



# MIT Open Access Articles

## *Unconditional Security of Time-Energy Entanglement Quantum Key Distribution Using Dual-Basis Interferometry*

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

<b>Citation</b>	Zhang, Zheshen, Jacob Mower, Dirk Englund, Franco N. C. Wong, and Jeffrey H. Shapiro. "Unconditional Security of Time-Energy Entanglement Quantum Key Distribution Using Dual-Basis Interferometry." Physical Review Letters 112, no. 12 (March 2014). © 2014 American Physical Society
<b>As Published</b>	<a href="http://dx.doi.org/10.1103/PhysRevLett.112.120506">http://dx.doi.org/10.1103/PhysRevLett.112.120506</a>
<b>Publisher</b>	American Physical Society
<b>Version</b>	Final published version
<b>Citable link</b>	<a href="http://hdl.handle.net/1721.1/89019">http://hdl.handle.net/1721.1/89019</a>
<b>Terms of Use</b>	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.

## Unconditional Security of Time-Energy Entanglement Quantum Key Distribution Using Dual-Basis Interferometry

Zheshen Zhang,<sup>\*</sup> Jacob Mower, Dirk Englund, Franco N. C. Wong, and Jeffrey H. Shapiro  
*Research Laboratory of Electronics, Massachusetts Institute of Technology,  
77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*  
(Received 4 November 2013; published 26 March 2014)

High-dimensional quantum key distribution (HDQKD) offers the possibility of high secure-key rate with high photon-information efficiency. We consider HDQKD based on the time-energy entanglement produced by spontaneous parametric down-conversion and show that it is secure against collective attacks. Its security rests upon visibility data—obtained from Franson and conjugate-Franson interferometers—that probe photon-pair frequency correlations and arrival-time correlations. From these measurements, an upper bound can be established on the eavesdropper's Holevo information by translating the Gaussian-state security analysis for continuous-variable quantum key distribution so that it applies to our protocol. We show that visibility data from just the Franson interferometer provides a weaker, but nonetheless useful, secure-key rate lower bound. To handle multiple-pair emissions, we incorporate the decoy-state approach into our protocol. Our results show that over a 200-km transmission distance in optical fiber, time-energy entanglement HDQKD could permit a 700-bit/sec secure-key rate and a photon information efficiency of 2 secure-key bits per photon coincidence in the key-generation phase using receivers with a 15% system efficiency.

DOI: [10.1103/PhysRevLett.112.120506](https://doi.org/10.1103/PhysRevLett.112.120506)

PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Dv

Quantum key distribution (QKD) [1] promises unconditionally secure communication by enabling one-time pad transmission between remote parties, Alice and Bob. Continuous-variable QKD (CVQKD) [2,3] and discrete-variable QKD (DVQKD) [4,5] utilize infinite-dimensional and finite-dimensional Hilbert spaces, respectively. CVQKD exploits the wave nature of light to encode multiple bits into each transmission, but it has been limited to 80 km in optical fiber [3,6,7] because the eavesdropper (Eve) can obtain partial information from a beam-splitting attack. The predominant DVQKD protocol is Bennett-Brassard 1984 (BB84), which uses a two-dimensional Hilbert space. The decoy-state BB84 protocol [8,9] has demonstrated nonzero secure-key rates (SKRs) over 144 km in free space [10] and 107 km in optical fiber [11], but its photon information efficiency (PIE) cannot exceed 1 key bit per sifted photon.

High-dimensional QKD (HDQKD) using single photons [12] can utilize the best features of the continuous and discrete worlds, with the Hilbert space of single-photon arrival times providing an appealing candidate for its implementation. The time-energy entanglement of photon pairs produced by spontaneous parametric down-conversion (SPDC) has been employed in HDQKD experiments [13,14], although these works lacked rigorous security proofs. Security proofs for time-energy entangled HDQKD have been attempted by discretizing the continuous Hilbert space to permit use of DVQKD security analyses [12,15], but the validity of the discretization approach has not been proven. CVQKD security analysis

[16,17] uses the quadrature-component covariance matrix to derive a lower bound on the SKR in the presence of a collective attack. We take an analogous approach—using the time-frequency covariance matrix (TFCM)—for our time-energy entanglement HDQKD protocol.

