IOP Publishing Quantum Sci. Technol. 9 (2024) 015018 https://doi.org/10.1088/2058-9565/ad0f6f

Quantum Science and Technology

OPEN ACCESS

RECEIVED
30 May 2023

REVISED
26 October 2023

ACCEPTED FOR PUBLICATION
23 November 2023

PUBLISHED
1 December 2023

PAPER

Large-alphabet time-bin quantum key distribution and Einstein–Podolsky–Rosen steering via dispersive optics

Kai-Chi Chang[1,3,*], **Murat Can Sarihan**[1,3,*], **Xiang Cheng**[1,3,*], **Zheshen Zhang**[2] and **Chee Wei Wong**[1,*]

[1] Fang Lu Mesoscopic Optics and Quantum Electronics Laboratory, Department of Electrical and Computer Engineering, University of California, Los Angeles, CA 90095, United States of America
[2] Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109, United States of America
[3] These authors contributed equally to this work.
[*] Authors to whom any correspondence should be addressed.

E-mail: uclakcchang@ucla.edu, mcansarihan@ucla.edu, chengxiang@ucla.edu and cheewei.wong@ucla.edu

Keywords: large-alphabet time-bin encoding, quantum key distribution, entanglement and Einstein–Podolsky–Rosen steering distribution, nonlocal dispersion cancellation

Abstract

Quantum key distribution (QKD) has established itself as a groundbreaking technology, showcasing inherent security features that are fundamentally proven. Qubit-based QKD protocols that rely on binary encoding encounter an inherent constraint related to the secret key capacity. This limitation restricts the maximum secret key capacity to one bit per photon. On the other hand, qudit-based QKD protocols have their advantages in scenarios where photons are scarce and noise is present, as they enable the transmission of more than one secret bit per photon. While proof-of-principle entangled-based qudit QKD systems have been successfully demonstrated over the years, the current limitation lies in the maximum distribution distance, which remains at 20 km fiber distance. Moreover, in these entangled high-dimensional QKD systems, the witness and distribution of quantum steering have not been shown before. Here we present a high-dimensional time-bin QKD protocol based on energy-time entanglement that generates a secure finite-length key capacity of 2.39 bit/coincidences and secure cryptographic finite-length keys at 0.24 Mbits s^{-1} in a 50 km optical fiber link. Our system is built entirely using readily available commercial off-the-shelf components, and secured by nonlocal dispersion cancellation technique against collective Gaussian attacks. Furthermore, we set new records for witnessing both energy-time entanglement and quantum steering over different fiber distances. When operating with a quantum channel loss of 39 dB, our system retains its inherent characteristic of utilizing large-alphabet. This enables us to achieve a secure key rate of 0.30 kbits s^{-1} and a secure key capacity of 1.10 bit/coincidences, considering finite-key effects. Our experimental results closely match the theoretical upper bound limit of secure cryptographic keys in high-dimensional time-bin QKD protocols (Mower *et al* 2013 *Phys. Rev.* A **87** 062322; Zhang *et al* 2014 *Phys. Rev. Lett.* **112** 120506), and outperform recent state-of-the-art qubit-based QKD protocols in terms of secure key throughput using commercial single-photon detectors (Wengerowsky *et al* 2019 *Proc. Natl Acad. Sci.* **116** 6684; Wengerowsky *et al* 2020 *npj Quantum Inf.* **6** 5; Zhang *et al* 2014 *Phys. Rev. Lett.* **112** 120506; Zhang *et al* 2019 *Nat. Photon.* **13** 839; Liu *et al* 2019 *Phys. Rev. Lett.* **122** 160501; Zhang *et al* 2020 *Phys. Rev. Lett.* **125** 010502; Wei *et al* 2020 *Phys. Rev.* X **10** 031030). The simple and robust entanglement-based high-dimensional time-bin protocol presented here provides potential for practical long-distance quantum steering and QKD with multiple secure bits-per-coincidence, and higher secure cryptographic keys compared to mature qubit-based QKD protocols.

1. Introduction

Quantum cryptography provides a means for securely transferring information between distant parties [1]. Among these fundamental tasks, the security of Quantum key distribution (QKD) with symmetric encryption relies on the security strength of the symmetric cryptographic algorithm itself. QKD with one-time pad stands out as one of the few methods capable of offering provable protection against different attacks [2–4]. The reliable and efficient transmission of photonic entanglement plays a vital role in numerous quantum information processing tasks, including entanglement distribution [5–10], QKD [11–18], quantum teleportation [19], and quantum repeater [20, 21]. Entangled photons are highly desirable as carriers of secure quantum information due to their unique property-entanglement, steering, and Bell nonlocality [22]. Any quantum state that violates a Bell inequality can be used for steering, and any steerable state is entangled, but not vice versa [22, 23]. In particular, for quantum cryptography, it makes a difference whether or not one assumes that the measurement devices are well characterized. For example, if a state is quantum steerable, its entanglement can be verified in a one-sided device-independent scenario, where Bob's measurements are characterized, but Alice's are not [23]. Therefore, any practical quantum cryptography protocol based on quantum nonlocality and steering requires fewer assumptions and can guarantee the production of cryptographic keys that are genuinely random and secure [1, 22, 23].

