Journal of Electronic Science and Technology xxx (xxxx) xxx

Contents lists available at ScienceDirect

Journal of Electronic Science and Technology

journal homepage: www.keaipublishing.com/en/journals/journal-of-electronic-science-and-technology/

Impact of fiber dispersion on the performance of entanglement-based dispersive optics quantum key distribution☆

Jing-Yuan Liu [a], Xu Liu [a], Wei Zhang [a,b,c,d,e,*], Yi-Dong Huang [a,b,c,d,e]

[a] Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China
[b] Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing, 100084, China
[c] Beijing Innovation Center for Future Chips, Tsinghua University, Beijing, 100084, China
[d] Frontier Science Center for Quantum Information, Beijing, 100084, China
[e] Beijing Academy of Quantum Information Sciences, Beijing, 100193, China

ARTICLE INFO

Keywords:
Dispersion compensation
Dispersive optics quantum key distribution (DO-QKD)
Fiber chromatic dispersion
Quantum networks

ABSTRACT

Dispersive optics quantum key distribution (DO-QKD) based on energy-time entangled photon pairs is an important QKD scheme. In DO-QKD, the arrival time of photons is used in key generation and security analysis, which would be greatly affected by fiber dispersion. In this work, we established a theoretical model of the entanglement-based DO-QKD system, considering the protocol, physical processes (such as fiber transmission and single-photon detection), and the analysis of security tests. Based on this theoretical model, we investigate the influence of chromatic dispersion introduced by transmission fibers on the performance of DO-QKD. By analyzing the benefits and costs of dispersion compensation, the system performance under G.652 and G.655 optical fibers are shown, respectively. The results show that dispersion compensation is unnecessary for DO-QKD systems in campus networks and even metro networks. Whereas, it is still required in DO-QKD systems with longer fiber transmission distances.

1. Introduction

Quantum key distribution (QKD) enables two remote parties to generate secure, random cryptographic keys, with unconditional security guaranteed by quantum mechanics [1–3]. Quantum secure communications based on QKD have great potential in modern communications [4]. There are mainly two schemes in the experimental implementation of QKD, which are the prepare-and-measurement scheme [5,6] and the entanglement-based scheme [7–9]. The entanglement-based QKD scheme naturally establishes network connections between users, showing advantages in the implementation of quantum networks [10–12]. The entangled photon pairs from the quantum light source are distributed to Alice and Bob, respectively. And the coincidence events between the two users are used to generate cryptographic keys. In addition, the high-dimensional encoding process can increase the information carried per coincidence event, which utilizes these quantum resources more effectively [13,14].

Dispersive optics quantum key distribution (DO-QKD) is a recently proposed QKD protocol [15]. In entanglement-based DO-QKD,

☆ This work was supported by the National Key R&D Program of China under Grants No. 2017YFA0303704 and No. 2018YFB2200400; Natural Science Foundation of Beijing under Grant No. Z180012; National Natural Science Foundation of China under Grants No. 61875101 and No. 91750206.

* Corresponding author. Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China.
E-mail addresses: liujy20@mails.tsinghua.edu.cn (J.-Y. Liu), lx17@mails.tsinghua.edu.cn (X. Liu), zwei@tsinghua.edu.cn (W. Zhang), yidonghuang@tsinghua.edu.cn (Y.-D. Huang).

https://doi.org/10.1016/j.jnlest.2021.100119
Received 3 March 2021; Received in revised form 13 May 2021; Accepted 3 June 2021
Available online xxxx

the energy-time entangled photon pairs are generated from the quantum light source [9,15,16]. Normal and anomalous dispersion components are introduced at Alice's and Bob's sides, constructing time and frequency bases. The arrival time of photons at the time base is further used for key generation. The high-dimensional encoding process is introduced in post-processing, in order to maximize the key generation rate under technical constraints. The security analysis of DO-QKD can be realized by the measurements of unbiased time-frequency bases, which has been proven to be secure against collective attacks [15]. However, chromatic dispersion introduced by optical fibers will lead to the broadening of the coincidence peak, consequently affecting the generation of secret keys. In our previous entanglement-based DO-QKD experiment over optical fibers [9], the dispersion compensation module (DCM) is used to compensate for fiber dispersion. Nevertheless, there is still a lack of analysis on the benefits and costs of the dispersion compensation. Recently, entanglement-based DO-QKD was applied to realize QKD networks through entanglement distribution based on passive beam splitting and wavelength division multiplexing [10,17]. Dispersion compensation was not applied since the fiber links were quite short in these experiments. However, it can be expected that fiber dispersion would be a serious problem in a large-scale network and the effects of dispersion compensation should be considered seriously.

