

PAPER • OPEN ACCESS

# High-dimensional quantum key distribution using energy-time entanglement over 242 km partially deployed fiber

To cite this article: Jingyuan Liu *et al* 2024 *Quantum Sci. Technol.* **9** 015003

View the [article online](#) for updates and enhancements.

You may also like

- [Practical aspects of measurement-device-independent quantum key distribution](#)  
Feihu Xu, Marcos Curty, Bing Qi et al.
- [Quantum cryptography and combined schemes of quantum cryptography communication networks](#)  
A.Yu. Bykovsky and I.N. Kompanets
- [Coexistence of continuous variable QKD with intense DWDM classical channels](#)  
Rupesh Kumar, Hao Qin and Romain Alléaume

# Quantum Science and Technology



## PAPER

# High-dimensional quantum key distribution using energy-time entanglement over 242 km partially deployed fiber

### OPEN ACCESS

#### RECEIVED

29 January 2023

#### REVISED

9 August 2023

#### ACCEPTED FOR PUBLICATION

28 September 2023



#### PUBLISHED

12 October 2023

Original Content from this work may be used under the terms of the [Creative Commons Attribution 4.0 licence](https://creativecommons.org/licenses/by/4.0/).

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.



Jingyuan Liu<sup>1</sup> , Zhihao Lin<sup>1</sup>, Dongning Liu<sup>1</sup>, Xue Feng<sup>1</sup>, Fang Liu<sup>1</sup>, Kaiyu Cui<sup>1</sup>, Yidong Huang<sup>1,2</sup> and Wei Zhang<sup>1,2,\*</sup> 

<sup>1</sup> Frontier Science Center for Quantum Information, Beijing National Research Center for Information Science and Technology (BNRist), Electronic Engineering Department, Tsinghua University, Beijing 100084, People's Republic of China

<sup>2</sup> Beijing Academy of Quantum Information Sciences, Beijing 100193, People's Republic of China

\* Author to whom any correspondence should be addressed.

E-mail: [zwei@tsinghua.edu.cn](mailto:zwei@tsinghua.edu.cn)

**Keywords:** : quantum key distribution, entanglement distribution, quantum communication, field test

## Abstract

Entanglement-based quantum key distribution (QKD) is an essential ingredient in quantum communication, owing to the property of source-independent security and the potential on constructing large-scale quantum communication networks. However, implementation of entanglement-based QKD over long-distance optical fiber links is still challenging, especially over deployed fibers. In this work, we report an experimental QKD using energy-time entangled photon pairs that transmit over optical fibers of 242 km (including a section of 19 km deployed fibers). The QKD is realized through the protocol of dispersive-optics QKD (DO-QKD) with high-dimensional encoding to utilize coincidence counts more efficiently. A reliable, high-accuracy time synchronization technology for long-distance entanglement-based QKD is developed based on the distribution of optical pulses in quantum channels. Our system operates continuously for more than 7 d without active polarization or phase calibration. We ultimately generate secure keys with secure key rates of 0.22 bps and 0.06 bps in the asymptotic and finite-size regimes, respectively. It shows that entanglement-based DO-QKD is reliable for long-distance realization in the field if its high requirement on time synchronization is satisfied.

## 1. Introduction

Quantum key distribution (QKD) establishes information-theoretically secure keys between two remote users [1]. Since the first QKD protocol (BB84) was proposed [2], many progresses have been achieved theoretically and experimentally in tackling the potential attack from eavesdropper [3–9], extending the QKD distance [10–18] and improving the secure key rate (SKR) [19, 20]. Among the different experimental implementations of QKD, the entanglement-based scheme [21, 22] exploits the intrinsic correlation of quantum entanglement to distribute cryptographic keys, which dispenses with the need for random number generators. It also has source-independent security and the possibility to realize device-independent QKD [5, 9]. Moreover, researchers have recently shown that through entanglement distribution between end users, large-scale quantum networks with fully-connected topology can be established [23, 24]. It can be expected that the long-distance entanglement-based QKD with deployed fiber is a crucial technology for future global quantum communication networks.

Enormous efforts have been made to realize entanglement-based QKD under long-distance fiber transmission in the laboratory [25, 26] and in the field [27]. Recently, researchers have shown the entanglement distribution of polarization entangled photon pairs along 248 km deployed fiber and calculated its SKRs [28]. Since the distribution of polarization entanglement over optical fibers is sensitive to environmental variations, dedicated polarization calibration is necessary for these works to compensate for polarization drift, and the active calibration process is required from time to time to reduce the quantum bit error rate (QBER) to a sufficiently low level [28, 29]. Among entanglement on different degrees of freedom

(DOFs), the energy-time entanglement and its discrete form, i.e. time-bin entanglement, are promising candidates for long-distance entanglement-based QKD thanks to its convenience in generation and manipulation, and resilience to environment variations in fiber transmission. To the best of our knowledge, the maximum fiber transmission distance of entanglement distribution of energy-time and time-bin entanglement is 300 km in the laboratory [30], and about tens of kilometers in the field [31, 32]. As for entanglement-based QKD using energy-time and time-bin entanglement, the researchers are mainly carried out in the laboratory environment [25, 26]. As far as we know, the longest implementation with deployed fiber is demonstrated in a link of a quantum network, with a total fiber length of 108 km including deployed fiber of 26.8 km [33]. The experiment was conducted for about 12 h with the aid of time synchronization and phase alignment. It makes the real-scenario implementation of entanglement-based QKD with longer transmission and long-term operation become a critical issue to be solved.

Quantum entanglement is the precious resource for entanglement-based QKD. To exploit detected photon pairs (or photons) more efficiently, high-dimensional QKD (HD-QKD) is proposed to perform multi-level encoding using qudits with dimension  $D > 2$  [34]. The HD-QKD can increase the shared secure keys between Alice and Bob for each detected photon pair (or photon), meanwhile, it would offer better robustness against channel noise. High-dimensional quantum information can be encoded in many DOFs, such as energy-time [19, 34], transverse momentum [35], and orbital angular momentum [36, 37]. Recently, many progresses have been made in dispersive-optics QKD (DO-QKD) [38–41], which encodes photons in continuous temporal modes in a large-alphabet way, combining the high-dimensional Hilbert spaces of continuous-variable QKD (CV-QKD) with single-photon detection. The DO-QKD protocol uses dispersive optics to construct frequency bases, avoiding the need for phase stabilization in Franson interferometers used in the regular time-bin entanglement QKD. However, previous entanglement-based DO-QKD experiments over optical fibers were all under laboratory conditions with limited fiber length. It is necessary to develop the techniques supporting its robust operation in the field over a long time, and to explore its capacity for ultra-long-distance realization.