The TFCM for our protocol can be obtained using the dispersive-optics scheme from [18], although dense wavelength-division multiplexing (DWDM) may be required to do so [19]. An experimentally simpler technique—utilizing a Franson interferometer—has been conjectured [13,14] to be sufficient for security verification. Its robustness against some specific attacks has been discussed [14,20], but security against collective attacks has not been proven and [20] suggests that such a proof may be impossible.

This Letter proves that time-energy entanglement HDQKD can be made secure against Eve's collective attack when a Franson interferometer is used for security verification in conjunction with a dispersion-based frequency-difference measurement. Our proof relates the Franson interferometer's fringe visibility to the TFCM's frequency elements that, together with the frequency-difference measurement, establishes an upper bound on Eve's Holevo information. We introduce another nonlocal interferometer—the conjugate-Franson interferometer—and link its fringe visibility to the TFCM's arrival-time elements [21]. Employing both interferometers increases the SKR.

Our fringe visibility results presume that the entanglement source emits at most one photon pair in a measurement frame, which need not be the case for SPDC. Thus, we

incorporate decoy-state operation [8,9] to handle multiple-pair emissions. We show that time-energy entanglement HDQKD could permit a 700 bit/sec SKR over a 200-km transmission distance in optical fiber. We also show that a PIE of 2 secure-key bits per photon coincidence can be achieved in the key-generation phase using receivers with a 15% system efficiency. Before beginning our security analysis, we provide a brief explanation of our protocol.

Suppose Alice has a repetitively pumped, frequency-degenerate SPDC source that, within a time frame of duration of  $T_f$  sec, which is centered at time  $t_m = 3mT_f$ , emits a single photon pair in the state [22]

$$|\psi_m\rangle_{SI} \propto \int dt_S \int dt_I e^{-(t_+ - t_m)^2/4\sigma_{\text{coh}}^2 - t_-^2/4\sigma_{\text{cor}}^2 - i\omega_p t_+} |t_S\rangle_S |t_I\rangle_I \quad (1)$$

for some integer  $m$ . In this expression,  $\omega_p$  is the pump frequency;  $|t_S\rangle_S$  ( $|t_I\rangle_I$ ) represents a single photon of the signal (idler) at time  $t_S$  ( $t_I$ );  $t_+ \equiv (t_S + t_I)/2$ ;  $t_- \equiv t_S - t_I$ ; the root-mean-square coherence time  $\sigma_{\text{coh}} = T_f/\sqrt{8 \ln(2)} \sim \text{nsec}$  is set by the pump pulse's duration; and the root-mean square correlation time  $\sigma_{\text{cor}} = \sqrt{2 \ln(2)}/2\pi B_{\text{PM}} \sim \text{psec}$  is set by the reciprocal of the full-width at half-maximum (FWHM) phase-matching bandwidth,  $B_{\text{PM}}$ , in Hz. Now suppose that, despite propagation losses and detector inefficiencies, Alice and Bob detect the signal and idler, respectively, from the preceding photon pair and record the associated arrival times [23,24]. After many such frames, they use public communication to reconcile their arrival-time data, resulting in their sharing  $n_R$  random bits per postselected frame, i.e., frames used for key generation in which Alice and Bob both made detections. How many of those bits are secure against Eve's collective attack? Before turning to the security analysis, we pause for a brief note about Eq. (1). This expression is an oft-used approximation for the postselected biphoton state produced by an SPDC source (see, e.g., [14]). Moreover, entanglement engineering can be employed to achieve a close match to a truly Gaussian biphoton wave function [25].

Our security analysis begins with the positive-frequency field operators,  $\hat{E}_S(t)$  and  $\hat{E}_I(t)$ , for the linearly polarized single spatial-mode signal and idler fields emitted by Alice's source, and their associated frequency decompositions:

$$\hat{E}_S(t) = \int \frac{d\omega}{2\pi} \hat{A}_S(\omega) e^{-i(\omega_p/2 + \omega)t}, \quad (2a)$$

$$\hat{E}_I(t) = \int \frac{d\omega}{2\pi} \hat{A}_I(\omega) e^{-i(\omega_p/2 - \omega)t}. \quad (2b)$$