In this work, we focus on the impact of fiber dispersion on the performance of the DO-QKD system. Firstly, we realize the theoretical modeling of the DO-QKD system. Based on the established model, the influence of fiber dispersion on the DO-QKD system is analyzed. Furthermore, we investigate the benefits and costs of dispersion compensation, and concluded that dispersion compensation is not unnecessary at short distances. Using G.652 fibers, the DO-QKD system without DCM has better performance, when the fiber length is less than 9 km, while the range can be increased to 30 km using G.655 fibers. The results show the potential of realizing a dispersion-compensation-free DO-QKD network on campus, or even metro scale.

2. Theoretical model of DO-QKD system

The sketch of a DO-QKD system is shown in Fig. 1, where SMF is the single mode fiber; DCM is the dispersion compensation module; ND is normal dispersion; AD is anomalous dispersion; BS is the 50:50 beam splitter. The telecom-band energy-time entangled photon pairs are generated by a quantum light source. Then, the signal and idler photons of the photon pairs are distributed to Alice and Bob through optical fibers, respectively. At Alice's side, the photons are separated into two paths by a beam splitter. In one path (A1), photons are detected by a single-photon detector directly and the times of these single-photon events are recorded. In the other path (A2), photons are detected after they pass through a dispersive component with normal dispersion. The similar setup is placed at Bob's side, with two paths denoted by B1 and B2. The only difference is that the dispersive component of Bob has anomalous dispersion, while, its absolute value is the same as that of the dispersive component of Alice. Path A1 and path B1 form the time base of the measurements for the photon pairs. In this base, the coincidence events show strong temporal correlation, which is indicated by a narrow coincidence peak, and they are used to generate keys. The coincidence events of path A2 and path B2 also show a narrow coincidence peak due to the nonlocal dispersion compensation effect of energy-time entangled photon pairs [16,18]. They form the frequency base, which contributes to security tests.

The raw keys are generated by time encoding of the coincidence events in the time base. The large-alphabet processing method [13] is applied, which is shown in the upper part of Fig. 2. Photons are recorded at both sides in a continuous stream of time, which is divided into consecutive time frames. A time frame includes M ($M=2^N$) consecutive slots and a slot includes I time bins. In the bin sifting process, Alice and Bob firstly communicate their recorded frame numbers which contain one single-photon event through public channel, and keep the frames in which both sides have single-photon events. Then, for each retained frame, they check the time bin numbers of the single-photon events, and only keep the frames that the single-photon events at the two sides have the same bin number. Finally, Alice and Bob generate the raw keys by the slot numbers of the single-photon events in these frames. In this process, Alice and Bob avoid communications of the slot numbers, hence, Eve cannot get the information of the keys directly from the communications in the public channel.

We established a theoretical model to investigate the performance of DO-QKD systems, considering the characteristics of quantum light source, the optical fiber transmission, and process of single-photon detection. The modeling method is described below.

2.1. Raw key generation rate and QBER

There are some key parameters to describe the DO-QKD system shown in Fig. 1. For the quantum light source, there are the generation rate of entangled photon pairs R, and the generation rates of noise photons on signal and idler sides, R_s and R_i. They can be

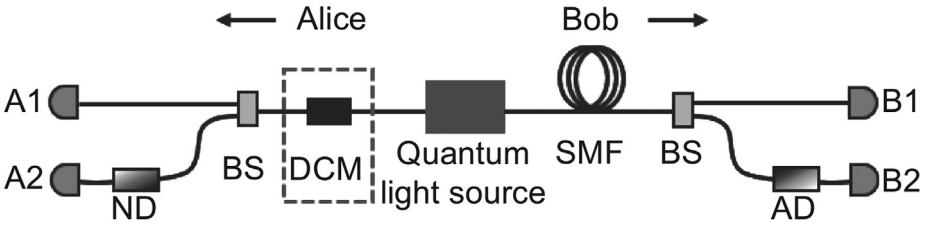

Fig. 1. Sketch of an entanglement-based DO-QKD system.

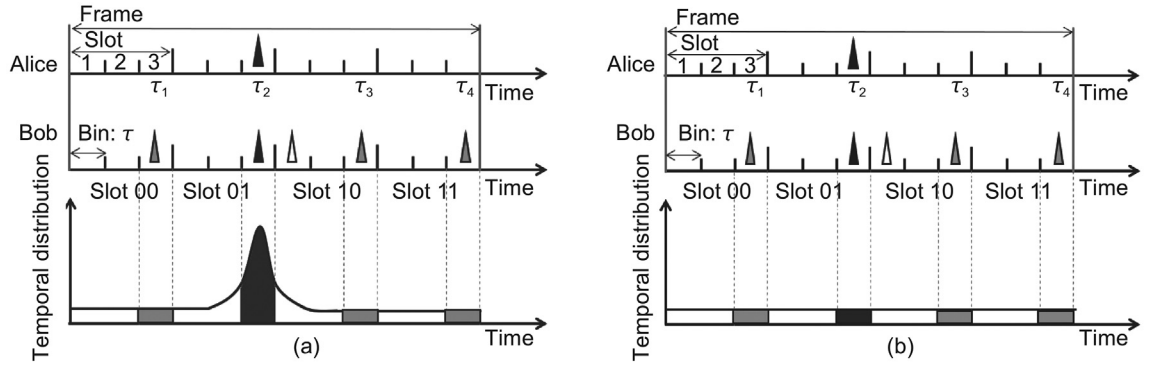

Fig. 2. Schematic diagram of the raw key generation rate and quantum bit error rate (QBER) in high-dimensional coding format of DO-QKD, when (a) Alice records signal-photon events and (b) Alice records noise events. A frame has 2^N slots and a slot has I bins. In the figure, $N=2$ and $I=3$.

