PHYSICAL REVIEW A **90**, 062331 (2014)

Entanglement-based quantum communication secured by nonlocal dispersion cancellation

Catherine Lee,[1,2] Zheshen Zhang,[1] Gregory R. Steinbrecher,[1] Hongchao Zhou,[1] Jacob Mower,[1] Tian Zhong,[1] Ligong Wang,[1] Xiaolong Hu,[1] Robert D. Horansky,[3] Varun B. Verma,[3] Adriana E. Lita,[3] Richard P. Mirin,[3] Francesco Marsili,[4] Matthew D. Shaw,[4] Sae Woo Nam,[3] Gregory W. Wornell,[1] Franco N. C. Wong,[1] Jeffrey H. Shapiro,[1] and Dirk Englund[1]

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

[2]*Department of Physics, Columbia University, New York, New York 10027, USA*

[3]*National Institute of Standards and Technology, Boulder, Colorado 80305, USA*

[4]*NASA Jet Propulsion Laboratory, Pasadena, California 91109, USA*

(Received 29 April 2014; published 22 December 2014)

Quantum key distribution (QKD) enables participants to exchange secret information over long distances with unconditional security. However, the performance of today's QKD systems is subject to hardware limitations, such as those of available nonclassical-light sources and single-photon detectors. By encoding photons in high-dimensional states, the rate of generating secure information under these technical constraints can be maximized. Here, we demonstrate a complete time-energy entanglement-based QKD system with proven security against the broad class of arbitrary collective attacks. The security of the system is based on nonlocal dispersion cancellation between two time-energy entangled photons. This resource-efficient QKD system is implemented at telecommunications wavelength, is suitable for optical fiber and free-space links, and is compatible with wavelength-division multiplexing.

DOI: 10.1103/PhysRevA.90.062331 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Ex, 42.65.Lm

I. INTRODUCTION

Symmetric encryption schemes, such as the one-time pad [1], can provide perfect secrecy if the users, Alice and Bob, share some secret key. Quantum key distribution (QKD) is presently the only demonstrated and provably secure way to generate such keys between multiple parties at a distance [2]. However, the rate of key generation is limited by instrumental constraints, most importantly the rate of generating and detecting nonclassical states of light. To address this problem, there has been growing interest in developing large-alphabet QKD schemes [3] that exploit high-dimensional degrees of freedom of photons to generate multiple bits of information per detection event. Such large-alphabet QKD schemes can also increase resilience to noise and photon loss [4].

Among the various photonic degrees of freedom considered for high-dimensional QKD, including position-momentum [5,6], time-energy [7–16], and orbital angular momentum (OAM) [17–20], the time-energy basis is particularly appealing for implementations in today's telecommunications infrastructure. Bright time-energy-entangled photon pair sources [21] and fast, efficient detectors [22] have been developed for the telecom band. Additionally, the time-energy correlations are compatible with wavelength division multiplexing (WDM) systems and robust in transmission through both fiber and free space, allowing for versatile, heterogeneous quantum communication networks.

High-dimensional time-energy entanglement-based (TEE-based) QKD schemes have recently been experimentally demonstrated [23], but they have not provided security against the broad case of arbitrary collective attacks, in which an eavesdropper, Eve, can make an arbitrary joint quantum measurement on all of the signals she captured [24]. Recently, theoretical studies have introduced new techniques to bound Eve's information and thus provide provable security for TEE-based QKD schemes, combining elements of discrete and continuous-variable (CV) security proofs [13,14]. Here, we report an experimental demonstration of provably secure high-dimensional TEE-based QKD with security against arbitrary collective attacks. Our system relies on measurements in the mutually unbiased time-frequency bases, which are implemented by the quantum mechanical phenomenon of nonlocal dispersion cancellation [25]. Because of the reliance on dispersive optics for measurements in the frequency basis, we termed this protocol dispersive-optics QKD, or DO-QKD [13]. Here, we demonstrate a full system implementation of DO-QKD in the telecommunications band, including error correction, privacy amplification, and finite-key analysis.

