Applied Physics Letters

Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km

Cite as: Appl. Phys. Lett. **114**, 141104 (2019); https://doi.org/10.1063/1.5089784
Submitted: 22 January 2019 . Accepted: 23 March 2019 . Published Online: 10 April 2019

Xu Liu, Xin Yao, Heqing Wang, Hao Li, Zhen Wang, Lixing You, Yidong Huang, and Wei Zhang

Applied Physics Letters ARTICLE scitation.org/journal/apl

Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km

Cite as: Appl. Phys. Lett. **114**, 141104 (2019); doi: 10.1063/1.5089784
Submitted: 22 January 2019 · Accepted: 23 March 2019 ·
Published Online: 10 April 2019

Xu Liu,[1,2] Xin Yao,[1,2] Heqing Wang,[3] Hao Li,[3] Zhen Wang,[3] Lixing You,[3] Yidong Huang,[1,2] and Wei Zhang[1,2,a)]

AFFILIATIONS

[1]Beijing National Research Center for Information Science and Technology (BNRist), Beijing Innovation Center for Future Chips, Electronic Engineering Department, Tsinghua University, Beijing 100084, China
[2]Beijing Academy of Quantum Information Sciences, Beijing 100193, China
[3]State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China

[a)]**Electronic mail:** zwei@tsinghua.edu.cn

ABSTRACT

An energy-time entanglement-based dispersive optics quantum key distribution (DO-QKD) is demonstrated experimentally over optical fibers of 20 km. In the experiment, the telecom band energy-time entangled photon pairs are generated through spontaneous four-wave mixing in a silicon waveguide. The arrival time of photons is registered for key generation and security test. High-dimensional encoding in the arrival time of photons is used to increase the information per coincidence of photon pairs. The bin sifting process is optimized by a three-level structure, which significantly reduces the raw quantum bit error rate (QBER) due to timing jitters of detectors and electronics. A raw key generation rate of 151 kbps with a QBER of 4.95% is achieved, in a time bin encoding format with 4 bits per coincidence. This experiment shows that the entanglement-based DO-QKD can be implemented in an efficient and convenient way, which has great potential for quantum secure communication networks in the future.

Quantum key distribution (QKD) permits remote parties to share secret keys. The secret keys can be further used for symmetric encryption, such as the one-time pad encryption scheme, which provides information-theoretic secure message transmission. Since the first protocol (BB84)[1] was proposed, the QKD has been developed significantly.[2–5] From the point of QKD implementation, there are mainly two kinds of QKD schemes, which are the prepare-and-measurement (P&M) schemes[6,7] and the entanglement-based schemes.[8,9] The entanglement-based QKD has inherent random local results and correlated outcomes. No extra random number generators are required in these schemes. On the other hand, if it could be swapped with high fidelity by quantum repeater nodes, photonic entanglement could be extended over long distances, which is promising to realize global scale quantum networks.[10] Hence, the entanglement-based QKD is important as a basic function of future quantum secure communication networks.

Dispersive optics QKD (DO-QKD) is a promising QKD protocol[11] developed in recent years, which is robust in system stability and convenient in implementation. In DO-QKD, normal and anomalous dispersion components are introduced at Alice and Bob's sides, constructing the time-frequency bases. The security test of DO-QKD can be realized by measurements of unbiased time-frequency bases, which has been proven to be secure against collective attacks.[11] The P&M protocols of DO-QKD have been demonstrated by field experiments with a high key rate of 1.2 Mbps over optical fibers of 43 km.[12] However, the entanglement-based DO-QKD was only demonstrated by short fiber links with relatively low key generation rates.[13] In this work, we experimentally realized the entanglement-based DO-QKD over single mode optical fibers of 20 km. Energy-time entangled photon pairs were used in this experiment, which were generated by spontaneous four-wave mixing (SFWM) in a piece of silicon waveguide. In order to enhance the key generation rate, high-dimensional encoding was used to increase the information per coincidence of photon pairs. On the other hand, the bin sifting process was optimized by a three-level structure, which significantly reduced the quantum bit error rate (QBER) of raw keys due to timing jitters of detectors and electronics.