obtained in the experiment by measuring the single-side photon count rates of signal and idler photons, and the coincidence count rate [19]. For the fiber transmission, there are the fiber length L, fiber loss coefficient α, and dispersion parameter β_2. The loss of DCM is denoted by l and its dispersion value is assumed to compensate that of the transmission fibers exactly. For single-photon detection, there are single-photon detection efficiency η_d, dark count rate of the detector d_d, and the timing jitter of the detectors (including the electronic circuits for counting) σ_d. In this model, all the detectors are assumed to have the same performance.

We start with analysis of the types of single-photon events recorded by Alice. For each event of Alice, she may record a signal photon which is one of an entangled photon pair, or a noise event (including noise photons and events of dark counts). If we set the arrival time of Alice's events as t_0, the probability distribution of the single-photon events recorded by Bob near t_0 could be derived. We number the slots in each frame by m ($m=1,\ 2,\ \cdots,\ 2^N$) and the bins in each slot by i ($i=1,\ 2,\ \cdots,\ I$). Let us consider the single-photon events of Alice recorded in a specific bin with a slot number of m_0 and a bin number of i_0. Since the single-photon events of Alice randomly fall into the time bin, we firstly derive the contributions of the events at Alice under a specific t_0 in the bin to the raw key rate and QBER. Then we calculate the average raw key rate and QBER as the final results by considering all the events at Alice in the bin, i.e., the contributions of events at Alice under different t_0 in the bin are calculated and accumulated.

For the case that Alice records signal photons, and ideally, energy-time entangled photon pairs would reach both sides simultaneously. However, the temporal correlation of the photon pairs decreases due to the timing jitters of the detectors, hence the arrival time of photons on each side will be uncertain. When we set the recorded arrival time of Alice's photons as a fixed value t_0, the uncertainty of the recorded arrival time of Bob's photons to t_0 is determined by the timing jitters of detectors on both sides. Its temporal distribution follows an approximate gaussian distribution with a mean of t_0, accompanied by a floor due to noise photons and dark counts, as shown in Fig. 2 (a). This temporal distribution at Bob's side is expressed as

$$B_1(t)=\frac{1}{2}10^{-\alpha L/10}\eta_d\frac{1}{\sqrt{2\pi}\sigma_{\text{inh}}}\exp\left[-\frac{(t-t_0)^2}{2\sigma_{\text{inh}}^2}\right]+\frac{1}{2}10^{-\alpha L/10}\eta_d R_i+d_d. \tag{1}$$

It can be derived from the known parameters of the source, transmission, and detectors. The variance σ_{inh} is mainly caused by the timing jitters of the single-photon detectors on both sides:

$$\sigma_{\text{inh}}^2=\sigma_0^2+2\sigma_d^2 \tag{2}$$

where σ_0 is the intrinsic correlation time between the two photons in a pair, after they pass through the filters. Usually, σ_0 is far smaller than the time jitters of single-photon detectors in typical DO-QKD experiments [9].

For the case that Alice records noise events, Bob's recorded events have no temporal correlation with Alice's records, forming accidental coincidence count events as shown in Fig. 2 (b). The temporal distribution of Bob's events is expressed as

$$B_2(t)=\frac{1}{2}10^{-\alpha L/10}\eta_d(R+R_i)+d_d. \tag{3}$$

Considering the two cases, we calculate the total number of correct coincidence events X_1, when Bob's recorded time is in the same bin with t_0. We also calculate the number of error coincidence events $X_{2,m}$ ($m\neq m_0$), when Bob's recorded time has the same bin number with t_0, but in the m slot (see details in Appendix A). The raw key generation rate b is considered to be the total number of coincidence events multiplied by the encoding dimension N, which is expressed as

$$b=NX_1+N\sum_{m=1,m\neq m_0}^{2^N}X_{2,m}. \tag{4}$$

If there is no bin sifting process, it is obvious that the adjacent slots between Alice and Bob are prone to misjudgment, resulting in bit

errors, as shown in the white triangles in Fig. 2. By sifting and keeping the coincidence counts of the same time bin number, the errors caused by this situation can be greatly eliminated, so QBER of the system is effectively reduced. However, there are still bit errors in the case of the same bin number but different slots, as shown in the gray triangles in Fig. 2. And QBER is expressed as

$$\mathrm{QBER}=\frac{\sum_{m=1,m\neq m_0}^{2^N}(X_{2,m}e_m)}{X_1+\sum_{m=1,m\neq m_0}^{2^N}X_{2,m}} \tag{5}$$

where e_m is the bit error ratio when Bob records an event in the m slot. Since one coincidence event generates N bits in the high-dimensional time coding format, e_m represents the ratio of error bit number to total bit number (N), if the recorded single-photon events of Alice and Bob are in different slots.