II. EXPERIMENT

The DO-QKD scheme is illustrated in Fig. 1. Alice produces wavelength-degenerate time-energy-entangled photon pairs by type-II spontaneous parametric down-conversion (SPDC) in a periodically poled potassium titanyl phosphate (PPKTP) waveguide source pumped at 780.64 nm, producing a high rate (9×10^6 pairs/s per mW of pump) of orthogonally polarized photon pairs in the telecommunications band, at 1561.28 nm. A polarizing beam splitter separates Alice's photon for her local measurement and feeds the other into the quantum channel toward Bob. A passive 50:50 beam splitter routes Alice's photons for detection in the time basis (TB) or frequency basis (FB). The TB corresponds to direct detection of photon arrival time; the FB is implemented by direct detection after a normal group-velocity dispersive element. Bob performs similar conjugate-basis measurements, except for using *anomalous* group-velocity dispersion. The absolute group delays of the dispersive elements are matched such that the group-velocity dispersion (GVD) is nonlocally canceled when Alice and Bob both measure in the FB [13,25]. In this demonstration, Alice (Bob) employs a dispersion emulator (compensator) consisting of a chirped fiber Bragg grating with a group-velocity delay slope of $D = 600$ ps/0.4 nm ($D = -600$ ps/0.4 nm) of dispersion [26]. The dispersive

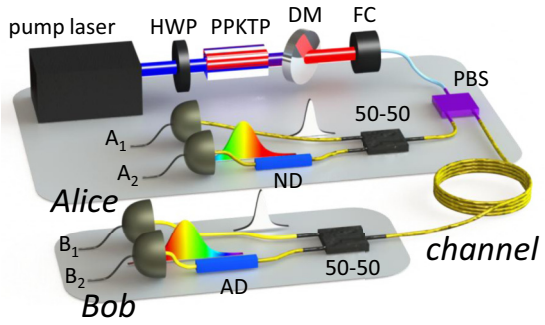

FIG. 1. (Color online) Schematic of the system. Alice pumps the PPKTP waveguide to produce wavelength-degenerate, orthogonally polarized entangled photon pairs. A half-wave plate (HWP) adjusts the pump polarization before the waveguide, and a dichroic mirror (DM) blocks the pump beam after the waveguide. The entangled photons are fiber coupled (FC) and separated by a polarizing beam splitter (PBS). Alice and Bob each use a 50:50 beam splitter to randomly switch between the time and frequency bases. ND: normal GVD; AD: anomalous GVD.

elements permit spectral measurements with a single detector, rather than an array of detectors commonly employed in spectroscopy. Alice and Bob time-tag photons using a total of four tungsten-silicide (WSi) superconducting nanowire single-photon detectors (SNSPDs) with system efficiencies in excess of 85%, full width at half maximum (FWHM) timing jitters $T_J \sim 80$–120 ps, and maximum count rates on the order of 10^6 counts per second (values vary based on the specific detector channel). The photon detection efficiency from source to detector was 3.3% and 0.77% for Alice and Bob, respectively, including all coupling losses.

Figure 2 plots photon coincidences recorded between Alice and Bob's four possible combinations of measurements in

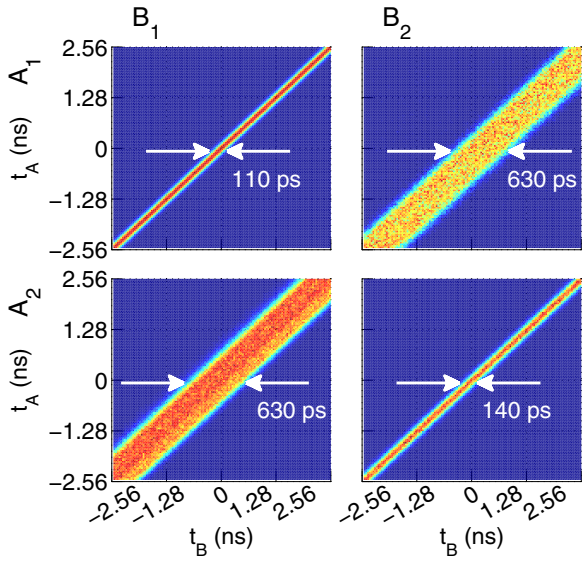

FIG. 2. (Color online) Photon coincidence measurements by Alice and Bob, using all possible combinations of detector pairs. The detection events are divided into 128 coincidence bins of $T_{\text{bin}} = 20$ ps each. This T_{bin} was chosen to enhance the resolution of the timing correlations.