This experiment shows an efficient and convenient way to realize the entanglement-based DO-QKD.

The experimental setup of energy-time entanglement-based DO-QKD is shown schematically in Fig. 1. At Alice's side, energy-time entangled photon pairs are generated through the SFWM effect in a piece of silicon waveguide under CW pumping. The length of the waveguide is 5 mm and the wavelength of the pump light is 1549.32 nm. Then, the signal and idler photons of each photon pair are selected out by a filter system made of cascaded dense wavelength division multiplexers. The central wavelengths of the generated signal and idler photons are 1546.12 nm and 1552.52 nm, respectively. Signal photons are used for Alice's local measurement. The idler photons are sent to Bob through single mode fibers of 20 km. A dispersion compensation module (DCM) is introduced to compensate the dispersion introduced by the optical fibers. On each side, a 50:50 fiber coupler routes photons into two paths randomly. In one path, photons are detected directly, which corresponds to the time basis, and the time of single photon detection events is recorded, which is mainly used for key generation. In the other path, photons are detected and recorded after a normal dispersion (ND, at Alice's side) or an abnormal dispersion (AD, at Bob's side) module (±1800 ps/nm), which correspond to the frequency basis and are used for security test. In the experiments, four NbN superconducting nanowire single-photon detectors (SNSPDs, fabricated by SIMIT, CAS, China) are used, with a detection efficiency of 50% at 1550 nm. Their dark-count rates are about 100 counts per second and the average timing jitters are 80 ps. Single photon events are precisely recorded with a time-to-digital converter (TCSPC, PicoQuant HydraHarp 400) at a resolution of 1 ps and then sent to a computer for data processing.

At Alice and Bob's sides, photons are detected by either the time basis or frequency basis, and their time resolved coincidences are used for security test. The coincidences between the photons of time bases on both sides show a narrow peak. The full width at half maximum (FWHM) of the coincidence peak is mainly determined by the timing jitters of single photon detectors. The coincidence of photons of frequency bases also shows a narrow peak, which is the effect of nonlocal dispersion cancelation introduced by the AD and ND components at Alice and Bob's sides. On the contrary, if the coincidence measurement is taken between the photons of different bases on the two sides, the coincidence peak is broadened by the dispersive component at the frequency basis. In this way, the unbiased time-frequency bases are constructed by introducing the dispersive components. Based on the single photon events detected under frequency bases and a part of events detected under time bases, joint measurements of time-frequency covariance matrix (TFCM) can be carried out. It is used to evaluate Shannon information between Alice and Bob and Eve's maximum accessible information, which are responsible for the system security.[11] The secure information that Alice and Bob could extract per coincidence[14,15] is expressed as

$$\Delta I = \beta I(A;B) - \chi(A;E), \tag{1}$$

where β is the reconciliation efficiency and $I(A;B)$ is the Shannon information between Alice and Bob. Eve's maximum accessible information is quantified by the Holevo information $\chi(A;E)$. To evaluate ΔI, the security analysis of DO-QKD follows the well-established proofs for protocols of the Gaussian continuous-variable quantum key distribution (CV-QKD), which are based on the optimality of Eve's Gaussian collective attack for a given TFCM.[15–17] Eve's actions will disturb Alice and Bob's initial TFCM. The excess spectral noise factor ξ_w is used to quantify the disturbance towards the TFCM, which is expressed as

$$\xi_w = \frac{\sigma_w^2}{\sigma_{w_0}^2} - 1, \tag{2}$$

where σ_w^2 quantifies the spectral correlation between the detected photons at Alice and Bob and $\sigma_{w_0}^2$ represents the noiseless correlation excluding the excess channel noise or Eve's intrusion. For practical measurements, we take the back-to-back experiment configuration with negligible channel loss as the noiseless correlation case. The corresponding correlation characteristics between Alice and Bob are treated as the noiseless correlation $\sigma_{w_0}^2$. Then, $I(A;B)$ and $\chi(A;E)$ can be calculated by the covariance matrix approach,[11,15] and ΔI can be estimated according to Eq. (1).

