High-dimensional quantum key distribution using dispersive optics

Jacob Mower, Zheshen Zhang, Pierre Desjardins, Catherine Lee, Jeffrey H. Shapiro, and Dirk Englund

Phys. Rev. A **87**, 062322 — Published 20 June 2013

DOI: 10.1103/PhysRevA.87.062322

High-dimensional quantum key distribution using dispersive optics

Jacob Mower,[1,2] Zheshen Zhang,[1] Pierre Desjardins,[3]
Catherine Lee,[1,4] Jeffrey H. Shapiro,[1] and Dirk Englund[1,2,3]

[1]*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139 USA*
[2]*Department of Electrical Engineering, Columbia University, New York, NY 10027 USA*
[3]*Department of Applied Physics and Applied Mathematics, Columbia University, New York, NY 10027 USA*
[4]*Department of Physics, Columbia University, New York, NY 10027 USA*

We propose a high-dimensional quantum key distribution protocol that employs temporal correlations of entangled photons. The security of the protocol relies on measurements by Alice and Bob in one of two conjugate bases, implemented using dispersive optics. We show that this dispersion-based approach is secure against collective attacks. The protocol is additionally compatible with standard fiber telecommunications channels and wavelength division multiplexers. We describe several physical implementations to enhance the transmission rate and describe a heralded qudit source that is easy to implement and enables secret-key generation at > 4 bits per character of distilled key across over 200 km of fiber.

I. INTRODUCTION

Quantum key distribution (QKD) [1, 2] enables two parties, Alice and Bob, to establish a private, shared cryptographic key. However, hardware constraints such as the optical state generation and photon-counting rates limit the rate of generating the key. By measuring photons in a high-dimensional Hilbert space, Alice and Bob may increase the shared information generated for each detected photon (or photon pair, in the case of entangled-photon QKD), thereby enabling greater key generation rates compared to measurements in low-dimensional Hilbert spaces. Furthermore, using high-dimensional correlations may provide greater robustness to noise [3]. Numerous degrees of freedom of photons have been investigated, including position-momentum [4], time [5–8], energy-time [9, 10], and orbital angular momentum (OAM) [11, 12], but to our knowledge, no security proofs for these protocols have been published against collective or coherent attacks.

Here, we introduce a high-dimensional QKD protocol that employs timing information of photons — analogous to pulse position modulation (PPM) — to maximize the secret-key capacity under technical constraints. We focus the discussion on a scheme employing entangled photon pairs generated by Alice at random times by spontaneous parametric down-conversion (SPDC) and sent to Bob over a quantum channel, and we discuss variations of the scheme that employ single-photon sources or weak classical light. For the entangled-photon protocol, we show security against collective attacks through measurements by Alice and Bob in two conjugate bases, which are implemented using single-photon detectors and simple dispersive optical elements. This protocol, which we term dispersive optics QKD (DO-QKD), benefits from the robustness of temporal correlations in single-mode fiber and free space. We estimate that practical implementations could reach a secret-key capacity of > 4 bits per character of distilled key (bpc) with transmission across over 200 km in fiber.

II. THE PROTOCOL

The principal steps for the protocol are state preparation and transmission, state detection, and classical information post-processing. We present a schematic for these steps in Fig. 1(a).

1.) State preparation and transmission: Alice generates a biphoton state via spontaneous parametric down-conversion (SPDC). For

a weak, continuous-wave pump at frequency ω_p and operation at frequency degeneracy, the down-converted state (cf. Ref. [7]) can be approximated by

$$|\Psi_{AB}\rangle = \iint \psi(t_A, t_B) e^{i\frac{\omega_p}{2}(t_A+t_B)} |t_A t_B\rangle \, dt_A dt_B, \quad (1)$$

where

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

$|t_A, t_B\rangle = \hat{a}_A^\dagger(t_A)\hat{a}_B^\dagger(t_B)|0\rangle$, and $\hat{a}_{A,B}^\dagger(t_j)$ denote the creation operators at time t_j for Alice and Bob, respectively. The superposition of temporal states in Eq. 1 occurs over the coherence time of the pump field, $\sigma_{\rm coh}$. The correlation time between photons, $\sigma_{\rm cor}$, is determined by the phase matching bandwidth of the SPDC source. $\sigma_{\rm coh}$ can be longer than a μs for a diode laser, and $\sigma_{\rm cor}$ is on the order of hundreds of fs to several ps for typical SPDC sources [13]. The resulting number of information eigenstates or alphabet 'characters' [14] given by the Schmidt number, approximately $d \equiv \sigma_{\rm coh}/\sigma_{\rm cor}$, can therefore be quite large [5].

In this investigation, we assume that Alice transmits the state to Bob over a standard telecom-band optical fiber, and $\omega_p/2 = 2\pi c/(1560\text{ nm})$.