the TB and FB. They sift their coincidence data into frames of duration $d \times T_{\text{bin}}$, comprised of d bins of duration T_{bin}. Retaining only the frames during which they both detected photons, Alice and Bob convert each detection event into a $\log_2 d$-bit symbol, based on the position of the event within the frame. The start time for each frame is determined by a shared clock. If Alice and Bob both record photons in the TB, they obtain narrow arrival-time correlations ~110 ps FWHM, corresponding to the timing jitter of Alice and Bob's detectors and time-tagging electronics. If Alice and Bob measure in different bases, the correlations are broadened to ~630 ps, as expected for the dispersive elements. If Alice and Bob both record photons in the FB, they recover narrow correlations of 140 ps, as expected for nonlocal dispersion cancellation in the limit of long pump laser coherence time. The dispersion stretches the ~1 ps photon envelope to ~640 ps. The stretched photon envelope exceeds the ~100 ps temporal resolution of the SNSPDs, enabling precise spectral correlation measurements. Although this GVD-based approach does not offer information about the absolute frequency of each individual photon, the measured two-photon spectral correlation, derived from the arrival-time correlations in the FB, yields a tight upper bound on the information accessible to Eve [13].

Alice and Bob use TB measurements for generating cryptographic keys and FB measurements for bounding Eve's maximum accessible information about the TB measurements, quantified as the Holevo information $\chi(A;E)$ for arbitrary collective attacks [27,28], and corrected here for a finite-length key [29,30]. Alice and Bob's information advantage over Eve per detected photon coincidence [24,31] can then be described as

$$r = \beta I(A;B) - \chi(A;E) - \Delta_{\text{FK}}, \tag{1}$$

where $0 \leqslant \beta \leqslant 1$ quantifies the efficiency of error correction, $I(A;B)$ is Alice and Bob's Shannon information, i.e., the information shared after making their arrival-time measurements, and Δ_{FK} accounts for the information penalty due to the finite-key length [29,30,32,33]. Thus, r represents the secure-key capacity in terms of bits per coincidence (bpc).

To upper-bound Eve's Holevo information about Alice's measurements in the TB, Alice and Bob use their experimentally measured excess spectral noise factor, $\xi_\omega = \sigma_\omega^2/\sigma_{\omega_0}^2 - 1$, where $\sigma_\omega^2 = \langle(\omega_A - \omega_B)^2\rangle$ quantifies the spectral correlation between Alice and Bob's detected photons, and $\sigma_{\omega_0}^2$ represents the noiseless correlation (i.e., excluding Eve's intrusion or excess channel noise), which is determined by the SPDC pump coherence time, σ_{coh} (or, equivalently, the pump linewidth). To measure ξ_ω, Alice pumps the SPDC source using Gaussian pulses of width σ_{coh} to produce pulsed entangled pairs with a spectral correlation σ_{ω_0} set by the time-bandwidth product. Alice and Bob's time-frequency covariance matrix (TFCM) contains ξ_ω. The calculation of $\chi(A;E)$ then follows from the symplectic decomposition of the TFCM [13,14]. In the limit where the two-photon correlation time after applying GVD, σ_t, is much greater than the two-photon correlation σ_{cor}, determined by the phase-matching bandwidth of the SPDC source, the frequency uncertainty is inversely proportional to the GVD, $\sigma_\omega = \sigma_t/|D|$: i.e., the greater the dispersion, the more precise the frequency measurement becomes. We note that taking the

difference between the time and the dispersed time effectively eliminates the effect of the original correlation time.

The discussion thus far assumed an infinite-key length, which is an unrealistic assumption that we now relax. A protocol with finite-key length can be only ε_s secure, where ε_s is the tolerated failure probability of the entire protocol [32]. We recently analyzed the finite-key effects for the DO-QKD protocol [29]. Choosing $\varepsilon_s = 10^{-5}$, as in Ref. [33], and including the finite-key effects on parameter estimation, we obtain an upper bound on the Holevo information of $\chi(A;E) = 1.56$ bpc.

To convert their time-tagged data to secure keys, Alice and Bob sift their time-tagged sequences into $d \times T_{\text{bin}}$-long frames, where $d \times T_{\text{bin}} \sim \sigma_{\text{coh}}$. Each frame is converted into a $\log_2 d$-bit symbol, based on the position of the detection event within the frame, relative to a shared clock. Only measurements made in the TB are used to generate keys; the FB measurements are used for the security check. Errors in the sifted keys are reconciled using a multilayer low-density parity-check (LDPC) code [34], which performs efficient large-alphabet error correction from the least significant to the most significant bit. The multilayer code is particularly effective at correcting errors caused by timing jitter, which are the vast majority of errors in the sifted keys. We experimentally achieved an efficiency $\beta > 90\%$ for all d (see Fig. 3). Finally,