Then the average raw key generation rate and QBER are calculated considering all the t_0 in the bin. Although the above analysis only considers the single-photon events of Alice recorded in a specific time bin, the same results could be expected if it is extended to other time bins. Hence, (4) and (5) can be used as final results to calculate the performance of an entanglement-based DO-QKD system.

2.2. Security analysis and secret key rate

Alice and Bob perform arrival-time measurements under unbiased time-frequency bases with outcomes described by random variables T_A and T_B. The security analysis can be performed by analyzing the numerical characteristics of the random variables (see details in Appendix B) and calculating the time-frequency covariance matrix [15]. The secret key rate extracted per coincidence count is expressed by the secret key capacity [20]:

$$\Delta I=\beta I(A;B)-\chi(A;E) \tag{6}$$

where β is the reconciliation efficiency, which is set to be 90% in this work. $I(A;B)$ is the Shannon information between Alice and Bob, and $\chi(A;E)$ is Eve's Holevo information.

2.3. Impact of fiber dispersion on DO-QKD

The chromatic dispersion introduced by transmission fibers will broaden the coincidence peak, which will greatly deteriorate the secret key rate. Considering the influence of fiber dispersion, the variance of the temporal distribution of Bob's photons in the first case is modified, which is expressed as

$$\sigma_{\mathrm{tot}}^2=\sigma_{\mathrm{inh}}^2+\sigma_{\mathrm{dis}}^2. \tag{7}$$

Nonlocal dispersion cancellation can eliminate most of the broadening caused by dispersion. However, the residual dispersion that has not been well compensated still causes broadening [15,18,21], which is characterized by

$$\sigma_{\mathrm{dis}}^2=(\beta_2 L)^2/\left(2\sigma_0^2\right). \tag{8}$$

The relationship between dispersion parameters D and β_2 is expressed as $D=(-2\pi c/\lambda^2)\beta_2$[22]. When there is residual dispersion, the variance σ_{inh} in the above formulas is replaced with σ_{tot}.

3. Results and discussion

3.1. Simulation results under experimental conditions

Based on the above analysis, the performance of the DO-QKD system under encoding parameters $N=4$ and $I=3$ is simulated. The main parameters used in the simulation (in accordance with the experiment in [9]) are shown in Table 1, where R and $R_{s,i}$ refer to the corresponding generation rates at the output of the quantum light source.

When the bin width is the same 160 ps that is the same with the experiment in [9], the raw key generation rate is 151 kbps with a QBER of 3.69%. Through security analysis, in the case of 20-km transmission with dispersion compensation, the Shannon information between Alice and Bob $I(A;B)$ is established as 3.83 bit per coincidence (bpc), and Eve's Holevo information $\chi(A;E)$ is 0.01 bpc. As a

Table 1
Major parameters (P) used in the simulation of DO-QKD system.

Parameter	Value	Parameter	Value	Parameter	Value
R	4.08×10^6 Hz	$R_{s,i}$	6.08×10^6 Hz	L	20 km
α	0.2 dB/km	D	17 ps/nm/km	l	3 dB
η_d	50%	d_d	100 Hz	σ_{inh}	63.7 ps

result, the secret key capacity ΔI is 3.44 bpc, leading to the secret key rate of 129.9 kbps. The simulation results are mostly consistent with the experimental results in the previous work [9]. It is believed that the model can be used to describe and further analyze the DO-QKD system.

3.2. Impact of DCM on DO-QKD

In order to investigate the impact of DCM on DO-QKD, the performance of the system under 20-km fiber transmission is shown in Fig. 3. The solid lines are the results of using DCM (with a loss of 3 dB) in the system, while the dashed lines show those without DCM. Without dispersion compensation, σ_{tot} of the temporal distribution at Bob's side under 20-km fiber transmission is broadened from 63.7 ps to 81.6 ps. The bin sifting process is affected as follows: The error bits caused by coincidence counts in different slots increases, hence QBER of the system increases. The bin width at the minimum QBER becomes wider, because the larger bin width is needed to cover the broadened temporal distribution. By introducing the three-level optimization format [9], we optimize the parameters of the bin sifting process, further reducing QBER and increasing the raw key rate. The bin width τ after the three-level optimization (under the QBER upper bound of 5%) is 260 ps with DCM, while it reduces to 230 ps without DCM. Since the loss introduced by DCM is avoided, the raw key rate is higher than that with dispersion compensation. However, the raw key rate is not necessarily related to QKD performance. It is necessary to perform security analysis on the system to obtain the secret key rate.

