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

Murphy Yuezhen Niu,[1] Feihu Xu,[1] Fabian Furrer,[2] and Jeffrey H. Shapiro[1]

[1]*Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*

[2] *NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, 243-0198, Japan*

(Dated: April 29, 2016)

Time-energy high-dimensional quantum key distribution (HD-QKD) leverages the high-dimensional nature of time-energy entangled biphotons and the loss tolerance from the discrete nature of single-photon detection thus enabling long-distance key distribution with high photon information efficiency (PIE). However, the security of HD-QKD has only been proven in the asymptotic regime, or in the finite-key regime against a limited set of attacks. Here we fill this gap by providing a rigorous HD-QKD security proof for general (coherent) attacks in the finite-key regime. The proof follows from a novel uncertainty relation for time and conjugate-time measurements, which bounds the secure information, and an efficient decoy-state protocol for parameter estimation. For the first time, we prove the feasibility of realizing secure and composable HD-QKD against the most powerful eavesdropping attacks across metropolitan-area distances.

Introduction: Current work on quantum key distribution (QKD) focuses on patching security holes in practical implementations, improving key rates and transmission distances, and unifying understanding of the plethora of different protocols. Existing QKD protocols can be divided into two major categories: discrete-variable (DV) [1] and continuous-variable (CV) [2] QKD. The predominant DV-QKD is more robust to loss than CV-QKD, and thus offers longer transmission distance. CV-QKD, on the other hand, offers higher photon information efficiency (PIE) than DV-QKD, and thus potentially higher key rates at short distances [3].

High-dimensional QKD (HD-QKD) protocols exploit the best features of DV and CV protocols to simultaneously achieve high PIE and long transmission distance [4]. Significant efforts in both theory and experiment have pushed forward the development of HD-QKD protocols over the past decade [5, 6]. One of the most appealing candidates for implementation is time-energy HD-QKD [6–10]. It generates keys 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 its first proposal [7–10]. Nonetheless, a rigorous security proof that satisfies the composable definition [11] and takes full account of the finite-size effects against *general* attacks has been missing. For this reason, the feasibility and security of metropolitan-scale HD-QKD within a reasonable time-frame for signal transmission has remained undemonstrated.

The main contributions of this work are two-fold. First, in contrast to existing results for time-energy HD-QKD, we provide, for the first time, a security proof in the finite-key regime that is valid against general attacks and meets the composability requirement. Second, we derive a new uncertainty relation between time and conjugate-time measurements through nonlocal dispersion cancellation. That relation is indispensable for analyzing coherent attacks. Although an entropic uncertainty relation for quadrature fields has been developed [12], and applied recently to CV-QKD security analysis [13], it cannot be directly applied to time-energy HD-QKD because time and conjugate-time measurements cannot be simply described by maximally incompatible operators [14], such as position and momentum. Facing this challenge, we construct a new uncertainty relation specifically for time and conjugate-time measurements. With this relation, we show that time-energy HD-QKD can permit a 140 kbits/s key rate over an 80-km-long optical fiber under realistic conditions. Consequently, two advantages of the HD-QKD protocol are demonstrated: (1) The maximum transmission distance of HD-QKD for coherent attacks (e.g., 160 km) substantially exceeds that of CV-QKD [13, 15], even in the case of reverse reconciliation (e.g., 16 km [16]). (2) HD-QKD can generate a much higher PIE (e.g., 4.3 bits/photon) than does decoy-state BB84 (e.g., 0.1 bits/photon [17]).

Protocol: 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 one. Alice and Bob each choose independently 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 [8]. The process repeats for N rounds until Alice and Bob obtain enough detection counts for post-processing. At the end of all measurements, the two sides reveal their basis choices and discard all data measured using 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. Using the decoy-state method [10, 17], Alice and Bob estimate the number of detections in T generated from the single-pairs of SPDC and the corresponding L_1 code distance d_{W} in the W basis. They abort the protocol if d_{W} exceeds a predetermined value d_0. Otherwise, they perform error correction and privacy amplification to generate the secure key. A detailed account of the protocol, including its use of decoy states, appears in Sec. I of [18].