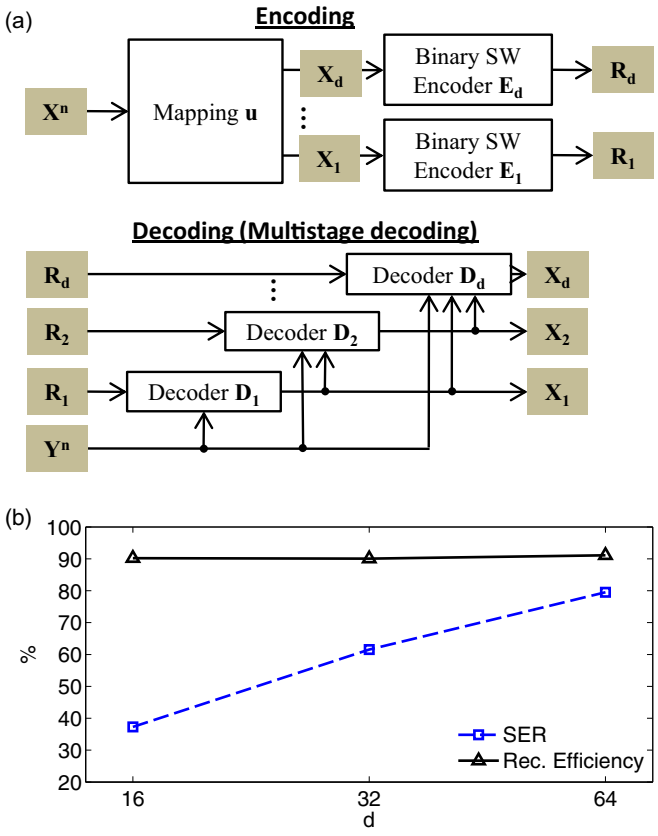

FIG. 3. (Color online) (a) Multilayer reconciliation scheme. Alice generates a message **R** by applying a binary Slepian-Wolf code to each bit layer $\mathbf{X_i}$, $1 \leqslant i \leqslant d$, for each character in her sifted key **X**. Bob receives **R** and tries to recover each layer $\mathbf{X_i}$, based on **R** and his sifted key **Y** [34]. (b) Experimentally obtained symbol-error rate (SER) and corresponding reconciliation efficiency β for different values of d at a photon pair generation rate of 0.28 pairs/pulse.

to eliminate Eve's information about the reconciled keys, Alice and Bob implement privacy amplification using hash functions based on multiplication by random Toeplitz matrices [35].

III. RESULTS AND DISCUSSION

For $\sigma_{\text{coh}} = 1.49$ ns and $d = 64$, we obtain a maximum secure-key capacity of 0.83 bpc after subtracting the finite-key penalty, Δ_{FK}. This value is below the theoretical maximum of $\log_2 s = 6$, where $s \equiv \sigma_{\text{coh}}/T_{\text{bin}}$ is the Schmidt number, i.e., the number of possible information eigenstates in the system, because (i) we subtract Eve's Holevo information of 1.56 bpc; (ii) we subtract the finite-key correction of 0.20 bpc; (iii) detector jitter, dark counts, and multiple SPDC pairs per frame reduce Alice and Bob's Shannon information $I(A;B)$ to 2.82 bpc; and (iv) the experimentally obtained reconciliation efficiency was 92%. The key length was $N \sim 3 \times 10^5$.

In this demonstration, the SPDC pump repetition rate was 8.3 MHz, and the average number of photon pairs generated was 0.28 pairs/pulse. The maximum observed secure-key rate was 456 bits per second (bps). Since the secure-key rate depends directly on the SPDC pump rate, a more useful figure of merit is the secure information generated per pump pulse, measured in bits per pulse (bpp). We obtained a maximum of 5.5×10^{-5} bpp.

It is clear that the secure-key rate can be increased by a higher SPDC pump pulse rate. A higher pump power leads to a greater entangled photon flux and also a potentially higher secure-key rate; however, increasing the SPDC pump power decreases r because the probability of multipair emissions per frame increases. An alternate strategy to raise the secure-key rate is to increase r; this is the benefit of a high-dimensional QKD protocol. By lengthening the SPDC pump pulse, we increase the maximum possible amount of information that can be generated in each frame. Care must be taken to choose the proper combination of pump power and pulse duration that keeps the multipair emission probability per frame sufficiently low while maximizing r. The optimal key generation rate occurs approximately when the detectors are close to saturation and we maximize the bpc by using the longest possible frame length that keeps the multipair emission probability per frame sufficiently low.