2.) State detection: Similar to the parties in the BB84 protocol, Alice and Bob choose randomly to measure their photons' arrival times in one of two bases: the basis of direct arrival-time measurements or a conjugate basis. These conjugate basis measurements can be achieved using a transformation $\hat{U}$ that transforms an eigenstate of the 'direct measurement basis' into a superposition of all such eigenstates. We find that such a transformation can be implemented easily using group velocity dispersion (GVD), or 'second-order dispersion.' An element with GVD imparts on each frequency state a phase $\phi \propto \beta_2\omega^2$. $\beta_2 = \partial^2/\partial\omega^2|_{\omega_0}(n_{\rm eff}\omega/c)$, where $n_{\rm eff}$ is the effective index of the mode, ω is the detuning from the mode's center frequency ω_0, and c is the speed of light in vacuum [15]. Physically, β_2 is proportional to the linear change in the group velocity as a function of frequency. The

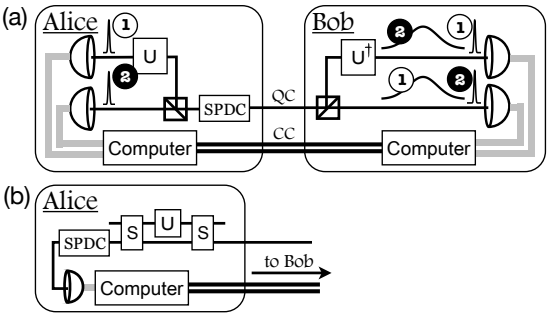

FIG. 1: (a) Alice and Bob measure in either the time or dispersed-time basis. In case (1), Alice measures in the dispersed-time basis and projects Bob's photon onto a dispersed state. In case (2), she projects Bob's photon onto an undispersed state. Only measurements in the same basis are correlated. QC represents quantum communication and CC represents classical communication. (b) An equivalent prepare-and-measure scheme in which Alice uses the arrival time of one photon as a sync time sent to Bob. She selects with a switch (S) whether or not to apply dispersion on her other photon and modulates the center time of the distribution that she sends to Bob using a Gaussian-distributed random number generator.

SOD operator, $\hat{U}$, is unitary and its frequency domain representation is diagonal.

Classically, a transform-limited pulse spreads out in time in a dispersive medium because its frequency components move out of phase. However, Ref. [16] showed that if the entangled photons pass through dispersive media, in the limit of large coherence time $\sigma_{\rm coh}$, the correlation time $\sigma_{\rm cor}$ becomes

$$\sigma_{\rm cor}'^2 \approx \frac{1}{\sigma_{\rm cor}^2}\left[\sigma_{\rm cor}^4 + (\beta_{2A}L_A + \beta_{2B}L_B)^2\right], \quad (2)$$

where β_{2A} (β_{2B}) is the GVD introduced by Alice (Bob) over length L_A (L_B). Now, suppose that $L_A = L_B = L$ and $\beta_{\rm tot} = \beta_{2A} + \beta_{2B}$. As $\beta_{\rm tot}$ increases, the temporal correlation between Alice's and Bob's photons decreases. However, $\sigma'_{\rm cor} = \sigma_{\rm cor}$ if $\beta_{2A} = -\beta_{2B} = \beta_2$, which requires that, to within a global phase, $\hat{U}_A = \int e^{-i\frac{1}{2}\beta_2 L\omega^2} |\omega\rangle_A \langle\omega| \, d\omega$ and $\hat{U}_B^\dagger = \int e^{-i\frac{1}{2}\beta_2 L\omega^2} |\omega\rangle_B \langle\omega| \, d\omega$, where ω is the

frequency detuning from the center frequency of the biphoton pulse, and $|\omega\rangle_X$ denotes a single photon at frequency $\omega_p/2+\omega$ in the setup of party X. If Alice applies normal dispersion, $\hat{U}_A$, on her photon, Bob can apply anomalous dispersion of equal magnitude on his photon to recover the temporal correlation between their photons. Thus, Alice's and Bob's measurements in the dispersed basis are also correlated, as required. In order for the measurement bases to be conjugate, $\beta_2 L \gg \sigma_{\text{coh}}\sigma_{\text{cor}}$. To generate this normal and anomalous dispersion, a variety of technologies can be used, including commercial fiber Bragg gratings, silicon photonic crystal waveguides [17], or optical cavities [18].

3.) Classical information post-processing: Alice and Bob build their distilled key from correlated timing events acquired in the same basis [7]. They therefore communicate their basis measurements and keep only the results where they registered clicks in the same basis. They additionally only consider frames during which both obtained one detection event. Using the security procedure detailed below, they determine their information advantage over Eve. If this is greater than zero, they then apply error correction and privacy amplification [19] on their data set to establish some amount of secret key.

III. SECURITY

To verify the security of the DO-QKD protocol against collective attacks, we calculate the secret-key capacity [20, 21] in terms of bpc, as

$$\Delta I = \beta I(A;B) - \chi(A;E), \tag{3}$$

where β is the reconciliation efficiency, $I(A;B)$ is the mutual information between Alice and Bob, and $\chi(A;E)$ is Eve's Holevo information about Alice's transmission [22]. Since the low-flux limit of the SPDC output (given in Eq. 1) is Gaussian and Gaussian attacks are optimal collective attacks for a measured covariance matrix [21, 23], we can calculate the secret-key capacity using a covariance matrix approach to establish an upper bound on Eve's information given collective attacks [24–26].

A. The noiseless covariance matrix, Γ

The covariance matrix Γ can be formulated using the measurement operators $\hat{T}_A$ ($\hat{T}_B$) and $\hat{D}_A$ ($\hat{D}_B$) corresponding to measurements by Alice (Bob) in the arrival time and dispersed arrival time bases, respectively. We first define these operators using several simplifying assumptions [27]:

- Alice and Bob's photons in $|\Psi_{AB}\rangle$ have a negligible zero-momentum component.
- Each photon in this state propagates in a single direction directly preceding detection.
- The timing resolution of Alice's and Bob's detectors is insufficient to observe the effect of photon energy delocalization from the photon position distribution [28].