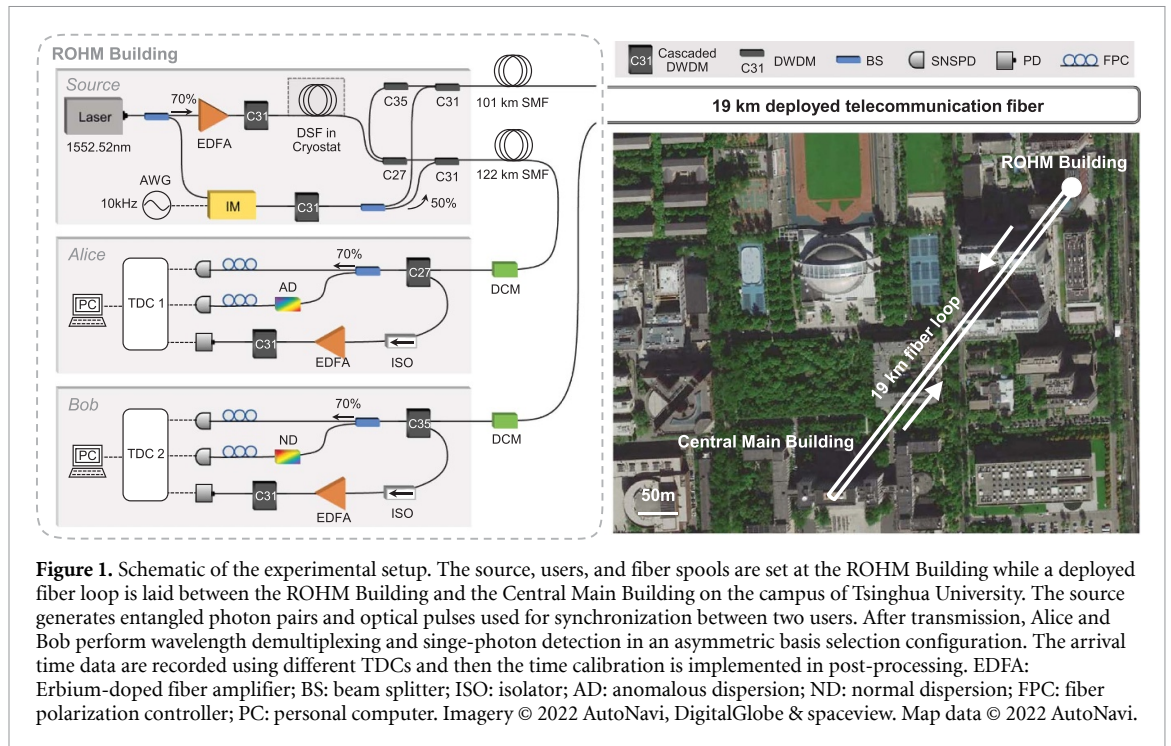
It is worth noting that the time synchronization between two independent users is an important technique in entanglement-based QKD field tests, especially in protocols where both raw key generation and security test are related to the arrival times of single-photon events at the two sides, such as DO-QKD. There have been several time synchronization methods used for entanglement distribution and entanglement-based QKD over optical fibers, such as using additional synchronization channels [42] and using Global Positioning System (GPS) signals for time reference accompanied by time-resolved coincidence measurement for time drift compensation [10, 28]. However, the time synchronization supporting entanglement-based DO-QKD field test over optical fibers has not been demonstrated, which should overcome the time fluctuations introduced in optical fibers with high accuracy. Therefore, a high-performance, robust, and convenient time synchronization method is crucial for the ultra-long-distance realization of entanglement DO-QKD over optical fibers.

In this work, we report an experimental demonstration of entanglement-based DO-QKD over fiber transmission of 242 km, including a 19 km deployed fiber. To realize time synchronization between distant users, we develop a reliable and high-accuracy time synchronization method based on the distribution of optical pulses in quantum channels. It supports accurate calibration of photons' arrival times at Alice's and Bob's sides, ensuring the robust operation of entanglement-based DO-QKD in the field condition, without additional time-resolved coincidence measurement in the time synchronization process. Our system shows excellent stability and robustness over 7 d of continuous operation, even without active polarization or phase calibration. In the key generation process, a high-dimensional encoding scheme is utilized to increase the number of secure keys extracted from each detected coincidence count. Finally, secure keys are generated in the asymptotic and finite-size regimes. As far as we know, it is the implementation with the longest distance of fiber-based entanglement-based QKD field test using energy-time entanglement.

## 2. Method

### 2.1. Experimental setup

We implement entanglement-based DO-QKD with a source-in-the-middle configuration. The illustration of experimental setup is schematically depicted in figure 1. The pump laser runs in continuous-wave mode with a central wavelength of 1552.52 nm, which corresponds to the 100 GHz International Telecommunication Union (ITU) channel of C31. A beam splitter separates the pump light into two parts, one of which pumps a 280 m dispersion shifted fiber (DSF) to generate energy-time entangled photon pairs through the spontaneous four-wave mixing (SFWM) effect. Then dense wavelength division multiplexers (DWDMs) separate signal and idler photons into 100 GHz ITU channels of C35 (1549.32 nm) and C27 (1555.75 nm), respectively. The other part of the pump light incidents an intensity modulator (IM) to generate



synchronization pulses. The IM is driven by a periodical electrical pulse signal generated by an arbitrary waveform generator with a 10 kHz repetition frequency and a 10 ns pulse width.

To track time fluctuation in transmission fibers, the generated signal and idler photons are multiplexed with synchronization pulses, then sent to Bob and Alice through quantum channels, respectively. The quantum channels have a total length of 242 km, composed of 223 km single mode fiber (SMF) spools and a 19 km deployed SMF link. The deployed fiber link includes 12 pieces of dark fibers in a fiber cable between two buildings on the campus of Tsinghua University (the ROHM Building and the Central Main Building of Tsinghua University, as shown in figure 1), which were spliced end-to-end. The quantum channel from the source to Alice composes of 122 km SMF spools with a loss of 24 dB, while that from the source to Bob composes of 101 km SMF spools and the 19 km deployed SMF loop with a total loss of 27 dB. The SMFs used in the experiment are standard telecommunication G.652 fibers with chromatic dispersion of  $17 \text{ ps} \cdot (\text{km} \cdot \text{nm})^{-1}$  at 1550 nm. The chromatic dispersion of transmission fibers is precisely compensated using dispersion compensation modules (DCMs).

At each user's end, the synchronization pulses are filtered out by cascaded DWDM components, amplified, and then detected by photodetectors (PDs). For single-photon detection, Alice and Bob use 70:30 beam splitters to randomly choose between the time and frequency bases. This asymmetric basis selection configuration can effectively increase the raw key rate, while it allows to accumulate enough coincidences for security analysis [43]. In time bases, the arrival times of photons are directly detected by superconducting nanowire single-photon detectors (SNSPDs). While in frequency bases, the arrival times of photons are detected after they pass through a dispersion module with anomalous (normal) dispersion at Alice's (Bob's) side. The nonlocal dispersion is cancelled by the intrinsic nature of energy-time entanglement when two photons of an entangled photon pair are both detected in frequency bases [44]. The electric pulses output from PDs and SNSPDs are then recorded by the time-to-digital converters (TDCs).