Alice and Bob build their raw keys from correlated single photon events acquired in the time bases. The single photon events are sifted in a large-alphabet way to increase the information per coincidence,[18] in a format of high-dimensional encoding shown in Fig. 2. In the format, a time frame includes $M(M=2^N)$ consecutive slots and a slot including I time bins. The bin width is denoted τ. In the sifting process, firstly, Alice and Bob communicate their frame numbers with one single photon detection event and keep the frames they both obtained in one event. Then, for each kept frame, Alice and Bob check their time bin numbers which indicate the time bins they recorded their detection events. In Fig. 2, the two pulses with red color indicate the correlated detection events and the two pulses with light green

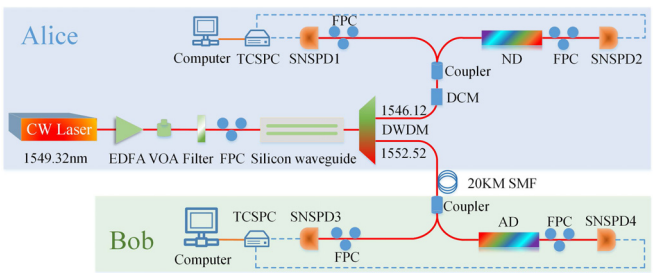

FIG. 1. The setup of an entanglement-based DO-QKD. EDFA: Erbium-doped fiber amplifier; VOA: variable optical attenuator; FPC: fiber polarization controller; DWDM: dense wavelength division multiplexing filter; DCM: dispersion compensation module; ND: normal dispersion; AD: anomalous dispersion; and TCSPC: time-correlated single-photon counting module.

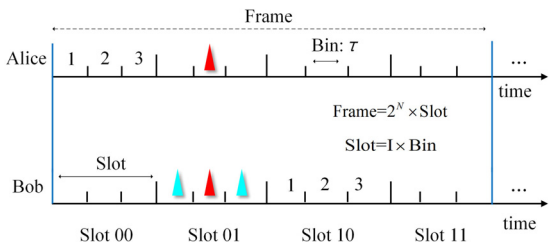

FIG. 2. The format of high-dimensional encoding in the experiment. A frame has $M=2^N$ slots and a slot has I bins. In this example, $I=3$, $N=2$, and $M=4$.

color indicate the possible errors due to the non-zero coincidence peak width, which is mainly due to timing jitters of single photon detectors in this experiment setup. It can be expected that the checking process of time bin numbers can significantly reduce the QBER.[18] If the time bin numbers of Alice and Bob are the same, the frame is selected in which the single photon detection events at Alice and Bob are considered as a coincidence event. Eventually, the raw keys are generated by the slot numbers of the coincidence events in the selected frames at Alice and Bob. Therefore, in this format, one coincidence event generates raw keys of $N = log_2 M$ bits. It can be seen that Alice and Bob do not directly communicate the information of slots and avoid revealing the slot numbers to Eve. The parameters of this bin sifting process should be optimized according to the system conditions, which determine the performance of key generation. After the bin sifting processes, raw keys are generated at Alice and Bob and then they proceed to perform error correction and privacy amplification to generate secret keys.

As shown in Fig. 1, the time bases and frequency bases at Alice and Bob's sides are marked as T1, F1, T2, and F2, respectively. The experiments were carried out with an optical fiber transmission of 20 km under a pump level that the single photon count rates of SNSPDs of the four corresponding bases were 554 kHz, 321 kHz, 315 kHz, and 245 kHz, respectively. Figure 3 shows the time resolved coincidence counts between Alice and Bob in four possible basis combinations, which were acquired in 5 s and used to take the calculation of security test of DO-QKD. The bin width for the coincidence measurement is 30 ps. It should be noted that only 30% of the single photon detection events of time bases at Alice and Bob were selected randomly to calculate the coincidences for the security test, and rest of them were used to generate raw keys.