In photonic-based QKD protocols, there are numerous degrees-of-freedoms have been investigated, including polarization [24–26], position-momentum [27, 28], spatial mode [29–34], orbital angular momentum [13, 15, 35–39], time [11, 17, 34, 40–46], and energy-time [12, 16, 18, 47–49]. The energy-time basis is particularly appealing for practical implementations in today's telecommunications infrastructure. Bright energy-time-entangled photon-pair sources [50], low-jitter [51], and superconducting nanowire single-photon detectors (SNSPDs) with high efficiency [52] have also been developed. Additionally, the intrinsic energy-time correlations are directly compatible with wavelength division multiplexing systems and robust in transmission through long-distance fiber links, allowing for versatile, multi-user quantum communication networks [48, 49, 53–58]. Nevertheless, to sustain the delicate entangled quantum states transmitted over long-distance channels, specific hardware and software requirements are necessary for the successful implementation of secure quantum communication protocols. High-dimensional quantum states, qudits (dimension $d > 2$) rather than qubits, provide a robust and efficient platform to overcome some of the practical challenges of current qubit-based QKD systems [11–18, 29, 30, 33–39, 45]. In essence, QKD systems employing qudit space exhibit two advantages over protocols based on qubits. First, they can increase the effective key generation rate by using large-alphabet encoding in systems limited by the dead time of the single-photon detectors. Secondly, high-dimensional QKD systems possess enhanced resilience against quantum channel noise compared to their qubit-based counterparts [9, 16, 34]. Although QKD with large-alphabet temporal encoding has been implemented before [11, 12, 16–18, 42, 45, 47], some of them are demonstrated with classical attenuated sources [17, 18, 45], some of them are only transmitted up to 20 km fiber distance [16, 47], and all of the entangled-based sources (different from classical attenuated sources) are operated with channel loss less than 17 dB [11, 12, 42, 47], which is far from the initial theoretical predictions [12, 59]. Furthermore, in entanglement-based qudit QKD systems with dispersive optics [12, 42, 47], the witness and distribution of Einstein–Podolsky–Rosen (EPR) steering have not been shown before.

In this study, we present an experimental demonstration of high-dimensional time-bin QKD in a 50 km fiber link, whose entanglement, steering witness, and security against collective Gaussian attacks are achieved simultaneously through commercially available dispersive optics [12, 42]. Time-frequency correlation measurements can bound Eve's Holevo information with finite-key effects via nonlocal dispersion cancelation capable of operating over extended fiber links without stabilizing interferometers. Furthermore, we extend our qudit-based QKD protocol to a high loss regime (up to 39 dB channel loss, as the current maximum attenuation available in our experiments) and are able to obtain over three hundred secret key rates (SKRs) per second with photon information efficiency (PIE) over 1 bit/coincidences, including the finite-key effects. By utilizing our specially designed $\pm$ 10 000 ps nm^{-1} dispersion emulator (compensator) at the optical telecommunications band, we show $\approx$ 1 order of magnitude improvement in both energy-time entanglement [60–62] and quantum steering [63] witness over a 50 km optical fiber. Leveraging our highly efficient single-photon detectors [10], and an effective error correction code [64, 65], specifically designed for large-alphabet encoding with robustness against high quantum bit error rate (QBER), we realize a high-dimensional QKD that generates an SKR of 0.66 (0.24) Mbit s^{-1} through 21 km (50 km) of single-mode fiber with a secure PIE of 2.65 (2.39) bits/photon coincidences with finite-key effects, respectively. Here we obtained a 7.5$\times$ higher asymptotic SKR (a 6.6$\times$ higher SKR with finite-key effects) compared to the reported highest record using dispersive optics [47], and measured a 0.24 Mbits s^{-1} SKR with finite-key effects at 50 km fiber distance using energy-time entangled qudit QKD protocol. We also note that by using classical attenuated resources, the prepare-and-measurement protocols of high-dimensional QKD using dispersive

optics have been demonstrated by field experiments with a key rate of 1.2 Mbits s^{-1} over optical fibers of 43 km [18]. Additionally, a high-dimensional QKD protocol using large-alphabet encoding of time-energy entangled photons with security against collective Gaussian attacks has been demonstrated and obtained a SKR of 2.7 Mbits s^{-1} at 20 km fiber [16]. Finally, we extend our high-dimensional protocol to the higher loss regime, where we realize that our system preserves a SKR of 0.30 kbits s^{-1} and a secure PIE of 1.10 bits/coincidences under a realistic maximum range of 195 km single-mode fiber (39 dB channel loss), approaching the upper bound of the theoretical limit of SKR [12, 59]. The obtained SKRs outperform recent demonstrated state-of-the-art qubit-based QKD protocols using standard single-photon detectors [25, 26, 66–69]. Our results demonstrate that not only the energy-time entanglement and quantum steering can be preserved over long-fiber distance, but also the potential of practical long-distance qudit QKD with multiple secure bits-per-coincidences and higher SKR over qubit-based QKD protocols.

2. Results

2.1. Violation of EPR steering inequality, Bell-like inequality, and high-dimensional QKD protocol

In figure 1(a), we present the schematic of our experimental setup. In our system, we employ a prepare-and-measure scheme, where Alice initiates the process by generating entangled continuous-wave spontaneous parametric down-conversion (SPDC) photon pairs. These pairs are created using a type-II phase-matched (signal photons have TE polarizations, and idler photons have orthogonal TM polarizations), single-spatial-mode periodically-poled potassium titanyl phosphate waveguide. For our SPDC source, the poling period of the waveguide is 78.74 μm, and the waveguide has a width of 3 μm (AdvR Inc.). The fiber polarization controller (FPC) is used to optimize the generation of orthogonally-polarized SPDC photons. The SPDC photons exiting the waveguide are directed into a short single-mode fiber and coupled into the free space setup via a collimator. In the free space setup, the residual pump photons are eliminated using a combination of a long-pass filter (LPF) and an angle-mounted band-pass filter (BPF). Here the BPF we used allows 95% of the desired passband transmission when filtered beam is incident in both perpendicular and oblique angles (Semrock NIR01-1570/3). Then, Alice uses a polarizing beam splitter (PBS) to separate her photon for local measurement and transmits the other entangled photon via an untrusted quantum channel to a distant receiver, Bob. Our quantum channel consists of two variations. In the first scenario, either 21 km or 50 km fiber spools are employed along with corresponding dispersion compensation modules (DCMs) to nullify the chromatic dispersion caused by the fiber spools. In the second part, a variable optical attenuator (VOA) introduces quantum channel losses of 18, 31, and 39 dB. We implemented a random selection of measurements between key generation and dispersive optics security checks using 90:10 fiber beam splitters. This asymmetric configuration maximizes the throughput of the system's key while ensuring sufficient number of coincidence counts for establishing security based on time-frequency mutually unbiased bases (MUB) [12, 18, 42].