We can further increase the secure-key rate while maintaining the security with simple improvements to the system. If Alice and Bob preferentially choose the time basis, increasing the probability of key generation [36], we expect a rise in the secure-key rate without compromising security for a sufficiently long key [29]. As the probability of detection in the TB approaches 1, we anticipate a factor of four increase in the secure-key rate. Additionally, there is room for improvement in the coupling efficiency of the SPDC source.

We note that the finite-key correction, $\Delta_{\text{FK}} = 0.20$ bpc, is large because our key length, $N \sim 10^5$, is relatively short. With only an order-of-magnitude increase in N, we can more than halve the finite-key correction to 0.07 bpc, and when $N \geqslant 10^8$, $\Delta_{\text{FK}} < 0.01$ bpc. We can easily increase N by using a longer integration time and/or asymmetric basis selection.

In conclusion, we have demonstrated a complete high-dimensional entanglement-based QKD system with security against arbitrary collective attacks. By extending recent results in CV-QKD security proofs [37–39], it may be possible

to expand the security of DO-QKD to include coherent attacks. The DO-QKD scheme is compatible with existing telecommunications equipment and makes efficient use of a limited photon budget. The security of the system is guaranteed by the quantum mechanical phenomenon of nonlocal dispersion cancellation, which allows Alice and Bob to measure the high-dimensional spectral correlations with one detector each. Measuring both time and frequency requires as few as two single-photon detectors per party, making the resource demands similar to those of any two-dimensional entanglement-based QKD protocol. It is also possible to implement the system using commercial indium gallium arsenide (InGaAs) avalanche photodiodes (APDs), which can operate in free-running mode with efficiencies up to 40% and timing resolution comparable to that of the WSi SNSPDs used in this demonstration [40]. Alternatively, the protocol could be run at near-infrared wavelengths, where efficient, low-noise silicon-based APDs are commercially available, or frequency up-conversion could be used to convert telecommunications photons to wavelengths detectable by silicon APDs [41].

The results reported here are for short fiber links with negligible loss. A longer fiber link would introduce propagation loss; the loss in standard single-mode telecom fiber is 0.2 dB/km at the wavelength used in this demonstration. A longer fiber link will lower the secure-key rate (bps), since more photons going toward Bob will be lost. However, the secure-key capacity (bpc) should not be affected because Alice and Bob generate shared information only from detected photon coincidences. Since the time-energy correlations are preserved over transmission through optical fiber, the amount of information generated by each coincidence is unaffected. We note that significant lengths of fiber would introduce unwanted chromatic dispersion; the dispersion coefficient for standard single-mode telecommunications fiber is 17 ps/(nm km) at the wavelength used in this demonstration. The unwanted dispersion can be compensated using either dispersion-compensating fiber or specialized dispersion compensating devices (such as the fiber Bragg grating-based dispersive elements used to implement the FB measurements). The dispersion compensation will introduce additional loss, but this has the same effect as propagation loss: the secure-key rate will decrease, but the secure-key capacity should not be affected. Since the time-energy correlations are robust over transmission through both optical fiber and free space, our results show promise for an efficient and secure high-capacity, heterogeneous QKD network, with increased channel capacity by virtue of high-dimensional encoding.

ACKNOWLEDGMENTS

This work was supported by the DARPA Information in a Photon program, through Grant No. W911NF-10-1-0416 from the Army Research Office, and the Columbia Optics and Quantum Electronics IGERT under NSF Grant No. DGE-1069420.

APPENDIX A: NONLOCAL DISPERSION CANCELLATION AND BASIS TRANSFORMATION

The state of the entangled pair produced by the spontaneous parametric down-conversion (SPDC) source can be approximated as

$$|\Psi\rangle = \iint dt_A dt_B f(t_A,t_B) e^{-i\omega_p(t_A+t_B)/2} |t_A t_B\rangle, \tag{A1}$$

where

$$f(t_A,t_B) \propto e^{-(t_A+t_B)/16\sigma_{\rm coh}^2} e^{-(t_A-t_B)/4\sigma_{\rm cor}^2}, \tag{A2}$$

$|t_A t_B\rangle = \hat{a}_A^\dagger(t_A)\hat{a}_B^\dagger(t_B)|0\rangle$, and $\hat{a}_{A,B}^\dagger(t_j)$ denotes the photon creation operator for Alice or Bob, respectively, at time t_j.