We can then approximate the arrival time operators as

$$\hat{T}_j = \int t_j \, |t_j\rangle \langle t_j| \, dt_j, \tag{4}$$

where $j \in \{A, B\}$. The dispersed arrival-time measurement operator $\hat{D}_j$ is related to $\hat{T}_j$ by a similarity transformation according to the dispersion operator $\hat{U}$ and a normalization giving units of frequency:

$$\begin{aligned} \hat{D}_j &= \frac{1}{\beta_{2j} L} \hat{U}_j^\dagger \hat{T}_j \hat{U}_j \qquad (5) \\ \hat{U} &= \frac{1}{\sqrt{\pi |k|}} \int\int e^{-i(t_1-t_2)^2/k} \, |t_1\rangle \langle t_2| \, dt_2 dt_1, \end{aligned}$$

where $k = 2\beta_2 L$. Note that $[\hat{T}_j, \hat{D}_j] = i$. Γ is a four-by-four matrix composed of four two-by-two submatrices denoted by

$$\Gamma = \begin{pmatrix} \gamma_{AA} & \gamma_{AB} \\ \gamma_{BA} & \gamma_{BB} \end{pmatrix}, \tag{6}$$

where, for example, the submatrix γ_{AB} describes the covariance between the measurements of Alice and Bob and is given by [26]

$$\gamma_{AB} = \frac{1}{2}\begin{pmatrix} \langle\{\hat{T_A}, \hat{T_B}\}\rangle & \langle\{\hat{T_A}, \hat{D_B}\}\rangle \\ \langle\{\hat{D_A}, \hat{T_B}\}\rangle & \langle\{\hat{D_A}, \hat{D_B}\}\rangle \end{pmatrix}, \quad (7)$$

assuming the detection times in the arrival time and dispersed arrival time bases are centered around time zero. The noiseless covariance matrix — i.e., the covariance matrix calculated in the absence of Eve's intrusion, channel effects and Alice's and Bob's setup imperfections — is therefore given by

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

where $u = 16\sigma_{\text{coh}}^2$ and $v = 4\sigma_{\text{cor}}^2$. In the limit of large dispersion where $k \to \infty$,

$$\Gamma \approx \begin{bmatrix} \frac{u+v}{16} & 0 & \frac{u-v}{16} & 0 \\ 0 & \frac{u+v}{uv} & 0 & -\frac{u-v}{uv} \\ \frac{u-v}{16} & 0 & \frac{u+v}{16} & 0 \\ 0 & -\frac{u-v}{uv} & 0 & \frac{(u+v)}{uv} \end{bmatrix} \quad (8)$$

which is equivalent to the covariance matrix calculated from arrival time and spectral measurement operators.

In the absence of noise, Alice and Bob perform photon arrival-time measurements with outcomes described by Gaussian-distributed random variables T_A and T_B, respectively. The dispersed arrival-time elements, as they appear in the covariance matrix, have been multiplied by $1/\beta_2^2L^2$ due to the normalization in Eq. 5. Before adding any timing noise due to Eve or the transmission channel, we first multiply these elements by $\beta_2^2L^2$ to convert the normalized variances with units of frequency back to temporal variances. Therefore, from this point on, we will assume that the Gaussian-distributed random variables D_A and D_B are given in units of time.

B. Covariance matrix Γ' used to calculate $\chi(A;E)$

We consider the effect of an eavesdropper and channel noise, which result in excess noise ϵ and a decrease in correlations η. Alice and Bob know how much noise is added to their measurements by dark counts and jitter and assume that Eve cannot control these sources of noise. Suppose that the temporal measurements by Alice and Bob, in the presence of Eve yield values T'_A, T'_B, D'_A, and D'_B. The variances of these primed values are related to the unprimed values (no Eve) according to

$$\text{COV}[T'_A, T'_B] = (1-\eta)\text{COV}[T_A, T_B] \quad (9)$$

$$\text{Var}[T'_A] = \text{Var}[T_A] \quad (10)$$

$$\text{Var}[T'_B] = (1+\epsilon)\,\text{Var}[T_B]. \quad (11)$$

The primed dispersed arrival time variables are related to the unprimed variables in an analogous way. Excess noise appears only in in Bob's measurements because Alice's photons do not leave her setup (cf. Fig. 1(a)).

C. Covariance matrix Γ'' used to calculate $I(A;B)$

While imperfections in Alice's and Bob's setups do not contribute to $\chi(A;E)$, they do lower $I(A;B)$. If we also include detector timing jitter and dark counts, Alice's and Bob's arrival-time measurements are described by

$$T''_A = \begin{cases} T'_A + N_A^J, & \text{with probability } R_{\nu A} \\ N_A^{dT}, & \text{with probability } R_{dA} \end{cases} \quad (12)$$

$$T''_B = \begin{cases} T'_B + N_B^J, & \text{with probability } R_{\nu B} \\ N_B^{dT}, & \text{with probability } R_{dB} \end{cases} \quad (13)$$

where $N_{A/B}^J$ is the noise due to detector jitter, $N_{A/B}^{dT}$ is the noise due to dark counts when measuring the temporal variance, and $R_{\nu A/B}$

($R_{dA/B}$) is the probability of registering a photon (dark count) given a single click on Alice's/Bob's detector.