The T_1T_2 bases correspond to the direct detection of photon arrival-time from both parties, and the F_1F_2 bases are the frequency basis that is mutually unbiased with respect to the temporal states. In the case of arrival-time large-alphabet encoding, Alice and Bob individually measure the arrival times of photons with a time slot τ, which establishes a time-bin. A time frame is created by both parties with N time-bins. Within each time frame, Alice and Bob make random selections to measure the arrival time-bin position of the photon, allowing them to extract a symbol consisting of $k = \log_2 N$ bits. Then, Alice and Bob carefully select a time frame in which each party detects precisely one event. Subsequently, they employ error correction and privacy amplification procedures. To ensure security, both parties conduct measurements involving time and frequency correlations. For time basis, Alice and Bob use their single-photon detectors to directly measure two-photon temporal correlation; while for frequency basis, they significantly spread out the single-photon wave packet such that its frequency components are well-resolved in time. Here we utilize a specially designed $\pm$ 10 000 ps nm^{-1} dispersion emulator (compensator) (using chirped fiber Bragg gratings, which provide a dispersion value equivalent to that of $\approx$ 600 km of standard single-mode fiber, but with a loss of only $\approx$ 3 dB) at telecom-band to realize nonlocal dispersion cancelation [70]. We conduct measurements of all feasible time-frequency bases utilizing SNSPDs with high detection efficiency (SNSPDs, $\approx$ 90% detection efficiency, root-mean-square timing jitter $\approx$ 55 ps, dark counts $\approx$ 100 counts/s, PhotonSpot Inc.). The typical coincidence to single counts ratio is 1:9 from the SPDC source generation. These detectors saturate when the detection rate exceeds 3 Megacounts/s. Detection events were time-stamped by both parties with time-to-digital converters (Picoharp 300).

Entangled sources play an important role in many important quantum information processing tasks, such as QKD [11, 15, 16], entanglement distribution [9, 10], quantum storage [71], and quantum teleportation [19]. The energy-time entangled photon-pairs, which have both strong temporal correlation and frequency anti-correlation, are of great interest for long-distance quantum communication because of

