Time–energy high-dimensional one-side device-independent quantum key distribution*

Hai-Ze Bao(包海泽)[1,2], Wan-Su Bao(鲍皖苏)[1,2,†], Yang Wang(汪洋)[1,2], Rui-Ke Chen(陈瑞柯)[1,2], Hong-Xin Ma(马鸿鑫)[1,2], Chun Zhou(周淳)[1,2], and Hong-Wei Li(李宏伟)[1,2]

[1] *Zhengzhou Information Science and Technology Institute, Zhengzhou* 450001, *China*

[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 13 January 2017 ; revised manuscript received 7 March 2017; published online 6 April 2017)

Compared with full device-independent quantum key distribution (DI-QKD), one-side device-independent QKD (1sDI-QKD) needs fewer requirements, which is much easier to meet. In this paper, by applying recently developed novel time–energy entropic uncertainty relations, we present a time–energy high-dimensional one-side device-independent quantum key distribution (HD-QKD) and provide the security proof against coherent attacks. Besides, we connect the security with the quantum steering. By numerical simulation, we obtain the secret key rate for Alice's different detection efficiencies. The results show that our protocol can performance much better than the original 1sDI-QKD. Furthermore, we clarify the relation among the secret key rate, Alice's detection efficiency, and the dispersion coefficient. Finally, we simply analyze its performance in the optical fiber channel.

Keywords: time–energy, high-dimensional device-indepenedent quantum key distribution

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/26/5/050302

1. Introduction

Using quantum key distribution (QKD), two distant communication parties, called Alice and Bob, can generate secret keys, with the security based on the fundamental laws of quantum mechanics.[1,2] Although QKD is unconditionally secure, some gaps exist in theoretical and practical security of QKD due to imperfections of QKD devices. Using these security loopholes, the eavesdropper Eve can perform some attacks, such as faked state attacks,[3,4] after-gate attacks,[5] dead time attacks,[6] and wavelength-dependent attacks.[7] Since the first QKD protocol, BB84 protocol,[8] was proposed, QKD gets quick development in theory and experiments,[9–13] and lots of work on eliminating these gaps have been done.[14–19]

One of the most promising approaches of eliminating these gaps is device-independent QKD (DI-QKD).[20,21] The security of DI-QKD is guaranteed by the observed violation of Bell inequalities[22] and it requires the minimal set of assumptions. However, to test the violation of Bell inequalities, detectors used in DI-QKD are required to ensure very high detection efficiencies.[21] Therefore, it is an extreme challenge to demonstrate DI-QKD in practice. To relax constraints of DI-QKD, some valuable proposals for QKD have been proposed as compromises between device-dependent QKD and device-independent QKD.

Based on dimension witnesses,[23] Pawłowski and Brunner[24] proposed a DI-QKD scenario with relaxed constraints, which is called semi-device-independent QKD (SDI-QKD), and proved its security against individual attacks. To remove detector side channel attacks, the idea of measurement-device-independent QKD (MDI-QKD)[25,26] is proposed and developed.[27–29] Some important aspects are studied in recent years.[30–33] Although those ideas can remove detector side channel attacks and double the secure transmittance distance, they require the perfect performance of the source. Furthermore, Branciard *et al.*[34] present a trade-off scenario, called one-side device-independent QKD (1sDI-QKD), between device-dependent QKD and device-independent QKD and analyze its security and feasibility by connecting the scenario with quantum steering.[35] 1sDI-QKD can be applied to some special conditions, e.g., establishing secret keys between a bank with its clients, where a bank can invest lots of money to set up reliable apparatus, while clients may use cheap and insecure terminals. In recent years, some relevant researches have been finished.[36–38]

However, in the original 1sDI-QKD, the photon information efficiency limits the rate of generation the key (no more than 1 bit per coincidence). Coding information in high-dimensional photonic degrees of freedom is a promising way to break the limitation. Furthermore, high-dimensional correlations can tolerate more noise.[39]

Some photonic degrees of freedom have been applied in HD-QKD, including position-momentum,[40] time–energy,[41–43] transverse momentum,[44] and orbital angular momentum.[45–47] Based on time–energy entanglement,

*Project supported by the National Basic Research Program of China (Grant No. 2013CB338002) and the National Natural Science Foundation of China (Grants Nos. 11304397 and 61505261).

†Corresponding author. E-mail: 2010thzz@sina.com

© 2017 Chinese Physical Society and IOP Publishing Ltd

Mower *et al.*[48] proposed a new high-dimensional QKD (HD-QKD) protocol using dispersive optics, which is called DO-QKD. Its security against collective attacks has been proven in Ref. [49] and its practical security analysis has been studied.[50–53] Recently, by deriving a novel entropic uncertainty relation for time and conjugate-time measurements using dispersive optics, Niu *et al.*[54] proved its security against general attacks.