The security analysis shows that the secret key capacity $\Delta I < 0$ in the case of 20-km transmission without dispersion compensation. It deteriorates greatly due to the uncompensated fiber dispersion. In this situation, no secret keys can be extracted from raw ones after error correction and privacy amplification. Therefore, dispersion compensation must be performed in the DO-QKD system under 20-km optical fiber transmission.

3.3. Results under different transmission conditions

Chromatic dispersion leads to the broadening of the temporal distribution of Bob's photons, which results in the increase of QBER and decrease of the secret key rate. The DCM can compensate for the dispersion, whereas it introduces additional losses on the optical links, which would reduce the coincidence counts available for key generation. Hence, the benefits and costs of dispersion compensation should be analyzed to obtain a higher secret key rate. There is a theoretical transmission range in which the performance of the DO-QKD system without dispersion compensation is better than that with dispersion compensation. In this case without dispersion compensation, the increase in the effective coincidence counts makes up for the decrease in the secret key capacity in terms of secret key generation.

The calculation results of a DO-QKD system with parameters set as Table 1 (except the variable fiber length L and dispersion parameter D) are shown in Fig. 4. Fig. 4 (a) shows the calculated secret key rate under increasing fiber length when G.652 fiber ($D = 17$ ps/km/nm at the wavelength of 1550 nm) is applied in the system. The black squares are the results that a DCM (with a loss of 3 dB) is used in the system. The white circles show those without DCM. It can be seen that when the transmission distance is relatively short, the system without DCM has better performance. However, the performance of the system with DCM is better when the transmission fiber is over 9 km, since the performance deterioration due to the fiber dispersion is larger than the impact of the loss of DCM. It proves that dispersion compensation is unnecessary in DO-QKD for the short-distance transmission.

Fig. 4 (b) shows the calculated secret key rate under increasing fiber length when G.655 fiber ($D = 5$ ps/km/nm with the wavelength of 1550 nm) is applied. It can be seen that the results are similar with those in Fig. 4 (a). Whereas, the system without DCM has better performance when the fiber length is less than 30 km due to the lower dispersion parameter of the G.655 fiber.

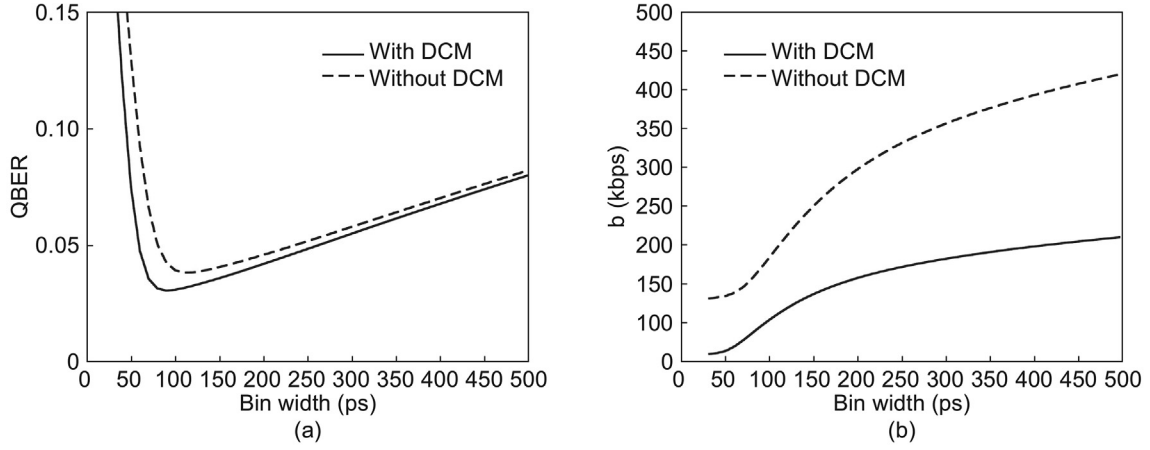

Fig. 3. Influence of dispersion compensation on (a) QBER and (b) raw key generation rate b. And high-dimensional encoding parameters: $N = 4$ and $I = 3$.