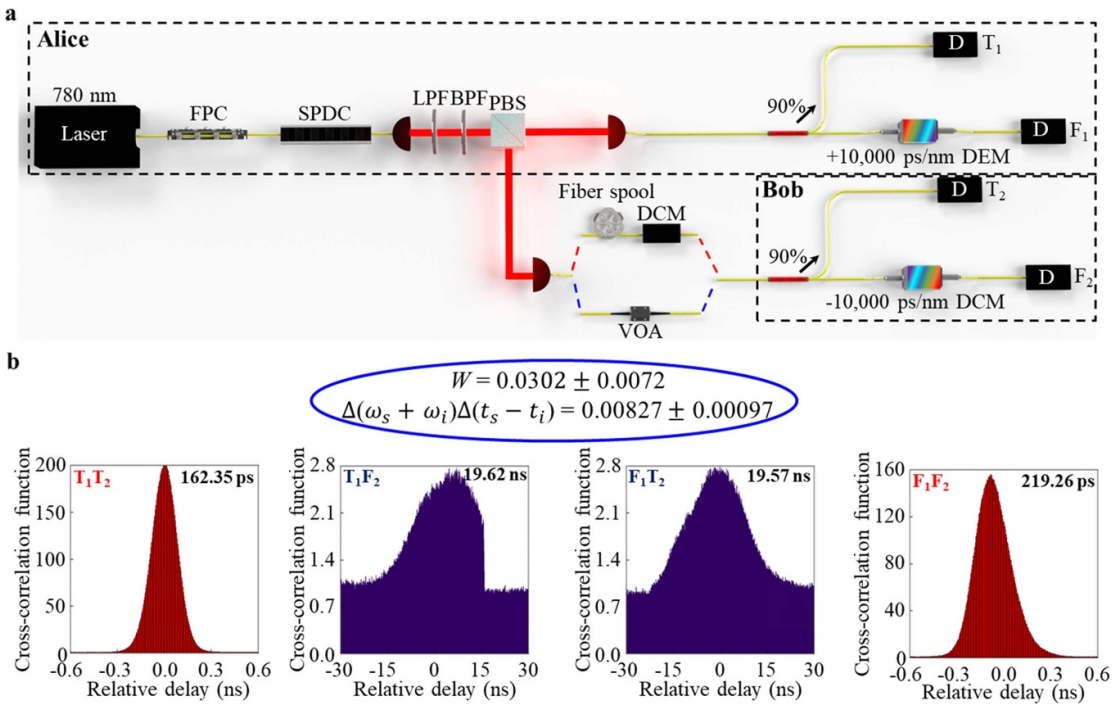

Figure 1. Schematic of entanglement, quantum steering witness, and high-dimensional time-bin QKD protocol. (a) Schematic of the experimental setup. FPC, fiber polarization controller; SPDC, spontaneous parametric down-conversion; LPF, long-pass filter; BPF, band-pass filter; PBS, polarization beam-splitter; D, detector; DCM, dispersion compensation modules; DEM, dispersion emulation modules; VOA, variable optical attenuators; T, Time; F, Frequency. Fiber beam splitters of 90:10 ratios are used for distributing keys and cross-correlation measurements. (b) Measured temporal cross-correlations between Alice and Bob, using all combinations of time-frequency pairs under noiseless conditions. The FWHMs of matched MUB are observed to be 162.35 and 219.26 ps, and those of unmatched MUB are 19.62 and 19.57 ns, respectively. Based on these measurements, we extract $W = 0.0302 \pm 0.0072$ to violate Wasak inequality (Bell-like inequality) by about 135 standard deviations and estimate a joint time-frequency uncertainty product of $\Delta(\omega_s+\omega_i)\Delta(t_s - t_i) = 0.00827 \pm 0.00097$, which violate not only the energy-time entanglement inequality but also the quantum steering inequality by about 1022, and 507 standard deviations, respectively.

their insensitivity to the birefringence effect of fibers. Nonlocality is considered a central feature of energy-time entanglement, which cannot be explained by classical or local hidden-variable theories [22, 23]. The quantum nonlocality can be tested via either a violation of time-frequency uncertainty relations [61, 63], a steering inequality [63], or a Bell-like inequality (Wasak inequality) [60, 62]. The Bell-like inequality is the most strict quantum nonlocality, while the steering inequality is intermediate and the entanglement witness is the most relax criteria. For two unentangled (separable) photons, they must satisfy the following inequality:

$$\Delta\ (\omega_s + \omega_i)\ \Delta\ (t_s - t_i)\ \geqslant\ 1 \tag{1}$$

where each photon, labeled as signal and idler, is described by its frequency ω and its time of arrival t, and Δ represents the standard deviation in the joint spectrum or joint temporal intensity. Hence, a violation of the above separability criterion implies entanglement. A sufficient and more strict condition to rule out the local realism is the quantum steering inequality [63, 72]:

$$\Delta\ (\omega_s + \omega_i)\ \Delta\ (t_s - t_i)\ < \frac{1}{2}. \tag{2}$$

For energy-time entangled photon-pairs, there is no lower limit for the joint frequency-time uncertainty product. Ideally, it can approach zero to witness both entanglement and quantum steering. Moreover, the quantum nonlocality nature can be verified by violation of a Bell-like inequality (Wasak inequality) [60, 62]:

$$W = \frac{\left\langle (\Delta\tau')^2 \right\rangle \left\langle (\Delta\tau)^2 \right\rangle}{\left\langle \left((\Delta\tau)^2 \right)^2 \right\rangle + (2\beta l)^2} \geqslant 1 \tag{3}$$

where $\Delta\tau$ and $\Delta\tau'$ are the variance in time difference before and after dispersive elements, respectively. $2\beta l$ is the magnitude of the applied dispersions on both parties. A violation of this inequality is a clear indication

that the photon-pairs have been initially prepared in an entangled state, and it cannot be obtained within the classical theory and local hidden hidden-variable theories.

A novel feature of our high-dimensional QKD system is that all the possible combinations of time-frequency correlation measurements (T_1T_2, T_1F_2, F_1T_2, and F_1F_2) enable the witness of nonlocal energy-time entanglement and quantum steering by violating Bell-like inequality (Wasak inequality), and time-frequency uncertainty relations simultaneously. Under noiseless conditions, we performed measurements of temporal cross-correlations between Alice and Bob, encompassing all combinations of time-frequency MUB, as shown in figure 1(b). The full width at half maximum (FWHM) of matched MUB are observed to be 162.35 and 219.26 ps, and those of unmatched MUB are 19.62 and 19.57 ns, respectively. Note that the asymmetric profile of correlation peaks in T_1F_2, F_1T_2, and F_1F_2 comes from the slightly mismatched dispersion between $\pm$10 000 ps nm^{-1} dispersion emulator (compensator) modules. This discrepancy in $\pm$10 000 ps nm^{-1} dispersion emulator (compensator) modules include two parts, the difference of the passband of the dispersion spectrum, and the difference on the values of dispersion coefficients. Our dispersion emulator has a passband from 1557.2–1562.7 nm, while our dispersion compensator's spectrum lies between 1557.7–1562.3 nm. At 1560.4 nm, the +10 000 ps nm $^{-1}$ dispersion emulator has dispersion coefficients of 10 024 ps nm^{-1}, and the −10 000 ps nm $^{-1}$ DCM has −9886 ps nm^{-1} dispersion coefficients (Proximion). The cutoff of T_1F_2 correlation peak around 15 ns appears because the limitation of the passband of Bob's −10 000 ps nm^{-1} DCM. Based on these measurements and an average $2\beta l = 20\,057$ ps^2, we extract $W = 0.0302 \pm 0.0072$ to violate Bell-like inequality (Wasak inequality) by about 135 standard deviations and estimate a joint time-frequency uncertainty product of $\Delta(\omega_s+\omega_i)\Delta(t_s - t_i) = 0.008\,27 \pm 0.000\,97$, which violates not only the energy-time entanglement inequality but also the quantum steering inequality by about 1022, and 507 standard deviations, respectively. Although we do not directly measure the joint spectrum intensity of biphotons due to the bandwidth limitation of commercial frequency filtering components, we can estimate the frequency product via transforming temporal correlation into spectral correlation using our $\pm$ 10 000 ps nm^{-1} dispersion emulator (compensator) modules. To the best of our knowledge, compared to previous works [61–63], we report new records on witnessing both energy-time entanglement and quantum steering by violating Bell-like inequality (Wasak inequality) and the joint time-frequency uncertainty product by 135 and 507 standard deviations, respectively.