The time-domain field operators  $\hat{E}_S(t)$  and  $\hat{E}_I(t)$  annihilate signal and idler photons, respectively, at time  $t$ , and

they obey the canonical commutation relations,  $[\hat{E}_J(t), \hat{E}_K^\dagger(u)] = \delta_{JK} \delta(t-u)$ , for  $J, K = S, I$ . Their frequency-domain counterparts,  $\hat{A}_S(\omega)$  and  $\hat{A}_I(\omega)$ , annihilate signal and idler photons at detunings  $\omega$  and  $-\omega$ , respectively. Our interest, however, is in the arrival-time and angular-frequency operators,

$$\hat{t}_J = \int dt t \hat{E}_J^\dagger(t) \hat{E}_J(t), \quad (3a)$$

$$\hat{\omega}_J = \int \frac{d\omega}{2\pi} \omega \hat{A}_J^\dagger(\omega) \hat{A}_J(\omega), \quad (3b)$$

for  $J = S, I$  when only one photon pair is emitted by the source. Restricting these time and frequency operators to the single-pair Hilbert space implies that they measure the arrival times and frequency detunings of the signal and idler photons. It also leads to the commutation relation  $[\hat{\omega}_J, \hat{t}_K] = i\epsilon_J \delta_{JK}$  [26], where  $\epsilon_S = -\epsilon_I = 1$ , making these operators conjugate observables analogous to the quadrature components employed in CVQKD and justifying our translating CVQKD's covariance-based security analysis [16,17] to our protocol.

To exploit the connection to CVQKD, we define an observable vector  $\hat{O} = [\hat{t}_S \ \hat{\omega}_S \ \hat{t}_I \ \hat{\omega}_I]^T$ . For a single-pair state, the mean value of  $\hat{O}$  is  $\mathbf{m} = \langle \hat{O} \rangle$ , and the TFCM is  $\mathbf{\Gamma} = \langle (\Delta \hat{O} \Delta \hat{O}^\dagger + \text{H.c.}) \rangle / 2$ , where  $\Delta \hat{O} \equiv \hat{O} - \mathbf{m}$  and H.c. denotes Hermitian conjugate. The characteristic function associated with the single-pair state is  $\chi(\boldsymbol{\xi}) = \langle e^{i\boldsymbol{\xi}^T \hat{O}} \rangle$ . Given the covariance matrix  $\mathbf{\Gamma}$ , the Gaussian state with  $\chi(\boldsymbol{\xi}) = e^{i\boldsymbol{\xi}^T \mathbf{m} - \boldsymbol{\xi}^T \mathbf{\Gamma} \boldsymbol{\xi} / 2}$  yields an  $\mathbf{m}$ -independent upper bound on Eve's Holevo information [16,17,27] when the SPDC source emits a single-pair state.

A direct, complete measurement of the TFCM is quite challenging, so we resort to indirect measurements—using a Franson interferometer and a conjugate-Franson interferometer—that provide useful partial information. A Franson interferometer [28], shown in the top panel of Fig. 1, consists of two unequal path-length Mach-Zehnder interferometers, with the signal going through one and the

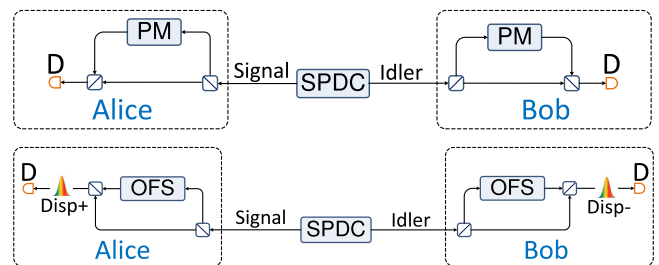


FIG. 1 (color online). (Top panel) Diagram for the Franson interferometer. (Bottom panel) Diagram for the conjugate-Franson interferometer. PM, phase modulator; OFS, optical-frequency shifter; Disp+, positive dispersion element; Disp-, negative dispersion element; D, detector.

idler going through the other. The time delay  $\Delta T$  between each Mach-Zehnder interferometer's long and short paths is much greater than the correlation time  $\sigma_{\text{cor}}$ , ruling out local interference in the individual interferometers. It is also greater than the FWHM detector timing jitter,  $\delta T$ , so that coincidences are only registered when both photons go through the long or the short path. Each long path is equipped with a phase modulator, imparting phase shifts  $e^{-i\phi_S}$  and  $e^{-i\phi_I}$  to the signal and the idler, respectively. The following lemma shows that Franson measurements, augmented by dispersion-based frequency measurements, bound the signal-idler frequency correlations [26].