We calculate R_ν and R_d as follows, ignoring for now the possibility of generating more than one photon pair per frame. The probability that Alice/Bob detects a photon and not a dark count $p_{A/B}$ is the probability that Alice's source generates a photon pair, a photon from the pair arrives at Alice's/Bob's detector, is detected, and a dark count is not registered. Therefore

$$p_{A/B} = p_\nu(1 - L_{A/B})(1 - p_d). \quad (14)$$

where L_A (L_B) is the loss in Alice's (Bob's) detection system (including the channel for Bob), p_d is the probability that Alice or Bob's detector registers a dark count in a frame, and p_ν is the probability of generating a pair in a given frame. The probability of either party registering a dark count given one detection event in a frame is

$$d_{A/B} = \left[p_\nu L_{A/B} + (1 - p_\nu)\right] p_d. \quad (15)$$

From these results, we have

$$R_{\nu A/B} = \frac{p_{A/B}}{p_{A/B} + d_{A/B}} \quad (16)$$

$$R_{dA/B} = \frac{d_{A/B}}{p_{A/B} + d_{A/B}}. \quad (17)$$

From Eq. 9-13, it follows that

$$\begin{aligned} \mathrm{COV}[T''_A, T''_B] &= \mathrm{COV}[R_{\nu A}T'_A, R_{\nu B}T'_B] \quad (18)\\ &= R_{\nu A}R_{\nu B}(1-\eta)\mathrm{COV}[T_A, T_B] \\ \mathrm{Var}[T''_A] &= R_{\nu A}(\mathrm{Var}[T_A] + \mathrm{Var}[N_A^J]) \\ &\quad + R_{dA}\mathrm{Var}[N_A^{dT}] \quad (19)\\ \mathrm{Var}[T''_B] &= R_{\nu B}(\mathrm{Var}[T_B] + \mathrm{Var}[N_B^J]) \\ &\quad + R_{dB}\mathrm{Var}[N_B^{dT}]. \quad (20) \end{aligned}$$

Alice's and Bob's dispersed arrival-time variables obey corresponding relations. The variance of $N^J_{A/B}$ is σ_J^2. Since dark counts are uniformly distributed, if Alice and Bob measure the variance in the arrival-time and dispersed arrival-time bases to three standard deviations of $T'_{A/B}$ and $D'_{A/B}$, the variances of $N^{dT}_{A/B}$ and $N^{dD}_{A/B}$ are

$$\mathrm{Var}[N^{dD}_{A/B}] = \frac{1}{E}\int_{-E/2}^{E/2} x^2 dx = \frac{1}{12}E^2, \quad (21)$$

$$\mathrm{Var}[N^{dT}_{A/B}] = \frac{1}{F}\int_{-F/2}^{F/2} x^2 dx = \frac{1}{12}F^2, \quad (22)$$

where $E \equiv 6\sqrt{\mathrm{Var}[D'_A]}$ and $F \equiv 6\sqrt{\mathrm{Var}[T'_A]}$. These covariances can then be used to calculate the secret key capacity, as detailed in Appendix A.

D. Noise parameters

While it is convenient to use ϵ and η to describe Eve's effect on the covariance matrix, it is easier experimentally to measure a different set of parameters. In particular, we consider ξ and θ defined as

$$\mathrm{Var}[T'_A - T'_B] = (1 + \xi)\mathrm{Var}[T_A - T_B], \quad (23)$$

and

$$\mathrm{Var}[T'_A + T'_B] = (1 - \theta)\mathrm{Var}[T_A + T_B]. \quad (24)$$

Both $\{\xi, \theta\}$ and $\{\epsilon, \eta\}$ can be used equivalently to bound Eve's information. These sets are related by

$$\epsilon = \frac{-2\eta(d^2 - \frac{1}{4}) + \xi}{d^2 + \frac{1}{4}}. \quad (25)$$

Therefore, if Alice and Bob measure only ξ and consider all physical ϵ and η according to Eq. 25, they can find a minimum secret-key capacity ΔI. This procedure is practical if, for a given ξ, ΔI has only a weak dependence on η and ϵ. To illustrate why this is useful, consider $\epsilon = \eta = 6.3 \cdot 10^{-5}$, $d = 64$, $\xi = 0.78$, and $\sigma_{\mathrm{cor}} = 30$ ps. ξ corresponds to a change in the correlation time, $\sigma_\Delta = \sigma_{\mathrm{cor}}(\sqrt{1+\xi} - 1) = 10$ ps. ϵ corresponds to an increase in the variance

of Bob's measurements by < 0.1 ps, which is more difficult to detect.

The range of physical values for ϵ and η are given by a number of constraints: (i) Eve cannot increase the mutual information of Alice and Bob by interacting with only Bob's photons due to the data processing inequality; (ii) The symplectic eigenvalues of the covariance matrix (see Appendix A) are greater than $\frac{1}{2}$; (iii) Eve can only degrade Alice and Bob's measured time correlation, i.e., $\mathrm{Var}[T'_A - T'_B] \geq \mathrm{Var}[T_A - T_B]$. Under these constraints, we can then calculate an upper bound on Eve's information.

To relate noise measures for different d, we use σ_Δ in the following calculations.

IV. KEY RATES

While we have considered photons generated by SPDC, it may not be possible to experimentally determine the covariance matrix elements for such a state. In Eq. 1, we assume that the biphoton amplitude is centered at times $\langle t_A \rangle = \langle t_B \rangle = 0$. However, since the pairs are generated at random times under continuous-wave excitation, Alice and Bob do not know the center time of the biphoton envelope. Therefore, Alice and Bob could use a prepare-and-measure scheme, shown in Fig. 1(b), in which Alice directly measures the arrival time of her photon, sends this time to Bob as a synchronization pulse, and then modulates the center time of the distribution that she sends to Bob using a Gaussian-distributed random number generator.