In this paper, we extend time–energy high-dimensional code into 1sDI-QKD and propose a new protocol, so-called time–energy high-dimensional one-side device-independent QKD protocol (1sDI-HDQKD). Using the novel time–energy entropic uncertainty relation, we prove the security of our protocol against coherent attacks. By numerical simulation, we show that our protocol achieves more bits information per coincidence and requires lower detection efficiencies than the original 1sDI-QKD protocol. Then we relate the security of our protocol to violation of an EPR steering inequality.

The rest of this paper is organized as follows. In Section 2, we briefly describe the time–energy 1sDI-HDQKD protocl. In Section 3, we prove the security of our protocol against coherent attacks by time–energy entropic uncertainty relation. We connect our protocol with quantum steering in Section 4. Results of numerical simulation are shown in Section 5, and the conclusion is summarized in Section 6.

2. Protocol description

The schematic of our protocol, the 1sDI-HDQKD protocol, is shown in Fig. 1. Our protocol is based on an entanglement-based 1sDI-QKD protocol with an untrusted source in Fig. 1(a) or with a trusted source in Fig. 1(b), which is equivalent to a prepare-and-measure 1sDI-QKD scheme.[34] We consider that Alice does not trust her measurement devices or she treats them as a black box, while Bob trusts his devices. Eve has the ability to completely control quantum channel but the classical channel is authenticated. In our protocol, particular, we use the result measured in time basis ($\mathbb{T}$ basis) by both Alice and Bob to extract a secret key, while results measured in conjugate-time basis ($\mathbb{W}$ basis) are used to estimate Eve's information. Here we use spontaneous parametric down-conversion (SPDC) source to generate time–energy entangled states. The coherent time of the pulsed pump field is denoted by σ_{coh}. The correlation time bin duration between two entangled particles is denoted by δ. We denote the duration of a frame by T_{f} ($T_{\text{f}} \approx \sigma_{\text{coh}}$). The dimension d is determined by $d = T_{\text{f}}/\delta$. The protocol is described as follows.

State preparation and distribution For each distribution, the source prepares a time–energy entangled state within a T_{f}-duration frame. Then the source sends one particle of the pair to Alice and the other to Bob via the quantum channel.

State measurements For each frame, Alice and Bob select a basis between $\mathbb{T}$ basis and $\mathbb{W}$ basis at random and independent. Then they perform measurements in their chosen bases and record their outcomes respectively. Since Alice's measurement apparatuses are untrusted, Eve has the ability to control whether the detector at Alice's side click depending on her received state and measurement setting. Therefore, we cannot simply discard Alice's no-detection events. Bob trusts his measurement apparatuses, which Eve cannot control. So we can safely consider only the cases where Bob gets detections.

Sifting After all signals are transmitted, both of them publish their basis choices over an authenticated public channel. They sift their raw keys only from correlated events acquired in $\mathbb{T}$ basis and use the corresponding measurement outcomes acquired in $\mathbb{W}$ basis for parameter estimation. Let X_{A} and X_{B} denote Alice and Bob's raw keys respectively. The outcomes in $\mathbb{W}$ basis are denoted by Y_{A} and Y_{B}.

Postselecting Alice publish her no-detection events and then they can postselect their raw keys on the events that Alice gets detections. Then Alice and Bob get postselected bit strings X_{A}^{ps} and X_{B}^{ps} respectively. Discarded data are denoted by $X_{\text{A}}^{\text{dis}}$ and $X_{\text{B}}^{\text{dis}}$. Let N denote the length of the strings X_{A} and X_{B}, and n denote the length of the strings X_{A}^{ps} and X_{B}^{ps}.

Post-processing After above steps, Alice and Bob perform parameter estimation and then test quantum steering. If they demonstrate quantum steering by the violation of an EPR-steering inequality, they apply error correction and privacy amplification (from Bob to Alice) on their data or abort the protocol.

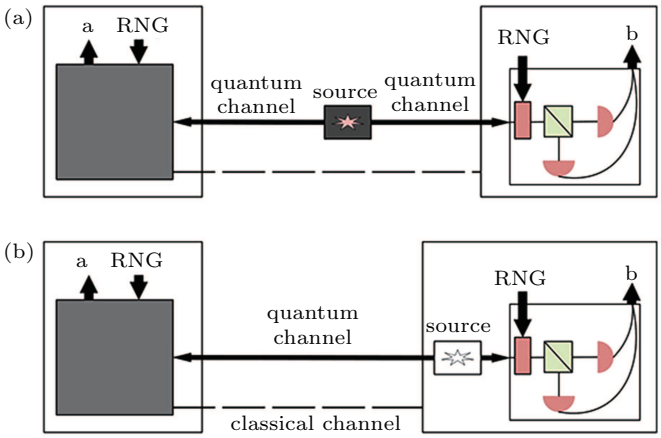


Fig. 1. (color online) The schematic of the 1sDI-HDQKD.