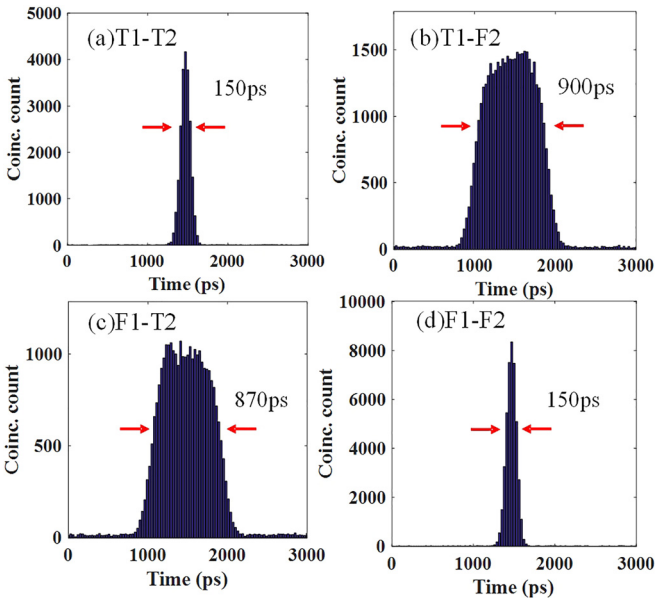

FIG. 3. Time resolved coincidence counts between Alice and Bob in four possible basis combinations. (a) Coincidence counts under T1 and T2. (b) Coincidence counts under T1 and F2. (c) Coincidence counts under F1 and T2. (d) Coincidence counts under F1 and F2. All the coincidence counts were acquired in 5 s.

Figure 3(a) shows the coincidence counts of T1-T2. It can be seen that the coincidence peak of single photon detection events recorded under time bases at both Alice and Bob is a narrow peak with a FWHM of 150 ps. The timing jitters of SNSPDs mainly contribute to the peak width. Figures 3(b) and 3(c) show the coincidences of T1-F2 and F1-T2, i.e., the single photon detection events are recorded under different bases at Alice and Bob. In these two cases, the coincidence peaks are broadened to 900 ps and 870 ps, respectively, by the dispersive components at the frequency bases. Figure 3(d) shows the coincidences of F1-F2. In this case, the single photon events were recorded under frequency bases on both sides. It can be seen that the narrow coincidence peak recovers due to the nonlocal dispersion cancelation with a FWHM of 150 ps. According to the experimental results shown in Fig. 3, the corresponding TFCM can be calculated. By further decomposing the TFCM, we obtained an upper bound on the Holevo information of $\chi(A; E) = 0.211$ bpc (bit per coincidence), which indicates the impact of the excess channel noise and the possible disturbance of Eve introduced by the fiber transmission.

For the key generation, Alice and Bob built their keys from 70% of the single photon detection events acquired in the time bases on both sides. Figure 4 shows the performances of the coincidence events for key generation. Figure 4(a) shows a typical coincidence peak between the detection events that Alice and Bob recorded at time bases. The coincidence was recorded with a time bin of 160 ps. The corresponding coincidence rate and the coincidence to accidental coincidence ratio (CAR) were 35.6 KHz and 217, respectively. It can be seen that the central time bin in the coincidence peak has the maximum contribution to the coincidence. Here, we defined the coincidence count rate record in this time bin as the effective coincidence count rate, since only the coincidence events in this bin contribute to the key generation according to the bin sifting process. It can be expected that the reduction of the bin width would lead to the decrease of the effective coincidence count rate if the bin width was smaller than the width of the coincidence peak. The effective CAR was defined as the ratio between the effective coincidence rate and the average accidental coincidence rate in bins outside the coincidence peak. Figure 4(b) shows the effective coincidence count rate and the effective CAR calculated with different time bin widths. It can be seen that the effective coincidence rate increases obviously with increasing time bin width, which shows that the increase in the bin width would improve

