Finite-key analysis for time-energy high-dimensional quantum key distribution

Murphy Yuezhen Niu,[1,2,*] Feihu Xu,[1] Jeffrey H. Shapiro,[1] and Fabian Furrer[3]
[1]*Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*
[2]*Department of Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[3]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
(Received 27 June 2016; published 18 November 2016)

Time-energy high-dimensional quantum key distribution (HD-QKD) leverages the high-dimensional nature of time-energy entangled biphotons and the loss tolerance of single-photon detection to achieve long-distance key distribution with high photon information efficiency. To date, the general-attack security of HD-QKD has only been proven in the asymptotic regime, while HD-QKD's finite-key security has only been established for a limited set of attacks. Here we fill this gap by providing a rigorous HD-QKD security proof for general attacks in the finite-key regime. Our proof relies on an entropic uncertainty relation that we derive for time and conjugate-time measurements that use dispersive optics, and our analysis includes an efficient decoy-state protocol in its parameter estimation. We present numerically evaluated secret-key rates illustrating the feasibility of secure and composable HD-QKD over metropolitan-area distances when the system is subjected to the most powerful eavesdropping attack.

DOI: 10.1103/PhysRevA.94.052323

I. INTRODUCTION

Quantum key distribution (QKD) enables secure communication based on fundamental laws of quantum physics [1,2], as opposed to the security that is presumed from computational complexity in conventional public-key cryptography. Current work on QKD focuses on patching security holes in practical implementations, increasing secret-key rates and secure-transmission distances, and unifying the understanding of the many different protocols [3]. Existing QKD protocols can be divided into two major categories: discrete-variable (DV) [1,4–6] and continuous-variable (CV) [7] QKD. The predominant discrete-variable QKD (DV-QKD) is more robust to loss than continuous-variable QKD (CV-QKD) and thus offers longer secure-transmission distance [8–11]. CV-QKD, on the other hand, offers higher photon information efficiency (PIE) than DV-QKD, and thus potentially higher key rates at short distances [12].

High-dimensional QKD (HD-QKD) exploits the best features of DV and CV protocols to simultaneously achieve high PIE and long secure-transmission distance [13–19]. One of the most appealing candidates for implementation is time-energy HD-QKD [17,20–25]. It generates keys by using the detection times of time-energy entangled photon pairs, whose continuous nature permits encoding of extremely large alphabets. The security analysis of time-energy HD-QKD has been improving ever since the protocol was proposed [20–25]. Nevertheless, a rigorous security proof that satisfies the composability condition [26] and takes full account of the finite-size effects against *general* attacks (the most powerful eavesdropping attack) has been missing. For this reason, the feasibility of secure, metropolitan-area, time-energy HD-QKD using a reasonable time interval for signal transmission has yet to be fully established.

In this paper we make three contributions. First, we derive an entropic uncertainty relation between time and conjugate-time measurements that are made via nonlocal dispersion cancellation. Second, we use the uncertainty principle to prove the composable security of time-energy HD-QKD in the finite-key regime against general (coherent) attacks. Third, we find the dispersion strength for the conjugate-time basis transformation [21] that maximizes HD-QKD's secret-key rate.

The entropic uncertainty relation is indispensable for analyzing general attacks against time-energy HD-QKD. Although an entropic uncertainty relation for field quadratures has been developed [27] and applied recently to CV-QKD security analysis [28], it cannot be directly applied to time-energy HD-QKD because time and conjugate-time measurements are not described by maximally incompatible operators [29], such as position and momentum. To overcome this challenge, we construct an entropic uncertainty relation specifically for time and conjugate-time measurements. Because entropic uncertainty relations figure prominently in quantum metrology [30], quantum randomness certification [31,32], entanglement witnesses [33,34], two-party cryptography [35,36], QKD security analysis [11,37–41], and other applications [42], we expect that our uncertainty relation for time and conjugate-time measurements may have uses well beyond what will be presented below.

The secret-key-rate formula we obtain by using our entropic uncertainty relation allows us to verify important advantages that HD-QKD offers over alternative protocols. In particular, HD-QKD offers higher PIE (3.3 bits/photon) than both CV-QKD (0.5 bits/photon [43]) and DV-QKD (0.1 bits/photon [44]), thus ensuring higher secret-key rates under photon-starved conditions, in which the photon-detection rate is much lower than the photon-generation rate because of the loss incurred in long-distance propagation and the relatively long recovery times of available single-photon detectors. Also, HD-QKD offers a longer maximum secure-transmission distance for general attacks (e.g., 160 km for a 30 min. session using the system parameters given below in Sec. V) as compared with that for CV-QKD [28,45], even in the case of reverse reconciliation (e.g., 16 km [43]). Furthermore, because our entropic uncertainty relation is parametrized by the

*Corresponding author: yzniu@mit.edu

HD-QKD protocol's time-bin duration, δ, and conjugate-time basis transformation's group-velocity dispersion (GVD) coefficient β_D, optimizing the β_D value can increase HD-QKD's secure-transmission distance to 210 km—and provide a 17 Mbit/s expected secret-key rate at zero distance—without resorting to a higher clock rate.

The remainder of the paper is organized as follows: The HD-QKD protocol is described briefly in Sec. II, with a detailed account—including its use of decoy states for channel estimation—appearing in Appendix A. The security analysis for coherent attacks in the finite-key regime is contained in Sec. III. Its security proof relies on the entropic uncertainty relation that is derived in Sec. IV. (For comparison, the entropic uncertainty relation obtained from the conventional dilation assumption is presented in Appendix B.) A numerical evaluation of HD-QKD's secret-key rate and PIE follows in Sec. V, which illustrates the advantages offered by this protocol, and Sec. VI provides a summarizing discussion.

II. PROTOCOL

Time-energy HD-QKD that relies on dispersive optics works as follows [21,22]: In each round, Alice generates a time-energy entangled photon pair from a spontaneous parametric down-conversion (SPDC) source, sends one photon to Bob and retains the other. Alice and Bob choose independently and at random to measure their photons in either the time basis T or the conjugate-time basis W, where the latter is a dispersive-optics proxy for a frequency measurement. Alice and Bob discretize their outcomes into time bins of duration δ. The process repeats for N rounds until Alice and Bob obtain enough detections to begin postprocessing. At the end of all measurements, the two sides reveal their basis choices and discard all data measured with mismatched bases. Secret keys are extracted from the events in which Alice and Bob both chose the T basis, while the W basis outcomes are publicly announced for parameter estimation. By using the decoy-state method [4–6,24,44], Alice and Bob estimate the number of detections in T that were generated from single-pair SPDC emissions, and the corresponding L_1 code distance in the W basis; see Appendix C for the details. They abort the protocol if this distance exceeds a predetermined value d_0 (see Appendix D). Otherwise, they perform error correction and privacy amplification to generate the secret key.

The conjugate-time measurement for the W basis is realized by direct detection at Alice and Bob's terminals after they have sent their photons through normal and anomalous GVD elements, respectively [21,22]. These GVD elements' dispersion coefficients have equal magnitudes (and opposite signs) so their effects are nonlocally canceled [46]. As a result, Alice and Bob's W-basis measurements are as strongly correlated as those in the T basis, i.e., the dispersion transformation allows them to perform a spectral-correlation measurement with only time-resolved single-photon detection [21,22].

III. SECURITY ANALYSIS

A. Security definition

Given that the parameter-estimation test is passed with probability p_{pass}, Alice and Bob end up with final keys that are classical random vectors, $\mathbf{K}_{\mathrm{A}}$ and $\mathbf{K}_{\mathrm{B}}$, which might be correlated with a quantum system $\mathbf{E}$ held by Eve. Mathematically, this situation corresponds to a classical-quantum state $\rho_{\mathrm{K_A E}} = \frac{1}{|\mathcal{S}|}\sum_s |s\rangle\langle s| \otimes \rho_{\mathrm{E}}^s$, where $\{|s\rangle\}$ denotes an orthonormal basis for Alice's dimension-$|\mathcal{S}|$ key space, and the subscript E indicates Eve's quantum state. We characterize a QKD protocol by its correctness and secrecy. For that we use a notion of security based on the approach developed in Ref. [26]. A protocol is called ϵ_c-*correct* if the probability that $\mathbf{K}_{\mathrm{A}}$ differs from $\mathbf{K}_{\mathrm{B}}$ is smaller than ϵ_c. We say that a protocol is ϵ_s-*secret* if the state $\rho_{\mathrm{K_A E}}$ is ϵ_s-close to the ideal situation described by the tensor product of uniformly distributed keys on Alice's side and Eve's quantum state, $U_{\mathrm{K_A}} \otimes \rho_{\mathrm{E}}$, such that $p_{\mathrm{pass}}\|\rho_{\mathrm{K_A E}} - U_{\mathrm{K_A}} \otimes \rho_{\mathrm{E}}\|_1 \leqslant \epsilon_s$. A QKD protocol is then said to be ϵ-secure if it is both ϵ_c-correct and ϵ_s-secret, with $\epsilon_c + \epsilon_s \leqslant \epsilon$. Our security definitions ensure that the protocol remains secure in combination with any other protocol, i.e., the protocol is secure in the universally composable framework [26].