Alice and Bob transform between the time basis (TB) and the frequency basis (FB) using group-velocity dispersion (GVD). Each frequency state acquires a phase $\phi \propto \beta_2\omega^2$. Here, $\beta_2 = \partial^2/\partial\omega^2|_{\omega_0}(n_{\rm eff}\omega/c)$, 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. Physically, β_2 is proportional to the linear change in the group velocity as a function of frequency.

Classically, when traveling through a dispersive medium, a transform-limited pulse spreads out in time because its frequency components move out of phase. However, Ref. [25] showed that if the entangled photons from Eq. (A2) pass through dispersive media, in the limit of large coherence time $\sigma_{\rm coh}$, the correlation time $\sigma_{\rm cor}$ becomes

$$\sigma_{\rm cor}'^2 \approx \frac{1}{\sigma_{\rm cor}^2}\left[\sigma_{\rm cor}^4 + (\beta_{2A}L_A + \beta_{2B}L_B)^2\right], \tag{A3}$$

where β_{2A} (β_{2B}) is the GVD introduced by Alice (Bob) over length L_A (L_B). Let $L_A = L_B = L$ and $\beta_{\rm tot} = \beta_{2A} + \beta_{2B}$. As $\beta_{\rm tot}$ increases, the temporal correlation between Alice's and Bob's photons degrades. However, $\sigma_{\rm cor}' = \sigma_{\rm cor}$ if $\beta_{2A} = -\beta_{2B} \equiv \beta_2$. Thus, if Alice applies normal dispersion on her photon, Bob can apply anomalous dispersion of equal magnitude on his photon to recover the temporal correlation between their photons. In the text, we defined $|D| \equiv \beta_2 L$ for notational simplicity.

APPENDIX B: TWO-PHOTON SPECTRAL CORRELATION AFTER APPLICATION OF GVD

The original two-photon correlation time is

$$\sigma_{\rm cor}^2 = \int dt du (t-u)^2 \langle \hat{E}_S^\dagger(t)\hat{E}_I^\dagger(u)\hat{E}_I(u)\hat{E}_S(t)\rangle, \tag{B1}$$

where $\hat{E}_S(t)$ ($\hat{E}_I(t)$) is the positive-frequency field operator for the signal (idler) field at time t. When applying GVD, the field operators are described in the frequency domain as

$$\hat{E}_S(t) = \int \frac{d\omega}{2\pi} \hat{A}_S(\omega) e^{-i\omega t} e^{i\beta_2 L\omega^2/2}, \tag{B2}$$

$$\hat{E}_I(t) = \int \frac{d\omega}{2\pi} \hat{A}_I(\omega) e^{-i\omega t} e^{-i\beta_2 L\omega^2/2}, \tag{B3}$$

where ω is defined as the detuning from $\omega_p/2$, and ω_p is the pump frequency of the SPDC source.

The two-photon correlation time after Alice applies normal GVD and Bob applies anomalous GVD is then

$$\sigma_t^2 = \int dtdu \frac{d\omega d\xi d\omega' d\xi'}{(2\pi)^4}(t-u)^2\langle \hat{A}_S^\dagger(\omega')\hat{A}_I^\dagger(\xi')\hat{A}_I(\xi)\hat{A}_S(\omega)\rangle e^{-it(\omega-\omega')-iu(\xi-\xi')}e^{i\beta_2 L(\omega^2-\xi^2-\omega'^2+\xi'^2)/2}. \tag{B4}$$

Let $t_\pm \equiv t \pm u$. Then,

$$\sigma_t^2 = \frac{1}{2}\int dt_+dt_- \frac{d\omega d\xi d\omega' d\xi'}{(2\pi)^4} t_-^2\langle \hat{A}_S^\dagger(\omega')\hat{A}_I^\dagger(\xi')\hat{A}_I(\xi)\hat{A}_S(\omega)\rangle e^{-i(\omega-\omega')(t_++t_-)/2-i(\xi-\xi')(t_+-t_-)/2}e^{i\beta_2 L(\omega^2-\xi^2-\omega'^2+\xi'^2)/2}. \tag{B5}$$

Let $\Omega_\pm \equiv \omega \pm \xi$ and $\Omega'_\pm \equiv \omega' \pm \xi'$. Using

$$\frac{1}{2}\int dt_+ e^{-it_+(\omega-\omega'+\xi-\xi')/2} = 2\pi\delta(\omega-\omega'+\xi-\xi'), \tag{B6}$$