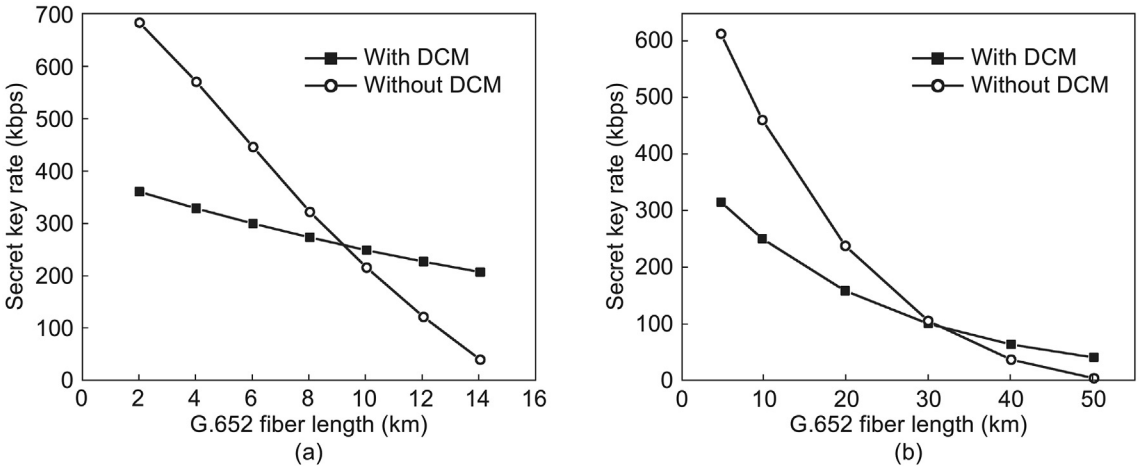

Fig. 4. Secret key rates (optimized with the QBER upper bound of 5%) under increasing fiber length: (a) transmission fiber is G.652 fiber and (b) transmission fiber is G.655 fiber.

4. Conclusions

In this work, we theoretically investigate the influence of chromatic dispersion introduced by transmission fiber on the performance of the DO-QKD system. We firstly establish a theoretical model of the entanglement-based DO-QKD system, and proved the feasibility of the model. Fiber dispersion will greatly deteriorate the performance of the DO-QKD system. However, it is shown that dispersion compensation is not unnecessary when the transmission distance is relatively short. Using G.652 fiber, the DO-QKD system without DCM has better performance when the fiber length is less than 9 km, while this range increases to 30 km using G.655 fiber due to its lower dispersion parameter. The above results provide theoretical guidance for practical applications of DO-QKD. It shows that in the application scenarios of campus networks and community access networks, the dispersion compensation in DO-QKD is not unnecessary. If transmission fibers with lower dispersion are applied, such as G.655 fiber, DO-QKD without dispersion compensation even can be used in metro networks.

Declaration of competing interest

The authors declare no conflicts of interest.

Acknowledgment

The authors would like to express their appreciation for the support of Tsinghua Initiative Scientific Research Program.

Appendix A. Number of coincidence events between Alice and Bob

For the cases that Alice records signal photons and noise events, the temporal distribution at Bob's side are expressed as the two distribution functions $B_1(t)$ and $B_2(t)$. It is regarded as a correct coincidence event when the time recorded by Bob is in the same bin with t_0. The number of correct coincidence events is denoted by X_1:

$$X_1 = \frac{1}{2}10^{-l/10}\eta_d R \int_{t_{m_0,i}}^{t_{m_0,e}} B_1(t)\mathrm{d}t + \left(\frac{1}{2}10^{-l/10}\eta_d R_s + d_d\right)\int_{t_{m_0,i}}^{t_{m_0,e}} B_2(t)\mathrm{d}t \tag{A1}$$

where $t_{m_0,i}$ and $t_{m_0,e}$ represent the initial and end time of the bin containing t_0, which is in the m_0 slot. The integrals with respect to t are shown in the black areas in Fig. 2.

Other coincidence events are regarded as error coincidence events. The number of error coincidence events in the m slot is denoted by $X_{2,m}(m \neq m_0)$:

$$X_{2,m} = \frac{1}{2}10^{-l/10}\eta_d R \int_{t_{m,i}}^{t_{m,e}} B_1(t)\mathrm{d}t + \left(\frac{1}{2}10^{-l/10}\eta_d R_s + d_d\right)\int_{t_{m,i}}^{t_{m,e}} B_2(t)\mathrm{d}t, \tag{A2}$$

where $t_{m,i}$ and $t_{m,e}$ represent the initial and end time of the bin with the same bin number of t_0 in the m slot. The integrals with respect to t are shown in the gray areas in Fig. 2. Hence the total number of error coincidence events is expressed as

$$X_2 = \sum_{m=1, m\neq m_0}^{2^N} X_{2,m} \tag{A3}$$

Appendix B. Numerical characteristics of random variables T_A and T_B

We assume that Alice and Bob both detect a single-photon event in a given time frame. At Alice's and Bob's sides, the arrival-time measurement parameters in the time base are described as

$$T_A = \begin{cases} T_{A1}, & \text{with probability } P_1 \\ T_{A2}, & \text{with probability } P_2 \end{cases} \tag{B1}$$

$$T_B = \begin{cases} T_{B1} \\ T_{B2} \end{cases} = \begin{cases} T_{A1} + X, & \text{with probability } P_1 \\ T_{B2}, & \text{with probability } P_2. \end{cases} \tag{B2}$$