B. Assumptions

Before deriving our lower bound on secret-key length, we first specify the assumptions that will be employed: (1) Alice's SPDC source produces independent, identically distributed biphotons whose correlation time and coherence time are well characterized. (2) For each pump pulse, Alice is able to randomly set her SPDC source's biphoton intensity (mean photon-pairs generated per pump pulse) to be either μ_1, μ_2, or μ_3 with probabilities p_{μ_1}, p_{μ_2}, and p_{μ_3}. (3) Alice and Bob's laboratories are secure, i.e., free from any information leakage. (4) Alice and Bob independently and randomly choose between measuring in the time and conjugate-time bases with probabilities q and $1-q$. Most of these assumptions are already made in conventional CV-QKD and DV-QKD security analysis.

C. Security proof

To characterize information leakage in a realistic quantum communication system with a finite number of communication rounds, we use smooth min-entropy instead of von Neumann entropy [26,47]. Discretizing Alice and Bob's photon-detection times to time bins of duration δ results in data vectors comprised of integers representing bin numbers. In particular, with random vectors $\mathbf{X}_{\mathrm{A}}$ and $\mathbf{X}_{\mathrm{B}}$ denoting Alice and Bob's raw keys from her μ_1-intensity transmissions, Eve's uncertainty (lack of knowledge) is measured by her difficulty in guessing Alice's raw key $\mathbf{X}_{\mathrm{A}}$, i.e., the conditional smooth min-entropy $H_{\min}(\mathbf{X}_{\mathrm{A}}|\mathbf{E})$, where $\mathbf{E}$ denotes Eve's quantum state. $H_{\min}(\mathbf{X}_{\mathrm{A}}|\mathbf{E})$ quantifies the randomness that can be extracted from $\mathbf{X}_{\mathrm{A}}$, which is statistically independent of $\mathbf{E}$ [26,47] with error probability ϵ.

The secret-key length ℓ that is ϵ_s-secret is given by [26]

$$\ell \geqslant H_{\min}^{\epsilon}(\mathbf{X}_{\mathrm{A}}|\mathbf{E}) - \mathrm{leak}_{\mathrm{EC}} + \log_2\left(\epsilon_s^2\epsilon_c\right). \tag{1}$$

Here, $\mathrm{leak}_{\mathrm{EC}}$ is the information leaked to Eve during error correction, which can be directly measured during that correction process, and $H_{\min}^{\epsilon}(\mathbf{X}_{\mathrm{A}}|\mathbf{E})$ is the smooth min-entropy maximized over states that are ϵ close to the classical-quantum

state $\rho_{\mathrm{X_A E}} = \frac{1}{|\mathcal{S}|}\sum_s |s\rangle\langle s| \otimes \rho_{\mathrm{E}}^s$. The correctness of the protocol is guaranteed by the key-verification step, which uses a two-universal hash function to ensure that Bob's corrected key differs from Alice's with probability at most ϵ_{hash}, implying that the protocol is ϵ_c-correct with $\epsilon_c = \epsilon_{\mathrm{hash}}$.

The essential insight is that Eve's information about the μ_1-intensity, T-basis detection times can be bounded by using the complementary W-basis measurements. In particular, if Alice and Bob's W-basis measurements are highly correlated, then Eve's knowledge about the outcome of their T-basis measurements is nearly zero, because the two observables are *incompatible*.

Let $\mathbf{Y}_{\mathrm{A}}$ and $\mathbf{Y}_{\mathrm{B}}$ be Alice and Bob's random vectors of μ_1-intensity conjugate-time measurement outcomes. Without loss of generality we set the length of these four classical strings to be equal: $|\mathbf{X}_{\mathrm{A}}| = |\mathbf{X}_{\mathrm{B}}| = |\mathbf{Y}_{\mathrm{A}}| = |\mathbf{Y}_{\mathrm{B}}| = n_{\mathsf{T},\mu_1}$. Then, from Refs. [27,28,38,39], we have the uncertainty relation

$$H_{\min}^{\epsilon}(\mathbf{X}_{\mathrm{A}}|\mathbf{E}) + H_{\max}^{\epsilon}(\mathbf{Y}_{\mathrm{A}}|\mathbf{Y}_{\mathrm{B}}) \geqslant -n_{\mathsf{T},\mu_1}\log_2[c(\delta,\beta_D)], \quad (2)$$

where the smooth max-entropy $H_{\max}^{\epsilon}(\mathbf{Y}_{\mathrm{A}}|\mathbf{Y}_{\mathrm{B}})$ measures the amount of information needed to reconstruct $\mathbf{Y}_{\mathrm{A}}$ given $\mathbf{Y}_{\mathrm{B}}$ with error probability bounded above by ϵ, and $c(\delta,\beta_D)$ is the overlap between the time and conjugate-time measurement operators, which depends on δ, the time-bin duration, and β_D, the magnitude of the GVD elements' dispersion coefficient.

With $\mathbf{\Pi} = \{\Pi_n\}$ and $\mathbf{\Pi'} = \{\Pi'_m\}$ being an arbitrary pair of positive operator-valued measurements (POVMs), their overlap $c(\mathbf{\Pi},\mathbf{\Pi'}) = \sup_{n,m} \|\sqrt{\Pi_n}\sqrt{\Pi'_m}\|^2$ quantifies their incompatibility, i.e., lower values of $c(\mathbf{\Pi},\mathbf{\Pi'})$ mean increased incompatibility. Our uncertainty bound involves the overlap-quantified incompatibility between the time and conjugate-time POVMs whose outcomes are used for key generation and parameter estimation, respectively. Typically (see Sec. V), lower $c(\delta,\beta_D)$ values allow longer secret keys to be extracted. Our tripartite entropic uncertainty relation and the security analysis that follows therefrom are adapted from CV-QKD's finite-key analysis [28], an approach that works for all QKD protocols that rely on a pair of incompatible continuous measurements for key generation and parameter estimation. In our case, the security analysis requires accounting for our use of discretized time and conjugate-time measurements that are obtained from underlying continuous POVMs. Note that the different measurement operators employed in different QKD protocols lead to different overlap behavior in their entropic uncertainty relations.

The major difficulty in determining $c(\delta,\beta_D)$ for our protocol comes from the absence of negative energy for electromagnetic-field modes, which implies that, under the conventional commutation relation, the time-measurement operator cannot be projective [48,49], thus preventing existing results [50] from being applied to the time and conjugate-time POVMs. We can, however, dilate the time and conjugate-time operators by forsaking the constraint of positive frequency on photon-annihilation operators [51,52]. Such dilations are well justified for the quantum theory of coincidence measurement [46,53], because the negative frequency components do not contribute to detection outcomes. But, because we are not assured that the dilation-assumption $c(\delta,\beta_D)$ will suffice for our security proof, we derive the following entropic uncertainty relation for time and conjugate-time measurements *without* dilation in Sec. IV:

$$H_{\min}^{\epsilon}(\mathbf{X}_{\mathrm{A}}|\mathbf{E}) + H_{\max}^{\epsilon}(\mathbf{Y}_{\mathrm{A}}|\mathbf{Y}_{\mathrm{B}}) \geqslant -n_{\mathsf{T},\mu_1}\log_2\left(\frac{1.37\delta^2}{2\pi^2\beta_D}\right). \quad (3)$$