*Lemma 1.*—For a single-pair state, let  $V_{\text{FI}}(\Delta T) = [P_{C_{\text{FI}}}(0) - P_{C_{\text{FI}}}(\pi)]/[P_{C_{\text{FI}}}(0) + P_{C_{\text{FI}}}(\pi)]$ , where  $P_{C_{\text{FI}}}(\phi_S + \phi_I)$  is Alice and Bob's coincidence probability, be the  $0-\pi$  fringe visibility when the Franson interferometer has delay  $\Delta T$ . Then the variance of the signal-idler frequency difference satisfies

$$\langle(\Delta\hat{\omega}_S - \Delta\hat{\omega}_I)^2\rangle \leq \frac{2[1 - V_{\text{FI}}(\Delta T)]}{\Delta T^2} + \frac{\langle(\tilde{\omega}_S - \tilde{\omega}_I)^4\rangle}{12} \Delta T^2, \quad (4)$$

where  $\tilde{\omega}_S$  ( $\tilde{\omega}_I$ ) is the random variable associated with the measured signal (idler) angular frequency from the conjugate-Franson interferometer with its frequency-shifted arms disabled, i.e., when dispersion enables frequency correlations to be measured from arrival-time coincidences.

A conjugate-Franson interferometer, shown in the bottom panel of Fig. 1, consists of two equal path-length Mach-Zehnder interferometers with one arm of each containing an electro-optic optical-frequency shifter. To rule out local interference, these devices shift the signal and idler frequencies by  $-\Delta\Omega$  and  $\Delta\Omega$ , respectively, while phase modulators (not shown) apply phase shifts  $e^{-i\phi_S}$  and  $e^{-i\phi_I}$ , as was done in the Franson interferometer. The positive and negative dispersion elements have coefficients  $\pm\beta_2$  satisfying  $\beta_2\Delta\Omega = \sqrt{2}T_g > \delta T$ , where  $T_g$  is the duration of detectors' coincidence gate [29]. They disperse the signal and idler's frequency components with respect to time so that two detectors suffice to measure their frequency coincidences [18,26]. The following lemma shows that conjugate-Franson measurements, augmented by arrival-time measurements, bound the signal-idler arrival-time correlations [26].

*Lemma 2.*—For a single-pair state, let  $V_{\text{CFI}}(\Delta\Omega) = [P_{C_{\text{CFI}}}(0) - P_{C_{\text{CFI}}}(\pi)]/[P_{C_{\text{CFI}}}(0) + P_{C_{\text{CFI}}}(\pi)]$ , where  $P_{C_{\text{CFI}}}(\phi_S + \phi_I)$  is Alice and Bob's coincidence probability, be the  $0-\pi$  fringe visibility when the conjugate-Franson interferometer has frequency shift  $\Delta\Omega$ . Then the variance of the signal-idler arrival-time difference satisfies

$$\langle(\Delta\hat{t}_S - \Delta\hat{t}_I)^2\rangle \leq \frac{2[1 - V_{\text{CFI}}(\Delta\Omega)]}{\Delta\Omega^2} + \frac{\langle(\tilde{t}_S - \tilde{t}_I)^4\rangle}{12} \Delta\Omega^2, \quad (5)$$

where  $\tilde{t}_S$  ( $\tilde{t}_I$ ) is the random variable associated with the measured signal (idler) arrival time from the Franson interferometer with its long arms disabled.

Lemmas 1 and 2 are used below to bound Eve's Holevo information for a frame in which Alice's source emits a single photon pair. Because there is no security assurance for multiple-pair emissions, we follow the lead of DVQKD by employing decoy states [8,9] to deal with this problem. In particular, Alice operates her SPDC source at several different pump powers, enabling Bob and her to estimate the fraction,  $F$ , of their coincidences that originated from single-pair emissions [30].