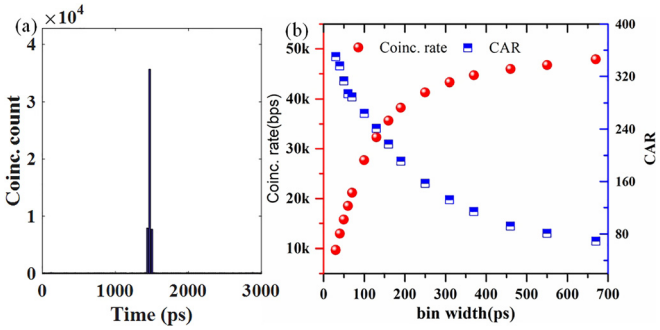

FIG. 4. The performance of coincidence events for key generation. (a) A typical time resolved coincidence peak with a time bin of 160 ps. (b) The coincidence rate and the coincidence to accidental coincidence ratio (CAR) at different time bin widths.

the key generation rate. While, the effective CAR decreases with increasing bin width since the accidental coincidence count rate in one bin increases more rapidly. It can be expected that a smaller bin width is preferred to reduce the QBER of the raw key. Hence, tradeoff should be taken on the bin width selection.

To optimize the performance of the DO-QKD system in this work, we firstly considered a specific three-level format, in which a frame has 16 slots, hence, $N = 4$. The raw key generation rate and the QBER were calculated according to the experimental data obtained with different bin widths τ and bin numbers I in a slot. The results are shown in Fig. 5.

Figure 5 shows that the raw key generation rate increases with increasing bin width; on the other hand, the QBER also mainly increases with increasing bin width for all the bin numbers I. These results can be explained by Fig. 4(b). However, in the case of $I = 3$, the QBER increases with decreasing bin width when the bin width is small. The reason is that if the slot is too narrow to cover the coincidence peak, the coincidence is located in the same bin but the adjacent slots on the two sides would introduce obvious errors. Hence, there is a bin width for the minimum QBER when $I = 3$. It can be expected that in the cases of $I = 4$ and 5, minimum QBERs also exist. However, they would appear at smaller bin widths which is not shown in Fig. 5, since they have larger slot widths if the bin width is fixed. To optimize the performance when $I = 3$, we could choose appropriate parameters to achieve a maximum raw key generation rate with a specific QBER requirement according to Fig. 5, which is determined by the need for the error correction efficiency considering the whole postprocessing execution speed and the throughput rate of the whole system. For example, if the requirement is set as QBER $\leq$ 5%, we could obtain the optimized parameters that the bin width τ of 160 ps and the bin number in a slot I as 3. In this case, the raw key generation rate is 151 kbps with a QBER of 4.95%.

Then, we calculated the system performance with different dimensions N and obtained the optimized format parameters and the corresponding system performance at QBER $\leq$ 5%. The results are shown in Fig. 6. It can be seen that the raw key generation rate reaches its maximum (151 kHz) when the dimension is $N = 4$ with a bin width

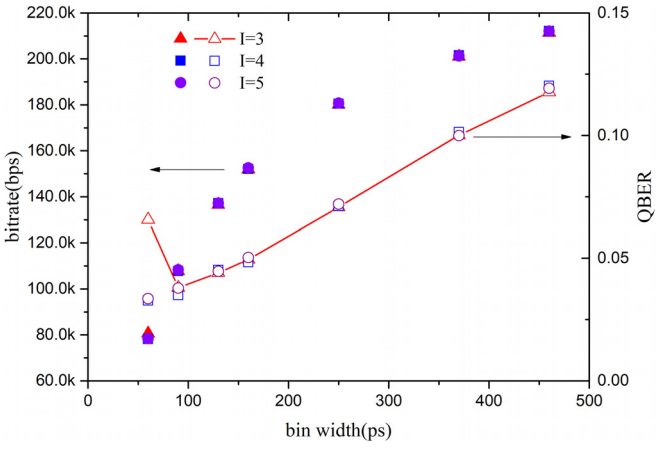

FIG. 5. Raw key generation rate and QBER at different bin widths τ and division numbers I.