3. Security proof and key rate

Recently, Niu *et al.*[54] proposed and proof a novel time–energy uncertainty relation for smooth entropies. By using the novel uncertainty relation, we present the secure key rate

of our time–energy HD-1sDI-QKD. Noted that Alice's measurement apparatuses are untrusted, the assumption that the devices are memoryless is needed as in Ref. [55].

Through the classical post-processing process, from the postselected n-bit strings $X_{\rm A}^{\rm ps}$ and $X_{\rm B}^{\rm ps}$, Alice and Bob can generate a secret key of length

$$l \approx H_{\min}^{\varepsilon}\left(X_{\rm B}^{\rm ps}|E\right) - {\rm leak}_{\rm EC}. \tag{1}$$

Here $H_{\min}^{\varepsilon}\left(X_{\rm B}^{\rm ps}|E\right)$ is the smooth min-entropy of $X_{\rm B}^{\rm ps}$, conditioned on Eve's quantum side information E;[56] ${\rm leak}_{\rm EC}$ is the leaked information in post-processing process.

According to the chain rule[57] and the data-processing[58] inequality for smooth min-entropies, we have the following relationship:

$$\begin{aligned} H_{\min}^{\varepsilon}(X_{\rm B}|E) &= H_{\min}^{\varepsilon}\left(X_{\rm B}^{\rm ps}, X_{\rm B}^{\rm dis}|E\right) \\ &\leq H_{\min}^{\varepsilon}\left(X_{\rm B}^{\rm ps}|X_{\rm B}^{\rm dis}E\right) + \log_2\left|X_{\rm B}^{\rm dis}\right| \\ &\leq H_{\min}^{\varepsilon}\left(X_{\rm B}^{\rm ps}|E\right) + (N-n)\log_2 d. \end{aligned} \tag{2}$$

Using the novel time–energy uncertainty relation for smooth min-entropies,[54] we have

$$H_{\min}^{\varepsilon}(X_{\rm B}|E) + H_{\max}^{\varepsilon}(Y_{\rm B}|Y_{\rm A}) \geqslant N\log_2\frac{1}{c(\delta,\beta_{\rm D})}, \tag{3}$$

where the smooth max-entropy $H_{\max}^{\varepsilon}(Y_{\rm B}|Y_{\rm A})$ measures the amount of information needed to reconstruct $Y_{\rm B}$ given $Y_{\rm A}$ with error probability bounded above by ε , and $c(\delta,\beta_{\rm D})$ is the overlap between the time and conjugate-time measurement operator. δ is the time bin duration and $\beta_{\rm D}$ is the magnitude of the group velocity dispersion (GVD) elements' dispersion coefficient. Using the result of Ref. [45], the smooth max-entropy follows the upper bound

$$H_{\min}^{\varepsilon}(Y_{\rm B}|Y_{\rm A}) \leq N\log_2\gamma(d_W), \tag{4}$$

where d_W is the corresponding L_1 code distance in the $\mathbb{W}$ basis and $\gamma(x)$ obeys

$$\gamma(x) = \left(x+\sqrt{1+x^2}\right)\left(\frac{x}{\sqrt{1+x^2}-1}\right)^x. \tag{5}$$

Since the basis is selected randomly, d_W is the same as the value without postselection.

Substituting Eqs. (3) and (4) into Eq. (2), we obtain

$$\begin{aligned} H_{\min}^{\varepsilon}\left(X_{\rm B}^{\rm ps}|E\right) \geqslant\ & N\log_2\frac{1}{c(\delta,\beta_{\rm D})} - (N-n)\log_2 d \\ & - N\log_2\gamma(d_W). \end{aligned} \tag{6}$$

Considering the imperfect reconciliation efficiency $\beta_{\rm e} \leq 1$, we have the equality[60]

$${\rm leak}_{\rm EC} = (1-\beta_{\rm e})\left(\log_2 d - H\left(X_{\rm B}^{\rm ps}|X_{\rm A}^{\rm ps}\right)\right) + H\left(X_{\rm B}^{\rm ps}|X_{\rm A}^{\rm ps}\right). \tag{7}$$

Using the upper bound on the smooth max-entropy like Eq. (4), we obtain

$${\rm leak}_{\rm EC} \leq n\log_2 d - \beta_{\rm e} n\left(\log_2 d - \log_2\gamma\left(d_{\rm T}^{\rm ps}\right)\right). \tag{8}$$

Then we obtain the length of secure keys

$$\begin{aligned} l \geqslant\ & \beta_{\rm e} n\left[\log_2 d - \log_2\gamma\left(d_{\rm T}^{\rm ps}\right)\right] \\ & - N\left[\log_2\gamma(d_W) + \log_2 d - \log_2\frac{1}{c(\delta,\beta_{\rm D})}\right]. \end{aligned} \tag{9}$$