Next, we use a generalized chain-rule result [54] to decompose $\mathbf{X}_{\mathrm{A}}$ into $\mathbf{X}_{\mathrm{A}}^0\mathbf{X}_{\mathrm{A}}^1\mathbf{X}_{\mathrm{A}}^{\mathrm{m}}$, which is a concatenation of the raw keys arising from vacuum, single-pair, and multipair coincidences. Neglecting the multipair contribution, we have $n_{\mathsf{T},\mu_1} \geqslant (\underline{n_{\mathsf{T},0}} + \underline{n_{\mathsf{T},1}})$, with $\underline{n_{\mathsf{T},0}}$ and $\underline{n_{\mathsf{T},1}}$ being lower bounds on $n_{\mathsf{T},0}$ and $n_{\mathsf{T},1}$, the coincidence-count contributions from vacuum and single-pair events, respectively, when Alice's SPDC intensity is μ_1 (see Appendix C). We then have the following lower bound on the smooth min-entropy [44]:

$$H_{\min}^{\epsilon}(\mathbf{X}_{\mathrm{A}}|\mathbf{E}) \geqslant -(\underline{n_{\mathsf{T},0}} + \underline{n_{\mathsf{T},1}}\log_2[c(\delta,\beta_D)] - H_{\max}^{\epsilon}(\mathbf{Y}_{\mathrm{A}}|\mathbf{Y}_{\mathrm{B}}). \quad (4)$$

By using a result from CV-QKD [28], we get the following upper bound on the smooth max-entropy:

$$H_{\max}^{\epsilon}(\mathbf{Y}_{\mathrm{A}}|\mathbf{Y}_{\mathrm{B}}) \leqslant n_{\mathsf{T},\mu_1}\log_2[\gamma(d_0+\Delta)], \quad (5)$$

where $\gamma(x)$ obeys

$$\gamma(x) = (x+\sqrt{1+x^2})\left(\frac{x}{\sqrt{1+x^2}-1}\right)^x. \quad (6)$$

The Δ parameter is the statistical fluctuation that quantifies how well the data subset used for parameter estimation represents the entire dataset:

$$\Delta \approx \frac{T_f}{\delta}\sqrt{\frac{1}{q^2(1-q)^2\underline{n_{\mathsf{T},01}}}\ln\left[\frac{1}{\epsilon_s/4 - 2f(p_\alpha,\underline{n_{\mathsf{T},01}})}\right]}, \quad (7)$$

where $f(p_\alpha,\underline{n_{\mathsf{T},01}}) = \{2[1-(1-p_\alpha)^{\underline{n_{\mathsf{T},01}}}]\}^{1/2}$, p_α is the probability, for a given pump pulse, that Alice and Bob detect photons separated by more than a frame duration T_f, and $\underline{n_{\mathsf{T},01}} = \underline{n_{\mathsf{T},0}} + \underline{n_{\mathsf{T},1}}$.

Combining the preceding results, we obtain the following lower bound on the secret-key length:

$$\ell \geqslant -\underline{n_{\mathsf{T},01}}\log_2[c(\delta,\beta_D)] - n_{\mathsf{T},\mu_1}\log_2[\gamma(d_0+\Delta)] - \mathrm{leak}_{\mathrm{EC}} + \log_2\left(\epsilon_s^2\epsilon_c\right). \quad (8)$$

IV. TIME-CONJUGATE TIME ENTROPIC UNCERTAINTY RELATION

To justify Eq. (3), we only need to evaluate the overlap, $c(\delta,\beta_D)$, in Eq. (2) for the discretized single-photon time and conjugate-time measurement operators that derive from their continuous-time counterparts, $T(t)$ and $W(t)$, by coarse-graining to time bins of duration δ. Here, we omit polarization degrees of freedom because they do not affect the overlap. Our starting point is the infinite-dimensional version of the general uncertainty relation for smooth min-entropy and smooth max-entropy [38] that was derived in Ref. [27].

We use $|\omega\rangle = a^\dagger(\omega+\omega_0)|0\rangle$ to denote the single-photon state detuned by frequency ω from some fixed center frequency ω_0. (Later, this center frequency will be $\omega_P/2$, i.e., half the SPDC source's pump frequency.) This state satisfies

the orthonormality condition $\langle\omega_1|\omega_2\rangle = 2\pi\delta(\omega_1-\omega_2)$. The single-photon Hilbert space is simply $\mathcal{H} = L^2(\Omega)$, i.e., the space of square-integrable, complex-valued functions on the frequency-domain region $\omega \in \Omega \equiv [\omega_{\min},\infty)$, where the minimum detuning satisfies $\omega_{\min} \geqslant -\omega_0$. In particular, we associate a function $f \in L^2(\Omega)$ to the state

$$|f\rangle = \int_\Omega \frac{d\omega}{2\pi} f(\omega)|\omega\rangle, \tag{9}$$

so the inner product between two such states, $|f\rangle$ and $|g\rangle$, is $\langle f|g\rangle = \int_\Omega \frac{d\omega}{2\pi} f^*(\omega)g(\omega)$.

By using the above notation we have that the time-measurement operator $T(t)$ can be expressed as

$$T(t) = \int_\Omega \frac{d\omega_1}{2\pi}\int_\Omega \frac{d\omega_2}{2\pi} e^{i(\omega_1-\omega_2)t}|\omega_1\rangle\langle\omega_2| = |\phi_t\rangle\langle\phi_t|, \tag{10}$$

where $\phi_t(\omega) = e^{i\omega t}$. Similarly, we can write

$$\begin{aligned} W(t) &= \int_\Omega \frac{d\omega_1}{2\pi}\int_\Omega \frac{d\omega_2}{2\pi} e^{i(\omega_1-\omega_2)t} e^{i\beta_D(\omega_1^2-\omega_2^2)/4}|\omega_1\rangle\langle\omega_2| \\ &= |\psi_t\rangle\langle\psi_t|, \end{aligned} \tag{11}$$

where $\psi_t(\omega) = e^{i(\omega t+\beta_D\omega^2/4)}$. We then introduce partitions, $\{I_k\}$ and $\{J_k\}$, of the time and conjugate-time axes, from which we obtain the coarse-grained versions of $T(t)$ and $W(t)$; namely, the POVMs $T^\delta = \{T_k\}$ and $W^\delta = \{W_k\}$, where

$$T_k = \int_{I_k} dt\, T(t) \text{ and } W_k = \int_{J_k} dt\, W(t). \tag{12}$$

From Refs. [27,38] the overlap for these discrete POVMs satisfies

$$\begin{aligned} c(\delta,\beta_D) = \bar{c}(T^\delta,W^\delta) &= \sup_{k,l} \|\sqrt{T_k}\sqrt{W_l}\|^2 \\ &= \sup_{s,t} \|\sqrt{T^\delta(s)}\sqrt{W^\delta(t)}\|^2, \end{aligned} \tag{13}$$

where $T^\delta(s) = \int_s^{s+\delta} du\, T(u)$ and $W^\delta(t) = \int_t^{t+\delta} du\, W(u)$.

Because the $\{T_k\}$ and $\{W_k\}$ are not projective, it is difficult to evaluate Eq. (13) directly. Instead, we will use the approximation from Ref. [27], in which an uncertainty relation is derived in the continuous-time case. We take $\mathcal{T}$ and $\mathcal{W}$ to represent the continuous-time classical outcomes of the time and conjugate-time measurements, and $\mathcal{T}_\delta$ and $\mathcal{W}_\delta$ to be their discretized versions. From Ref. [27] we have that

$$H_{\min}(\mathcal{T}_\delta|\mathbf{E}) \geqslant h_{\min}(\mathcal{T}|\mathbf{E}) - \log_2(\delta), \tag{14}$$

$$H_{\max}(\mathcal{W}_\delta|\mathbf{B}) \geqslant h_{\max}(\mathcal{W}|\mathbf{B}) - \log_2(\delta), \tag{15}$$

where $h_{\min}(\mathcal{T}|\mathbf{E})$ and $h_{\max}(\mathcal{T}|\mathbf{B})$ are the differential min-entropy and differential max-entropy of the continuous-time outcome $\mathcal{T}$ conditioned on Eve's state $\mathbf{E}$ and Bob's state $\mathbf{B}$, respectively. We also know that these differential entropies satisfy [27]

$$h_{\min}(\mathcal{T}|\mathbf{E}) + h_{\max}(\mathcal{W}|\mathbf{B}) \geqslant -\log_2[\bar{c}_\infty(T,W)], \tag{16}$$

where

$$\bar{c}_\infty(T,W) = \liminf_{\delta\to 0}\left[\frac{\bar{c}(T^\delta,W^\delta)}{\delta^2}\right]. \tag{17}$$

Inequalities (14) and (15) yield the following uncertainty relation for coarse-grained measurements:

$$H_{\min}(\mathcal{T}_\delta|\mathbf{E}) + H_{\max}(\mathcal{W}_\delta|\mathbf{B}) \geqslant -\log_2[\bar{c}_\infty(T,W)\delta^2]. \tag{18}$$