When Alice and Bob receive a pair of entangled photons, there is a strong temporal correlation between the recorded events of them. The probability of this case over all the coincidence counts is P_1. In other cases, there is no temporal correlation between the recorded events of both sides. We have

$$P_1 = \frac{R_{\text{co}}}{R_{\text{co}} + R_{\text{ac}}} \text{ and } P_2 = \frac{R_{\text{ac}}}{R_{\text{co}} + R_{\text{ac}}} \tag{B3}$$

where R_{co} is the coincidence count rate, R_{ac} is the accidental coincidence count rate in the time frame with width T, and $T \equiv 6\sigma_{\text{tot}}$. They are expressed by the known parameters as

$$R_{\text{co}} = \frac{1}{4} 10^{-(\alpha L + l)/10} \eta_d^2 R \tag{B4}$$

$$R_{\text{ac}} = \left[\frac{1}{2} 10^{-l/10} \eta_d (R + R_s) + d_d\right] \left[\frac{1}{2} 10^{-\alpha L/10} \eta_d (R + R_i) + d_d\right] T. \tag{B5}$$

At Alice's side, we assume that the arrival time T_A follows the uniform distribution in a time T, with zero mean. The numerical characteristics of T_A are expressed as

$$E[T_A] = 0 \text{ and } \text{Var}[T_A] = T^2/12. \tag{B6}$$

where $E[\cdot]$ means the mean of a random variable and $\text{Var}[\cdot]$ means the variance of a random variable. At Bob's side, the time difference X between T_{A1} and T_{B1} follows a gaussian distribution with zero mean and variance. $\sigma_{tot} T_{B2}$ also follows the uniform distribution in the time T, with zero mean. The random variables T_{A1} and X, T_{A2} and T_{B2} are independent. Since both the situations at Bob's side have zero mean, the numerical characteristics of T_B are simplified as:

$$E[T_B] = P_1 E[T_{B1}] + P_2 E[T_{B2}] = 0, \tag{B7}$$

$$\text{Var}[T_B] = P_1 \text{Var}[T_{B1}] + P_2 \text{Var}[T_{B2}] = T^2/12 + P_1 \sigma_{\text{tot}}^2. \tag{B8}$$

Based on the above analysis, the statistical characteristics between the random variables of both sides are derived as

$$\text{Cov}[T_A, T_B] = P_1 T^2/12, \tag{B9}$$

$$\text{Var}[T_B - T_A] = P_1 \sigma_{\text{tot}}^2. \tag{B10}$$

where $\text{Cov}[\cdot, \cdot]$ means the covariance between two random variables. The arrival-time parameters in the frequency base obey corresponding relations. We used the above statistical characteristics in security analysis to obtain the secret key rate [15].

References

[1] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proc. Of the Intl. Conf. on Computers, Systems, and SignaI Processing, Bangalore, 1984, pp. 175–179.
[2] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74 (1) (Jan. 2002) 145–195.
[3] H.-K. Lo, H.F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science 283 (5410) (Mar. 1999) 2050–2056.
[4] N. Gisin, R. Thew, Quantum communication, Nat. Photonics 1 (Mar) (2007) 165–171.