Considering the asymptotic limit of infinite key lengths, the fraction $\frac{n}{N}$ of photons that Alice detects, given Bob detected one, can be treated as the detection efficiency of Alice, which is denoted by $\eta_{\rm A}$. Then we can write the secure key rate in bit per coincidence (bpc) as

$$\begin{aligned} r = \frac{l}{N} \geqslant\ & \beta_{\rm e}\eta_{\rm A}\left[\log_2 d - \log_2\gamma\left(d_{\rm T}^{\rm ps}\right)\right] \\ & - \left[\log_2\gamma(d_W) + \log_2 d - \log_2\frac{1}{c(\delta,\beta_{\rm D})}\right]. \end{aligned} \tag{10}$$

The positive raw key is the precondition of generating positive secret key. Considering raw key, the raw key rate can be written as

$$\begin{aligned} r_{\rm raw} \geqslant\ & \eta_{\rm A}\left[\log_2 d - \log_2\gamma\left(d_{\rm T}^{\rm ps}\right)\right] \\ & - \left[\log_2\gamma(d_W) + \log_2 d - \log_2\frac{1}{c(\delta,\beta_{\rm D})}\right]. \end{aligned} \tag{11}$$

As is shown in Eq. (11), the inequality "right side of Eq. (11)$\leq$ 0" is violated. More explicitly, the following inequality is violated:

$$\begin{aligned} & \eta_{\rm A}\log_2\gamma\left(d_{\rm T}^{\rm ps}\right) + \log_2\gamma(d_W) + (1-\eta_{\rm A})\log_2 d \\ \geqslant\ & \log_2\frac{1}{c(\delta,\beta_{\rm D})}. \end{aligned} \tag{12}$$

On the other hand, positive raw key rate can be generated between Alice and Bob if and only if they check that they share entanglement, which amounts to demonstrating quantum steering. In the next section, we will show that equation (12) is an EPR-steering inequality[35] and equation (11) demonstrates quantum steering.

4. Connection to EPR steering

We first denote $\mathbb{M}_k \in \{\mathbb{T}_{\rm A}, \mathbb{W}_{\rm A}\}$, $k = 1,2$ in Alice's measurement and for $k = 1$ and 2, $\mathbb{M}_k$ represents $\mathbb{T}_{\rm A}$ and $\mathbb{W}_{\rm A}$, respectively. The similar definition is $\mathbb{N}_t \in \{\mathbb{T}_{\rm B}, \mathbb{W}_{\rm B}\}$ in Bob's measurement. Extending the proof in Ref. [34] using a local hidden state model,[35] the statistics of a local model can be measured by Alice and Bob and be decomposed as[61]

$$P(\tilde{a}_i, b_j) = \sum_{\lambda} P(\lambda)\, P(\tilde{a}_i|\lambda) P_{\rm Q}(b_j|\lambda), \tag{13}$$

where $\tilde{a}_i = (a_i, s)$, with a_i and b_j denoting the experimental outcomes corresponding to measurements $\mathbb{M}_k$ and $\mathbb{N}_{\rm t}$, and s denoting whether Alice gets a detection ($s = 1$) or not ($s = 0$).

In case of no detection, Alice's result a_i is chosen to be random bit values in our protocol and will contribute to the bit string $Y_{\rm A}^{\rm dis}$. The variable λ represents Bob's received quantum state. Bob's statistics are identified by quantum mechanics: $P_{\rm Q}(b_j|\lambda) = {\rm Tr}[E_j\rho_\lambda]$, where ρ_λ is a quantum state and set $\{E_j\}$ are the positive operators that describe his measurements.

According to Eq. (13), we know that, for Alice, the way to obtain maximal information about Bob's results is to get it through λ. By the conditional entropies, the result can be indicated as

$$H\left(\mathbb{N}_k|\tilde{\mathbb{M}}_K\right) \geqslant H\left(\mathbb{N}_k|\Theta\right). \tag{14}$$

Here $H\left(\mathbb{N}_k|\tilde{\mathbb{M}}_k\right) = \sum_{k,\tilde{a}_i} P(\tilde{a}_i) H(\mathbb{N}_k|\tilde{a}_i)$ and $H(\mathbb{N}_k|\Theta) = \sum_\lambda P(\lambda) H(\mathbb{N}_k|\lambda)$ are the average conditional entropies of Bob's measurement $\mathbb{N}_k$ respectively, under the knowledge of the result of $\tilde{\mathbb{M}}_k$ and of λ, with $H(\mathbb{N}_k|\tilde{a}_i) = -\sum_{b_i} P(b_i|\tilde{a}_i)\log_2 P(b_i|\tilde{a}_i)$ and $H(\mathbb{N}_k|\lambda) = -\sum_{b_i} P_{\rm Q}(b_i|\lambda)\log_2 P_{\rm Q}(b_i|\lambda)$.