We can find the overlap for the differential entropies via

$$\begin{aligned} \bar{c}_\infty(T,W) &= \liminf_{\delta\to 0}\left[\frac{\bar{c}(T^\delta,W^\delta)}{\delta^2}\right] \\ &= \sup_{s,t}\liminf_{\delta\to 0}\left[\frac{1}{\delta^2}\|\sqrt{T^\delta(s)}\sqrt{W^\delta(t)}\|^2\right] \\ &= \sup_{s,t}\liminf_{\delta\to 0}\left\|\sqrt{\frac{T^\delta(s)}{\delta}}\sqrt{\frac{W^\delta(t)}{\delta}}\right\|^2 \\ &= \sup_{s,t}\|\sqrt{T(s)}\sqrt{W(t)}\|^2, \end{aligned} \tag{19}$$

where we have used $\lim_{\delta\to 0}\frac{1}{\delta}\int_s^{s+\delta} dt\, T(t) = T(s)$ and similarly for W. Inserting the definitions of $T(s)$ and $W(t)$ from Eqs. (10) and (11), we obtain

$$\bar{c}_\infty(T,W) = \sup_{s,t}|\langle\phi_s|\psi_t\rangle|^2. \tag{20}$$

A simple calculation now gives us

$$\bar{c}_\infty(T,W) = \sup_{s,t}\left|\int_\Omega \frac{d\omega}{2\pi} e^{i\omega(t-s)}e^{-i\beta_D\omega^2/4}\right|^2. \tag{21}$$

For $\Omega = [\omega_{\min},\infty)$, performing the optimization with $\omega_{\min} \geqslant -\omega_0$ and $-\infty < t, s < \infty$ yields the maximum overlap

$$\bar{c}_\infty(T,W) \approx \frac{1.37}{2\pi^2\beta_D}. \tag{22}$$

Inserting the above result into Eq. (18) gives us the overlap for the discrete measurements used in the secret-key length bound

$$c(\delta,\beta_D) \approx \frac{1.37\delta^2}{2\pi^2\beta_D}. \tag{23}$$

This uncertainty bound is *tighter* than the $c(\delta,\beta_D) = \delta^2/2\pi^2\beta_D$ overlap obtained in Appendix B when dilation is used by taking $\Omega = (-\infty,\infty)$ so that the $T(t)$ and $W(t)$ operators become projective and maximally incompatible, i.e., analogous to position and momentum. These overlap results showcase the subtle difference between the entropic uncertainty relation of quantum time and conjugate-time measurements and that of the homodyne measurements from Ref. [28]. Indeed, the factor of 1.37 in Eq. (23) is crucial for the general-attack security of HD-QKD, because a secret-key length that presumed the dilation result for the overlap would be insecure.

V. PERFORMANCE EXAMPLE

Based on the secret-key rate formula (8), we numerically evaluated the performance of the time-energy HD-QKD protocol in the finite-key regime under general attacks. See Table I for the parameters that were assumed. The calculated secret-key rates and PIEs at different lengths of standard telecom fiber are shown in Figs. 1(a) and 1(b). We see that HD-QKD can easily tolerate a 100 km standard fiber within a reasonable running time for transmission (e.g., 10 min.).

TABLE I. List of parameters, mostly from Ref. [17], used in numerical evaluation: detection efficiency η_d, dark-count rate Y_0, detector time jitter σ_{jit} [55], fiber-loss coefficient α, GVD coefficient β_D, system clock rate R_{rep}, biphoton correlation time σ_{cor}, pump coherence time $\sigma_{\text{coh}} \approx T_f$, time-bin duration δ, reconciliation (error-correction) efficiency β_e, probability of choosing the time basis q, and overall security bound ϵ.

η_d	Y_0	σ_{jit}	α	β_D	R_{rep}
90%	1 kHz	18 ps	0.21 dB/km	2×10^4 ps^2	55.6 MHz[a]
σ_{cor}	σ_{coh}	δ	β_e	q	ϵ
2 ps	6 ns	20 ps	0.91	0.9	10^{-10}

[a]The clock rate is assumed to be the inverse of three times the pump coherence time.

TABLE II. Performance comparison for different protocols with finite-key analysis against general attacks. The first and second rows compare the PIEs and the secret-key rates at 0 km fiber length. The third row compares the maximum secure-transmission distance. All three protocols are evaluated at the block size of 10^9, equivalent to 1 min. running time in HD-QKD with the parameters specified in Table I.

Parameters	BB84 [44]	CV-QKD [43]	HD-QKD
PIE (bits/photon)[a]	≈0.1	0.5	3.3
Key rate at 0 dist. (bits/s)	≈8 M[b]	≈6 M[c]	8.6 M
Max dist. (km)	170	16	96

[a]PIE in HD-QKD is defined as secret bits per single photon detection by Bob given that Alice has made a detection in the same basis, PIE in BB84 is defined as secret bits per use [56], and PIE in CV-QKD is defined as secret bits per signal [43].
[b]Assumes a decoy-state BB84 system with a 1 GHz clock rate [56].
[c]Assumes a CV-QKD system with the same 55.6 MHz clock rate as HD-QKD.

This secure-transmission distance significantly exceeds that of CV-QKD (around 10 km [43]). In addition, the secret-key rate of HD-QKD at zero distance is about 8.6 Mbit/s (see Table II), which is comparable to that of CV-QKD with the same 55.6 MHz clock rate, and to that of decoy-state BB84 with a state-of-the-art 1 GHz clock rate [56]. Moreover, HD-QKD can offer a higher PIE, up to 4.3 bits/photon (with 30 min. running time), than does decoy-state BB84 [44], whose PIE can never exceed 1 bit per use.

In Fig. 1(c) we show the secret-key rate as a function of block size. Here we see that the minimum required block size for HD-QKD is slightly larger than those of decoy-state BB84 [44] and CV-QKD [43]. Finally, Fig. 1(d) plots the secret-key rate versus transmission distance for different

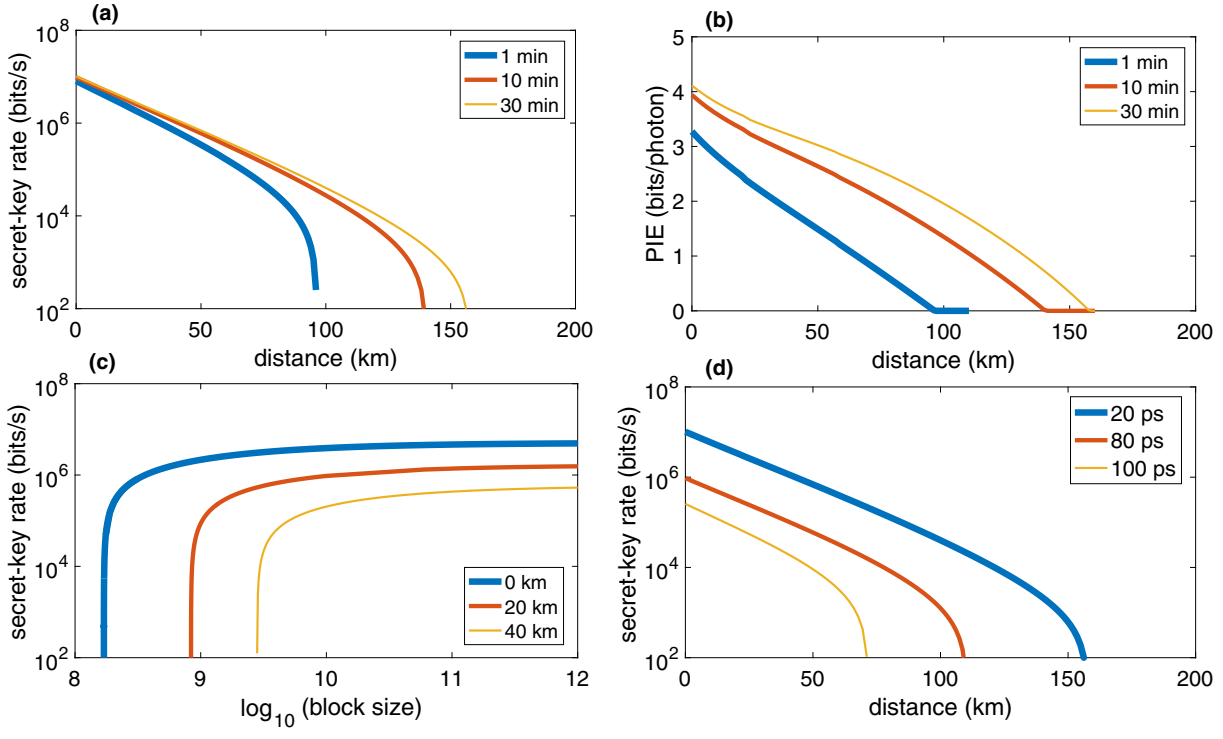

FIG. 1. Numerically evaluated performance of time-energy HD-QKD with threshold code distance $d_0 = 2$ and other parameters as listed in Table I. (a) Secret-key rate (bits/s) versus transmission distance (km) for different total running times of transmission: top curve (yellow) 30 min., middle curve (red) 10 min., bottom curve (blue) 1 min. (b) PIE (bits/photon) versus transmission distance (km) for different running times: top curve (yellow) 30 min., middle curve (red) 10 min., bottom curve (blue) 1 min. (c) Secret-key rate (bits/s) versus block size (running time/clock rate) for different transmission distances: top curve (blue) 0 km, middle curve (red) 20 km, bottom curve (yellow) 40 km. (d) Secret-key rate (bits/s) versus transmission distance (km) for different time-bin durations δ, where the running time is fixed at 30 min.: top curve (blue) 20 ps, middle curve (red), 80 ps, bottom curve (yellow) 100 ps.

time-bin durations, showing that shorter duration time bins offer higher key rates for a given biphoton source. We remark that detectors with less than 20 ps jitter have already been demonstrated in recent experiments [55].