In addition to enabling measurement of the covariance matrix, this technique allows Alice to increase the photon generation rate. Assuming Alice has high system detection efficiency, she can determine if multiple pairs are emitted in each frame and remove them with an amplitude modulator. This heralding and post-selection scheme *allows Alice to send nearly one photon per frame with a low probability of sending multiple photons.* We find that the multi-pair probability can then be bounded below 0.01, even when the expected pair generation rate per frame, $\mu_f \approx 1$ (see derivation in Appendix B). This ability for efficient post-selection points to an important advantage of using high-dimensional encoding: for high d, the purity of the single photon source after post-selection increases for a given pump power. We will use this post-selection scheme now to analyze the DO-QKD protocol when it uses on the order of one photon per frame.

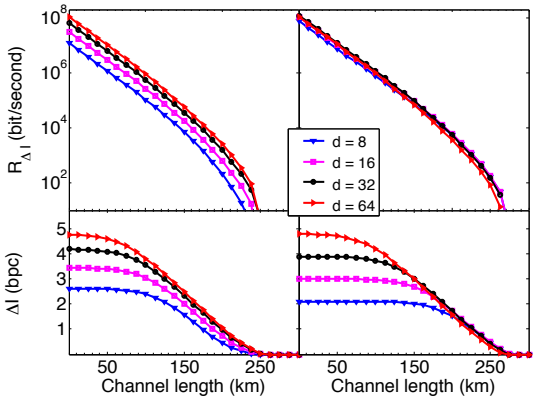

FIG. 2: (left) Secret-key capacity as a function of channel length, assuming equal photon pair generation rate $\gamma_\nu = p_\nu/6\sigma_{\mathrm{coh}}$ and $\sigma_{\mathrm{coh}} = 64 \cdot 30$ ps for all d; propagation loss $\alpha = 0.2$ dB/km; detector timing jitter $\sigma_J = 20$ ps; Alice and Bob system detection efficiencies 93%; $\sigma_\Delta = 10$ ps; dark count rate, $r_D = 1000$ s^{-1}; $\beta = 0.9$; expected number of pairs per frame assuming heralding, $p_\nu = \{0.607, 0.411, 0.231, 0.119\}$ for $d = \{64, 32, 16, 8\}$, respectively (see Appendix B). (right) The secret-key capacity given the same parameters, but with $\gamma_\nu = p_\nu/(6d \cdot \sigma_{\mathrm{cor}})$ and $\sigma_{\mathrm{cor}} = 30$ ps for all d. Upper plots show bps. Lower plots show bpc, i.e., bits per frame in which Alice and Bob measure in the same basis and register only one detection event.

The secret-key rate, $R_{\Delta I}$, with units of secure bits per second (bps) is given by $R_{\Delta I} = \Delta I \cdot P_C \cdot \gamma_\nu$, where $\gamma_\nu = p_\nu/6\sigma_{\mathrm{coh}}$, P_C is the probability that both Alice and Bob register one click in a given frame, and ΔI is the secret-key capacity from Eq. 3. The factor of 6 serves to separate the center time of photons in neighboring frames by more than 6 standard deviations.

Even for collective attacks, Alice and Bob can share a large amount of information per sec-

ond using the DO-QKD protocol. Pair generation rates in excess of 10^9 s^{-1} are possible using moderate pump powers [13], enabling secure communication rates > 100 Mb/s. In Fig. 2, we plot ΔI and $R_{\Delta I}$ as a function of fiber channel length. With $\sigma_\Delta = 10$ ps, over ~ 200 km transmission length can be achieved.

Fig. 3 plots the dependence of ΔI on σ_Δ for different d, assuming the parameters given in the Fig. 2 caption. Even if Alice and Bob measure σ_Δ to be on the order of tens of picoseconds for $\sigma_{\rm cor} = 30$ ps, they can extract a positive ΔI. Since we assume detector timing jitter of 20 ps, σ_Δ of this order is not difficult to measure.

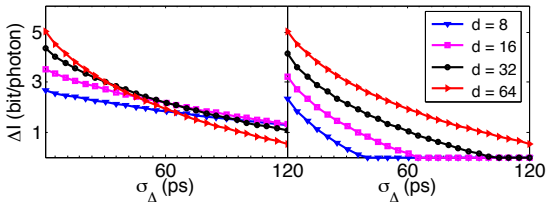

FIG. 3: ΔI as a function of offset parameter σ_Δ assuming the parameters given in the caption of Fig. 2. (left) Photon pair generation rate $\gamma_\nu = p_\nu/6\sigma_{\rm coh}$ and $\sigma_{\rm coh} = 64 \cdot 30$ ps for all d. (right) $\gamma_\nu = p_\nu/(6d \cdot \sigma_{\rm cor})$ and $\sigma_{\rm cor} = 30$ ps for all d.

V. DISCUSSION

We have so far considered a passive selection of basis measurements by Bob, using a beamsplitter followed by two single-photon detectors, as shown in Fig. 1(a). This number of detectors could be reduced to only one if the beam splitter were replaced by an active switch, as shown in Fig. 1(b) Additional detectors would be required to register instances in which multiple photons arrived at the detector within its reset time. In particular, detecting instances in which m photon pairs are generated requires at least m detectors. But this probability, which is given by the g-fold degenerate Bose-Einstein distribution (see Appendix B), rapidly diminishes with m. Thus, even for $\mu \sim 1$, only a few extra detectors would be required. The DO-QKD protocol can therefore be very resource efficient, whereas other protocols that employ high-dimensional states in frequency [9, 10] or OAM modes [11, 12] require a number of detectors that grows linearly with the dimensionality d.