The conjugate-time measurement for the W basis is realized by direct detection after sending photons through nor-

mal and anomalous group-velocity dispersion (GVD) elements, respectively, on Alice's and Bob's side [8]. If Alice and Bob both choose the W basis and their GVD elements have equal-magnitude, opposite-sign GVD coefficients, then group-velocity dispersion is nonlocally canceled [19]. As a result, their measurement outcomes in the W basis are as strongly correlated as those in the T basis. The dispersion transformation enables us to perform spectral measurement with only time-resolved single-photon detection [8].

Security Definitions: Given that the parameter-estimation test is passed with probability p_{pass}, Alice and Bob end up with two classical random vectors, $\mathbf{K}_{\text{A}}$ and $\mathbf{K}_{\text{B}}$, which might be correlated with a third quantum system, $\mathbf{E}$, held by Eve. Mathematically, this situation corresponds to a classical-quantum state $\rho_{\text{K}_\text{A}\text{E}} = \sum_s |s\rangle\langle s| \otimes \rho_{\text{E}}^s$, where $\{|s\rangle\}$ denotes an orthonormal basis representing Alice'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 [11]. A protocol is called ϵ_c-*correct* if the probability that $\mathbf{K}_{\text{A}}$ differs from $\mathbf{K}_{\text{B}}$ is smaller than ϵ_c. We say that a protocol is ϵ_s-*secret* if the state $\rho_{\text{K}_\text{A}\text{E}}$ is ϵ_s-close to the ideal situation described by the tensor product of uniform distribution of all keys on Alice's side and Eve's quantum state, $U_{\text{K}_\text{A}} \otimes \rho_{\text{E}}$, such that $p_{\text{pass}} \|\rho_{\text{K}_\text{A}\text{E}} - U_{\text{K}_\text{A}} \otimes \rho_{\text{E}}\|_1 \leq \epsilon_s$. Following the above definition, a QKD protocol is said to be ϵ-secure if it is both ϵ_c-correct and ϵ_s-secret, with $\epsilon_c + \epsilon_s \leq \epsilon$. 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 [11].

Security analysis: The essential insight of our security analysis is to exploit the entropic uncertainty relations for the smooth entropies [20] of time-energy HD-QKD. In particular, we derive an uncertainty relation for the time and conjugate-time measurement operators (see Sec. III of [18]) by generalizing the uncertainty relation for position and momentum [12] to half-bounded measurement operators such as time and frequency. Moreover, based on [17], we extend the previous decoy-state method [10] for parameter estimation in HD-QKD.

Our principal result is that a time-energy HD-QKD protocol is ϵ-secure with secret-key length (see Sec. II in [18]):

$$\ell \geq -(\underline{n_{\text{T},0}} + \underline{n_{\text{T},1}}) \log_2[c(\delta, \beta_D)] - \underline{n_{\text{T},1}} \log_2[\gamma(d_0 + \Delta)] - \text{leak}_{\text{EC}} + \log_2[\epsilon_c \epsilon_s^2]. \quad (1)$$

Here: $\underline{n_{\text{T},0}}$ lower bounds the vacuum coincidences; $\underline{n_{\text{T},1}}$ lower bounds the single-photon-pair coincidences; and $\overline{d_0}$ is a predetermined threshold that upper bounds the L_1 distance, $\overline{d_{\text{W},1}}$, in the W basis. The parameters $\underline{n_{\text{T},0}}$, $\underline{n_{\text{T},1}}$, and $\overline{d_{\text{W},1}}$ can be estimated using the decoy-state method from the observed statistics (see Sec. IV of [18]). The overlap, $c(\delta, \beta_D)$, between conjugate measurements in the T and W bases is given by (see Sec. III of [18])

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

in terms of the GVD coefficient β_D and the time-bin duration δ. The function $\gamma(d_0 + \Delta)$ is an upper bound on the smooth max-entropy given d_0 and Δ, the statistical fluctuation in the distance measure that quantifies how well the data subset used for parameter estimation represents the entire dataset [13]. The leak_{EC} term represents the amount of information that is leaked to Eve during error correction.