Our work clarifies how the secret-key rate of time-energy HD-QKD using dispersive optics depends on the time-bin duration δ and the GVD coefficient β_D. Indeed, a higher GVD coefficient and a lower detector time jitter—so that time-bin duration may be decreased—might increase HD-QKD's secret-key rate. The secret-key rates shown in Fig. 1 have already presumed a bin duration limited by state-of-the-art detector time jitter, but the β_D value used is achievable with commercial devices [16]. Increasing the GVD coefficient without changing the other system parameters, however, does not always increase the secret-key rate. In particular, Eq. (8) shows that a K-fold increase in β_D increases secret-key length by $\underline{n_{\mathrm{T},01}}\log_2(K)$, *if* there is no offsetting increase in the error rate between Alice and Bob's raw keys, as quantified by the $\gamma(d_0+\Delta)$ term in Eq. (5). Our numerical evaluation of the secret-key rate at zero distance versus β_D—using the other parameters from Table I and the $d_0=2$ threshold code distance employed in Fig. 1—verifies this insight, see Fig. 2. Here we see the secret-key rate initially increasing linearly with increasing $\log_{10}(\beta_D)$, until it saturates and begins to decrease. Saturation occurs because our protocol requires $d_0 > d_{\min}$ for there to be a positive secret-key rate, and the minimum threshold code distance increases with increasing β_D, as shown in Appendix D. So, the secret-key rate saturation and decay in Fig. 2 results from the d_0 increases that are required at high β_D values. That said, Fig. 2 still shows that the highest key rate, 17 Mbit/s, is realized with the experimentally feasible $\beta = 2\times10^6$ ps^2 [16], and we have found that the maximum distance for a nonzero secret-key rate is then 210 km.

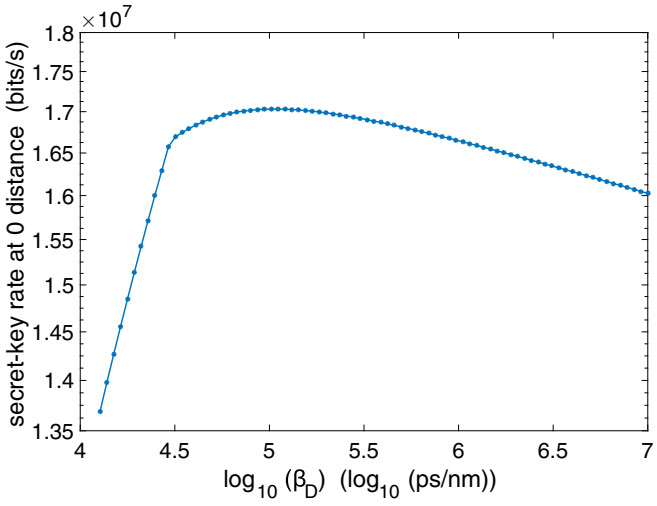

FIG. 2. Secret-key rate at zero distance versus GVD coefficient $\log_{10}(\beta_D)$ for 30 min. running time. The conventional units for β_D are employed here: ps per nm of bandwidth at telecom wavelength. The secret-key rate at zero distance achieves its 17 Mbit/s maximum at $\beta_D = 10^5$ ps/nm at telecom wavelength, which is equivalent to 2×10^6 ps^2 in the units used in Table I.

VI. SUMMARY

We have reported a general-attack security analysis for the time-energy HD-QKD protocol in the finite-key regime by combining the entropic uncertainty-relation security analysis of CV-QKD with the decoy-state technique from DV-QKD. In particular, we derived an entropic uncertainty relation for the time and conjugate-time operators by using optical dispersion transformations. This result validates the difference between the uncertainty relation of time and conjugate-time operators and that of conventional maximally incompatible operators, such as position and momentum. With the uncertainty bound, we showed that, under the most powerful attacks, time-energy HD-QKD can produce a higher PIE than conventional decoy-state BB84 and CV-QKD and still tolerate long-distance fiber transmission. We also showed that optimizing the HD-QKD protocol's GVD coefficient enables realizing a 17 Mbit/s secret-key rate at zero distance and a 210 km maximum secure-transmission distance, the latter being comparable to that of state-of-the-art decoy-state BB84. We expect this finding will provide theoretical support for optimizing HD-QKD implementations. Our results constitute an important step toward a unified understanding of distinct QKD schemes that is needed for development of practical long-distance high-rate quantum communication.

ACKNOWLEDGMENTS

The authors thank Zheshen Zhang, Catherine Lee, Darius Bunandar, and Franco N. C. Wong for many helpful discussions. We acknowledge support from ONR Grant No. N00014-13-1-0774 and AFOSR Grant No. FA9550-14-1-0052. F. Xu acknowledges support from an NSERC postdoctoral fellowship.

APPENDIX A: PROTOCOL

a. Preliminaries. Before contacting Bob, Alice makes measurements on her trusted spontaneous parametric down-conversion (SPDC) source of time-energy entangled biphotons to determine the coherence time of the pulsed pump field σ_{coh}, the biphoton correlation time σ_{cor}, and the SPDC intensities $\{\mu_1,\mu_2,\mu_3\}$, i.e., the mean photon pairs generated per pump pulse with different pump powers. Then, Alice and Bob use a preshared key to authenticate each other, after which they negotiate parameters to be employed during the protocol run.

b. Biphoton preparation and distribution. Alice pumps her SPDC source at a clock rate (repetition rate) R_{rep}. For each pump pulse, Alice prepares a time-energy entangled state within a T_f-duration ($T_f \approx \sigma_{\mathrm{coh}}$) frame centered on the peak of the pump pulse. She sends one photon to Bob via a quantum channel (e.g., an optical fiber) and retains the companion photon for her own measurements. To implement decoy states [5,6,24], Alice randomly pumps the SPDC source to select intensities $\mu_k \in \{\mu_1,\mu_2,\mu_3\}$ with probabilities $p_k \in \{p_{\mu_1},p_{\mu_2},p_{\mu_3}\}$.

c. Measurement phase. For each frame, Alice and Bob select their measurement basis at random and independently from $\{\mathsf{T},\mathsf{W}\}$ with probabilities $\{q,1-q\}$ and perform measurements in their chosen bases. Their T-basis measurements are made by using time-resolved single-photon detectors

with a temporal resolution set primarily by the detectors' time jitter σ_{jit} [17]. They sort their data into time bins of duration δ, where $\sigma_{\text{cor}} \ll \sigma_{\text{jit}} < \delta \ll \sigma_{\text{coh}}$, that will generate $\log_2(T_f/\delta)$ raw-key bits when they both obtain T-basis photon detections in the same frame. Their W-basis measurements are realized by means of dispersive optics and single-photon detection [21], i.e., they pass their photons through normal and anomalous group-velocity dispersion (GVD) elements, respectively, measure them with time-resolved single-photon detectors, and then sort that data into duration-δ time bins.

d. Basis reconciliation. Alice and Bob announce their measurement bases over an authenticated public channel and discard all measurement results for frames in which they measured in different bases. They are then left with detection-time coincidence measurements of n_{T} (n_{W}) frames in which they both used the T (W) basis and both obtained one photon detection.