## 2.2. Time synchronization process

To realize time synchronization, each optical pulse generated from the source is split into two, which travel in the quantum channels to Alice and Bob, respectively. Then, they are detected separately at the two users' sides. Their arrival times track the time fluctuation in fibers and provide an accurate time delay between the time frames of Alice and Bob. Based on it, the time synchronization is implemented locally by Alice and Bob in the post-processing process with high accuracy. The time synchronization includes several steps. Firstly, Alice and Bob initialize the TDCs independently before the measurement starts. At the beginning of each measurement, a change in repetition frequency of the synchronization pulses is introduced, i.e. from 10 kHz to 20 kHz and back to 10 kHz, to provide a starting point for the measurement. From the starting point, Alice and Bob can pair the pulses received by them exactly. Then the pulses with a constant repetition frequency of 10 kHz are maintained throughout the subsequent measurement, providing the users with

stable optical timing signals to establish synchronization periods. The time synchronization performance of optical pulses is verified by the time-resolved coincidence measurement when the optical pulses travel through the two quantum channels with long-distance fibers and the detected signals of Alice and Bob are recorded by the same TDC. The full width at half maximum (FWHM) of the coincidence peak is about 60 ps, which is the additional timing jitter introduced by this synchronization method in our experiment. In the tests, the arrival times of single-photon events at Alice's and Bob's sides are rescaled in post-processing by determining the position of photons in the synchronization periods. Then the calibrated arrival times are utilized in key generation and security analysis.

It can be seen that this time synchronization method does not need additional time-resolved coincidence measurement of single-photon events. It can support accurate calibration of photons' arrival times at Alice's and Bob's sides, ensuring the robust operation of entanglement-based DO-QKD in the field. Obviously, this time synchronization method can also be applied in entanglement distribution networks (especially QKD networks based on entanglement distribution) by distributing optical pulses from the source to multiple end users.

### 2.3. DO-QKD protocol

To fully exploit every recorded coincidence event, a high-dimensional encoding format is utilized in key generation. Alice and Bob sift their keys in a three-level bin-sifting process [41]. The time streams of two users are divided into consecutive time frames, time slots, and time bins. A frame contains  $M = 2^D$  slots and a slot contains  $I$  bins. Each user selects the frames which contain only one single-photon event and then discards other frames. Then they communicate the frame number and bin number of every retained single-photon event on each side through a classical channel. Only photons from two users have the same frame number and the same bin number would be registered as a successful coincidence event. This strategy effectively decreases the QBER caused by timing jitters of detectors and electronic devices. Then the raw keys are generated by the slot numbers of the single-photon events.

The security analysis of DO-QKD is based on the treatment of single-photon events and the well-established proofs of Gaussian CV-QKD [45, 46] (see details in appendix B). By calculating the time-frequency covariance matrix between the photons' arrival times of Alice and Bob, the security of protocol against Eve's Gaussian collective attacks has been proven [38]. The secure key capacity represents the number of secure keys that can be extracted from each coincidence count. It is denoted as

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

where  $\beta$  is the reconciliation efficiency,  $I(A; B)$  is Shannon mutual information between Alice and Bob,  $\chi(A; E)$  is Eve's Holevo information, and  $\Delta_{FK}$  accounts for the penalty of finite-size effect.

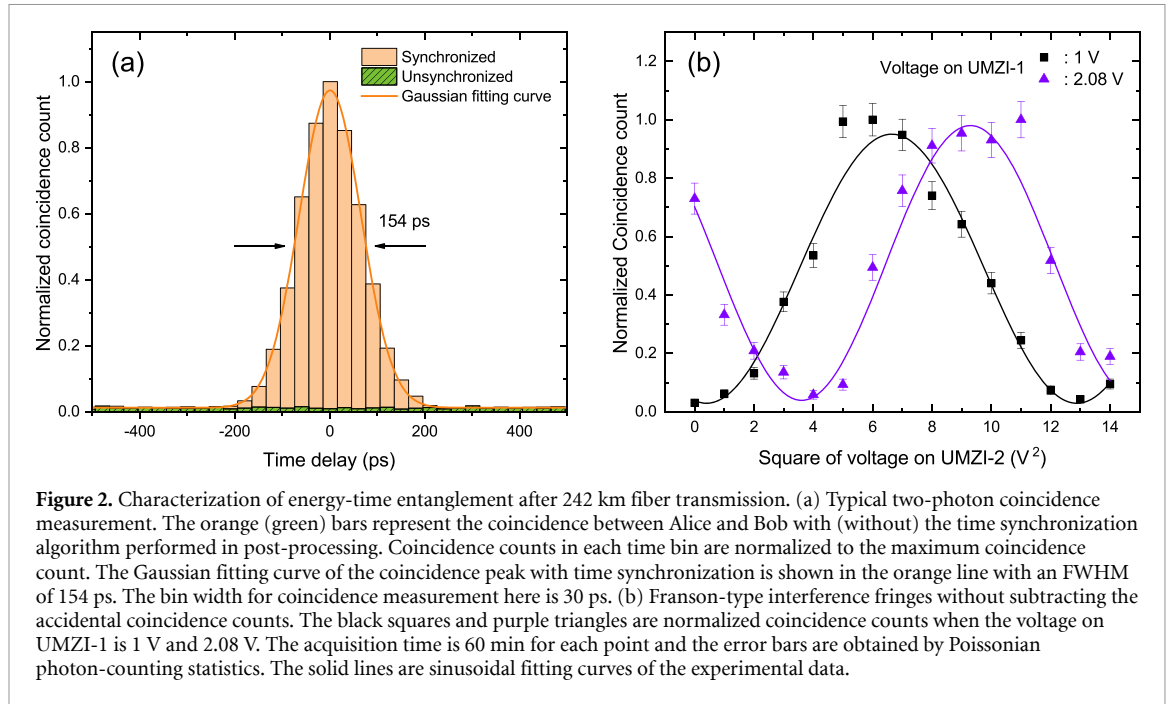
When considering the finite length of generated keys, each stage of the QKD protocol has a probability to fail [47]. The tolerated failure probability of the whole protocol  $\varepsilon_s$  is denoted as  $\varepsilon_s = \varepsilon_{\text{ver}} + \varepsilon_{PA} + n_{PE}\varepsilon_{PE} + \bar{\varepsilon}$ . It is the sum of failure probabilities in stages of error correction and verification, privacy amplification, parameter estimation, and estimating the smooth min-entropy. In the process of information reconciliation, we combine symmetric blind information reconciliation [48], which is based on low-density parity-check codes, with a layered scheme [49] suitable for large-alphabet QKD to further improve the reconciliation efficiency. Then hash-function-based verification [50] is introduced to reduce the QBER after information reconciliation. Finally, to extract secure keys from reconciled keys, privacy amplification is implemented using Toeplitz matrix [51].