Then Bob's statistics conditioned on λ are given by a quantum state assumption. So they must fulfill all quantum uncertainty relations, and particularly

$$H(\mathbb{N}_1|\lambda) + H(\mathbb{N}_2|\lambda) \geqslant \log_2 \frac{1}{c(\delta,\beta_{\rm D})}. \tag{15}$$

Then using Eq. (14), we obtain

$$H\left(\mathbb{N}_1|\tilde{\mathbb{M}}_1\right) + H\left(\mathbb{N}_2|\tilde{\mathbb{M}}_2\right) \geqslant \log_2 \frac{1}{c(\delta,\beta_{\rm D})}. \tag{16}$$

Denoting $\mathbb{M}_1^{\rm ps}$ for $\mathbb{M}_k$ when $s=1$ and $\mathbb{M}_1^{\rm dis}$ for $\mathbb{M}_k$ when $s=0$ and the corresponding probability is $P(s=1)=\eta_{\rm A}$, we have

$$H\left(\mathbb{N}_1|\tilde{\mathbb{M}}_1\right) = \eta_{\rm A} H\left(\mathbb{N}_1^{\rm ps}|\tilde{\mathbb{M}}_1^{\rm ps}\right) + (1-\eta_{\rm A}) H\left(\mathbb{N}_1^{\rm dis}|\tilde{\mathbb{M}}_1^{\rm dis}\right). \tag{17}$$

Substituting the uncertainty relation $H(\mathbb{N}|\mathbb{M}) \leq \log_2 \gamma(d)$ into Eq. (16), we have

$$H\left(\mathbb{N}_1|\tilde{\mathbb{M}}_1\right) \leq \eta_{\rm A}\log_2\gamma\left(d_{\rm T}^{\rm ps}\right) + (1-\eta_{\rm A})\log_2 d. \tag{18}$$

On the other hand, we have

$$H\left(\mathbb{N}_2|\tilde{\mathbb{M}}_2\right) \leq H(\mathbb{N}_2|\mathbb{M}_2) \leq \log_2\gamma(d_W). \tag{19}$$

Substituting Eqs. (18) and (19) in Eq. (16), we get Eq. (12). Thus equation (12) defines an EPR-steering inequality.

5. Numerical simulation

Before performing the numerical simulation, we should confirm some parameters.

According the time–energy uncertainty relation, we can determine the overlap $c(\delta,\beta_{\rm D})$ as[54]

$$c(\delta,\beta_{\rm D}) = \frac{1.37\delta^2}{2\pi^2\beta_{\rm D}}. \tag{20}$$

The corresponding L_1 code distance in the $\mathbb{T}(\mathbb{W})$ basis can be bounded by

$$\overline{d_{T(W)}} = \sqrt{\frac{2}{\pi}\overline{\sigma^2_{{\rm cor},T(W)}}}. \tag{21}$$

Here $\overline{\sigma^2_{{\rm cor},T(W)}}$ is the upper bound on $\sigma^2_{{\rm cor},T(W)}$, which is the mean-square difference of correlation time between entangled pairs measured in $\mathbb{T}$ ($\mathbb{W}$) basis. Due to excess noise $\xi_{T(W)}$, we have

$$\overline{\sigma^2_{{\rm cor},T(W)}} = \left(1+\xi_{T(W)}\right)\sigma^2_{{\rm cor},T(W)}. \tag{22}$$

Consider a typical experimental setup, where a source sends maximally entangled states to Alice and Bob, through a depolarizing channel with time (conjugate-time) visibility $V_{T(W)}$. With Alice's detection efficiency $\eta_{\rm A}$ and dual-basis interferometry used in time–energy QKD,[49] the excess noise can be determined by

$$\xi_T = \Phi(\eta_{\rm A}V_T, S_{\rm F}) - 1, \tag{23}$$

$$\xi_W = \Phi(V_W, S_{\rm F}) - 1, \tag{24}$$

where $\Phi(x)$ is a function related to the visibility and the setting of interferometry $S_{\rm F}$. Using results in Refs. [49], [54], and [62], we can obtain thresholds of d_T and d_W as

$$d_{T,\min} = \sqrt{\frac{2(1+\xi_T)\sigma_{\rm cor^2}}{\pi\delta^2}}, \tag{25}$$

$$d_{W,\min} = \sqrt{\frac{16(1+\xi_W)\sigma^2_{\rm coh}\sigma^2_{\rm cor}+\beta^2_{\rm D}}{8\pi\sigma^2_{\rm coh}\delta^2}}. \tag{26}$$

The code distance determines if the QKD protocol is aborted or not, so we should choose a much bigger value than thresholds in order to have non-zero key rate. In the HDQKD protocol with two trustworthy parties, the value is set as 2.0.[54] In our protocol, it should not be less than that. All other parameters are taken from Ref. [54] and listed in Table 1.

Table 1. Parameters used in numerical simulation.