2.2. High-dimensional time-bin QKD and EPR steering witness over 50 km optical fibers

Next, given that we have a highly entangled source, we report the entangled-based large-alphabet QKD key throughput and PIE at the local fiber link (with negligible loss). The raw key rate can be extracted directly from the time stamps using the high-dimensional QKD protocol and our layered error correction code. Upon capturing the time stamps of entangled photons, we proceeded to parse them into $\log_2 N$ bit symbols for each time frame in which Alice and Bob had a single coincidence detection. Then, we use a layered error correction [64, 65] on all layers of the raw k-bit symbols, which maintains a high reconciliation efficiency β, even when facing a high QBER [16, 42]. The secure PIE can be expressed as $\Delta I_{\mathrm{AB}} = \beta I_{\mathrm{AB}} - \chi^{\mathrm{E}} - \Delta_{FK}$, measured in bits-per-coincidence. Here I_{AB} represents the Shannon information shared between both parties, χ^{E} denotes Eve's eavesdropping in the infinite-key limit [12, 47], and Δ_{FK} accounts for the finite-key length [16, 18, 42]. In our approach, we employ a finite-key security parameter of $\varepsilon_s = 10^{-5}$, which encompasses error correction ($\varepsilon_{\mathrm{EC}}$), privacy amplification ($\varepsilon_{\mathrm{PA}}$), smooth min-entropy estimation ($\bar{\varepsilon}$), and security parameter estimation ($\varepsilon_{\mathrm{PE}}$) failures. We set $\varepsilon_{\mathrm{EC}} = \varepsilon_{\mathrm{PA}} = \bar{\varepsilon} = 10^{-10}$, and approximate $\varepsilon_{\mathrm{PE}}$ to be around 10^{-5}, following similar methods used in previous studies [16, 18, 42]. By using a finite-key length on the order of 10^6, we estimate an uncertainty in the excess spectral noise parameter $\xi_\omega \approx 0.002$, over the Eve's Holevo leak in the finite-key limit [16, 18, 42]. As for changing the bits/photon in figure 2(a), we can change either the time-bin size or the number of time-bins per frame. Considering the temporal uncertainty of our SNSPDs surpasses the SPDC correlation time (≈4 ps from the spectral bandwidth of our source), we opt for a time-bin size of 100 ps in our experiments. This selection ensures maximum throughput in our system. In figure 2(a), by using large-alphabet temporal encoding, we record the raw key rate and PIE of our photon-efficient energy-time entangled source to be 1.94 Mbits s^{-1} at 10 bits/photon encoding, and 3.88 bits/coincidences for 7 bits/photon encoding, respectively. By performing back-to-back T_1T_2 and F_1F_2 correlation peak measurements in figure 1(b), we calculate the time-frequency covariance matrix to obtain an upper bound on Eve's Holevo information of 0.226 bits/coincidences, including the finite-key effects.

Then, we extract the secure PIE and SKR of our SPDC source with finite-key effects at noiseless conditions, with the maximum SKR, and secure PIE of 1.62 Mbits s^{-1} and 3.55 bits/coincidences, respectively. We are operating near capacity-achieving conditions, where the gap between raw Shannon information capacity in terms of PIE and secure PIE is minimized due to high reconciliation efficiency β of 0.86, and strict Holevo bounds obtained from T_1T_2 and F_1F_2 correlation peaks. The increasing error bars in