## 3. Results

### 3.1. Entanglement distribution

The high-quality entanglement distribution of energy-time entangled photon states is demonstrated with 242 km transmission fiber. First of all, we perform coincidence measurement between signal and idler photons received by two users with a slightly different experimental setup from that in figure 1. After being separated from synchronization pulses, the signal and idler photons are directly detected by SNSPDs and their arrival times are recorded by TDCs at each user's end. Figure 2(a) shows the typical coincidence measurement after transmission with normalized amplitude. The coincidence measurement with calibrated arrival times of photons after time synchronization is given in the orange bars. It reveals that the temporal correlation between entangled photon pairs is well preserved after transmission to distant synchronized users. A Gaussian fitting is implemented on the coincidence peak, shown in the orange line. The FWHM of the coincidence peak is 154 ps, which mainly attributes to the timing jitters of detectors and electronic circuits. Strict temporal filtering is applied to reduce the accidental coincidence counts caused by noise



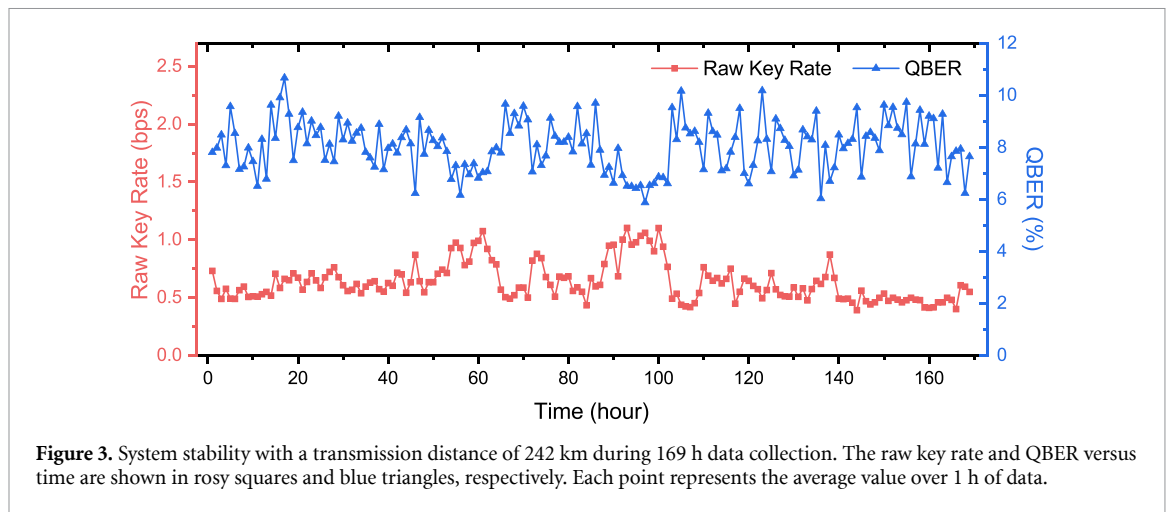


photons. Under a coincidence window of 240 ps, covering most of the coincidence peak, the coincidence count rate is 0.59 cps with a coincidence to accidental coincidence ratio (CAR) of 64.9. For comparison, we also present coincidence measurement with the raw arrival time data without time synchronization, given in the green bars. In this case, instead of an accumulated coincidence peak, the coincidences are full of accidental events with equal probability in every time bin. The temporal correlation is undetectable due to the asynchronous clocks of two TDCs and the time fluctuation caused by long-distance fibers. The following tests of the paper are implemented with the time synchronization algorithm performed in post-processing.

To evaluate the quality of the energy-time entanglement after long-distance transmission, we perform Franson-type interference [52]. The signal and idler photons are detected and recorded after they pass through two unbalanced Mach-Zehnder interferometers (UMZI) placed at each user's side, UMZI-1 and UMZI-2, respectively. The unbalanced time  $\Delta T$  between the two arms of the UMZI is about 400 ps, which is much larger than the single-photon coherence time of about 6 ps to avoid single-photon interference. By applying voltage on one arm of a UMZI, we can change the phase difference between its two arms. The voltage of the UMZI-1 is set to be 1 V and 2.08 V, constructing two non-orthogonal bases with a phase difference of  $\pi/2$ , while scanning the voltage of UMZI-2 to obtain interference fringes. We select the central coincidence peak with a coincidence window of 250 ps and the interference results are shown in figure 2(b). The coincidence counts in two sets are normalized to the maximum values of each set. It can be seen that after transmission of 242 km, the visibilities of two-photon interference are  $94.1 \pm 1.9\%$  and  $92.4 \pm 5.4\%$  in two non-orthogonal bases, without subtracting the accidental coincidence counts. We calculate the S parameter to be  $2.61 \pm 0.15$ , with a violation of the Clauser–Horne–Shimony–Holt (CHSH) Bell inequality  $S \leq 2$  by 4 deviations [53]. The result of Franson-type interference in back-to-back configuration is given in appendix A. Our results confirm that the energy-time entanglement is well-preserved after long-distance entanglement distribution.

### 3.2. QKD

Using the distributed energy-time entangled photon pairs, the entanglement-based QKD is demonstrated. In the QKD setting, the time bases and frequency bases are constructed at each user's end, as depicted in figure 1. Alice and Bob use all the coincidence events which they both detected in frequency bases to perform parameter estimation. For coincidence events which they both detected in time bases, they take a part of them for parameter estimation. The amount of this part is equal to those detected in frequency bases. The remained coincidence events are used for key generation. Before the QKD starts, Alice and Bob need to optimize and determine the time-encoding parameters for key generation. A higher encoding dimension or a larger time bin width would result in a higher raw key rate, however, it may also lead to a higher QBER. The value of QBER affects the length of reconciled keys after error correction so it is also crucial to the SKR. Hence, a trade-off between raw key rate and QBER should be carefully made in parameter optimization. In

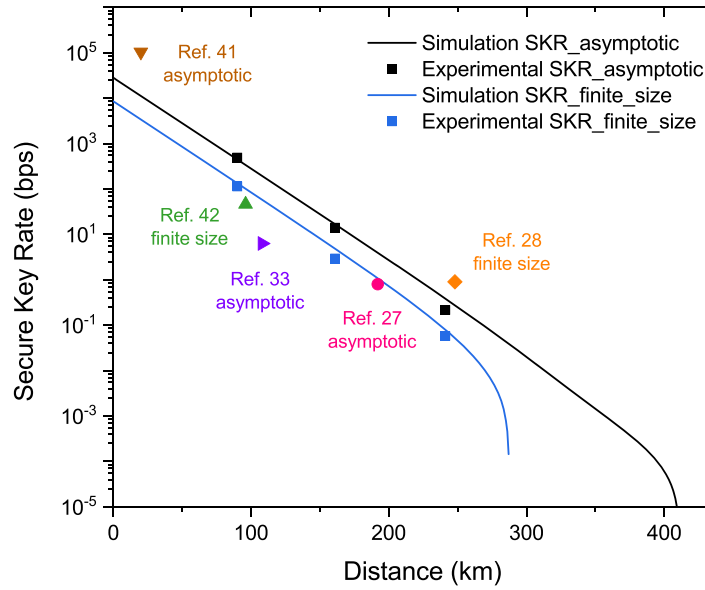


our experiment, the QBER is set to below an upper bound of 8% and the encoding parameters are optimized accordingly to maximize the key rate.

The 242 km DO-QKD system operates continuously for an acquisition time of 169 h, demonstrating the stability and robustness of the QKD link without active phase or polarization calibration. All the arrival times of single-photon events are recorded and calibrated with the time synchronization algorithm by Alice and Bob. Then, the raw key generation is performed on data of every hour with time-encoding parameters of  $D = 3$ ,  $I = 3$ , and bin width = 240 ps. Hourly raw key rates and QBERs versus time are shown in figure 3. The raw key rate distribution is concentrated around 0.63 bps with a standard deviation of 0.16 bps, and the corresponding QBER values have a mean value of 8.04% with a standard deviation of 0.98%. The experimental system is robust to the polarization fluctuations in optical fibers since the raw key generation and security test are based on the arrival times of single-photon events recorded by Alice and Bob. However, a little impact on the SKR could be expected due to the polarization-dependence of the SNSPDs used in the system, as shown in the fluctuations in figure 3. The system is also robust to the time fluctuations in optical fibers since the optical pulses for time synchronization propagate in the same fibers as the entangled photon pairs. After 169 h of data acquisition, we obtain raw keys with a total number of 385 665 bits.