$\sigma_{\rm coh}$	$\sigma_{\rm cor}$	δ	$\beta_{\rm D}$	$\beta_{\rm e}$
6 ns	2 ps	20 ps	2×10^4 ps^2	0.91

Figure 2 shows bounds on the secret key rate as a function of Alice's detection efficiency $\eta_{\rm A}$ for different code distances. Compared with the original 1sDI-QKD protocol, our protocol requires much lower Alice's detection efficiency and achieves more secure bits information per coincidence. For $d_{T(W)}=2$ in Fig. 2, one gets a positive secret key rate for all $\eta_{\rm A}>50\%$. This means that Alice's measurement apparatus can tolerate more Eve's intrusion (less events that the $\mathbb{T}$ basis is actually chosen by both Alice and Bob).

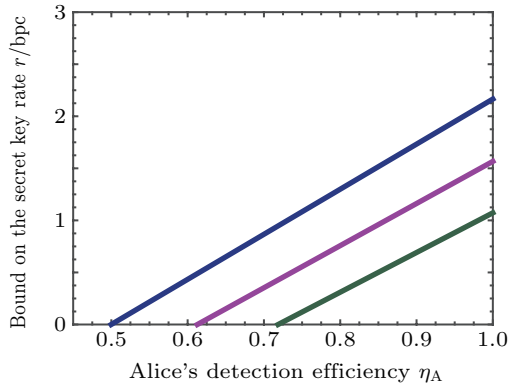


Fig. 2. (color online) Bounds on the secret key rate r in a typical implementation of 1SDI-QKD, as a function of Alice's detection efficiency η_A, for corresponding L_1 code distance $d_{T(W)} = 2.0$, 2.5 and 3.0 (from top to bottom), which are well above thresholds even $\xi_{T(W)}$ is big (e.g., $\xi_T = \xi_W = 100$).

It seems that increasing the GVD coefficient β_D will increase the entropy uncertainty so the secret key rate will be increased. However, the error rate, quantified by $\gamma(d_{T(W)})$, between Alice and Bob's raw keys will also increase with increasing β_D. To show the relation clearly, we consider a special condition, Alice's detection efficiency $\eta_A = 1$ when $d_{T(W)} = 2.0$ without changing other system parameters. Figure 3 plots the secret-key rate versus the GVD coefficient β_D.

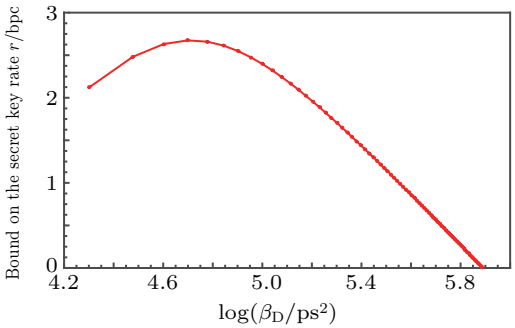


Fig. 3. (color online) Bound on the secret key rate versus the GVD coefficient $\log_{10}(\beta_D)$.

From Fig. 3, we can see the secret key rate is not always increased with β_D increasing. Under above parameter settings, the maximal secret key rate is 2.7 bits per coincidence with the GVD coefficient $\beta_D = 5.0 \times 10^4$ ps^2.

For clarifying the relation among the secret key rat r, Alice's detection efficiency η_A, and the GVD coefficient β_D, figure 4 is plotted.

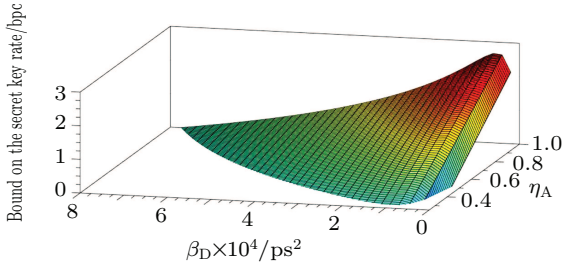


Fig. 4. (color online) Relation among the secret key rate r, Alice's detection efficiency η_A, and the GVD coefficient β_D.

Then we consider the performance of our protocol in the standard optical fiber channel. For simplifying the analysis, we adapt the scenario shown in Fig. 1(a) and assume the on-demand single-photon source. We set propagation loss $\alpha = 0.21$ dB/km and the channel transmittance $\eta_P = 10^{-\alpha L/10}$, where L is the transmission distance. Alice's average detection efficiency is denoted by η^*. All other parameters are the same as those in Table 1. After postselection and post-processing processes, we have the secret key rate

$$r_s \geqslant \eta_P \eta^* \beta_e [\log d - \log \gamma(d_T)] - \left[\log \gamma(d_W) + \log d - \log \frac{1}{c(\delta, \beta_D)}\right]. \quad (27)$$

Figure 5 plots the bound on the secret key rate in the optical fiber channel. All detection efficiencies are chosen from thresholds in DI-QKD and original 1sDI-QKD. Compare with recent results in Ref. [38], our protocol performs much better no matter in the secure bits per coincidence or the transmission distance. Note that, in our protocol, the losses between the source and Bob's side do not affect the security of the protocol due to postselecting process. Eve can only decrease the key rate proportionally to the decrease of Bob's detection efficiency. Hence, long distances can in principle be reached if the source stays close to Alice.

