bob measured dark counts without detecting photons.

The probability density functions for each of the above cases are

$$p_{T_A,T_B|1}(t_A,t_B|\,1) = p_{BG}(t_A,t_B;\Lambda), \tag{B2a}$$
$$p_{T_A,T_B|2}(t_A,t_B|\,2) = p_G(t_A;\sigma_A^2)p_G(t_B;\sigma_B^2), \tag{B2b}$$
$$p_{T_A,T_B|3}(t_A,t_B|\,3) = p_G(t_A;\sigma_A^2)p_U(t_B;T_f), \tag{B2c}$$
$$p_{T_A,T_B|4}(t_A,t_B|\,4) = p_U(t_A;T_f)p_G(t_B;\sigma_B^2), \tag{B2d}$$
$$p_{T_A,T_B|5}(t_A,t_B|\,5) = p_U(t_A;T_f)p_U(t_B;T_f), \tag{B2e}$$

where $p_{BG}(t_A,t_B;\Lambda)$ is a bivariate Gaussian probability density function with zero means and covariance matrix Λ; $p_G(t;\sigma^2)$ is a Gaussian probability density function with zero mean and variance σ^2; and $p_U(t;T_f)$ is a uniform probability density function over the interval $[-T_f/2,T_f/2]$.

Moreover, the probabilities for each of the cases discussed above, given that a particular frame has been postselected, are

$$\pi_1 = \mu e^{-\mu}\eta_A\eta_B\eta_P(1-p_d)^2/P_\mu, \tag{B3a}$$
$$\pi_2 = \sum_{n=2}^{\infty}\frac{\mu^n e^{-\mu}}{n!P_\mu}\left[1-(1-\eta_A)^n\right]\left[1-(1-\eta_B\eta_P)^n\right] + \frac{\mu e^{-\mu}}{P_\mu}\eta_A\eta_B\eta_P p_d(2-p_d), \tag{B3b}$$
$$\pi_3 = \sum_{n=1}^{\infty}\frac{\mu^n e^{-\mu}}{n!P_\mu}\left[1-(1-\eta_A)^n\right]\left[p_d(1-\eta_B\eta_P)^n\right], \tag{B3c}$$
$$\pi_4 = \sum_{n=1}^{\infty}\frac{\mu^n e^{-\mu}}{n!P_\mu}\left[p_d(1-\eta_A)^n\right]\left[1-(1-\eta_B\eta_P)^n\right], \tag{B3d}$$
$$\pi_5 = \sum_{n=0}^{\infty}\frac{\mu^n e^{-\mu}}{n!P_\mu}p_d^2(1-\eta_A)^n(1-\eta_B\eta_P)^n, \tag{B3e}$$

where η_A, η_B, η_P and p_d have been defined in Sec. III A.

The conditional probability density functions defined above, as well as their occurence probabilities, allow us to define the arrival-time joint probability density function:

$$p_{T_A,T_B}(t_A,t_B) = \sum_{i=1}^{5}\pi_i\, p_{T_A,T_B|i}(t_A,t_B|\,i). \tag{B4}$$

Using this joint probability density function, we can calculate Alice and Bob's mutual information via

$$I(A;B)_\mu = \int \mathrm{d}t_A\mathrm{d}t_B\; p_{T_A,T_B}(t_A,t_B) \times \log_2\left(\frac{p_{T_A,T_B}(t_A,t_B)}{p_{T_A}(t_A)p_{T_B}(t_B)}\right), \tag{B5}$$

where $p_{T_A}(t_A) = \int \mathrm{d}t_B\; p_{T_A,T_B}(t_A,t_B)$ and $p_{T_B}(t_B) = \int \mathrm{d}t_A\, p_{T_A,T_B}(t_A,t_B)$ are the marginal probability density functions.

It is important to note that when the detector timing jitter σ_J exceeds the correlation time σ_{cor}, Alice and Bob's mutual information $I(A;B)$ cannot approach its limit of $\log_2 d$. In this case, WDM [55] that makes σ_{cor} in each WDM channel comparable to σ_J should be applied, and secure-key must be obtained from both arrival-time and frequency measurements.

