Entanglement-based quantum communication secured by nonlocal dispersion cancellation

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://dx.doi.org/10.1103/PhysRevA.90.062331">http://dx.doi.org/10.1103/PhysRevA.90.062331</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>American Physical Society</td>
</tr>
<tr>
<td>Version</td>
<td>Final published version</td>
</tr>
<tr>
<td>Accessed</td>
<td>Fri Apr 12 08:38:18 EDT 2019</td>
</tr>
<tr>
<td>Citable Link</td>
<td><a href="http://hdl.handle.net/1721.1/92715">http://hdl.handle.net/1721.1/92715</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.</td>
</tr>
<tr>
<td>Detailed Terms</td>
<td></td>
</tr>
</tbody>
</table>
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,1 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 Englund1

1Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
2Department of Physics, Columbia University, New York, New York 10027, USA
3National Institute of Standards and Technology, Boulder, Colorado 80305, USA
4NASA 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 ($9 \times 10^6$ 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 $D = 600 \text{ ps}/0.4 \text{ nm}$ ($D = -600 \text{ ps}/0.4 \text{ nm}$) of dispersion [26]. The dispersive
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 the TB and FB. They sift their coincidence data into frames of duration $d \times T_{\text{bin}}$, comprised of $d$ bins of duration $T_{\text{bin}}$. 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 $\sim 110$ 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 $\sim 630$ 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 $\sim 1$ ps photon envelope to $\sim 640$ ps. The stretched photon envelope exceeds the $\sim 100$ 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

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

where $0 \leq \beta \leq 1$ 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 $\Delta_{\text{FK}}$ 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, $\xi_0 = \sigma_0^2/\sigma_{\text{coh}}^2 - 1$, where $\sigma_0^2 = (\omega_A - \omega_B)^2$ quantifies the spectral correlation between Alice and Bob’s detected photons, and $\sigma_{\text{coh}}^2$ represents the noiseless correlation (i.e., excluding Eve’s intrusion or excess channel noise), which is determined by the SPDC pump coherence time, $\sigma_{\text{coh}}$ (or, equivalently, the pump linewidth). To measure $\xi_0$, Alice pumps the SPDC source using Gaussian pulses of width $\sigma_{\text{coh}}$ to produce pulsed entangled pairs with a spectral correlation $\sigma_{oo}$ set by the time-bandwidth product. Alice and Bob’s time-frequency covariance matrix (TFCM) contains $\xi_0$. 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, $\tau_j$, is much greater than the two-photon correlation $\tau_{\text{cor}}$, determined by the phase-matching bandwidth of the SPDC source, the frequency uncertainty is inversely proportional to the GVD, $\sigma_f = \sqrt{\tau_j/|D|}$; i.e., the greater the dispersion, the more precise the frequency measurement becomes. We note that taking the

![Diagram](image-url)
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 $\varepsilon_s$ secure, where $\varepsilon_s$ is the tolerated failure probability of the entire protocol [32].

We recently analyzed the finite-key effects for the DO-QKD protocol [29]. Choosing $\varepsilon_s = 10^{-3}$, 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 $d \times T_{bin}$-long frames, where $d \times T_{bin} \sim \sigma_{coh}$. 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, 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 $\sigma_{coh} = 1.49$ ns and $d = 64$, we obtain a maximum secure-key capacity of 0.83 bpc after subtracting the finite-key penalty, $\Delta_{FK}$. This value is below the theoretical maximum of log$_2 s = 6$, where $s \equiv \sigma_{coh}/T_{bin}$ 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 $5.5 \times 10^3$ 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, $\Delta_{FK} = 0.20$ 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 $N \geq 10^6$, $\Delta_{FK} < 0.01$ 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 non-local 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 between their photons. In the text, we defined σ_{cor} the correlation time σ_{cor} becomes

\[ σ_{cor}^2 \approx \frac{1}{σ_{cor}^2} \left[ σ_4^2 + \left( β_{2A} L_A + β_{2B} L_B \right)^2 \right], \]

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 β_{2A} = β_{2B} = β_2. As β_{2A} increases, the temporal correlation between Alice’s and Bob’s photons degrades. However, σ_{cor}^2 = σ_{cor} if β_{2A} = −β_{2B} ⇒ β_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| ≡ β_2 L for notational simplicity.

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

The original two-photon correlation time is

\[ σ_{cor}^2 = \int dt du (t - u)^2 \langle \hat{E}_S^\dagger (t) \hat{E}_S^\dagger (u) \hat{E}_S (u) \hat{E}_S (t) \rangle, \]

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

\[ \hat{E}_S (t) = \int \frac{dω}{2π} \hat{A}_S (ω) e^{-iωt} e^{iβ_2 Lω^2/2}, \]

\[ \hat{E}_I (t) = \int \frac{dω}{2π} \hat{A}_I (ω) e^{-iωt} e^{-iβ_2 Lω^2/2}, \]
The two-photon correlation time after Alice applies normal GVD and Bob applies anomalous GVD is then

\[ \sigma^2_{\gamma} = \int dt du \frac{d\Omega_{\pm} d\Omega_{\pm}}{(2\pi)^4} d\Omega'_{\pm} d\Omega'_{\pm} \left( t - u \right)^2 \left( \Omega'_{\pm} \Omega'_{\pm} \right) \hat{A}(t) \hat{A}(u) \hat{A}^\dagger(t) \hat{A}^\dagger(u) e^{-it(t-u) - iu(t-x)} e^{i\beta L \left( \Omega^2 - \Omega'^2 + \omega^2 \right)/2}. \] (B4)