After the raw keys are generated, efficient information reconciliation is performed to eliminate error bits between the two users. In the case of 242 km fiber transmission, we experimentally achieve a reconciliation efficiency of 89.7% by combining the symmetric blind information reconciliation method [48] with a layered scheme [49]. The tolerated failure probability  $\varepsilon_s$  is set as  $10^{-5}$  in the experiment, and the failure probability of error correction and verification  $\varepsilon_{\text{ver}}$  is  $2 \times 10^{-12}$ . By calculating the time-frequency covariance matrix and excess noise factor introduced by the quantum channel and potential eavesdropper [38], the Shannon mutual information between Alice and Bob  $I(A; B)$  is determined as 1.87 bpc, and Eve's maximum accessible information  $\chi(A; E)$  is 0.65 bpc in the asymptotic regime. When considering the finite-size effect with the number of total coincidence counts  $N$  of  $\sim 2 \times 10^5$  between Alice and Bob, the  $\chi(A; E)$  increases to 1.02 bpc while an additional subtraction  $\Delta_{FK}$  of 0.39 bpc should be considered. The secure key capacity is 1.02 bpc and 0.27 bpc in the asymptotic and finite-size regimes, while the corresponding SKR is 0.22 bps and 0.06 bps, respectively. Privacy amplification based on Toeplitz matrix further extracts finite-size secure keys of 34 905 bits.

Figure 4 shows the SKRs of DO-QKD under different transmission distances. In the experiment, we conduct DO-QKD tests under 90 km, 161 km, and 242 km by changing the length of fiber spools while the 19 km deployed fiber loop is included in the system throughout the experiments. In each case, the chromatic dispersion of transmission fibers is compensated by DCMs, ensuring that the temporal correlation is well-preserved after transmission. The parameters for key generation are optimized case by case to maximize key rates (see details in appendix B). To accumulate enough coincidence events for finite-size analysis, the acquisition times of the three cases are 5 min, 3.5 h, and 169 h, respectively, and the number of total coincidence events  $N$  is  $\sim 2 \times 10^5$  in all cases. The experimental results are shown in figure 4, in which the asymptotic and finite-size SKRs are shown in black and blue squares, respectively. Moreover, we simulate the expected performance of the DO-QKD system based on a previously proposed theoretical model [54], considering the process of the quantum light source, transmission, single-photon detection, and post-processing. The simulation model of DO-QKD is based on the assumption that if one photon in an entangled photon pair is detected at a specific time at Alice's side, the detection time of the other photon in the pair at Bob's side would have a Gaussian distribution, and noise photons always have a uniform



**Figure 4.** SKRs of the fiber-based entanglement-based DO-QKD experiment. SKR values are plotted versus the length of the transmission fiber. The results in the asymptotic and finite-size regimes are shown by the black and blue squares, respectively. Correspondingly, the black and blue curves show the simulation results. The number of total coincidence events  $N$  in simulation and experiment is  $\sim 2 \times 10^5$ . The sum of the dark count rate of SNSPD and the noise photon rate introduced by synchronization pulses is  $\sim 300$  Hz. Other symbols represent recent experimental results of entanglement-based QKDs with SPDC (spontaneous parametric down-conversion) source [27, 28, 33, 42] and SFWM source [41] for comparison.

distribution in a time frame. The parameters used in the simulation are the averaged values of experimental parameters of three cases. The simulation curves are also shown in figure 4. It shows that the experimental results are in good agreement with those of the simulation. Our result reveals that the entanglement-based DO-QKD scheme shown in figure 1 can tolerate a transmission of 400 km in the asymptotic regime and about 270 km in the finite-size regime.

#### 4. Discussion

By using a high-accuracy optical time synchronization method, our QKD system using energy-time entanglement exhibits excellent stability over a long time and system robustness against channel fluctuation. In the experiment over 7 d, the system suffered from several transient perturbations manifested by missing several synchronization pulses which may be caused by the unstable electrical environment. The impact of these perturbations can be removed in post-processing by discarding the single-photon events in these transient periods and maintaining synchronization after the perturbations. Notably, there is no active phase or polarization calibration implemented in our experiment, while it still shows long-term stability over 7 d with a fully passive experimental setup.

It is worth noting that the security test of DO-QKD follows the well-established security test of Gaussian CV-QKD. It does not directly involve QBER. On one hand, in the experimental system of entanglement-based DO-QKD, the QBER would increase with an increasing raw key rate when the encoding dimension increases. On the other hand, a high QBER would result in a high cost in the process of error correction, reducing the SKR. Therefore, by selecting the encoding parameters, a trade-off is made between the raw key rate and QBER to achieve a high SKR. The QBER could be reduced under a lower encoding dimension, which would reduce the possibility of noise counts in a time frame. Besides, a quantum light source with lower noise photons and detectors with lower dark counts are also helpful to reduce the QBER.

We have shown that our system can tolerate more than 51 dB transmission loss with a distance of over 242 km. The corresponding finite-size SKR is at the order of  $10^{-2}$  bps, which is at a relatively low level in our experiment. On the source side, we choose a moderate pump power to mitigate the multi-pair emission in a time frame. The coincidence count rate is restricted in this situation so an efficient encoding method becomes rather necessary. We use a high-dimensional encoding format to maximize the use of coincidence counts in key generation. In our work, the encoding dimension  $D$  is 3, and we obtain a secure key capacity of 1.02 bpc in the asymptotic regime and 0.27 bpc in the finite-size regime. A detailed performance comparison between our work with other fiber-based entanglement-based QKD works is shown in table 1. It can be seen that this work has the longest time of continuous operation, showing the stability of the entanglement-based



**Table 1.** Comparison of some recent entanglement-based QKD experiments over optical fibers. Here SMF is single mode fiber; NZ-DSF is non-zero dispersion shifted fiber.

References	Length (km)	Fiber type	DOF	Operation time (h)	Asymptotic SKR (bps)	Finite-size SKR (bps)
Liu <i>et al</i> [41]	20	Laboratory SMF	Energy-time (DO-QKD)	—	104k	—
Wengerowsky <i>et al</i> [42]	96	Deployed NZ-DSF	Polarization	2.5	57.5	46
Wengerowsky <i>et al</i> [27]	192	Deployed NZ-DSF	Polarization	6.5	0.8	—
Fitzke <i>et al</i> [33]	108	Partially deployed SMF	Time-bin	13	6.3	—
Neumann <i>et al</i> [28]	248	Deployed SMF	Polarization	110 (effective 82)	1.4	0.9
This work	242	Partially deployed SMF	Energy-time (DO-QKD)	169	0.22	0.06

DO-QKD system with the proposed synchronization method. What is more, there is no time-resolved coincidence needed in the experiment to compensate for GPS time drift or to recover the clock. Hence, no additional consumption is required for time synchronization, which is desired for ultra-long-distance QKD when the single-photon events are precious.