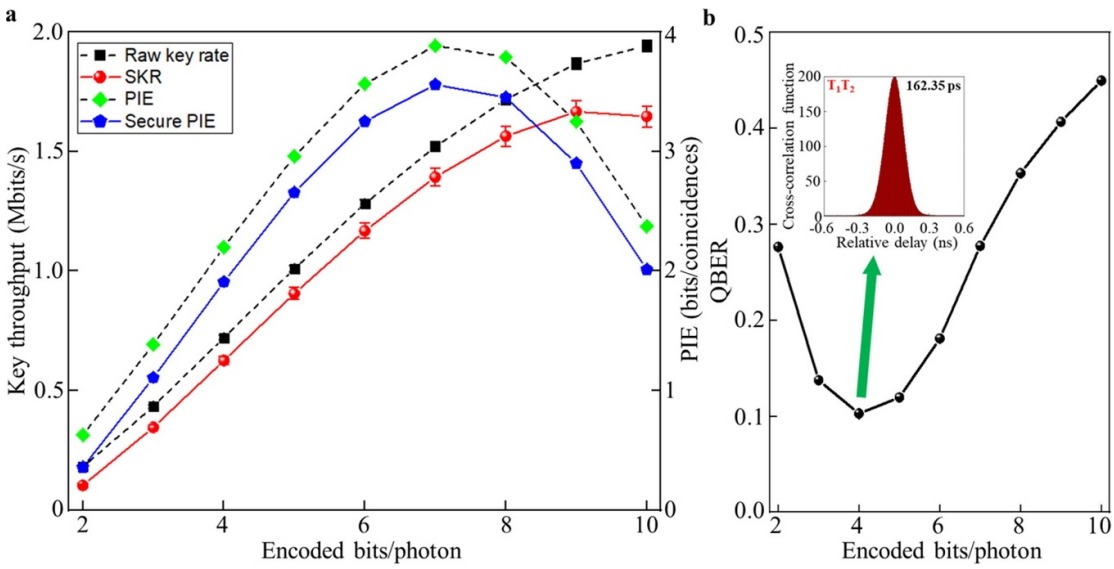

Figure 2. High-dimensional time-bin QKD performances of entangled source at local fiber link. (a) Here we measured secure PIE and SKR using our source at a 5 m local link, and the maximum SKR with finite-key effects is 1.62 Mbits s^{-1} at 10 bits/photon encoding, with the maximum secure PIE is measured to be 3.55 bits/coincidences at 7 bits/photon encoding. The error bars in the presented data are determined by calculating the standard deviation from 3 separate QKD sessions for each data set. (b) For four encoded bits/photon, due to the coincide of T_1T_2 correlation peak (example plot in the inset, also shown in figure 1(b)) and the time frame window, the error will occur in a less significant manner, causing the minimum of QBER. On the other hand, larger encoded bits/photon will increase time frame size, which leads to more accidental coincidence counts and higher QBER. At 4-bits encoding, the minimum QBER is 10.28%, while the QBER error rate reaches 44.96% at 10-bits encoding. Note that the measurement condition here is when detector bias is not fully applied due to the saturation of single counts of our SNSPDs (≈ 3 million single counts per channel).

key throughput for larger encoded bits/photon is resulting from increasing time frame size, which leads to larger accidental coincidences. The error bars in the presented data are determined by calculating the standard deviation from three separate QKD sessions for each data set, and each data is recorded in 3 s. In figure 2(b), we report the QBER of our entangled SPDC source at the local fiber link. For four encoded bits/photon, due the coincidence of T_1T_2 correlation peak (example plot in inset, also shown in figure 1(b)) and the time frame window, the error will occur in less significant manner, causing the minimum of QBER. On the other hand, larger encoded bits/photon will increase time frame size, which leads to more accidental coincidence counts and higher QBER. At 4-bits encoding, the minimum QBER is 10.28%, while the error rate increases to 44.96% at 10-bit encoding. In figure 2, our results confirm that the large-alphabet encoding with optimized key throughout can be achieved with high reconciliation efficiency β and tolerate high QBER. Note that the measurement condition for figure 2 is when detector bias is not fully applied (not operating at maximum detection efficiency) due to the saturation of single counts of our SNSPDs (≈3 million single counts per channel), causing the difficulty in detecting coincidence count rate in a reasonable duration. For all the other measurements presented in this work, we use maximum detection efficiency (fully biased) for best QKD performance.

So far, the experimental maximum transmitted fiber distance using entangled sources and high-dimensional QKD arrival-time encoding has been limited to 20 km [16, 47]. Here, we present the experimental measurements of key throughput and PIE of energy-time entangled high-dimensional QKD at 50 km fiber distance, as shown in figure 3. For longer distance qudit QKD measurements, we introduced two fiber spools with equal lengths L, between the source and the detectors of both Alice and Bob. Utilizing a matched-fiber configuration helps overcome the technical challenge of aligning two temporal peaks that are more than 10 μs apart. Our time-correlated single-photon counting module imposes this limitation. These matched fibers allowed us to proceed with our measurements and experiments effectively. Including finite-key effects, we measured SKR (raw key rate) and secure PIE at 21 km of 0.66 Mbits s^{-1} (0.83 Mbits s^{-1}), 2.65 (3.04) bits/coincidences, respectively. We achieved a 7.5× higher asymptotic SKR (a 6.6× higher SKR with finite-key effects) compared to the reported highest record using dispersive optics [47]. We also note that by using classical attenuated resources, the prepare-and-measurement protocols of high-dimensional QKD using dispersive optics have been demonstrated by field experiments with a key rate of 1.2 Mbits s^{-1} over optical fibers of 43 km [18]. Additionally, a high-dimensional QKD protocol using large-alphabet encoding of time-energy entangled photons with security against collective Gaussian attacks has been demonstrated and obtained a SKR of 2.7 Mbits s^{-1} at 20 km fiber [16]. At a 50 km fiber link, we

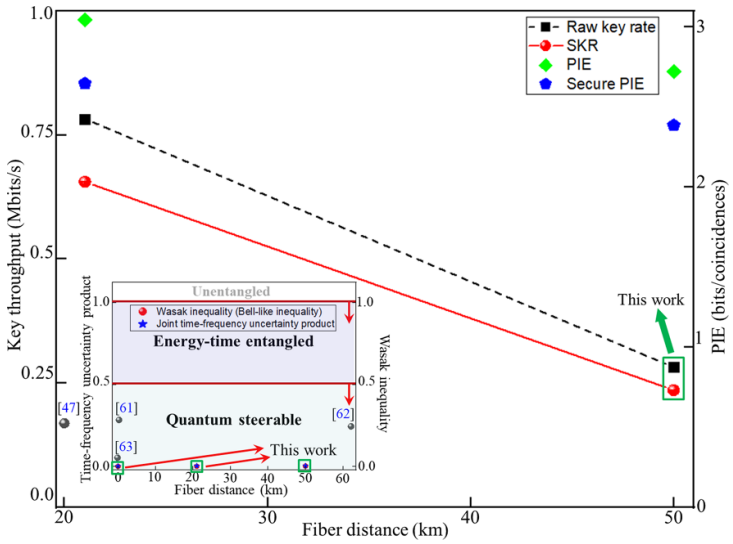

Figure 3. Experimental high-dimensional time-bin QKD and EPR steering witness over a 50 km optical fiber. Including finite-key effects, the measured SKR (raw key rate) and secure PIE at 21 km are 0.66 Mbits s^{-1} (0.83 Mbits s^{-1}), 2.65 (3.04) bits/coincidences, respectively. At 50 km fiber distance, we measured maximized SKR (raw key rate) and secure PIE of 0.24 (0.30) Mbits s^{-1}, 2.39 (2.72) bits/coincidences, considering finite-key effects, respectively. The SKR (raw key rate) and secure PIE are optimized with 8 and 6 bits/photon encoding, respectively. Inset: distributed energy-time entanglement and EPR steering. At 50 km fiber distance, we extract $W = 0.0332 \pm 0.0127$ to violate Bell-like inequality (Wasak inequality) by about 76 standard deviations. Furthermore, at this fiber distance, we estimate a joint time-frequency uncertainty product of $\Delta(\omega_s + \omega_i)\Delta(t_s - t_i)$ of 0.00847 ± 0.00102, which violates not only the energy-time entanglement inequality (shaded region) but also the quantum steering inequality (shaded region) by about 972, and 482 standard deviations, respectively. Here we can still outperform previous works [61–63] and maintain records of energy-time entanglement and quantum steering witness after a 50 km fiber link.