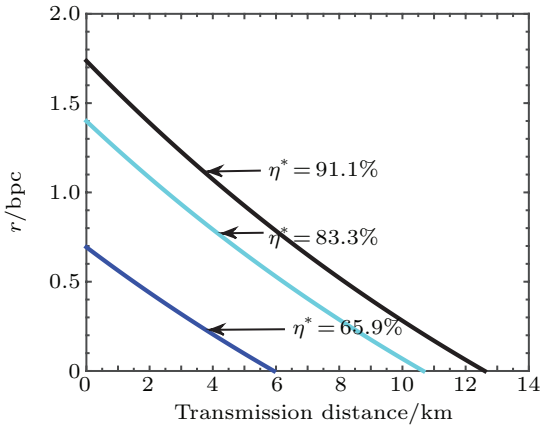


Fig. 5. (color online) Bound on the secret key rate in the optical fiber channel as a function of transmission distance L for different Alice's average detection efficiency $\eta^* = 65.9\%$, 83.3%, and 91.1%.

6. Conclusion

In this paper, we propose a new time–energy high-dimensional 1sDI-QKD protocol and present the proof of security against coherent attacks. Besides, we connect our protocol with quantum steering. Our results shows that our protocol also requires the violation of an EPR-steering inequality. By numerical simulation, we shows that our protocol need fewer requirements than the original 1sDI-QKD protocol while can achieve higher secret key rate. Typically we can achieve non-zero key rate with $\eta_A = 50\%$, which is much lower than the original 1sDI-QKD protocol. Besides, we achieve 0.74 bit and 1.4 bits per coincidence with $\eta_A = 65.9\%$ and $\eta_A = 83.3\%$

(different thresholds of Alice's detection efficiency in the original 1sDI-QKD), and we also achieve 1.74 bits per coincidence with $\eta_{\mathrm{A}} = 91.1\%$, which is the threshold of DI-QKD. Compared with recent results, our protocol can reach further transmission distance with higher secret key rate. In future works, the security with finite resources will be considered.