There are several possible improvements to our QKD system. Firstly, the generation rate of entangled photon pairs still has space to be increased, under the limit that the possibility of multi-pair emission in a time frame is sufficiently low. Secondly, the performance of QKD would improve considerably if we use an advanced commercial SNSPD system with detection efficiency over 90% and timing jitter lower than 50 ps. Thirdly, by employing a longer acquisition time, the finite-size SKR would closely approach the asymptotic SKR when increasing the total number of coincidences  $N$  between two users [47]. We estimate the potential performance of the DO-QKD system with the above improvements. Through theoretical calculation, it can be expected that the finite-key SKR under 242 km transmission would be improved to the order of 1 bps using a periodically poled LiNbO<sub>3</sub> source described in [55], offering a higher generation rate of entangled photon pairs and a higher CAR (see details in appendix C).

## 5. Conclusion

In summary, we have demonstrated a high-dimensional DO-QKD system with 242 km transmission fiber including deployed fiber of 19 km. The time synchronization method based on the distribution of optical pulses in quantum channels is developed, which is suitable for long-distance entanglement-based QKD. The high-quality entanglement distribution is verified using Franson-type interference. The raw visibilities are  $94.1 \pm 1.9\%$  and  $92.4 \pm 5.4\%$  in two non-orthogonal bases, indicating the violation of CHSH Bell inequality by 4 deviations. Then the DO-QKD system continuously operates for over 7 d with time synchronization of the two users. We perform high-dimensional key generation, efficient information reconciliation, and privacy amplification to generate secure keys with an asymptotic SKR of 0.22 bps and a finite-size SKR of 0.06 bps. The result shows outstanding stability and robustness of our system without active phase or polarization calibration. It has great potential for realizing entanglement-based QKD in large-scale optical fiber networks, which is promising in future global quantum communication networks.

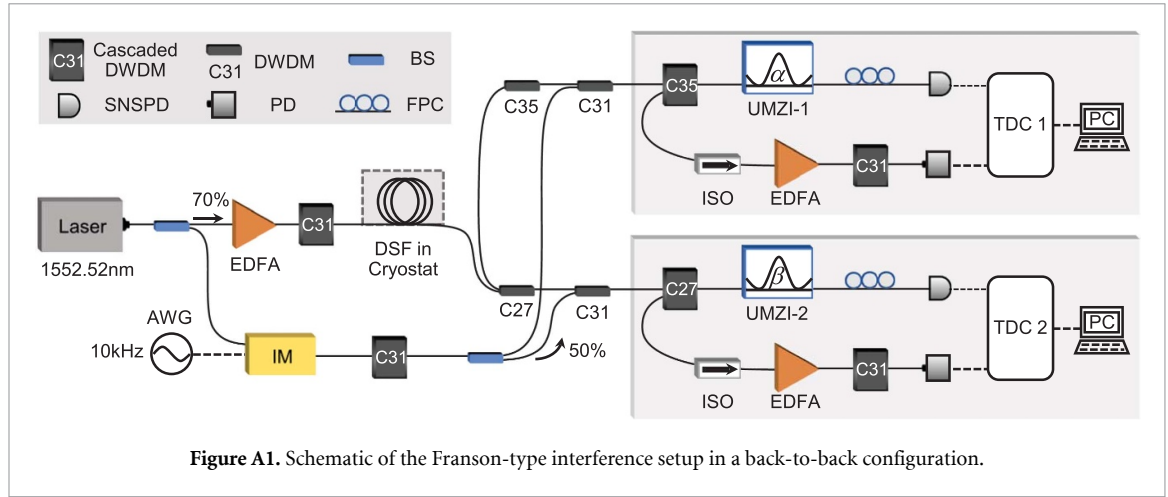
## Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

## Acknowledgments

This work has been supported by the National Key R&D Program of China (2018YFB2200400), Natural Science Foundation of Beijing (Z180012), National Natural Science Foundation of China (61875101, 91750206), Tsinghua Initiative Scientific Research Program, and Tsinghua University-Zhuhai Huafa Industrial Share Company Joint Institute for Architecture Optoelectronic Technologies (JIAOT).

W Z and J L proposed the scheme. J L, Z L and D L performed experiments. J L perform simulation and data analysis. Z L perform error correction and privacy amplification. W Z, J L wrote the manuscript. Y H revised the manuscript and supervised the project. X F, F L, K C contributed to experiment design and the revision of the manuscript.



## Appendix A. Characterization of entanglement source

In our work, we use a 280 m DSF as the nonlinear medium of the quantum light source based on the SFWM effect. The DSF is placed in a cryostat and cooled to  $\sim 2.2$  K to reduce the noise introduced by spontaneous Raman scattering. The pump power of the quantum light source is 19.4 dBm, producing about  $8.8 \times 10^6$  entangled photon pairs per second.

To test the quality of energy-time entanglement photon pairs output from the quantum light source, we perform Franson-type interference in a back-to-back configuration, as shown in figure A1. The setup for time synchronization is also included in this test to investigate the effect of synchronization noise on the quality of energy-time entanglement. The voltage of the UMZI-1 is set to be 1 V and 2.08 V, constructing two non-orthogonal bases with a phase difference of  $\pi/2$ , while scanning the voltage of UMZI-2 to obtain interference fringes. We select the central coincidence peak with a coincidence window of 150 ps. The raw visibilities are  $96.4 \pm 1.8\%$  and  $94.6 \pm 0.6\%$  of the fringes in two non-orthogonal bases, without subtracting the accidental coincidence counts. The S parameter is  $2.68 \pm 0.02$  with a violation of the CHSH Bell inequality by 34 deviations. It shows that our source generates high-quality energy-time entangled photon pairs and the synchronization noise has little effect on the quality of energy-time entanglement.

## Appendix B. Secure key generation

In the security analysis of DO-QKD, the time-frequency covariance matrix is calculated to bound Eve's Holevo information [38]. In the process, the estimation of characteristic parameters from experimental results is necessary. Using the recorded single-photon events, the excess noise factor  $\xi$  is estimated to quantify the disturbance from the eavesdropper, channel noise, and setup imperfections on the time-frequency covariance matrix. It can be obtained by analyzing the increase in the correlation time between photons received by Alice and Bob, as denoted by

$$\xi = \frac{\sigma_{\text{cor}}'^2}{\sigma_{\text{cor}}^2} - 1, \quad (\text{B.1})$$

where  $\sigma_{\text{cor}}'$  is the correlation time after transmission and  $\sigma_{\text{cor}}$  is an ideal noiseless result which we take the back-to-back result in the experiment. The Shannon information is calculated by estimating the correlation coefficient of photons' arrival times between Alice and Bob.