It is interesting to consider why the DO-QKD protocol can reach a much longer transmission length than continuous variable QKD (CV-QKD) protocols, which are so far limited to 80 km [29]. We believe that a primary reason for the shorter transmission length in CV-QKD is that ϵ and η increase with photon loss/channel length. By contrast, in DO-QKD, ϵ and η are constant with photon loss/channel length (we believe that this would be the case for any single photon QKD protocol employing continuous variables). Ultimately, the transmission length in DO-QKD is limited not by an increase in the Holevo information between Alice and Eve, but rather by a decrease in the mutual information between Alice and Bob; ΔI decreases to zero with increasing channel length as the probability of registering a dark count approaches the probability of Bob detecting a photon from Alice.

Transmission > 200 km is realistic because the DO-QKD protocol is ideally suited for fiber telecommunications networks and photonic integrated circuits (PIC), which are designed for high-bandwidth temporal encoding. In Ref. [30], a protocol was proposed using PICs for the efficient generation of single photons on-demand [31], and PICs can be used to implement dispersive elements, as noted in Sec. II.

To further reduce the complexity of Alice's setup, she could use an attenuated classical source instead of an entangled photon source. As in pulse position modulation (PPM), Alice would simply modulate the optical field to generate random code-words. Two switches could then be used for randomly transforming the PPM signals into one of the temporal bases before sending them onward to Bob (note that the loss introduced by these switches can be compensated by increasing the light intensity). Note that Alice no longer requires a photon detector in this implementation: she only needs

a modulated light source and dispersive optics. This attenuated-light implementation could be paired with a decoy state protocol [32] to protect against photon number splitting attacks.

For channel bandwidths of $\sim 1/\sigma_{\mathrm{cor}}$, DO-QKD can operate at the Heisenberg measurement limit, while for larger bandwidths, dense wavelength division multiplexing (DWDM) could allow operation on hundreds of independent wavelength channels.

VI. CONCLUSION

We have introduced a scheme to perform high-dimensional QKD to maximize the key generation rate given experimental limitations such as detector reset time or finite brightness of entangled photon sources. Because the protocol relies on temporal correlations, it is ideally suited for fiber communication systems. It is also resource efficient and can be implemented with as few as two detectors using entangled photon pairs. If Alice used PPM and dispersion, only Bob would require a single photon detector. The DO-QKD protocol allows the generation of > 4 bpc with communication rates exceeding 100 Mb/s and communication distances over 200 km. We show that this protocol is secure against collective attacks. Moreover, single photon heralding with high dimensionality d can be used to increase the communication rate. Future work will focus on increasing the rate at which Alice and Bob can perform the necessary post-processing for secure communication, as this remains a rate-limiting step for single-photon QKD protocols.

This work was supported by the DARPA Information in a Photon program, through grant W911NF-10-1-0416 from the Army Research Office, by the Sloan Research Fellowship, and the Columbia Optics and Quantum Electronics IGERT under NSF grant DGE-1069420.

Appendix A: Symplectic decomposition of the covariance matrix

The quantum state described in Eq. 1 is the post-selected, low-flux limit of the Gaussian state generated by spontaneous parametric down-conversion, and can be fully characterized by Γ'. Here, we consider the collective attack, in which Eve performs only individual interactions with the photons flowing to Bob, but makes a collective measurement on the joint state she derives from all such interactions.

The Holevo information under this attack can be found by [33]

$$\chi(A;E) = S(\rho_E) - \frac{1}{2}(H_T + H_\Omega) \tag{A1}$$

$$H_T = \int p(t_A = t) S(\rho_{E|t_A=t}) dt \tag{A2}$$

$$H_\Omega = \int p(\omega_A = \omega) S(\rho_{E|\omega_A=\omega}) d\omega \tag{A3}$$

where $S(\rho)$ is the von Neumann entropy of the quantum state ρ, $p(t_A = t)$ is the probability density for Alice to measure t_A in the arrival-time basis, and $p(\omega_A = \omega)$ is the probability density for Alice to measure ω_A in the dispersed arrival-time basis. Since Alice, Bob, and Eve's overall quantum state ρ_{ABE} is a pure state, $S(\rho_E) = S(\rho_{AB})$. After Alice's measurement, the quantum state shared by Bob and Eve is pure. Therefore, $S(\rho_{E|t_A=t}) = S(\rho_{B|t_A=t})$ and $S(\rho_{E|\omega_A=\omega}) = S(\rho_{B|\omega_A=\omega})$. Furthermore, given the fact that all states are Gaussian, Bob and Eve's conditional quantum state is independent of Alice's measurement result. Thus, we can drop the integrals in Eqs. A2 and A3 since the integrand is a constant. Then Eq. A1 becomes

$$\chi(A;E) = S(\rho_{AB}) - \frac{1}{2}\left[S(\rho_{B|t}) + S(\rho_{B|\omega})\right]. \tag{A4}$$

After Eve's interaction, Alice and Bob's covariance matrix becomes

$$\Gamma' = \begin{bmatrix} \gamma_{\mathrm{AA}} & (1-\eta)\gamma_{\mathrm{AB}} \\ (1-\eta)\gamma_{\mathrm{BA}} & (1+\varepsilon)\gamma_{\mathrm{BB}} \end{bmatrix}. \tag{A5}$$