η_d	Y_0	σ_{jit}	α	β_D	R_{rep}
90%	1 kHz	18 ps	0.21 dB/km	1000 ns/nm	55.6 MHz
σ_{cor}	σ_{coh}	δ	β_e	q	ϵ
2 ps	6 ns	20ps	0.91	0.9	10^{-10}

TABLE I: List of parameters, mostly from [6], used in numerical evaluation: detection efficiency η_d, dark count rate Y_0, detector time jitter σ_{jit} [21], fiber-loss coefficient α, GVD coefficient β_D, system repetition rate R_{rep}, biphoton correlation time σ_{cor}, pump coherence time σ_{coh}, time-bin duration for decoding δ, reconciliation (error-correction) efficiency β_e, probability of choosing the time basis q and overall security bound ϵ.

Parameters	BB84 [17]	CV-QKD [16]	HD-QKD
PIE (bits)	≈0.1	0.5	4.3
Key rate (bits/s)	≈8 M[a]	≈10 M[b]	10 M
Max Dist. (km)	170	16	140

[a] Assumes a decoy-state BB84 system with 1 GHz clock rate [23].
[b] Assumes a CV-QKD system with 100 MHz clock rate [22].

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 keys rate at 0 km fiber length: HD-QKD can generate a key rate that is comparable to BB84 and CV-QKD, but it can produce a much higher PIE. The third row compares the maximum transmission distance: although HD-QKD's range is slightly shorter than BB84's, it it greatly exceeds CV-QKD's.

Numerical evaluation: 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., 1–30 minutes). This transmission distance significantly exceeds that of CV-QKD (less than 10 km [16]). In addition, HD-QKD can produce key rates that are comparable to those of CV-QKD and decoy-state BB84. In particular, the secure key rate of HD-QKD at zero distance is about 10 Mbits/s (see Table II), which similar to CV-QKD and decoy-state BB84 performance, even assuming the state-of-the-art 100 MHz [22] and 1 GHz clock rates [23] for those protocols. However, HD-QKD can offer a much higher PIE, up to 4.3 bits/photon, than does decoy-state BB84. Moreover, we show the secure key rate as a function of running time in Fig. 1(c), where we see that the minimum required block size for HD-QKD is only slightly larger than that of

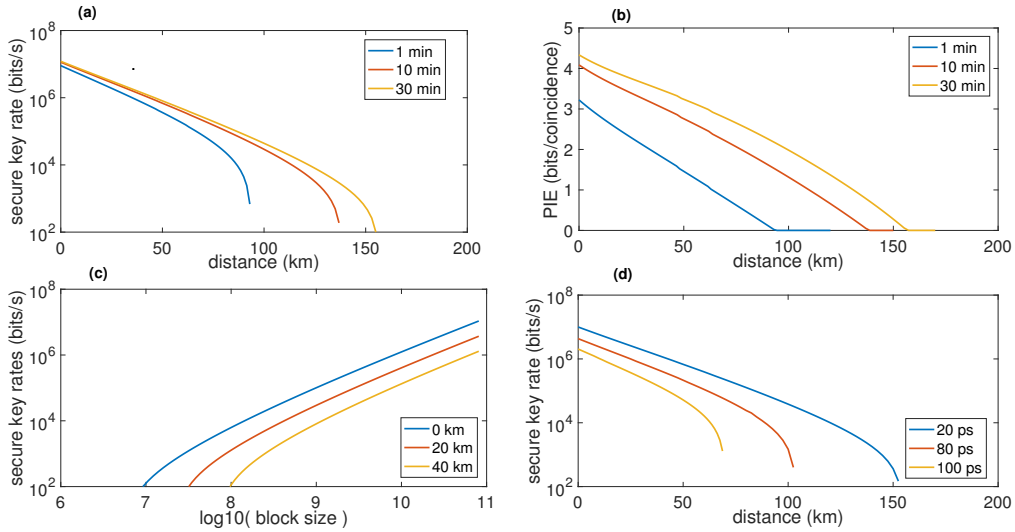

FIG. 1: Numerically evaluated performance of HD-QKD. (a) Secure key rate (bits/s) versus transmission distance (km) for different total running time of transmission. (b) PIE (bits/coincidence) versus transmission distance (km) for different running times. (c) Secure key rate (bits/s) versus block size (running time/repetition rate) for different transmission distances. (d) Secure key rate (bits/s) versus transmission distance (km) for different time-bin durations δ, where the running time is fixed at 30 mins. The parameters assumed are listed in Table I.