[1] L. Zhang, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **100**, 110504 (2008).
[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984) pp. 175–179.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[5] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[6] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).
[7] L. Sheridan and V. Scarani, Phys. Rev. A **83**, 039901(E) (2011).
[8] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[9] R. T. Thew, A. Acin, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **93**, 010503 (2004).
[10] B. Qi, Opt. Lett. **31**, 2795 (2006).
[11] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. **98**, 060503 (2007).
[12] J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith, Opt. Express **21**, 15959 (2013).
[13] S. Etcheverry, G. Canas, E. S. Gomez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, Sci. Rep. **3** (2013).
[14] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature **412**, 313 (2001).
[15] A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **89**, 240401 (2002).
[16] G. Molina-Terriza, A. Vaziri, J. Rehacek, Z. Hradil, and A. Zeilinger, Phys. Rev. Lett. **92**, 167903 (2004).

[17] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, Phys. Rev. A **88**, 032305 (2013).

[18] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, Phys. Rev. A **87**, 062322 (2013).

[19] Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. Lett. **112**, 120506 (2014).

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

[21] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[22] M. Navascués, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).

[23] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[24] J. D. Franson, Phys. Rev. A **45**, 3126 (1992).

[25] J. D. Franson, Phys. Rev. Lett. **62**, 2205 (1989).

[26] I. A. Khan and J. C. Howell, Phys. Rev. A **73**, 031801 (2006).

[27] R. H. Brown and R. Q. Twiss, Nature **177**, 27 (1956).

[28] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[29] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[30] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[31] N. Lütkenhaus and M. Jahma, New Journal of Physics **4**, 44 (2002).

[32] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[33] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[34] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[35] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[36] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014).

[37] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007).

[38] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).

[39] X. Ma and H.-K. Lo, New Journal of Physics **10**, 073018 (2008).

[40] M. Curty, X. Ma, B. Qi, and T. Moroder, Phys. Rev. A **81**, 022310 (2010).

[41] M. Curty, X. Ma, H.-K. Lo, and N. Lütkenhaus, Phys. Rev. A **82**, 052325 (2010).

[42] B. Xu, X. Peng, and H. Guo, Phys. Rev. A **82**, 042301 (2010).

[43] Y. Zhang, W. Chen, S. Wang, Z.-Q. Yin, F.-X. Xu, X.-W. Wu, C.-H. Dong, H.-W. Li, G.-C. Guo, and Z.-F. Han, Opt. Lett. **35**, 3393 (2010).

[44] S. Krapick, M. S. Stefszky, M. Jachura, B. Brecht, M. Avenhaus, and C. Silberhorn, Phys. Rev. A **89**, 012329 (2014).

[45] Q.-C. Sun, W.-L. Wang, Y. Liu, F. Zhou, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Chen, X. Ma, Q. Zhang, and J.-W. Pan, Laser Physics Letters **11**, 085202 (2014).

[46] C. Lee, J. Mower, Z. Zhang, J. H. Shapiro, and D. Englund, arXiv:1311.1233 [quant-ph].

[47] C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R. D. Horansky, V. B. Verma, A. E. Lita, R. P. Mirin, F. Marsili, M. D. Shaw, S. W. Nam, G. W. Wornell, F. N. C. Wong, J. H. Shapiro, and D. Englund, Phys. Rev. A **90**, 062331 (2014).

[48] T. Zhong, F. N. Wong, T. D. Roberts, and P. Battle, Opt. Express **17**, 12019 (2009).

[49] C. K. Law and J. H. Eberly, Phys. Rev. Lett. **92**, 127903 (2004).

[50] I. Devetak and A. Winter, Proc. Royal. Soc. A **461**, 207 (2005).

[51] X.-s. Ma, S. Zotter, J. Kofler, T. Jennewein, and A. Zeilinger, Phys. Rev. A **83**, 043814 (2011).

[52] H. D. Riedmatten, V. Scarani, I. Marcikic, A. Acín, W. Tittel, H. Zbinden, and N. Gisin, Journal of Modern Optics **51**, 1637 (2004).

[53] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Nat Photon **7**, 210 (2013).

[54] 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).

[55] J. Mower, F. N. C. Wong, J. H. Shapiro, and D. Englund, arXiv:1110.4867 [quant-ph].