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.
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 multipletime-energy entanglement 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, frequencydegenerate SPDC source that, within a time frame of duration of $T_f$ sec, emits a single photon pair in the state [22]

$$|\psi_m\rangle_{SI} \propto \int dt_S \int dt_I e^{-\left(t_s-t_m^2\right)/4\sigma_{coh}^2} e^{-i\omega t_I} \langle t_S | t_I \rangle_f$$

(1)

for some integer $m$. In this expression, $\omega_p$ is the pump frequency; $|t_S\rangle_f$ ($|t_I\rangle_f$) represents a single photon of the signal (idler) at time $t_S$ ($t_I$); $t_i \equiv (t_S + t_I)/2$; $t_s \equiv t_S - t_I$; the root-mean-square coherence time $\sigma_{coh} = T_f/\sqrt{8 \ln(2)}$ ~ nsec is set by the pump pulse’s duration; and the root-mean-square correlation time $\sigma_{cor} = T_f/\sqrt{2 \ln(2)/2\pi B_{PM}}$ ~ psec is set by the reciprocal of the full-width at half-maximum (FWHM) phase-matching frequency; $\Delta$ is an oft-used approximation for the postselected biphoton pair state, the mean value of $\langle \hat{O} \rangle_{SI}$, for a single-pair state, the mean value of $\langle \hat{O} \rangle$ is $m = \langle \hat{O} \rangle$, and the TFCM is $\Gamma = \langle (\Delta \hat{O} \Delta \hat{O}^\dagger + H.c.)/2 \rangle$, 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 $\chi(\xi) = \langle e^{i\xi^\dagger \hat{O}} \rangle$. Given the covariance matrix $\Gamma$, the Gaussian state with $\chi(\xi) = e^{i\xi^\dagger \mathbf{m} - \xi^\dagger \xi / 2}$ yields an m-independent upper bound on Eve’s Holevo information [16,17,27] when the SPDC source emits a single-pair state.

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:

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

(2a)

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

(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, $[\hat{E}_J(t), \hat{E}_K^\dagger(u)] = \delta_{JK}(t-u)$, 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,

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

(3a)

$$\hat{\omega}_J(t) = \int \frac{d\omega}{2\pi} \omega \hat{A}_J(\omega),$$

(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 $[\hat{\omega}_J, \hat{t}_K] = i\epsilon_{JK}$ [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 $m = \langle \hat{O} \rangle$, and the TFCM is $\Gamma = \langle (\Delta \hat{O} \Delta \hat{O}^\dagger + H.c.)/2 \rangle$, 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 $\chi(\xi) = \langle e^{i\xi^\dagger \hat{O}} \rangle$. Given the covariance matrix $\Gamma$, the Gaussian state with $\chi(\xi) = e^{i\xi^\dagger \mathbf{m} - \xi^\dagger \xi / 2}$ yields an 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
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 $\sigma_{cor}$, 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 $V_{\text{FI}}(\Delta T) = [P_{C_M}(0) - P_{C_M}(\pi)]/[P_{C_M}(0) + P_{C_M}(\pi)]$, where $P_{C_M}(\phi_S + \phi_I)$ is Alice and Bob’s coincidence probability, be the 0-π fringe visibility when the Franson interferometer has delay $\Delta T$. Then the variance of the signal-idler frequency difference satisfies

$$
\langle (\Delta \omega_S - \Delta \omega_I)^2 \rangle \leq \frac{2[1 - V_{\text{FI}}(\Delta T)]}{\Delta T^2} + \frac{\langle (\Delta \omega_S - \Delta \omega_I)^4 \rangle}{12} \Delta T^2,
$$

(4)

where $\Delta \omega_S$ ($\Delta \omega_I$) 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 $V_{\text{CFI}}(\Delta \Omega) = [P_{C_M} (0) - P_{C_M} (\pi)]/[P_{C_M} (0) + P_{C_M} (\pi)]$, where $P_{C_M} (\phi_S + \phi_I)$ is Alice and Bob’s coincidence probability, be the 0-π fringe visibility when the conjugate-Franson interferometer has frequency shift $\Delta \Omega$. Then the variance of the signal-idler arrival-time difference satisfies

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

(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, $\langle \Delta \omega_S^2 \rangle$ and $\langle \Delta \omega_I^2 \rangle$ 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 $\langle \Delta t_S \Delta t_I \rangle \neq 0$, 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 $1 + \xi_S \equiv \langle (\Delta \omega_S - \Delta \omega_I)^2 \rangle / \langle (\Delta \omega_S - \Delta \omega_I)^2 \rangle$ and $1 + \xi_I \equiv \langle (\Delta \omega_I - \Delta \omega_S)^2 \rangle / \langle (\Delta \omega_I - \Delta \omega_S)^2 \rangle$, where $\langle (\Delta \omega_S - \Delta \omega_I)^2 \rangle$ and $\langle (\Delta \omega_I - \Delta \omega_S)^2 \rangle$ 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 $[\hat{\omega}_S, \hat{\omega}_I] = i \epsilon_S \hat{\omega}_I$. For each TFCM $\Gamma \in \mathcal{M}$, the Gaussian state $\chi(\xi) = e^{-\xi^2/2}$ affords Eve the maximum Holevo information [16,17,27]. Using $\chi_f^E(A; E)$ to denote that Holevo information, our partial information about $\Gamma$ gives us the upper bound $\chi_f^\text{UB}_{\text{SKR}}(A; E) = \text{sup}_{\Gamma \in \mathcal{M}} [\chi^E_f (A; E)]$ 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]:

$$
\text{SKR} \geq \frac{q p_r}{3 T_f} [\beta I(A; B) - (1 - F) n_R - F \chi_f^\text{UB}_{\text{SKR}} (A; E)].
$$

(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 ($n_A$) and Bob’s ($n_B$) receivers, which use superconducting nanowire single-photon detectors. To calculate the $s_{\omega_S}$, we assume that the measured $V_{\text{FI}}$ values are their ideal values—93.25% for $T_f = 168 T$ and 98.27% for $T_f = 32 T$—multiplied by 0.995. (These $V_{\text{FI}}$ values are achievable; see [32] in which a 99.6% fringe
In our protocol, Alice and Bob generate key from the time a single pulse arrives in one basis disturbs correlation in the conjugate basis. Entangled-pair flux: $(\gamma)_{\text{max}}$ = 0.01 pairs/frame; detector timing jitter $\Delta T = 30$ ps; $\beta_{\text{PM}}$ = 200 GHz; $\Delta T/\sqrt{2} = T_f = 3.68$ T; $\Delta T/2\pi = 5$ GHz; $g = 0.5$; $\beta = 0.9$; $n_\text{d} = 8$; dark-count rate = $10^{-4}$ sec; and fiber loss = 0.2 dB/km. Solid curves: $T_f = 16\Delta T$ and $\xi_\text{DF} = 0.22$. Dashed curves: $T_f = 32\Delta T$ and $\xi_\text{DF} = 1.01$. Blue curves: $\eta = \eta_f = 95\%$. Red and blue curves: $\eta = 41.5$. Black curves: $\xi_f = 400$.

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 $T_f = 1024\Delta T$ 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.
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 $\chi_{UB}^{\xi}$. 


[29] The various time intervals associated with our protocol satisfy $T_f = \sqrt{8 \ln(2)} \sigma_{coh} > \Delta T > T_g > \delta T \gg \sigma_{cor}$.