decoy-state BB84 [17], but it is comparable to that for CV-QKD [16]. Furthermore, Fig. 1(d) plots the secure key rate versus transmission distance for different time-bin durations, showing that shorter duration time bins offer higher key rates for a given biphoton source. We remark that detectors with about 20 ps jitter have already been demonstrated in recent experiments [21]. In time-energy HD-QKD based on dispersive-optics the secure key rate also depends on the GVD coefficient β_D: higher β_D gives higher secure key rate (see Sec. III of [18] for details). These results provide motivation for increasing the GVD coefficient of dispersive elements and reducing the time jitter of single-photon detectors.

Conclusion: We have completed the 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 a new uncertainty relation for the time and conjugate-time operators using optical dispersion transformations. With the new uncertainty bound, we showed that under general attacks HD-QKD can produce a higher PIE than conventional decoy-state BB84, and still tolerate long-distance fiber transmission. Our results constitute an important step toward unified understanding of distinct QKD schemes that is crucial for practical long-distance high-rate quantum communication.

[1] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Vol. 175

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

[3] P. Jouguet, *et al.*, *Nat. Photon.*, **7**, 378 (2013)

[4] N. J. Cerf, *et al.*, *Phys. Rev. Let.* **88**, 127902 (2002); I. Ali-Khan, *et al.*, *Phys. Rev. Lett.* **98**, 060503 (2007).

[5] L. Zhang, *et al.*, *Phys. Rev. Lett.* **100**, 110504 (2008); C. Lee, *et al.*, *Phys. Rev. A* **90**, 062331 (2014); M. Mirhosseini, *et al.*, *New J. Phys.* **17**, 033033 (2015).

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

[7] T. Brougham, *et al.*, *J Phys. B Atom. Mol. Opt. Phys.* **46**, 104010 (2013).

[8] J. Mower, *et al.*, *Phys. Rev. A* **87**, 062322 (2013); C. Lee, *et al.*, *Quant. Inf. Proc.* **14**, 1005 (2013).

[9] Z. Zhang, *et al.*, *Phys. Rev. Lett.* **112**, 120506 (2014).

[10] D. Bunandar, *et al.*, *Phys. Rev. A* **91**, 022336 (2015).

[11] R. Renner, PhD Thesis, ETH No.16242, *arXiv: quant-ph/0512258* (2005).

[12] M. Tomamichel and R. Renner, *Phys. Rev. Lett.* **106**, 110506 (2011); F. Furrer, *et al.*, *J. Math. Phys.* **55**, 122205 (2014)

[13] F. Furrer, *et al.*, *Phys. Rev. Lett.* **109**, 100502 (2012).

[14] H. Atmanspacher, *et al.*, *Foundations of Physics*, **32**, 3, 379–406 (2002)

[15] A. Leverrier, *Phys. Rev. Lett.* **110**, 030502 (2013).

[16] F. Furrer, *Phys. Rev. A.* **90**, 042325 (2014).

[17] C. C. W. Lim, *et al.*, *Phys. Rev. A.* **89**, 022307 (2014).

[18] Supplementary Material at `http://web.mit.edu/yzniu/www/AppendixQcryptv5.pdf`.

[19] J. D. Franson, *Phys. Rev. A.* **45**, 3126 (1992).

[20] M. Tomamichel, *et al.*, *Nat. Commun.* **3**, 634 (2012).

[21] W. H. P. Pernice, *et al.*, *Nat. Commun.*, **3** 1325 (2012).

[22] D. Huang, *et al.*, *Opt. Lett.*, **40** 3695 (2015).

[23] M. Lucamarini, *et al.*, *Opt. Express* , **21** 24550 (2013).