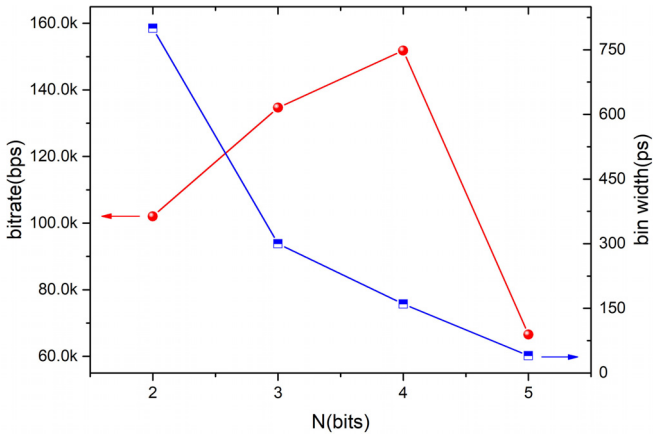

FIG. 6. Optimized bit rate and the corresponding bin widths with different dimensions N with QBERs all bounding below 5%.

of 160 ps. If N is smaller than 4, the key generation per coincidence is limited. On the other hand, if the dimension N increases to $N = 5$, a smaller bin width is required to guarantee QBER $\leq$ 5%, which highly reduces the effective coincidence count rate. It is worth noting that in this work the QBER is highly restrained by the three-level bin sifting process. The QBER of raw keys would be up to ~25% if the bin sifting process was not carried out. It is well known that a complete QKD protocol requires error reconciliation processes and the raw key error rate would highly impact the expense of the error correction processes.[19] Hence, the bin sifting is necessary to reduce the raw key error and save the expense of error reconciliation. It is interesting to compare the bin sifting process and the error correction algorithms. The classical error correction algorithms deal with all the errors, whatever their sources. Previous works have shown that the error reconciliation based on these algorithms still have space to be optimized.[20] On the other hand, the bin sifting process is designed to overcome a specific error source in high dimensional time encoding with high efficiency. Hence, the bin sifting process may provide a way to further improve the performance of error reconciliation of QKD protocols with high-dimensional time encoding, if it is introduced as a step of error reconciliation.

We optimized the parameters of the format according to Figs. 5 and 6. As a result, a raw key generation rate of 151 kbps with a QBER of 4.95% can be achieved at $N = 4$, $I = 3$ and $\tau = 160$ ps. Then, in this case, secret keys were extracted from raw ones after error correction and privacy amplification. Based on the acquired raw key with a low QBER, the low-density parity-check (LDPC) code[21] was adopted for error correction, which was efficient in data interaction. The reconciliation efficiency $\beta = 90\%$ was achieved at this low QBER (4.95%). Privacy amplification was implemented using hash functions.[22] The secret key rate could be estimated using Eq. (1). The analysis of Fig. 3 has shown that Eve's Holevo information $\chi(A; E)$ is 0.211 bpc, which is estimated by the calculated TFCM. The Shannon information between Alice and Bob $I(A; B)$ can be estimated in a similar way, which is 3.48 bpc in this experimental system. As a result, the secret key capacity ΔI is 2.92 bpc according to Eq. (1), leading to a secret key rate of 104 kbps.