To put an upper bound on Eve's Holevo information, we start from the following points: (1) Symmetry dictates that only 10 TFCM elements need to be found. Of these,  $\langle\Delta\hat{\omega}_S^2\rangle$  and  $\langle\Delta\hat{t}_S^2\rangle$  are immune to Eve's attack because Eve does not have access to Alice's apparatus, which contains the SPDC source. (2) Given the Franson and conjugate-Franson interferometer's fringe visibilities, making  $\langle\Delta\hat{t}_J\Delta\hat{\omega}_K\rangle \neq 0$ , for  $J, K = S, I$ , does not increase Eve's Holevo information [26]. (3) From lemmas 1 and 2, we can determine upper bounds on the excess noise factors  $1 + \xi_\omega \equiv \langle(\Delta\hat{\omega}_S - \Delta\hat{\omega}_I)^2\rangle/\langle(\Delta\hat{\omega}_{S_0} - \Delta\hat{\omega}_{I_0})^2\rangle$  and  $1 + \xi_t \equiv \langle(\Delta\hat{t}_S - \Delta\hat{t}_I)^2\rangle/\langle(\Delta\hat{t}_{S_0} - \Delta\hat{t}_{I_0})^2\rangle$ , where  $\langle(\Delta\hat{t}_{S_0} - \Delta\hat{t}_{I_0})^2\rangle$  and  $\langle(\Delta\hat{\omega}_{S_0} - \Delta\hat{\omega}_{I_0})^2\rangle$  are the source's variances as measured by Alice during her source-characterization phase.

Points 1–3 specify a set,  $\mathcal{M}$ , of physically allowed TFCMs that preserve the Heisenberg uncertainty relations for the elements of  $\hat{O}$ , which are implied by  $[\hat{\omega}_J, \hat{t}_K] = i\epsilon_{JK}\delta_{JK}$ . For each TFCM  $\Gamma \in \mathcal{M}$ , the Gaussian state  $\chi(\xi) = e^{-\xi^T \Gamma \xi/2}$  affords Eve the maximum Holevo information [16,17,27]. Using  $\chi_\Gamma(A; E)$  to denote that Holevo information, our partial information about  $\Gamma$  gives us the upper bound  $\chi_{\xi_r, \xi_\omega}^{\text{UB}}(A; E) = \sup_{\Gamma \in \mathcal{M}} [\chi_\Gamma(A; E)]$  on what Eve can learn from a collective attack on a single-pair frame. Thus, Alice and Bob's SKR (in bits per second) has the lower bound [9,26,31]:

$$\text{SKR} \geq \frac{q p_r}{3 T_f} [\beta I(A; B) - (1 - F)n_R - F \chi_{\xi_r, \xi_\omega}^{\text{UB}}(A; E)]. \quad (6)$$

Here,  $q$  is the fraction of the frames used for key generation (as opposed to Franson or conjugate-Franson operation or decoy-state transmission for parameter estimation);  $p_r$  is the probability of registering a coincidence in a frame;  $\beta$  is the reconciliation efficiency; and  $I(A; B)$  is Alice and Bob's Shannon information.

In Fig. 2, the left panel plots Alice and Bob's SKR versus transmission distance for two frame durations and two system efficiencies for Alice ( $\eta_A$ ) and Bob's ( $\eta_B$ ) receivers, which use superconducting nanowire single-photon detectors. To calculate the  $\xi_\omega$ s, we assume that the measured  $V_{\text{FI}}$  values are their ideal values—93.25% for  $T_f = 16\delta T$  and 98.27% for  $T_f = 32\delta T$ —multiplied by 0.995. (These  $V_{\text{FI}}$  values are achievable; see [32] in which a 99.6% fringe