Eq. (B5) becomes

$$\sigma_t^2 = \frac{1}{4}\int dt_- \frac{d\Omega_+ d\Omega_- d\Omega'_+ d\Omega'_-}{(2\pi)^4} t_-^2 \left\langle \hat{A}_S^\dagger\left(\frac{\Omega'_+ + \Omega'_-}{2}\right)\hat{A}_I^\dagger\left(\frac{\Omega'_+ - \Omega'_-}{2}\right)\hat{A}_I\left(\frac{\Omega_+ - \Omega_-}{2}\right)\hat{A}_S\left(\frac{\Omega_+ + \Omega_-}{2}\right)\right\rangle$$
$$\times 2\pi\delta(\Omega_+ - \Omega'_+)e^{-it_-(\Omega_- - \Omega'_-)/2}e^{i\beta_2 L(\Omega_+\Omega_- - \Omega'_+\Omega'_-)/2}. \tag{B7}$$

Since

$$\frac{1}{4}\int dt_- t_-^2 e^{-it_-(\Omega'_- - \Omega_-)/2} = -4\pi\frac{d^2}{d(\Omega'_-)^2}\delta(\Omega_- - \Omega'_-), \tag{B8}$$

evaluating Eq. (B7) requires integration by parts twice. Doing so, and carrying out the integral over Ω'_+, yields

$$\sigma_t^2 = -2\int \frac{d\Omega_+ d\Omega_- d\Omega'_-}{(2\pi)^3}\left[\frac{d^2}{d(\Omega'_-)^2}\left\langle \hat{A}_S^\dagger\left(\frac{\Omega_+ + \Omega'_-}{2}\right)\hat{A}_I^\dagger\left(\frac{\Omega_+ - \Omega'_-}{2}\right)\hat{A}_I\left(\frac{\Omega_+ - \Omega_-}{2}\right)\hat{A}_S\left(\frac{\Omega_+ + \Omega_-}{2}\right)\right\rangle\right.$$
$$\left.\times e^{i\beta_2 L\Omega_+(\Omega_- - \Omega'_-)/2}\right]2\pi\delta(\Omega_- - \Omega'_-). \tag{B9}$$

To differentiate the expectation value in Eq. (B9), the operators are rewritten in the time domain as

$$\hat{A}(\omega) = \int dt\,\hat{E}(t)e^{i\omega t}, \tag{B10}$$

giving us

$$\int \frac{d\Omega_+ d\Omega_- d\Omega'_-}{(2\pi)^3}\left\langle \hat{A}_S^\dagger\left(\frac{\Omega_+ + \Omega'_-}{2}\right)\hat{A}_I^\dagger\left(\frac{\Omega_+ - \Omega'_-}{2}\right)\hat{A}_I\left(\frac{\Omega_+ - \Omega_-}{2}\right)\hat{A}_S\left(\frac{\Omega_+ + \Omega_-}{2}\right)\right\rangle$$
$$= \int \frac{d\Omega_+ d\Omega_- d\Omega'_-}{(2\pi)^3} dtdudt'du'\langle \hat{E}_S^\dagger(t')\hat{E}_I^\dagger(u')\hat{E}_I(u)\hat{E}_S(t)\rangle e^{-i\Omega_+(t'+u'-u-t)/2}e^{-i\Omega_-(u-t)/2}e^{-i\Omega'_-(t'-u')/2}. \tag{B11}$$

After differentiating Eq. (B11) twice with respect to Ω'_-, the right-hand side (RHS) becomes

$$\frac{d^2}{d(\Omega'_-)^2}\mathrm{RHS} = -\frac{1}{4}\int \frac{d\Omega_+ d\Omega_- d\Omega'_-}{(2\pi)^3} dtdudt'du' 2\pi\delta(\Omega_- - \Omega'_-)(t'-u')^2\langle \hat{E}_S^\dagger(t')\hat{E}_I^\dagger(u')\hat{E}_I(u)\hat{E}_S(t)\rangle$$
$$\times e^{-i\Omega_+(t'+u'-u-t)/2}e^{-i\Omega_-(u-t)/2}e^{-i\Omega'_-(t'-u')/2}. \tag{B12}$$