Considering the finite length of the key, the calculation of secure key capacity includes a subtraction caused by the finite-size effect [47]:

$$\Delta_{\text{FK}} = \frac{1}{n} n_{\text{ver}} + \frac{2}{n} \log_2 \frac{1}{\varepsilon_{\text{PA}}} + (2 \log_2 D + 3) \sqrt{\frac{\log_2(2/\varepsilon)}{n}}, \quad (\text{B.2})$$

where  $n$  is the number of coincidence counts between photons in the time bases of Alice and Bob,  $n_{\text{ver}}$  is the information leakage in the verification step after error correction [50]. And we need to consider the uncertainty in estimating correlation time with a finite-length dataset. The estimate for  $\sigma_{\text{cor}}'$ , denoted  $\hat{\sigma}_{\text{cor}}'$ , has a  $\chi^2$  distribution [47] and we can obtain the upper bound of  $\sigma_{\text{cor}}'$  and  $\xi$ :

$$(\sigma_{\text{cor,max}}')^2 = \sigma_{\text{cor}}^2 + \frac{2}{\sqrt{m}} \text{erf}^{-1}(1 - \varepsilon_{\text{PE}}) \sigma_{\text{cor}}'^2, \quad (\text{B.3})$$

**Table B1.** Details of finite-size key generation with different transmission distances. Here SER is symbol error rate. Alice(Bob)-T(F) represents time (frequency) basis of Alice (Bob).

Length (km)		90	161	242
Acquisition time		5 min	3.5 h	169 h
	Alice-T	225.5	8.2	6.9
Average count rate (kcps)	Alice-F	26.9	1.2	1.0
	Bob-T	110.9	99.0	2.7
	Bob-F	22.0	21.8	0.6
$D$		3	3	3
$I$		3	3	3
Bin width (ps)		350	250	240
SER (%)		13.93	13.91	13.79
QBER (%)		7.92	7.94	7.90
$\beta I(A;B)$ (bpc)		1.70	1.69	1.68
$\chi(A;E)$ (bpc)		1.03	1.01	1.02
$\Delta_{FK}$ (bpc)		0.39	0.39	0.39
$\Delta I$ (bpc)		0.28	0.29	0.27
SKR (bps)		113.97	2.94	0.06
Raw key (bit)		371 631	374 454	385 665
Secure key (bit)		33 951	36 693	34 905

$$\xi_{\max} = \frac{(\sigma'_{\text{cor,max}})^2}{\sigma_{\text{cor}}^2} - 1, \quad (\text{B.4})$$

where  $m$  is the number of coincidence counts between photons in the frequency bases of Alice and Bob. Then  $I(A;B)$  and  $\chi(A;E)$  can be calculated based on the treatment of the covariance matrix, and finally the secure key capacity is obtained according to equation (1).

The DO-QKD performances with three different transmission distances are shown in the main text. The details of key generation in finite-size regime are shown in table B1. The time encoding parameters are  $D = 3$  and  $I = 3$  for all cases. We maximize the time bin in each case to obtain a higher key rate when the QBER is below an upper bound of 8%. In error correction, shortening and puncturing technique are used to optimize the reconciliation efficiency, by adding shortened and punctured bits in each block with a block length of 1944 [48, 50]. The raw keys are divided into multiple groups to perform error correction, and the secure keys are generated by the raw keys in these groups.

### Appendix C. Simulation of DO-QKD system

In the simulation model of DO-QKD, we consider the performance of quantum light source, optical fiber transmission, and single-photon detection as characteristic parameters to simulate the system performance (see [54] for details). In the key generation process, the types of photons received by Alice are first analyzed. Alice may receive one of the entangled photon pair, the idler photon in the experiment, or a noise photon. In each case, the arrival time of photons at Alice's side is set as  $t_0$ , then the temporal distribution of the single-photon events recorded by Bob could be derived. When Alice receives idler photons, the photons received by Bob could be the signal photons or noise photons. The temporal distribution of Bob's photons follows an approximate Gaussian distribution accompanied by uniform distribution noise:

$$B_1(t) = \eta \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(t-t_0)^2}{2\sigma^2}\right) + \eta R_s + d, \quad (\text{C.1})$$

where  $\eta$  is the channel transmittance at Bob's side,  $\sigma$  is the variance of Gaussian distribution,  $R_s$  represents the generation rate of Raman noise photons at the signal side, and  $d$  is the dark count rate of detectors. These parameters are obtained by experimental results. When Alice receives noise photons, Bob also receives noise photons that have no temporal correlation with Alice's photons. The temporal distribution of Bob's photons follows a uniform distribution:

$$B_2(t) = \eta(R + R_s) + d, \quad (\text{C.2})$$

where  $R$  represents the generation rate of entangled photon pairs. Then we derive the number of coincidence events in high-dimensional encoding based on the temporal distribution of Bob's photons. The statistical characteristics of photons are also used to perform security analysis.

In the discussion part, we simulate the potential performance of the DO-QKD system with a higher generation rate of entangled photon pairs, higher detection efficiency, and longer acquisition time. The quality of the quantum light source in [55], which is based on second-order nonlinear process, is used for simulation. Through the given results in the reference, we estimate that a generation rate of entangled photon pairs at 13 MHz is accessible with a corresponding CAR of about 200. In our simulation, the detection efficiency of SNSPDs is set to 90% and the timing jitter is 50 ps. The sum of the dark count rate of SNSPD and the noise photon rate introduced by synchronization pulses is 200 Hz. The acquisition time is 169 h to perform finite-size analysis at 242 km transmission, which corresponds to  $N$  of  $3.5 \times 10^6$ . Other parameters are the same as those in our experiment.