e. Decoy-state processing. Alice announces her SPDC intensity choice for each frame. Alice and Bob thus identify sets $\mathcal{T}_{\mu_k}$ and $\mathcal{W}_{\mu_k}$ for $\mu_k \in \{\mu_1,\mu_2,\mu_3\}$, in which they have both made T-basis or W-basis measurements when Alice's SPDC source intensity was μ_k. They repeat their quantum communication, i.e., steps (b)–(e), until the cardinality of these sets satisfies $|\mathcal{T}_{\mu_k}| \geqslant n_{\mathsf{T},\mu_k}$ and $|\mathcal{W}_{\mu_k}| \geqslant n_{\mathsf{W},\mu_k}$, where $\{n_{\mathsf{T},\mu_k},n_{\mathsf{W},\mu_k}\}$ are prechosen values that ensure sufficient quality in the ensuing parameter-estimation steps. Note that $n_{\mathsf{T}} = \sum_{\mu_k} n_{\mathsf{T},\mu_k}$. Next, they publicly announce their W-basis detection times $\{t^w_{a,j,\mu_k},\ t^w_{b,j,\mu_k}\}$ for each SPDC intensity, where a, b denote Alice and Bob, j indexes the frame, and each detection-time value is relative to the peak of its associated pump pulse. After that, they compute these detection times' mean-squared differences for each μ_k, viz., $\sigma^2_{\text{cor},\mathsf{W},\mu_k} = \sum_j (t^w_{a,j,\mu_k} - t^w_{b,j,\mu_k})^2/n_{\mathsf{W},\mu_k}$. By virtue of their use of normal and anomalous GVD elements, $\sigma^2_{\text{cor},\mathsf{W},\mu_k}$ can be used to find the anticorrelation between the detunings from the SPDC outputs' center frequencies of the single-photon pairs (i.e., biphotons) that Alice and Bob detected in their W-basis measurements when Alice's SPDC intensity was μ_k [21]; see Appendix C.

f. Parameter estimation. Alice and Bob use only their μ_1 data for secret-key generation, while they use their μ_2 and μ_3 data for parameter estimation. Alice and Bob use their T-basis data to estimate $n_{\mathsf{T},0}$, the number of frames out of their n_{T,μ_1} that are due to vacuum coincidences (either Alice or Bob did not detect a photon), and $n_{\mathsf{T},1}$, the number of frames out of their n_{T,μ_1} that are due to single-pair coincidences (Alice and Bob each detected one photon). They use their W-basis data to estimate $d_{\mathsf{W},1}$, which is the L_1 distance between their detected photons' frequency detunings (after accounting for their anticorrelation) that is due to single-pair coincidences [24,44] (see Appendix C). Finally, they check that $d_{\mathsf{W},1}$ is less than d_0, where d_0 is a predetermined threshold (see Appendix D). If this condition is not met, they abort the protocol. Otherwise they proceed to the protocol's next step.

g. Key generation and error correction. Alice and Bob use their T-basis data to generate raw keys $(\mathbf{X}_{\mathrm{A}},\mathbf{X}_{\mathrm{B}})$ from the frames in which Alice's SPDC intensity was μ_1. Each frame used in generating these raw keys contains $\log_2(T_f/\delta)$ bits. Alice and Bob perform error correction on their raw keys by using an algorithm with reconciliation efficiency $\beta_e \leqslant 1$ [57]. This procedure reveals at most leak_{EC} bits of information to Eve. Next, to ensure that they have shared identical keys, Alice and Bob perform key verification by using a two-universal hash function that publishes $\lceil \log_2(1/\epsilon_{\text{hash}}) \rceil$ bits of information, with ϵ_{hash} being the probability that a pair of nonidentical keys passes the test.

h. Calculation of secret-key length. By using the results from steps (f) and (g), Alice and Bob calculate the secret-key length ℓ. If ℓ is negative, they abort the protocol. Otherwise, they apply another (different) two-universal hash function (for privacy amplification) to their error-corrected raw keys to produce the length-ℓ secret keys, $\mathbf{K}_{\mathrm{A}}$ and $\mathbf{K}_{\mathrm{B}}$.

APPENDIX B: TIME-FREQUENCY UNCERTAINTY RELATION FOR DILATED MEASUREMENTS

To compare with the overlap developed in the main text, we derive the overlap with dilation in this appendix. Instead of the frequency domain, it is now more convenient to work in the time domain, using $|t\rangle = a^\dagger(t)|0\rangle$ to denote the single-photon localized at time t that satisfies the orthonormality condition $\langle t_1|t_2\rangle = \delta(t_1 - t_2)$. The single-photon Hilbert space is simply $\mathcal{H} = L^2(T)$, i.e., the space of square-integrable, complex-valued functions on the time-domain $t \in T$. We evaluate the overlap under dilation [51,52] when $T = (-\infty,\infty)$. In this case, the POVMs $T(t)$ and $W(t)$ for the time and conjugate-time measurements are projection valued [21]:

$$T(t) = |t\rangle\langle t|, \tag{B1}$$

$$W(t) = UT(t)U^\dagger. \tag{B2}$$

Here, $W(t)$ is obtained from $T(t)$ via the unitary transformation

$$U = \frac{1}{\sqrt{\pi\beta_D}} \int_{-\infty}^{\infty} dt_1 \int_{-\infty}^{\infty} dt_2 e^{-i(t_1-t_2)^2/\beta_D} |t_1\rangle\langle t_2|. \tag{B3}$$

The associated time and conjugate-time observables are then

$$O_t = \int_{-\infty}^{\infty} dt\, t |t\rangle\langle t|, \tag{B4}$$

$$D_t = \frac{1}{\pi\beta_D} \int_{-\infty}^{\infty} dt\, t \int_{-\infty}^{\infty} dt_1 \int_{-\infty}^{\infty} dt_2 e^{-i(t_1^2-t_2^2)/\beta_D} \times e^{2i(t_1-t_2)t/\beta_D} |t_1\rangle\langle t_2|. \tag{B5}$$

The conjugate-time observable can be further simplified as follows:

$$D_t = \frac{1}{\pi\beta_D} \int_{-\infty}^{\infty} dt_1 \int_{-\infty}^{\infty} dt_2 e^{-i(t_1^2-t_2^2)/\beta_D} \times \left(\frac{\partial}{\partial t_1} \int_{-\infty}^{\infty} dt \frac{\beta_D}{2i} e^{2i(t_1-t_2)t/\beta_D} \right) |t_1\rangle\langle t_2| \tag{B6}$$

$$= \frac{\beta_D}{2i} \int_{-\infty}^{\infty} dt_1 e^{-it_1^2/\beta_D} |t_1\rangle \times \left(\frac{\partial}{\partial t_1} \int_{-\infty}^{\infty} dt_2 e^{it_2^2/\beta_D} \delta(t_1 - t_2) \langle t_2| \right) \tag{B7}$$

$$= \int_{\infty}^{\infty} dt_1 t_1 |t_1\rangle\langle t_1| + \frac{\beta_D}{2i} \int_{-\infty}^{\infty} dt_1 |t_1\rangle \frac{\partial}{\partial t_1} \langle t_1| \tag{B8}$$

$$= O_t + \pi\beta_D O_\omega, \tag{B9}$$

where $O_\omega = \int_{-\infty}^{\infty} \frac{d\omega}{2\pi}\omega|\omega\rangle\langle\omega|$ is the conventional unbounded-frequency observable that is maximally incompatible with the time observable. It immediately follows that

$$[O_t, D_t] = i\pi\beta_D. \tag{B10}$$

Finally, by using the overlap result for maximally incompatible observables [50], we obtain

$$c(\delta,\beta_D) = \frac{\delta^2}{2\pi^2\beta_D}, \tag{B11}$$

for the dilated measurements. Compared with the overlap derived with nonprojective POVM in Sec. IV, this overlap is slightly smaller and thus offers a weaker bound on the uncertainty relation. In the paper we therefore used the nondilated overlap in bounding the secret-key length.