In this paper, we experimentally demonstrate the entanglement-based DO-QKD with high-dimensional encoding over optical fibers of 20 km, in which the energy-time entangled photon pairs are generated by the SFWM in a piece of silicon waveguide. A DCM is utilized to compensate the chromatic dispersion introduced by single mode fibers of 20 km. By three-level bin sifting towards the single photon events measured based on the time bases, the QBER is significantly reduced to about 4.95% at a raw key rate of 151 kbps. The whole system is secured by nonlocal dispersion cancelation based on dispersive optics. Finally, a secure key capacity of 2.92 bpc is achieved after subtracting Eve's Holevo information. These experimental results show that an entanglement-based DO-QKD protocol can be implemented in an efficient and practicable way. It has great potential for quantum secure communication networks in the future.

This work was supported by the National Key R&D Program of China under Contract No. 2017YFA0303704 and No. 2017YFA0304000; the National Natural Science Foundation of China under Contract No. 61575102, No. 91750206, No. 61671438, No. 61875101 and No. 61621064; Beijing National Science Foundation under Contract No. Z180012; and Beijing Academy of Quantum Information Sciences under Contract No. Y18G26.

REFERENCES

[1]H. Bennett Ch and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computers, Systems and Signal Processing* (Bangalore, India, 1984), pp. 175–179.
[2]C. H. Bennett, G. Brassard, and N. David Mermin, "Quantum cryptography without bell's theorem," Phys. Rev. Lett. **68**, 557–559 (1992).
[3]X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
[4]Y. Zhao, B. Qi, and H.-K. Lo, "Experimental quantum key distribution with active phase randomization," Appl. Phys. Lett. **90**(4), 044106 (2007).
[5]A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 GHz time-bin quantum key distribution," Appl. Phys. Lett. **112**(17), 171108 (2018).
[6]C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," Phys. Rev. Lett. **98**, 010505 (2007).
[7]M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," Opt. Express **21**(21), 24550–24565 (2013).
[8]X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," Phys. Rev. A **76**, 012307 (2007).
[9]I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," Appl. Phys. Lett. **89**(10), 101122 (2006).
[10]H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," Phys. Rev. Lett. **81**, 5932–5935 (1998).
[11]J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, "High-dimensional quantum key distribution using dispersive optics," Phys. Rev. A **87**, 062322 (2013).
[12]C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. Ben Dixon, F. N. C. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, "High-rate field demonstration of large-alphabet quantum key distribution," preprint arXiv:1611.01139 (2016).
[13]C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R. D. Horansky, V. B. Verma, A. E. Lita, R. P. Mirin, F. Marsili, M. D. Shaw, S. W. Nam, G. W. Wornell, F. N. C. Wong, J. H. Shapiro, and D. Englund, "Entanglement-based quantum communication secured by nonlocal dispersion cancellation," Phys. Rev. A **90**, 062331 (2014).
[14]I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A: Math., Phys. Eng. Sci. **461**(2053), 207–235 (2005).
[15]R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," Phys. Rev. Lett. **97**, 190503 (2006).
[16]C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621–669 (2012).
[17]A. Serafini, F. Illuminati, and S. De Siena, "Symplectic invariants, entropic measures and correlations of Gaussian states," J. Phys. B: At., Mol. Opt. Phys. **37**(2), L21 (2004).
[18]I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states," Phys. Rev. Lett. **98**, 060503 (2007).
[19]L. Qiong, L. Dan, M. Haokun, N. Xiamu, L. Tian, and G. Hong, "Study on error reconciliation in quantum key distribution," Quantum Inf. Comput. **14**(13-14), 1117–1135 (2014).
[20]D. Elkouss, J. Martinez-Mateo, and V. Martin, "Information reconciliation for quantum key distribution," Quantum Inf. Comput. **11**(3&4), 226–238 (2011).
[21]R. Gallager, "Low-density parity-check codes," IRE Trans. Inf. Theory **8**(1), 21–28 (1962).
[22]D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," Phys. Rev. Lett. **77**, 2818–2821 (1996).