Let \( t_\pm \equiv t \pm u \). Then,

\[ \sigma^2_{\gamma} = \frac{1}{2} \int dt du \frac{d\Omega_{\pm} d\Omega_{\pm}}{(2\pi)^4} d\Omega'_{\pm} d\Omega'_{\pm} \left( t - u \right)^2 \left( \Omega'_{\pm} \Omega'_{\pm} \right) \hat{A}(t) \hat{A}(u) \hat{A}^\dagger(t) \hat{A}^\dagger(u) e^{-it(t-u) - iu(t-x)} e^{i\beta L \left( \Omega^2 - \Omega'^2 + \omega^2 \right)/2}. \] (B5)

Let \( \Omega_{\pm} \equiv \omega \pm \xi \) and \( \Omega'_{\pm} \equiv \omega' \pm \xi' \). Using

\[ \frac{1}{2} \int dt e^{-it(t-u') - iu'(t-x')/2} = 2\pi \delta(\omega - \omega' + \xi - \xi'). \] (B6)

Eq. (B5) becomes

\[ \sigma^2_{\gamma} = \frac{1}{4} \int dt d\Omega_{\pm} d\Omega_{\pm} d\Omega'_{\pm} d\Omega'_{\pm} \left( t - u \right)^2 \left( \Omega'_{\pm} \Omega'_{\pm} \right) \hat{A}(t) \hat{A}(u) \hat{A}^\dagger(t) \hat{A}^\dagger(u) e^{-it(t-u) - iu(t-x)} e^{i\beta L \left( \Omega^2 - \Omega'^2 + \omega^2 \right)/2}. \] (B7)

Since

\[ \frac{1}{2} \int dt d\Omega_{\pm} \left( t - u \right)^2 e^{-it(t-u) - iu(t-x)} = -4\pi \int d\Omega_{\pm} \left( \Omega^2 - \Omega' \right)/2 \] (B8)

evaluating Eq. (B7) requires integration by parts twice. Doing so, and carrying out the integral over \( \Omega'_{\pm} \), yields

\[ \sigma^2_{\gamma} = -2 \int dt d\Omega_{\pm} d\Omega_{\pm} \left[ \frac{d^2}{d\Omega_{\pm}^2} \left( \Omega_{\pm} + \Omega_{\pm}' \right) \hat{A}(t) \hat{A}(u) \hat{A}^\dagger(t) \hat{A}^\dagger(u) e^{-it(t-u) - iu(t-x)} \right]. \] (B9)

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

\[ \hat{A}(\omega) = \int dt \hat{E}(t) e^{i\omega t}. \] (B10)

giving us

\[ \int dt d\Omega_{\pm} d\Omega_{\pm} \left( t - u \right)^2 \hat{A}(t) \hat{A}(u) \hat{A}^\dagger(t) \hat{A}^\dagger(u) e^{-it(t-u) - iu(t-x)} \right]. \] (B11)

After differentiating Eq. (B11) twice with respect to \( \Omega'_{\pm} \), the right-hand side (RHS) becomes

\[ \frac{d^2}{d\Omega_{\pm}^2} \text{RHS} = -\frac{1}{4} \int dt d\Omega_{\pm} d\Omega_{\pm} d\Omega'_{\pm} d\Omega'_{\pm} \left( t - u \right)^2 \hat{E}^\dagger(t') \hat{E}(u) \hat{E}(t) \hat{E}(u) \] (B12)

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

\[ \sigma^2_{\gamma} = \frac{(\beta_2 L)^2}{2} \int dt d\Omega_{\pm} d\Omega_{\pm} \left( t - u \right)^2 \hat{A}(t) \hat{A}(u) \hat{A}^\dagger(t) \hat{A}^\dagger(u) e^{-it(t-u) - iu(t-x)} \] (B13)

Since \( \Omega_{\pm} \equiv \omega \pm \xi \),

\[ \sigma^2_{\gamma} = (\beta_2 L)^2 \int d\omega d\xi d\xi \hat{A}(\omega) \hat{A}(\xi) \hat{A}^\dagger(\xi) \hat{A}^\dagger(\omega) \] (B14)
Because the frequency-domain field operators were defined in terms of the detuning from $\omega_p/2$, $\omega$ and $\xi$ have opposite signs. The first term of Eq. (B14) is therefore $\sigma^2_{\omega}$, the two-photon spectral correlation after applying GVD. Thus, according to Eq. (B14), $\sigma^2 = (\beta_2 L)^2 \sigma^2_{\omega} + \sigma^2_{\text{cor}}$. In the limit when $\sigma_t \gg \sigma_{\text{cor}}$, the two-photon spectral correlation is given by $\sigma_{\omega} = \sigma_t / (|\beta_2| L) = \sigma_t / |D|$.