APPENDIX C: DECOY STATES WITH FINITE KEYS

A decoy-state method for HD-QKD in the asymptotic regime was previously derived in Ref. [24]. Here, based on Ref. [44], we extend the work in Ref. [24] to the finite-key case against *general* attacks (i.e., without any assumptions on the statistical distributions). We presume that Alice randomly chooses between three intensity levels, μ_1, μ_2, and μ_3 for her SPDC source. Let $s_{\mathsf{T},n}$ be the number of frames in which Alice and Bob both measure in the T basis and Alice's source has emitted n biphotons in each frame, so that $n_{\mathsf{T}} = \sum_{n=0}^{\infty} s_{\mathsf{T},n}$ is the total number of frames in which Alice and Bob both made T-basis measurements. In the asymptotic regime, n_{T,μ_k}, the number frames in which Alice's source intensity was μ_k and she and Bob made T-basis measurements approaches its ensemble-average value; namely,

$$n_{\mathsf{T},\mu_k} \to n^*_{\mathsf{T},\mu_k} = \sum_{n=0}^{\infty} p_{\mu|\mathsf{n}}(\mu_k|n)s_{\mathsf{T},n} \quad \text{for } \mu_k \in \{\mu_1,\mu_2,\mu_3\},$$

where $p_{\mu|\mathsf{n}}(\mu_k|n)$ is the conditional probability of Alice's source emitting $\mathsf{n} = n$ biphotons in a frame, given its source intensity was $\mu = \mu_k$. For finite sample sizes, Hoeffding's inequality for independent events [58] implies that n_{T,μ_k} will satisfy

$$|n^*_{\mathsf{T},\mu_k} - n_{\mathsf{T},\mu_k}| \leqslant \zeta(n_{\mathsf{T}},\epsilon_1), \tag{C1}$$

with probability at least $1-2\epsilon_1$, where $\zeta(n_{\mathsf{T}},\epsilon_1) := \sqrt{n_{\mathsf{T}}\ln(1/\epsilon_1)/2}$. Note that the deviation term $\zeta(n_{\mathsf{T}},\epsilon_1)$ is the same for all μ_k. Inequality (C1) allows us to establish a relation between the asymptotic values $\{n^*_{\mathsf{T},\mu_k}\}$ and the observed values $\{n_{\mathsf{T},\mu_k}\}$. More precisely, we have the following bounds for finite-key analysis:

$$n^*_{\mathsf{T},\mu_k} \leqslant n_{\mathsf{T},\mu_k} + \zeta(n_{\mathsf{T}},\epsilon_1) =: \overline{n_{\mathsf{T},\mu_k}}, \tag{C2}$$

$$n^*_{\mathsf{T},\mu_k} \geqslant n_{\mathsf{T},\mu_k} - \zeta(n_{\mathsf{T}},\epsilon_1) =: \underline{n_{\mathsf{T},\mu_k}}. \tag{C3}$$

1. Lower-bound on the number of vacuum coincidences, $\underline{n_{\mathsf{T},0}}$

The following lower bound on $s_{\mathsf{T},0}$ was derived in Ref. [44]:

$$s_{\mathsf{T},0} \geqslant \underline{s_{\mathsf{T},0}} = \frac{\tau_0}{(\mu_2-\mu_3)}\left(\frac{\mu_2 e^{\mu_3}\underline{n_{\mathsf{T},\mu_3}}}{p_{\mu_3}} - \frac{\mu_3 e^{\mu_2}\overline{n_{\mathsf{T},\mu_2}}}{p_{\mu_2}}\right). \tag{C4}$$

By using this result we obtain the lower bound on the number of vacuum coincidences when Alice's source intensity is μ_1 given by

$$n_{\mathsf{T},0} \geqslant \underline{n_{\mathsf{T},0}} = \underline{s_{\mathsf{T},0}}p_{\mu|\mathsf{n}}(\mu_1|0).$$

2. Lower bound on the number of single-pair coincidences, $\underline{n_{\mathsf{T},1}}$

The following lower bound on $s_{\mathsf{T},1}$ was derived in Ref. [44]:

$$\begin{aligned} s_{\mathsf{T},1} &\geqslant \underline{s_{\mathsf{T},1}} \\ &= \frac{\mu_1\tau_1}{\mu_1(\mu_2-\mu_3)-(\mu_2^2-\mu_3^2)} \\ &\quad\times\left[\frac{e^{\mu_2}\underline{n_{\mathsf{T},\mu_2}}}{p_{\mu_2}} - \frac{e^{\mu_3}\overline{n_{\mathsf{T},\mu_3}}}{p_{\mu_3}} + \frac{\mu_2^2-\mu_3^2}{\mu_1^2}\left(\frac{s_{\mathsf{T},0}}{\tau_0} - \frac{e^{\mu_1}\overline{n_{\mathsf{T},\mu_1}}}{p_{\mu_1}}\right)\right]. \end{aligned} \tag{C5}$$

By using this result we obtain the lower bound on the number of single-pair coincidences when Alice's source intensity is μ_1 given by

$$n_{\mathsf{T},1} \geqslant \underline{n_{\mathsf{T},1}} = \underline{s_{\mathsf{T},1}}p_{\mu_1|1} - \zeta(\underline{s_{\mathsf{T},1}}p_{\mu|\mathsf{n}}(\mu_1|1),\epsilon_2),$$

with probability at least $1-2\epsilon_2$.

3. Upper bound on the L_1 distance of single-pair coincidences, $\overline{d_{\mathsf{W},1}}$

After the nonlocal dispersion cancellation that occurs when Alice and Bob both make W-basis measurements on the same frame, their mean-square time difference, $\sigma^2_{\mathrm{cor},\mathsf{W},\mu_k}$ for $\mu_k \in \{\mu_1,\mu_2,\mu_3\}$, can be written as

$$\begin{aligned} \sigma^2_{\mathrm{cor},\mathsf{W},\mu_k} &= \frac{p_{\mu|\mathsf{n}}(\mu_k|1)s_{\mathsf{W},1}}{n_{\mathsf{W},\mu_k}}\sigma^2_{\mathrm{cor},\mathsf{W},1} \\ &\quad + \left(1 - \frac{p_{\mu|\mathsf{n}}(\mu_k|1)s_{\mathsf{W},1}}{n_{\mathsf{W},\mu_k}}\right)\sigma^2_{\mathrm{cor},\mathsf{W},m}, \end{aligned}$$

where $\sigma^2_{\mathrm{cor},\mathsf{W},1}$ and $\sigma^2_{\mathrm{cor},\mathsf{W},m}$ are the mean-squared differences due to single-pair and multiple-pair coincidences including *all* source intensities, and $s_{\mathsf{W},1}$ is the number of frames in which Alice and Bob both measure in the W basis given that Alice's source has emitted 1 biphoton in each frame. Then, we have

$$\begin{aligned} &n_{\mathsf{W},\mu_2}\sigma^2_{\mathrm{cor},\mathsf{W},\mu_2} - n_{\mathsf{W},\mu_3}\sigma^2_{\mathrm{cor},\mathsf{W},\mu_3} \\ &= s_{\mathsf{W},1}\sigma^2_{\mathrm{cor},\mathsf{W},1}[p_{\mu|\mathsf{n}}(\mu_2|1) - p_{\mu|\mathsf{n}}(\mu_3|1)] + \sigma^2_{\mathrm{cor},\mathsf{W},m} \\ &\quad\times[n_{\mathsf{W},\mu_2} - n_{\mathsf{W},\mu_3} + p_{\mu|\mathsf{n}}(\mu_3|1)s_{\mathsf{W},1} - p_{\mu|\mathsf{n}}(\mu_2|1)s_{\mathsf{W},1}], \end{aligned} \tag{C6}$$

where the $\sigma^2_{\mathrm{cor},\mathsf{W},m}$ term on the right is non-negative for $\mu_2 > \mu_3$. Dropping the $\sigma^2_{\mathrm{cor},\mathsf{W},m}$ term, the preceding result can be rearranged to provide the lower bound

$$\sigma^2_{\mathrm{cor},\mathsf{W},1} \leqslant \overline{\sigma^2_{\mathrm{cor},\mathsf{W},1}} = \frac{\overline{n_{\mathsf{W},\mu_2}}\sigma^2_{\mathrm{cor},\mathsf{W},\mu_2} - \underline{n_{\mathsf{W},\mu_3}}\sigma^2_{\mathrm{cor},\mathsf{W},\mu_3}}{\underline{s_{\mathsf{W},1}}[p_{\mu|\mathsf{n}}(\mu_2|1) - p_{\mu|\mathsf{n}}(\mu_3|1)]}, \tag{C7}$$

where the $s_{\mathsf{W},1}$ lower bound, $\underline{s_{\mathsf{W},1}}$, can be derived by using the same method employed in Ref. [44] to obtain inequality (C5). Our upper bound on the L_1 distance of single-pair coincidences

is then

$$\overline{d_{\mathsf{W},1}} = \sqrt{\frac{2}{\pi}\overline{\sigma^2_{\mathrm{cor},\mathsf{W},1}}}, \tag{C8}$$

where the $\sqrt{2/\pi}$ factor arises from relating the L_1 distance to the mean-squared difference of jointly Gaussian random variables.