After combining the result of Eq. (B12) with Eq. (B9),

$$\sigma_t^2 = \frac{(\beta_2 L)^2}{2}\int \frac{d\Omega_+ d\Omega_-}{(2\pi)^2}\Omega_+^2\left\langle \hat{A}_S^\dagger\left(\frac{\Omega_+ + \Omega_-}{2}\right)\hat{A}_I^\dagger\left(\frac{\Omega_+ - \Omega_-}{2}\right)\hat{A}_I\left(\frac{\Omega_+ - \Omega_-}{2}\right)\hat{A}_S\left(\frac{\Omega_+ + \Omega_-}{2}\right)\right\rangle$$
$$+\frac{1}{2}\int \frac{d\Omega_+ d\Omega_-}{(2\pi)^2} dtdudt'du'(t'-u')^2\langle \hat{E}_S^\dagger(t')\hat{E}_I^\dagger(u')\hat{E}_I(u)\hat{E}_S(t)\rangle e^{i\Omega_+(-t'+u'-u-t)/2}e^{-i\Omega_-(t'-u'-+u-t)/2}. \tag{B13}$$

Since $\Omega_\pm \equiv \omega \pm \xi$,

$$\sigma_t^2 = (\beta_2 L)^2\int d\omega d\xi(\omega+\xi)^2\langle \hat{A}_S^\dagger(\omega)\hat{A}_I^\dagger(\xi)\hat{A}_I(\xi)\hat{A}_S(\omega)\rangle + \int dtdu(t-u)^2\langle \hat{E}_S^\dagger(t)\hat{E}_I^\dagger(u)\hat{E}_I(u)\hat{E}_S(t)\rangle. \tag{B14}$$

Because the frequency-domain field operators were defined in terms of the detuning from $\omega_p/2$, ω and ξ have opposite signs. The first term of Eq. (B14) is therefore σ_ω^2, the two-photon spectral correlation after applying GVD. Thus, according to Eq. (B14), $\sigma_t^2 = (\beta_2 L)^2\sigma_\omega^2 + \sigma_{\rm cor}^2$. In the limit when $\sigma_t \gg \sigma_{\rm cor}$, the two-photon spectral correlation is given by $\sigma_\omega = \sigma_t/(|\beta_2|L) = \sigma_t/|D|$.

[1] G. S. Vernam, J. Am. Inst. Electr. Eng. **45**, 109 (1926).
[2] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[3] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[4] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[5] L. Zhang, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **100**, 110504 (2008).
[6] S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, Sci. Rep. **3**, 2316 (2013).
[7] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[8] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **66**, 062304 (2002).
[9] R. T. Thew, A. Acín, 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] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, Phys. Rev. A **87**, 062322 (2013).
[14] Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. Lett. **112**, 120506 (2014).
[15] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, J. Phys. B **46**, 104010 (2013).
[16] T. Brougham and S. M. Barnett, J. Phys. B **47**, 155501 (2014).
[17] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature (London) **412**, 313 (2001).
[18] A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **89**, 240401 (2002).
[19] G. Molina-Terriza, A. Vaziri, J. Řeháček, Z. Hradil, and A. Zeilinger, Phys. Rev. Lett. **92**, 167903 (2004).
[20] 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).
[21] T. Zhong, F. N. C. Wong, A. Restelli, and J. C. Bienfang, Opt. Express **20**, 26868 (2012).
[22] 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).
[23] T. Zhong, Ph.D. thesis, Massachusetts Institute of Technology, 2013.
[24] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[25] J. D. Franson, Phys. Rev. A **45**, 3126 (1992).
[26] The chirped fiber Bragg gratings apply GVD periodically over 50-GHz channels matched to the International Telecommunication Union (ITU) grid; thus, the magnitude of the applied group-velocity delay slope is $|D| = 600$ ps/0.4 nm.
[27] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[28] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[29] C. Lee, J. Mower, Z. Zhang, J. H. Shapiro, and D. Englund, arXiv:1311.1233.
[30] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
[31] I. Devetak and A. Winter, Proc. R. Soc. A: Math. Phys. Engineer. Sci. **461**, 207 (2005).
[32] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[33] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).
[34] H. Zhou, L. Wang, and G. Wornell, in *Proc. Information Theory and Applications Workshop (ITA), 2013* (IEEE, Piscataway, NJ, 2013), pp. 1–10.
[35] G. van Assche, *Quantum Cryptography and Secret-Key Distillation* (Cambridge University Press, Cambridge, 2006).
[36] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
[37] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[38] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
[39] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[40] InGaAs Single-Photon Counter data sheet, Micro Photon Devices S.r.l., available online at www.micro-photon-devices.com.
[41] G.-L. Shentu, J. S. Pelc, X.-D. Wang, Q.-C. Sun, M.-Y. Zheng, M. M. Fejer, Q. Zhang, and J.-W. Pan, Opt. Express **21**, 13986 (2013).