measured maximized SKR (raw key rate) and secure PIE of 0.24 (0.30) Mbits s^{-1}, 2.39 (2.72) bits/coincidences, including finite-key effects, respectively. The SKR (raw key rate) and secure PIE are optimized with 8 and 6 bits/photon encoding, respectively. We have successfully maintained a secure PIE of 2.39 bits/coincidences and an SKR of 0.24 Mbits s^{-1} after the loss of 50 km standard telecom fiber spools ($\approx$ 10 dB) and the corresponding DCM ($\approx$ 2.6 dB), using our entangled photon-pair source. With an extended time frame, the secure PIE drops mainly as a result of the increased occurrence of multi-pair events. All the measured T_1T_2 and F_1F_2 correlation peaks are presented in figure A1 in appendix. The error bars are based on the standard deviation of three QKD sessions (3 s for each recording) for each data set. All of the other experimental key throughput and PIE data corresponding to different encoding bits/photon is given in figure A2 (see appendix).

In figure 3 inset, we report the distributed energy-time entanglement and EPR steering witness for 21 and 50 km fiber distances. At a 50 km fiber distance, we extract $W = 0.0332 \pm 0.0127$ to violate Bell-like inequality (Wasak inequality) by about 76 standard deviations. At this fiber distance, we estimate a joint time-frequency uncertainty product $\Delta(\omega_s + \omega_i)\Delta(t_s - t_i)$ of 0.00847 ± 0.00102, which violates both the energy-time entanglement inequality and the EPR steering inequality by about 972, and 482 standard deviations, respectively. Compared to the noiseless condition in figure 1(b), we can still outperform prior works [61–63] and maintain records of energy-time entanglement and quantum steering witness after distributing in a 50 km fiber link. Our findings from the quantum steering witness after a 50 km fiber distance suggest promising avenues for future experimental investigations into high-dimensional one-sided device-independent QKD, whose security is linked to the violation of quantum steering inequality [73–75].

2.3. Experimental maximum tolerance of channel loss in qudit time-bin QKD protocol

After demonstrating high-dimensional time-bin QKD and EPR steering via 50 km fiber distance, here we extend the maximum SKR and secure PIE of our entanglement-based high-dimensional QKD protocol up to 39 dB (as the current maximum attenuation available in our experiments), as shown in figure 4. For 18, 31, and 39 dB channel losses measurements, we utilize the VOA in figure 1(a), and the FWHM of T_1T_2 and F_1F_2 bases are consistent with the FWHM of T_1T_2 and F_1F_2 bases under the noiseless condition in figure 1(b), due to the VOA's negligible dispersion. At 18 dB loss, we are able to obtain a maximum SKR and a secure PIE of 38.33 kbits s^{-1} and 1.70 bits/coincidences, with 7 and 5 bits/photon encoding, respectively. For 31 dB channel loss, we observe an SKR and a secure PIE of 1.80 kbits s^{-1}, 1.19 bits/coincidences with 6 and 5 bits/photon encoding, respectively. Finally, under a 39 dB quantum channel loss (equivalently to $\approx$ 244 km-long ultra-low-loss fibers or 195 km standard single-mode fibers), we achieve an experimental SKR and a secure

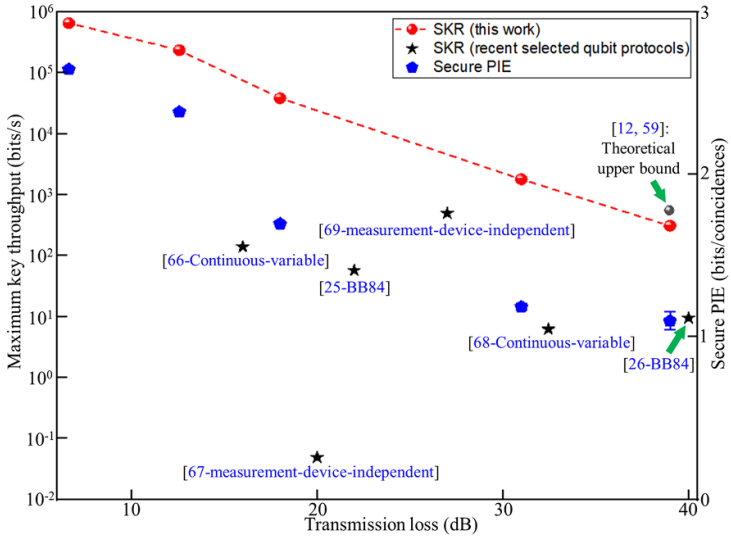

Figure 4. Maximum experimental tolerable loss of large-alphabet time-bin QKD protocol. Here we present the maximum SKR and secure PIE of our protocol with channel losses from 6.63 dB (corresponding to losses at 21 km fiber distance) to 39 dB. Under 39 dB channel loss (equivalently to ≈ 244 km ultra-low-loss fibers, or 195 km standard single-mode fibers) and finite-key effects, we achieve a SKR and a secure PIE of 0.30 kbits s^{-1} and 1.10 bits/coincidences with 5 bits/photon encoding. For variable attenuations, the increasing error bars in key throughput and PIE is resulting from the increasing noise in a quantum channel. The error bars represent the standard deviation of three QKD sessions for every dataset. Our experimental results are closely match with theoretical upper bound limit of SKR at 39 dB channel loss from high-dimensional QKD protocols [12, 59], and outperform recent state-of-the-art qubit QKD protocols using commercial single-photon detectors [25, 26, 66–69].