APPENDIX D: THEORETICAL MODEL FOR THRESHOLD d_0

To find the threshold d_0 for the mean-squared difference between Alice and Bob's single-pair W-basis measurements beyond which Alice and Bob will abort the QKD protocol, we start from the time and frequency wave functions for the biphoton emission when Alice's SPDC source is pumped by a pulse centered at time $t = 0$ [23], i.e.,

$$\psi(t_S,t_I) = \frac{\exp\left(-t_-^2/4\sigma^2_{\mathrm{coh}} - t_+^2/4\sigma^2_{\mathrm{cor}} - i\omega_P t_+\right)}{\sqrt{2\pi\sigma_{\mathrm{coh}}\sigma_{\mathrm{cor}}}}, \tag{D1}$$

$$\Psi(\omega_S,\omega_I) = \frac{\exp\left(-\omega_-^2\sigma^2_{\mathrm{cor}}/4 - 4\omega_+^2\sigma^2_{\mathrm{coh}}\right)}{\sqrt{\pi/2\sigma_{\mathrm{coh}}\sigma_{\mathrm{cor}}}}. \tag{D2}$$

Here, t_S and t_I denote the times of the biphoton's signal and idler photons, and ω_S and ω_I denote their frequencies; $t_+ := (t_S + t_I)/2, t_- := t_S - t_I, \omega_+ := (\omega_S + \omega_I)/2$, and $\omega_- := \omega_S - \omega_I$; and we have assumed that Alice's source is phase matched at frequency degeneracy for its pump's ω_P center frequency.

When both Alice and Bob choose the conjugate-time basis, they send their photons into normal and anomalous group-velocity-dispersion elements whose dispersion coefficients have common magnitude β_D but opposite signs. After propagation through the dispersive elements at Alice and Bob's terminal, the frequency wave function becomes

$$\Psi_D(\omega_S,\omega_I) = \frac{\exp\left[-\omega_-^2\sigma^2_{\mathrm{cor}}/4 - 4\omega_+^2\sigma^2_{\mathrm{coh}} + i\beta_D/4\left(\omega_S^2 - \omega_I^2\right)\right]}{\sqrt{\pi/2\sigma_{\mathrm{coh}}\sigma_{\mathrm{cor}}}}, \tag{D3}$$

from which the associated time wave function can be found via

$$\psi_D(t_S,t_I) = \frac{1}{2\pi}\int_\infty^\infty d\omega_S \int_{-\infty}^\infty d\omega_I \Psi_D(\omega_S,\omega_I) e^{-i(\omega_S t_S + \omega_I t_I)}. \tag{D4}$$

The W-basis mean-squared time difference in the absence of Eve is therefore

$$\sigma^2_{\mathrm{cor},\mathsf{W}} = \int_{-\infty}^\infty dt_S \int_{-\infty}^\infty dt_I (t_S - t_I)^2 |\psi_D(t_S,t_I)|^2 \tag{D5}$$

$$= \frac{\sigma^2_{\mathrm{coh}}\sigma^2_{\mathrm{cor}} + (\beta_D/4)^2}{\sigma^2_{\mathrm{coh}}} \tag{D6}$$

$$= \sigma^2_{\mathrm{cor}} + \frac{\beta_D^2}{16\sigma^2_{\mathrm{coh}}}. \tag{D7}$$

This correlation time measures how strongly Alice and Bob's single photons are correlated in the conjugate-time basis in the absence of Eve. Subsequently, we find the minimum L_1 distance for conjugate-time measurement outcomes without any third-party interference to be

$$d_{\min} = \sqrt{\frac{16\sigma^2_{\mathrm{coh}}\sigma^2_{\mathrm{cor}} + \beta_D^2}{8\pi\sigma^2_{\mathrm{coh}}\delta^2}}, \tag{D8}$$

where the $1/\delta$ factor normalizes the root-mean-square time difference into time bins and the $\sqrt{2/\pi}$ factor converts root-mean-square bin difference into L_1 distance. The d_0 that determines when Alice and Bob will abort their QKD protocol thus should be bigger than $d_{\min}$ in order to have nonzero key rate. In our performance evaluation, whose results are shown in Fig. 1, we chose $d_0 = 2$. This value is well above this $d_{\min}$ lower bound for the parameter values given in Table I.

[1] 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.

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

[3] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014).

[4] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[5] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

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

[7] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[8] Y. Liu *et al.*, Opt. Express **18**, 8587 (2010).

[9] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Opt. Lett. **37**, 1008 (2012).

[10] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photon. **9**, 163 (2015).

[11] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).

[12] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).

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

[14] R. Thew, A. Acin, H. Zbinden, and N. Gisin, Quantum Inf. Comput. **4**, 93 (2004).

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

[16] C. Lee *et al.*, Phys. Rev. A **90**, 062331 (2014).

[17] T. Zhong *et al.*, New J. Phys. **17**, 022002 (2015).

[18] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O. Sullivan, B. Rodenburg, M. Malik, M. P. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, New J. Phys. **17**, 033033 (2015).

[19] K. Bradler, M. Mirhosseini, R. Fickler, A. Broadbent, and R. Boyd, New J. Phys. **18**, 073030 (2016).

[20] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, J. Phys. B: At., Mol. Opt. Phys. **46**, 104010 (2013).
[21] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, Phys. Rev. A **87**, 062322 (2013).
[22] C. Lee, J. Mower, Z. Zhang, J. H. Shapiro, and D. Englund, Quantum Inf. Process. **14**, 1005 (2015).
[23] Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. Lett. **112**, 120506 (2014).
[24] D. Bunandar, Z. Zhang, J. H. Shapiro, and D. R. Englund, Phys. Rev. A **91**, 022336 (2015).
[25] H. Bao, W. Bao, Y. Wang, C. Zhou, and R. Chen, J. Phys. A: Math. Theor. **49**, 205301 (2016).
[26] R. Renner, arXiv:quant-ph/0512258.
[27] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, J. Math. Phys. **55**, 122205 (2014).
[28] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[29] H. Atmanspacher, H. Römer, and H. Walach, Found. Phys. **32**, 379 (2002).
[30] M. J. W. Hall and H. M. Wiseman, New J. Phys. **14**, 033040 (2012).
[31] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Phys. Rev. A **90**, 052327 (2014).
[32] F. Xu, J. H. Shapiro, and F. N. C. Wong, Optica **3**, 1266 (2016).
[33] O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).
[34] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[35] F. Dupuis, O. Fawzi, and S. Wehner, IEEE Trans. Inf. Theory **61**, 1093 (2015).
[36] R. König, S. Wehner, and J. Wullschleger, IEEE Trans. Inf. Theory **58**, 1962 (2012).
[37] M. Koashi, J. Phys.: Conf. Ser. **36**, 98 (2006).
[38] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
[39] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
[40] Y. Wang, W.-S. Bao, H.-W. Li, C. Zhou, and Y. Li, Phys. Rev. A **88**, 052322 (2013).
[41] C. Zhou, W.-S. Bao, H.-W. Li, Y. Wang, Y. Li, Z.-Q. Yin, W. Chen, and Z.-F. Han, Phys. Rev. A **89**, 052328 (2014).
[42] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, arXiv:1511.04857.
[43] F. Furrer, Phys. Rev. A **90**, 042325 (2014).
[44] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014).
[45] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
[46] J. D. Franson, Phys. Rev. A **45**, 3126 (1992).
[47] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 5524 (2011).
[48] P. Busch, M. Grabowski, and P. J. Lahti, Phys. Lett. A **191**, 357 (1994).
[49] V. Delgado and J. G. Muga, Phys. Rev. A **56**, 3425 (1997).
[50] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Nat. Commun. **6**, 8795 (2015).
[51] R. Werner, Ann. Inst. Henri Poincaré **47**, 429 (1987).
[52] J. Kiukas, A. Ruschhaupt, P. O. Schmidt, and R. F. Werner, J. Phys. A: Math. Theor. **45**, 185301 (2012).
[53] J. H. Shapiro, IEEE J. Sel. Top. Quantum Electron. **15**, 1547 (2009).
[54] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, IEEE Trans. Inf. Theory **59**, 2603 (2013).
[55] W. H. Pernice, C. Schuck, O. Minaeva, M. Li, G. Goltsman, A. Sergienko, and H. Tang, Nat. Commun. **3**, 1325 (2012).
[56] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, Opt. Express **21**, 24550 (2013).
[57] H. Zhou, L. Wang, and G. Wornell, in *2013 Information Theory and Applications Workshop (ITA)* (IEEE, New York, 2013), p. 1.
[58] W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).