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[2] Lo H K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595
[3] Makarov V and Hjelme D R *J. Mod. Opt.* **52** 691
[4] Makarov V and Skaar J 2008 *Quant. Inf. Comp.* **8** 0622
[5] Wiechers C, Lydersen L, Wittmann C, Else D, Skaar J, Marquardt C, Makarov V and Leuchs G 2011 *New J. Phys.* **13** 013043
[6] Weier H, Krauss H, Rau M, Fürst M, Nauerth S and Weinfurter H 2011 *New J. Phys.* **13** 073024
[7] Li H, Wang S, Huang J, Chen W, Yin Z, Li F, Zhou Z, Liu D, Zhang Y, Guo G, Bao W and Han Z 2011 *Phys. Rev. A* **84** 062308
[8] Bennett C H and Brassard G 1984 *in Proceedings IEEE International Conference on Computers, Systems and Signal Processing*, 1984 Bangalore, India, pp. 175–179
[9] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C and Han Z F 2015 *Nat. Photon.* **9** 832
[10] Wang S, Chen W, Guo J F, Yin Z Q, Li H W, Zhou Z, Guo G C and Han Z F 2012 *Opt. Lett.* **37** 1008
[11] Wang S, Chen W, Yin Z Q, *et al.* 2014 *Opt. Express* **22** 21739
[12] Wang S, Chen W, Yin Z Q, Zhang Y, Zhang T, Li H W, Xu F X, Zhou Z, Yang Y, Huang D J, Zhang L J, Li F Y, Liu D, Wang Y G, Guo G C and Han Z F 2010 *Opt. Lett.* **35** 2454
[13] Li F Y, Wang D, Wang S, Li M, Yin Z Q, Li H W, Chen W and Han Z F 2014 *Chin. Phys. B* **23** 124201
[14] Garapo K, Mafu M and Petruccione F 2016 *Chin. Phys. B* **25** 070303
[15] Gu Y B, Bao W S, Wang Y and Chou C 2016 *Chin. Phys. Lett.* **33** 040301
[16] Li J, Chen Y H, Pan Z S, Sun F Q, Li N and Li L L 2016 *Acta Phys. Sin.* **65** 030302 (in Chinese)
[17] Ma H X, Bao W S, Li H W and Chou C 2016 *Chin. Phys. B* **25** 080309
[18] Wang Y, Bao W S, Zhou C, Jiang M S and Li H W 2016 *Phys. Rev. A* **94** 032335
[19] Wang Y, Bao W S, Li H W, Zhou C and Li Y 2014 *Chin. Phys. B* **23** 080303
[20] Acín a, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[21] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 *New J. Phys.* **11** 045021
[22] Bell J S 1964 *Physics* **1** 195
[23] Gallego R, Brunner N, Hadley C and Acín A 2010 *Phys. Rev. Lett.* **105** 230501
[24] Pawłowski M and Brunner N 2011 *Phys. Rev. A* **84** 010302
[25] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[26] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[27] Wang C, Wang S, Yin Z Q, Chen W, Li H W, Zhang C M, Ding Y Y, Guo G C and Han Z F 2016 *Opt. Lett.* **41** 5596
[28] Wang C, Song X T, Yin Z Q, Yin Z Q, Wang S, Chen W, Zhang C M, Guo G C and Han Z F 2015 *Phys. Rev. Lett.* **115** 160502
[29] Li F Y, Yin Z Q, Li H W, Chen W, Wang S, Wen H, Zhao Y B and Han Z F 2014 *Chin. Phys. Lett.* **31** 070302
[30] Ma X and Razavi M 2012 *Phys. Rev. A* **86** 062319
[31] Zhou C, Bao W, Zhang H, Li H, Wang Y, Li Y and Wang X 2015 *Phys. Rev. A* **91** 022313
[32] Chen R, Bao W, Wang Y, Bao H, Zhou C and Li H 2016 *Opt. Express* **24** 6594
[33] Pirandola S, Ottaviani C, Spedalieri G, *et al.* 2015 *Nat. Photon.* **9** 397
[34] Branciard C, Cavalcanti E G, Walborn S P, Scarani V and Wiseman H M 2012 *Phys. Rev. A* **85** 010301
[35] Cavalcanti E G, Jones S J, Wiseman H M and Reid M D 2009 *Phys. Rev. A* **80** 032112
[36] Wang y, Bao W, Li H, Zhou C and Li Y 2013 *Phys. Rev. A* **88** 052322
[37] Gehring T, Händchen V, Duhme J, *et al.* 2015 *Nat. Commun.* **6** 8795
[38] Walk N, Hosseini S, Geng J, *et al.* 2016 *Optica* **3** 634
[39] Cerf N J, Bourennane M, Karlsson A and Gisin N 2002 *Phys. Rev. Lett.* **88** 127902
[40] Zhang L, Silberhorn C and Walmsley I A 2008 *Phys. Rev. Lett.* **100** 110504
[41] Tittel W, Brendel J, Zbinden H and Gisin N 2000 *Phys. Rev. Lett.* **84** 4737
[42] Ali-Khan I, Broadbent C J and Howell J C 2007 *Phys. Rev. Lett.* **98** 060503
[43] Nunn J, Wright L J, Soller C, Zhang L, Walmsley I A and Smith B J 2013 *Opt. Express* **21** 15959
[44] Etcheverry S, Cañas G, Gómez E S, Nogueira W A T, Saavedra C, Xavier G B and Lima G 2013 *Sci. Rep.* **3** 2316
[45] Mair A, Vaziri A, Weihs G and Zeilinger A 2001 *Nature* **412** 313
[46] Molina-Terriza G, Vaziri A, Rehacek J, Hradil Z and Zeilinger A 2004 *Phys. Rev. Lett.* **92** 167903
[47] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M, Padgett M J, Konrad T, Petruccione F, Lütkenhaus N and Forbes A 2013 *Phys. Rev. A* **88** 032305
[48] Mower J, Zhang Z, Desjardins P, Lee C, Shapiro J H and Englund D 2013 *Phys. Rev. A* **87** 062322
[49] Zhang Z, Mower J,Englund D, Wong F and Shapiro J H 2014 *Phys. Rev. Lett.* **112** 120506
[50] Bunandar D, Zhang Z, Shapiro J H and Englund D 2015 *Phys. Rev. A* **91** 022336
[51] Lee C, Mower J, Zhang Z,Shapiro J H and Englund D 2015 *Quantum Inf. Process.* **14** 1005
[52] Bao H Z, Bao W S, Wang Y, Zhou C and Chen R K 2016 *J. Phys. A: Math. Theor.* **49** 205301
[53] Bao H Z, Bao W S, Wang Y, Chen R K, Zhou C, Jiang M S and Li H W 2016 *Opt. Express* **24** 22159
[54] Niu M Y, Xu F, Furrer F and Shapiro J H 2016 *Phys. Rev. A* **94** 052323
[55] Masanes L, Pironio S and Acín A 2011 *Nat. Commun.* **2** 238
[56] Tomamichel M and Renner R 2011 *Phys. Rev. Lett.* 106 110506
[57] Renes J M and Renner R 2012 *IEEE Trans. Inf. Theory* **58** 1985
[58] Tomamichel M, Colbeck R and Renner R 2010 *IEEE Trans. Inf. Theory* **56** 4674
[59] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 *Phys. Rev. Lett.* **109** 100502
[60] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev. A* **81** 062343
[61] Wiseman H M, Jones S J and Doherty A C 2007 *Phys. Rev. Lett.* **98** 140402
[62] Lee C, Zhang Z, Steinbrecher G R, *et al.* 2014 *Phys. Rev. A* **90** 062331