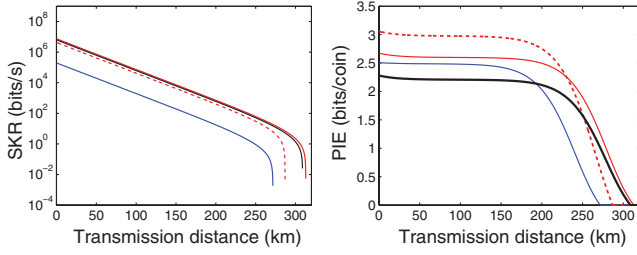


FIG. 2 (color). (Left panel) Alice and Bob’s SKR versus transmission distance. (Right panel) Alice and Bob’s PIE versus transmission distance. Both assume the following values. Entangled-pair flux: 0.01 pairs/frame; detector timing jitter  $\delta T = 30$  ps;  $B_{PM} = 200$  GHz;  $\Delta T/\sqrt{2} = T_g = 3.6\delta T$ ;  $\Delta\Omega/2\pi = 5$  GHz;  $\beta_2\Delta\Omega = \sqrt{2}T_g$ ;  $q = 0.5$ ;  $\beta = 0.9$ ;  $n_R = 8$ ; dark-count rate =  $10^3$ /sec; and fiber loss = 0.2 dB/km. Solid curves:  $T_f = 16\delta T$  and  $\xi_\omega = 0.22$ . Dashed curves:  $T_f = 32\delta T$  and  $\xi_\omega = 1.01$ . Blue curves:  $\eta_A = \eta_B = 15\%$ . Red and black curves:  $\eta_A = \eta_B = 90\%$ . Red and blue curves:  $\xi_t = 41.5$ . Black curves:  $\xi_t = 400$ .

visibility was reported.) For the red and blue curves, we calculate the  $\xi_t$ s by assuming that the measured  $V_{CFIs}$  are their ideal values—99.96% for both  $T_f = 16\delta T$  and  $T_f = 32\delta T$ —multiplied by 0.995. For the black curve,  $\xi_t$  represents jitter-limited raw arrival-time measurements. We see that QKD is possible out to 200 km when Alice and Bob have receivers with 15% system efficiency. Going to 90% system efficiency allows QKD out to 300 km and increases the SKR by nearly 2 orders of magnitude.

There is an important point to make about the SKR curves associated with the two  $\xi_t$  values we have employed. Constraining Eve to  $\xi_t = 41.5$  requires the use of a conjugate-Franson interferometer because jitter-limited raw arrival-time measurements cannot measure finer than  $\xi_t = 400$  with our system parameters. Surprisingly,  $\xi_t = 400$  still yields a positive SKR. This is because eavesdropping in one basis disturbs correlation in the conjugate basis. In our protocol, Alice and Bob generate key from the time basis, so degradation in the timing correlation does not increase Eve’s Holevo information, although it slightly reduces Alice and Bob’s mutual information and hence their SKR.

The PIE is defined to be the number of secure-key bits per photon coincidence in the key-generation phase,  $PIE = SKR \times 3T_f/qp_r$ . The right panel of Fig. 2 plots PIE versus transmission distance. It shows that Alice and Bob achieve  $PIE \geq 2$  secure-key bits per coincidence in the key-generation phase out to 200 km when their receivers have a 15% system efficiency.

Our protocol sacrifices potential SKR when detector timing jitter,  $\delta T$ , exceeds the SPDC source’s correlation time,  $\sigma_{cor}$ ; i.e.,  $I(A; B)$  cannot approach the ultimate limit of  $\log_2(\sigma_{coh}/\sigma_{cor})$  bits per coincidence that is set by the source’s Schmidt number. That limit can be achieved with DWDM that makes the two-photon correlation time in each

DWDM channel comparable to the detector timing jitter [19] and deriving key from time-frequency coincidences. In this case, the conjugate-Franson interferometer becomes crucial because part of the secure key information is obtained by frequency measurements. Nevertheless, the TFCM is still sufficient to bound Eve’s Holevo information.

Before concluding, it behooves us to compare our security predictions with the individual-attack results reported in Brougham *et al.* [20]. The comparison is not entirely straightforward because those authors considered a time-binned version of time-energy entanglement HDQKD with no multiple-pair emissions or dark counts, whereas our protocol operates in continuous time and includes both of those effects. Consider the 1024-bin example from [20], in which Eve obtains 6 of 10 bits when the Franson interferometer’s fringe visibility is 99.2% and 5 bits when that visibility is 99.8%. To compare our results with those, we set  $T_f = 1024\sqrt{2}\delta T$  so that Alice and Bob’s mutual information equals 10 bits per coincidence in the presence of  $\delta T$  timing jitter when there are neither dark counts nor multiple-pair emissions. Under these conditions, our security analysis sets upper bounds of 6.07 and 5.83 bits on Eve’s Holevo information for 99.2% and 99.8% Franson interferometer visibility, respectively.

In summary, we adapted the Gaussian-state security analysis for CVQKD to our time-energy entanglement HDQKD protocol. We showed that a Franson interferometer’s fringe visibility suffices against arbitrary collective attacks when that measurement is used in conjunction with decoy states, which allow the fraction of single-pair SPDC frames to be estimated. Adding a conjugate-Franson interferometer to the system enables tighter constraints on the TFCM, leading to a higher SKR. Our protocol promises QKD over 200 km and multiple secure bits per coincidence.