γ_{AA} remains unchanged because Eve does not

have access to Alice's photon. We define

$$\begin{aligned} I_1 &= \det[\gamma_{AA}] + \det[(1+\epsilon)\gamma_{BB}] + 2\det[(1-\eta)\gamma_{AB}] \\ I_2 &= \det[\Gamma'] \\ d_\pm &= \frac{1}{\sqrt{2}}\sqrt{I_1 \pm \sqrt{I_1^2 - 4I_2}}. \end{aligned} \tag{A6}$$

$S(\rho_{AB})$ is evaluated by $S(\rho_{AB}) = f(d_+) + f(d_-)$, where

$$f(x) = (x+\frac{1}{2})\log_2(x+\frac{1}{2}) - (x-\frac{1}{2})\log_2(x-\frac{1}{2}). \tag{A7}$$

To calculate the conditional terms in Eq. A4, we first need to derive Bob's conditional covariance matrices $\gamma_{B|t}$ and $\gamma_{B|\omega}$, which are given by

$$\gamma_{B|t} = \gamma_{BB} - \gamma_{BA}\left(X_t\gamma_{AA}X_t\right)^{-1}\gamma_{AB} \tag{A8a}$$

$$\gamma_{B|\omega} = \gamma_{BB} - \gamma_{BA}\left(X_\omega\gamma_{AA}X_\omega\right)^{-1}\gamma_{AB}, \tag{A8b}$$

where $X_t = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $X_\omega = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, and the matrix inverse is carried out by the Moore-Penrose pseudoinverse. The entropy of the conditional states reads

$$S(\rho_{B|t}) = f(\sqrt{\det[\gamma_{B|t}]}) \tag{A9a}$$

$$S(\rho_{B|\omega}) = f(\sqrt{\det[\gamma_{B|\omega}]}). \tag{A9b}$$

We next calculate the mutual information between Alice and Bob. The classical mutual information $I(A;B)$ can be evaluated from Γ'' by

$$I(A;B) = \frac{1}{4}\left[\log_2\left(\frac{1}{1-\mu_T^2}\right) + \log_2\left(\frac{1}{1-\mu_D^2}\right)\right], \tag{A10}$$

where μ_T and μ_D are the correlation coefficients for Alice and Bob's arrival-time and dispersed arrival-time measurements, given by

$$\begin{aligned} \mu_T &= \frac{\mathrm{COV}[T_A'', T_B'']}{\sqrt{\mathrm{Var}[T_A'']\mathrm{Var}[T_B'']}} \\ \mu_D &= \frac{\mathrm{COV}[D_A'', D_B'']}{\sqrt{\mathrm{Var}[D_A'']\mathrm{Var}[D_B'']}} \end{aligned} \tag{A11}$$

for T_A'' and T_B'' defined in the text.

Appendix B: Optimizing the photon source and detectors

The security analysis in the text assumed that at most a single pair was generated by Alice in each frame. However, for an SPDC source, the probability of generating m pairs over some time interval is given by g-fold degenerate Bose-Einstein statistics as [34]

$$p(\mu, m, g) = \frac{(\mu/g)^m/(g-1)}{[1+(\mu/g)^{m+g}]B(m+1, g-1)} \tag{B1}$$

where μ is the expected number of pairs generated during that interval, g is the mode degeneracy and $B(x,y)$ is the Beta function. We take $g = d$ in our calculations. Thus to suppress the multi-pair emission probability, one must suppress μ, reducing the probability of generating any photons at all. One can avoid this by employing a heralding scheme [35], whereby the detection of Alice's photon heralds the existence of Bob's, and Alice blocks the channel such that no more than one signal photon leaves her setup per frame. Alice then randomizes the center time of the photon distribution sent to Bob according to a Gaussian distribution to generate the Gaussian measurement statistics assumed in our analysis.

The relevant period over which to consider multi-photon events is the time bin instead of the protocol time frame, which can allow Alice to increase the pair generation rate while suppressing multi-pair generation.

The experimental setup is depicted in Fig. 4. Alice prepares $|\Psi_{AB}\rangle$ and sends her photons directly to a single photon detector. Detection at this stage heralds the presence of Bob's photons. If she detects more than one photon per frame, she chooses one photon at random to pass to Bob and modulates the SPDC output channel with a modulator (Mod) to remove all other photons. We assume 93% detection efficiency [36] and 1 dB attenuation in the switch. The detection can occur at the required rate > 100 MHz assuming the use of detector arrays [37]. Since the dark count rate is roughly six orders of magnitude lower than the pair generation rate,

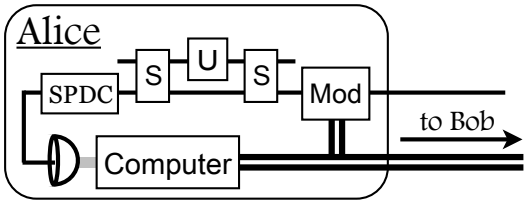

FIG. 4: A prepare-and-measure scheme in which Alice additionally modulates the output channel according to the heralding scheme outlined in the text using the element, Mod. Arrival time measurements from her idler photon are fed forward to Mod enabling Alice to suppress multiphoton emission during each frame.

we can safely neglect them in these calculations.