## ORCID iDs

Jingyuan Liu  <https://orcid.org/0000-0001-6771-8496>

Wei Zhang  <https://orcid.org/0000-0002-6848-6807>

## References

- [1] Pirandola S *et al* 2020 Advances in quantum cryptography *Adv. Opt. Photonics* **12** 1012–236
- [2] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* pp 175–9
- [3] Lo H K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504
- [4] Wang X B 2005 Beating the photon-number-splitting attack in practical quantum cryptography *Phys. Rev. Lett.* **94** 230503
- [5] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 Device-independent quantum key distribution secure against collective attacks *New J. Phys.* **11** 045021
- [6] Braunstein S L and Pirandola S 2012 Side-channel-free quantum key distribution *Phys. Rev. Lett.* **108** 130502
- [7] Lo H K, Curty M and Qi B 2012 Measurement-device-independent quantum key distribution *Phys. Rev. Lett.* **108** 130503
- [8] Yin H L *et al* 2016 Measurement-device-independent quantum key distribution over a 404 km optical fiber *Phys. Rev. Lett.* **117** 190501
- [9] Zhang W *et al* 2022 A device-independent quantum key distribution system for distant users *Nature* **607** 687–91
- [10] Scheidl T *et al* 2009 Feasibility of 300 km quantum key distribution with entangled states *New J. Phys.* **11** 085002
- [11] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 Fundamental limits of repeaterless quantum communications *Nat. Commun.* **8** 15043
- [12] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Overcoming the rate-distance limit of quantum key distribution without quantum repeaters *Nature* **557** 400–3
- [13] Yin J *et al* 2020 Entanglement-based secure quantum cryptography over 1,120 kilometres *Nature* **582** 501–5
- [14] Chen J-P *et al* 2021 Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas *Nat. Photon.* **15** 570–5
- [15] Wang S *et al* 2022 Twin-field quantum key distribution over 830-km fibre *Nat. Photon.* **16** 154–61
- [16] Zeng P, Zhou H, Wu W and Ma X 2022 Mode-pairing quantum key distribution *Nat. Commun.* **13** 3903
- [17] Xie Y-M, Lu Y-S, Weng C-X, Cao X-Y, Jia Z-Y, Bao Y, Wang Y, Fu Y, Yin H-L and Chen Z-B 2022 Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference *PRX Quantum* **3** 020315
- [18] Zhou L, Lin J, Xie Y M, Lu Y S, Jing Y, Yin H L and Yuan Z 2023 Experimental quantum communication overcomes the rate-loss limit without global phase tracking *Phys. Rev. Lett.* **130** 250801
- [19] Ali-Khan I, Broadbent C J and Howell J C 2007 Large-alphabet quantum key distribution using energy-time entangled bipartite states *Phys. Rev. Lett.* **98** 060503
- [20] Pseiner J, Achatz L, Bulla L, Bohmann M and Ursin R 2021 Experimental wavelength-multiplexed entanglement-based quantum cryptography *Quantum Sci. Technol.* **6** 035013
- [21] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3
- [22] Bennett C H, Brassard G and Mermin N D 1992 Quantum cryptography without Bell's theorem *Phys. Rev. Lett.* **68** 557–9
- [23] Wengerowsky S, Joshi S K, Steinlechner F, Hubel H and Ursin R 2018 An entanglement-based wavelength-multiplexed quantum communication network *Nature* **564** 225–8
- [24] Liu X *et al* 2022 40-user fully connected entanglement-based quantum key distribution network without trusted node *Photonix* **3** 2
- [25] Honjo T *et al* 2008 Long-distance entanglement-based quantum key distribution over optical fiber *Opt. Express* **16** 19118–26
- [26] Takesue H, Harada K-ichi, Tamaki K, Fukuda H, Tsuchizawa T, Watanabe T, Yamada K and Itabashi S-ichi 2010 Long-distance entanglement-based quantum key distribution experiment using practical detectors *Opt. Express* **18** 16777–87
- [27] Wengerowsky S *et al* 2020 Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre *npj Quantum Inf.* **6** 5
- [28] Neumann S P, Buchner A, Bulla L, Bohmann M and Ursin R 2022 Continuous entanglement distribution over a transnational 248 km fiber link *Nat. Commun.* **13** 6134
- [29] Treiber A, Poppe A, Hentschel M, Ferrini D, Lorünser T, Querasser E, Matyus T, Hübel H and Zeilinger A 2009 A fully automated entanglement-based quantum cryptography system for telecom fiber networks *New J. Phys.* **11** 045013
- [30] Inagaki T, Matsuda N, Tadanaga O, Asobe M and Takesue H 2013 Entanglement distribution over 300 km of fiber *Opt. Express* **21** 23241–9

- [31] Tittel W, Brendel J, Zbinden H and Gisin N 1998 Violation of Bell inequalities by photons more than 10 km apart *Phys. Rev. Lett.* **81** 3563–6
- [32] Salart D, Baas A, Branciard C, Gisin N and Zbinden H 2008 Testing the speed of ‘spooky action at a distance’ *Nature* **454** 861–4
- [33] Fitzke E, Bialowons L, Dolejsky T, Tippmann M, Nikiforov O, Walther T, Wissel F and Gunkel M 2022 Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding *PRX Quantum* **3** 020341
- [34] Thew R T, Acín A, Zbinden H and Gisin N 2004 Bell-type test of energy-time entangled qutrits *Phys. Rev. Lett.* **93** 010503
- [35] Etcheverry S, Canas G, Gomez E S, Nogueira W A, Saavedra C, Xavier G B and Lima G 2013 Quantum key distribution session with 16-dimensional photonic states *Sci. Rep.* **3** 2316
- [36] Molina-Terriza G, Vaziri A, Rehacek J, Hradil Z and Zeilinger A 2004 Triggered qutrits for quantum communication protocols *Phys. Rev. Lett.* **92** 167903
- [37] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M, Padgett M J, Konrad T, Petruccione F, Lütkenhaus N and Forbes A 2013 Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases *Phys. Rev. A* **88** 032305
- [38] Mower J, Zhang Z, Desjardins P, Lee C, Shapiro J H and Englund D 2013 High-dimensional quantum key distribution using dispersive optics *Phys. Rev. A* **87** 062322
- [39] Lee C et al 2014 Entanglement-based quantum communication secured by nonlocal dispersion cancellation *Phys. Rev. A* **90** 062331
- [40] Lee C, Bunandar D, Zhang Z, Steinbrecher G R, Ben Dixon P, Wong F N C, Shapiro J H, Hamilton S A and Englund D 2019 Large-alphabet encoding for higher-rate quantum key distribution *Opt. Express* **27** 17539–49
- [41] Liu X, Yao X, Wang H, Li H, Wang Z, You L, Huang Y and Zhang W 2019 Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km *Appl. Phys. Lett.* **114** 141104
- [42] Wengerowsky S et al 2019 Entanglement distribution over a 96-km-long submarine optical fiber *Proc. Natl. Acad. Sci. USA* **116** 6684–8
- [43] Lo H-K, Chau H F and Ardehali M 2004 Efficient quantum key distribution scheme and a proof of its unconditional security *J. Cryptol.* **18** 133–65
- [44] Franson J D 1992 Nonlocal cancellation of dispersion *Phys. Rev. A* **45** 3126–32
- [45] Serafini A, Illuminati F and De Siena S 2004 Symplectic invariants, entropic measures and correlations of Gaussian states *J. Phys. B: At. Mol. Opt. Phys.* **37** L21–L28
- [46] Garcia-Patron R and Cerf N J 2006 Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution *Phys. Rev. Lett.* **97** 190503
- [47] Lee C, Mower J, Zhang Z, Shapiro J H and Englund D 2015 Finite-key analysis of high-dimensional time-energy entanglement-based quantum key distribution *Quantum Inf. Process.* **14** 1005–15
- [48] Kiktenko E O, Trushechkin A S, Lim C C W, Kurochkin Y V and Fedorov A K 2017 Symmetric blind information reconciliation for quantum key distribution *Phys. Rev. Appl.* **8** 044017
- [49] Zhou H, Wang L and Wornell G 2013 Layered schemes for large-alphabet secret key distribution *2013 Information Theory and Applications Workshop (ITA)* pp 1–10
- [50] Fedorov A K, Kiktenko E O and Trushechkin A S 2018 Symmetric blind information reconciliation and hash-function-based verification for quantum key distribution *Lobachevskii J. Math.* **39** 992–6
- [51] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 Generalized privacy amplification *IEEE Trans. Inf. Theory* **41** 1915–23
- [52] Franson J D 1989 Bell inequality for position and time *Phys. Rev. Lett.* **62** 2205–8
- [53] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Proposed experiment to test local hidden-variable theories *Phys. Rev. Lett.* **23** 880–4
- [54] Liu J-Y, Liu X, Zhang W and Huang Y-D 2021 Impact of fiber dispersion on the performance of entanglement-based dispersive optics quantum key distribution *J. Electron. Sci. Technol.* **19** 297–307
- [55] Zhang Z et al 2021 High-performance quantum entanglement generation via cascaded second-order nonlinear processes *npj Quantum Inf.* **7** 123