We thank T. Zhong for valuable discussions. This work was supported by the DARPA Information in a Photon Program through Army Research Office Grant No. W911NF-10-1-0416.

\*zszhang@mit.edu

- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [2] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, *Nature (London)* **421**, 238 (2003).
- [3] J. Lodewyck *et al.*, *Phys. Rev. A* **76**, 042305 (2007).
- [4] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
- [5] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [6] Q. D. Xuan, Z. Zhang, and P. L. Voss, *Opt. Express* **17**, 24244 (2009).

- [7] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, *Nat. Photonics* **7**, 378 (2013).
- [8] X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [9] H.-K. Lo, X. F. Ma, and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [10] T. Schmitt-Manderbach *et al.*, *Phys. Rev. Lett.* **98**, 010504 (2007).
- [11] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, *Phys. Rev. Lett.* **98**, 010503 (2007).
- [12] L. Zhang, C. Silberhorn, and I. A. Walmsley, *Phys. Rev. Lett.* **100**, 110504 (2008).
- [13] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Phys. Rev. Lett.* **84**, 4737 (2000).
- [14] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, *Phys. Rev. Lett.* **98**, 060503 (2007).
- [15] J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith, *Opt. Express* **21**, 15959 (2013).
- [16] M. Navascués, F. Grosshans, and A. Acín, *Phys. Rev. Lett.* **97**, 190502 (2006).
- [17] R. García-Patrón and N. J. Cerf, *Phys. Rev. Lett.* **97**, 190503 (2006).
- [18] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, *Phys. Rev. A* **87**, 062322 (2013).
- [19] J. Mower, F. N. C. Wong, J. H. Shapiro, and D. Englund, [arXiv:1110.4867](https://arxiv.org/abs/1110.4867).
- [20] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, *J. Phys. B* **46**, 104010 (2013).
- [21] A similar interferometer was suggested in W. Grice *et al.*, *Digest of Frontiers in Optics 2010* (Optical Society of America, Washington, DC, 2010), paper FTuG3.
- [22] We take  $T_f$  to be the full-width-at-half-maximum coherence time of the SPDC source and put  $T_f$ -second-long buffer intervals on both sides of each frame to minimize the likelihood of more than one pair per frame being emitted.
- There will be many empty frames because the average number of pairs per frame will be much smaller than one.
- [23] The SPDC source's pair flux will be kept well below one pair per  $T_f$ -sec frame. Nevertheless, security demands that multiple-pair frames be accounted for. Later we describe how that is done via decoy states.
- [24] Alice and Bob's clocks must be synchronized to better than their detectors' timing jitters, but this is not problematic. Synchronization of remote optical clocks is an active research area that focuses on femtosecond and subfemtosecond precision, which is far better than the  $\sim 10$  ps we require [see, e.g., J. Kim, J. A. Cox, J. Chen, and F. X. Kärtner, *Nat. Photonics* **2**, 733 (2008); K. Predehl *et al.*, *Science* **336**, 441 (2012)]. Furthermore, although Eve's manipulation of Alice and Bob's timing channel could degrade their Shannon information, any information it affords Eve about their raw key is still bounded above by  $\chi_{\xi, \xi'}^{UB}(A; E)$ .
- [25] P. B. Dixon, J. H. Shapiro, and F. N. C. Wong, *Opt. Express* **21**, 5879 (2013).
- [26] See the Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.112.120506> for the proof.
- [27] M. M. Wolf, G. Giedke, and J. I. Cirac, *Phys. Rev. Lett.* **96**, 080502 (2006).
- [28] J. D. Franson, *Phys. Rev. Lett.* **62**, 2205 (1989).
- [29] The various time intervals associated with our protocol satisfy  $T_f = \sqrt{8 \ln(2)} \sigma_{\text{coh}} > \Delta T > T_g > \delta T \gg \sigma_{\text{cor}}$ .
- [30] Alice and Bob use all frames in which they have coincidences. The Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.112.120506> explains how they deal with frames that contain multiple coincidences.
- [31] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Quantum Inf. Comput.* **4**, 325 (2004).
- [32] T. Zhong and F. N. C. Wong, *Phys. Rev. A* **88**, 020103(R) (2013).