[5] M. Lucamarini, K.A. Patel, J.F. Dynes, et al., Efficient decoy-state quantum key distribution with quantified security, Opt Express 21 (21) (Oct. 2013) 24550–24565.
[6] C.-Z. Peng, J. Zhang, D. Yang, et al., Experimental long-distance decoy-state quantum key distribution based on polarization encoding, Phys. Rev. Lett. 98 (1) (Jan. 2007), 010505.
[7] X. Ma, C.-H.F. Fung, H.-K. Lo, Quantum key distribution with entangled photon sources, Phys. Rev. A 76 (1) (2007), 012307.
[8] I. Marcikic, A. Lamas-Linares, C. Kurtsiefer, Free-space quantum key distribution with entangled photons, Appl. Phys. Lett. 89 (10) (Sept. 2006) 101122.
[9] X. Liu, X. Yao, H.-Q. Wang, et al., Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km, Appl. Phys. Lett. 114 (14) (2019) 141104.
[10] X. Liu, X. Yao, R. Xue, et al., An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution, APL Photonics 5 (7) (Jul. 2020), 076104.
[11] S. Wehner, D. Elkouss, R. Hanson, Quantum Internet: a vision for the road ahead, Science 362 (6412) (Oct. 2018) eaam9288.
[12] S. Wengerowsky, S.K. Joshi, F. Steinlechner, H. Hubel, R. Ursin, An entanglement-based wavelength-multiplexed quantum communication network, Nature 564 (7735) (Dec. 2018) 225–228.
[13] I. Ali-Khan, C.J. Broadbent, J.C. Howell, Large-alphabet quantum key distribution using energy-time entangled bipartite states, Phys. Rev. Lett. 98 (6) (Feb. 2007), 060503.
[14] D. Bunandar, Z. Zhang, J.H. Shapiro, D.R. Englund, Practical high-dimensional quantum key distribution with decoy states, Phys. Rev. A 91 (2) (Feb. 2015), 022336.
[15] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J.H. Shapiro, D. Englund, High-dimensional quantum key distribution using dispersive optics, Phys. Rev. A 87 (6) (Jun. 2013), 062322.
[16] C. Lee, Z. Zhang, G.R. Steinbrecher, et al., Entanglement-based quantum communication secured by nonlocal dispersion cancellation, Phys. Rev. A 90 (6) (Dec. 2014), 062331.
[17] X. Liu, R. Xue, H.-Q. Wang, et al., Fully Connected Entanglement-based Quantum Communication Network without Trusted Node [Online]. Available, https://arxiv.org/abs/2011.11319.
[18] J.D. Franson, Nonlocal cancellation of dispersion, Phys. Rev. A 45 (5) (Mar. 1992) 3126–3132.
[19] Q. Zhou, W. Zhang, J.-R. Cheng, Y.-D. Huang, J.-D. Peng, Noise performance comparison of 1.5 μm correlated photon pair generation in different fibers, Opt Express 18 (16) (Aug. 2010) 17114–17123.
[20] R. Garcia-Patron, N.J. Cerf, Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution, Phys. Rev. Lett. 97 (19) (Nov. 2006), 190503.
[21] J.A. Grieve, Y. Shi, H.S. Poh, C. Kurtsiefer, A. Ling, Characterizing nonlocal dispersion compensation in deployed telecommunications fiber, Appl. Phys. Lett. 114 (13) (Apr. 2019) 131106.
[22] G.P. Agrawal, Nonlinear Fiber Optics, sixth ed., Academic Press, London, 2019, pp. 6–8.

Jing-Yuan Liu was born in Beijing in 1998. She received the B.S. degree in applied physics from Beijing University of Posts and Telecommunications, Beijing in 2020. She is currently pursuing the Ph.D. degree with the Department of Electronic Engineering, Tsinghua University, Beijing. Her research interests include quantum cryptography and quantum networks.

Xu Liu was born in 1990. He received the B.S. and M.S. degree from the College of Information Science and Engineering, Northeastern University, Shenyang in 2014 and 2017. He is currently pursuing the Ph.D. degree with the Department of Electronic Engineering, Tsinghua University. His current research interests include quantum cryptography and quantum networks, especially entanglement-based DO-QKD.

Wei Zhang was born in 1974. He received his B.S. degree from Tsinghua University in 1998 and his Ph.D. degree in physical electronics from the Institute of Information Optoelectronics, Department of Electronic Engineering, Tsinghua University in 2003. Then, he joined the Department of Electronic Engineering, Tsinghua University as a faculty. At present, he is the tenured professor with the Department of Electronic Engineering, Tsinghua University. At the same time, he works with the Beijing National Research Center for Information Science and Technology, Tsinghua University; with the Beijing Innovation Center for Future Chips, Tsinghua University; with Frontier Science Center for Quantum Information, Beijing; with Beijing Academy of Quantum Information Sciences, Beijing. His research interests include micro/nano-photonic quantum devices and their applications.

Yi-Dong Huang was born in Beijing. She received the B.S. and Ph.D. degrees in optoelectronics from Tsinghua University in 1988 and 1994, respectively. From 1991 to 1993, she was with Arai Laboratories, Tokyo Institute of Technology, Tokyo, on leave from Tsinghua University. Her Ph.D. dissertation was mainly concerned with strained semiconductor quantum well lasers and laser amplifiers. In 1994, she joined the Photonic and Wireless Devices Research Laboratories, NEC Corporation, Tokyo, where she was engaged in the research on semiconductor laser diodes for optical-fiber communications and became an assistant manager in 1998. She received "Merit Award" and "Contribution Award" from NEC Corporation in 1997 and 2003, respectively. She joined the Department of Electronic Engineering, Tsinghua University in 2003, as a professor, and was appointed as the Changjiang Distinguished Professor and the National Talents Engineering in 2005 and 2007, respectively. She was the Vice Chair of the Department of Electronic Engineering, Tsinghua University from 2007 to 2012 and the Chair of the department from 2013 to 2019. At present, she is the Vice Chair of Academic Committee of Tsinghua University. At the same time, she works with the Beijing National Research Center for Information Science and Technology, Tsinghua University; with the Beijing Innovation Center for Future Chips, Tsinghua University; with Frontier Science Center for Quantum Information; with Beijing Academy of Quantum Information Sciences. She is presently engaged in the research on micro/nano-structured optoelectronics.