The protocol can only succeed if Alice registers a heralding event. She does so with probability $1 - p_{\text{fail}}$, where

$$p_{\text{fail}} = \sum_{k=0}^{\infty} p(\mu_f, k, d) \cdot D_0(k). \tag{B2}$$

Here,

$$D_0(k) = (1 - \eta_d)^k, \tag{B3}$$

where η_d is the single photon detector efficiency, is the probability that 0 out of k photons are detected.

From this, the probability of generating m photons on the output is

$$p_H(m) = (1 - p_{\text{fail}}) \sum_{k=m}^{\infty} p(\mu_b, k, d) D(k) + p_{\text{fail}} \delta_{m,0} \tag{B4}$$

where μ_b is the expected number of pairs generated in each time bin and $\delta_{x,y}$ is the Kronecker delta function.

In Eq. B4,

$$D(k) = \binom{k}{m} \eta_s^m (1 - \eta_s)^{k-m}, \tag{B5}$$

where η_s is the transmissivity of the modulator in the 'on' position, is the probability that m of the k generated photons make it through the switching element.

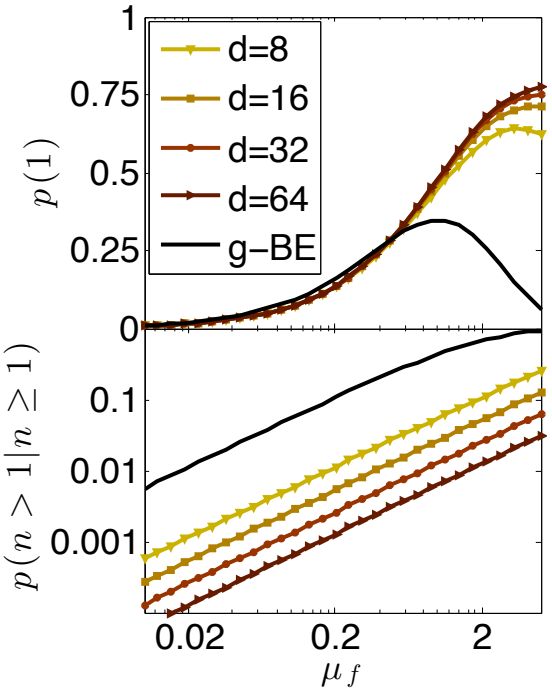

FIG. 5: (upper) The probability of Alice sending one photon per frame to Bob, $p(1)$, as a function of μ_f using the heralding circuit with the d shown and for unheralded g-fold degenerate Bose-Einstein statistics, "g-BE." (lower) The probability of Alice sending more than one photon per frame given that one or more photons were sent for the heralded and thermal statistics as above. We limit this probability to be less than 0.01, which places an upper bound on μ_f.

We plot the results of this analysis in Fig. 5. As d increases for a given μ_f, the average pair generation rate per time bin decreases resulting in a suppression of multiphoton emission during the frame. By limiting the probability of emitting multiple photons per frame given one or more photons were emitted, we determine the probability for generating one photon, $p(1) \approx p_\nu$. For $d = \{64, 32, 16, 8\}$, $p_\nu = \{0.607, 0.411, 0.231, 0.119\}$, respectively.

[1] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[4] L. Zhang, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **100**, 110504 (2008).

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

[6] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).

[7] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. **98**, 060503 (2007).

[8] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).

[9] B. Qi, Opt. Lett. **31**, 2795 (2006).

[10] J. Mower, F. Wong, J. Shapiro, and D. Englund, arxiv:1110.4867 [quant-ph].

[11] A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **89**, 240401 (2002).

[12] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature **412**, 313 (2001).

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

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

[15] R. M. Osgood, N. C. Panoiu, J. I. Dadap, X. Liu, X. Chen, I.-W. Hsieh, E. Dulkeith, W. M. Green, and Y. A. Vlasov, Adv. Opt. Photon. **1**, 162 (2009).

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

[17] S. Assefa and Y. A. Vlasov, Opt. Express **15**, 17562 (2007).

[18] C. Madsen, G. Lenz, A. Bruce, M. Cappuzzo, L. Gomez, and R. Scotti, Photonics Technology Letters, IEEE **11**, 1623 (1999).

[19] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[20] I. Devetak and A. Winter, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science **461**, 207 (2005).

[21] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[22] A. Holevo, Probl. Peredachi Inf. **9**, 3 (1973).

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

[24] A. S. Holevo, M. Sohma, and O. Hirota, Phys. Rev. A **59**, 1820 (1999).

[25] A. Serafini, F. Illuminati, and S. D. Siena, Journal of Physics B: Atomic, Molecular and Optical Physics **37**, L21 (2004).

[26] 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).

[27] V. Delgado and J. G. Muga, Phys. Rev. A **56**, 3425 (1997).

[28] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Section 12.11 (Cambridge University Press, 1995), 1st ed.

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

[30] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. A **66**, 042303 (2002).

[31] J. Mower and D. Englund, Phys. Rev. A **84**, 052326 (2011).

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

[33] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[34] L. Mandel, in *Proceedings of the Physical Society* (1959), vol. 74, pp. 233–24.

[35] L. Yang, X. Ma, X. Guo, L. Cui, and X. Li (2011).

[36] F. Marsili, B. Verma, A. Stern, S. Harrington, A. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. Shaw, R. Mirin, et al., Nature Photonics **7**, 210 (2013).

[37] E. Dauler, B. Robinson, A. Kerman, J. K. W. Yang, K. Rosfjord, V. Anant, B. Voronov, G. Gol'tsman, and K. Berggren, Applied Superconductivity, IEEE Transactions on **17**, 279 (2007).