PIE of 0.30 kbits s^{-1} and 1.10 bits/coincidences with 5 bits/photon encoding. Note that for all the reported SKR and secure PIE here, we include the penalties from the finite-key effects. For variable attenuations, the increasing error bars in key throughput and PIE result from the increasing noise in a quantum channel. The error bars are based on the standard deviation of three QKD sessions for each data set. All of the other experimental key throughput and PIE data corresponding to different encoding bits/photon is shown in figure A3 (see appendix). Our highly efficient SNSPDs exhibit consistent jitter and low dark counts, regardless of the detection rate. As a result, the error bars across all measurement data sets remain small. For this theoretical upper bound SKR calculation at 39 dB channel loss, we use our experimental parameters and the channel modeling from prior works [12, 59]. By using our measurement results and their corresponding quantum channel losses, we extrapolate to calculate the realistic photon-pair source flux at negligible loss condition, as this particular measurement is limited by the saturation of single counts in our SNSPDs (also noted in figure 2). For this particular analysis, we use a time frame size of 3.2 ns (5 bits/photon encoding and 100 ps time-bin size), and the FWHM of T_1T_2 and F_1F_2 from figure 1(b) to calculate the measured excess spectral noise factor ξ_ω [12, 42]. Other experimental parameters are given as follows: timing jitter of our SNSPDs ≈ 155 ps; ≈ 90% detection efficiency; dark counts ≈ 100 counts s^{-1}; maximum reconciliation efficiency β of 0.86. Here our results show that under a high loss regime of 39 dB, our entangled source and qudit-based QKD protocol can preserve its large-alphabet nature and still deliver several hundreds of secret keys per second. Compared to recently demonstrated BB84 [25, 26], and continuous-variable [66, 68] QKD protocols, we have over two orders of magnitude improvement on SKR under the same channel loss, while we have over one order of magnitude higher SKR than a recent measurement-device-independent QKD protocol [69]. To summarize, our experimental results closely match the theoretical upper bound limit of SKR at 39 dB channel loss from high-dimensional time-bin QKD protocols [12, 59], and outperform recent state-of-the-art qubit QKD protocols using standard single-photon detectors [25, 26, 66–69].

3. Conclusion

Through our experiments, we have demonstrated a high-dimensional time-bin QKD protocol in a 50 km fiber link and under channel loss up to 39 dB, considering the finite-key effects. By using a specially designed ± 10 000 ps nm^{-1} dispersion emulator (compensator) at the telecom band to realize nonlocal dispersion cancelation, we are able to set new records on witnessing both energy-time entanglement and EPR steering after a 50 km fiber distribution. The security implementation of our entanglement-based qudit protocol is commercially available and robust, without the need to stabilize a Franson interferometer over long fiber transmission distances [16], and the dimensionality d of our temporal encoded states scales favorably

without the requirement of $2d - 1$ interferometers [17]. Here we measured a SKR and a secure PIE at 21 km of 0.66 Mbits s^{-1}, and 2.65 bits/coincidences, respectively. We achieved a 7.5× higher SKR (a 6.6× higher SKR with finite-key effects) compared to the prior highest record using dispersive optics [47]. We also note that by using classical attenuated resources, the prepare-and-measurement protocols of high-dimensional QKD using dispersive optics have been demonstrated by field experiments with a key rate of 1.2 Mbits s^{-1} over optical fibers of 43 km [18]. Additionally, a high-dimensional QKD protocol using large-alphabet encoding of time-energy entangled photons with security against collective Gaussian attacks has been demonstrated and obtained a SKR of 2.7 Mbits s^{-1} at 20 km fiber [16]. Here we obtained a SKR and secure PIE of 0.24 Mbits s^{-1} and 2.39 bits/coincidences at 50 km distance. Finally, we explore the maximum range of our entanglement-based qudit time-bin protocol under the high loss regime, including the finite-key effects. Under a 39 dB quantum channel loss (equivalently to ≈ 244 km ultra-low-loss fibers or 195 km standard single-mode fibers), we are able to preserve intrinsic high-dimensional nature to achieve an experimental SKR and a secure PIE of 0.30 kbits s^{-1} and 1.10 bits/coincidences, respectively. Our experimental results closely match the theoretical upper bound limit of SKR in energy-time entanglement-based high-dimensional QKD protocols [12, 59], and outperform recent state-of-the-art qubit-based QKD protocols using commercial single-photon detectors [25, 26, 66–69]. Our simple and robust entanglement-based qudit time-bin protocol is promising for practical long-distance quantum steering and qudit QKD with multiple secure bits-per-coincidence and higher SKR than mature qubit-based QKD protocols. In the future, it is possible to combine existing theoretical analysis against general attacks in the finite-key regime [76, 77] to our experimental hardware. Furthermore, the usage of energy-time entangled photons in the current large-alphabet QKD system is directly compatible with multi-user quantum networks, and is likely to play a vital role in the future implementation of quantum repeater technologies.

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors.

Acknowledgments

We thank useful discussions with Charles Ci Wen Lim, Jacob Mower, Jing-Yuan Liu, Patrick Hayden, Graeme Smith, and Alexander Euk Jin Ling; discussions on the superconducting nanowire single-photon detectors with Vikas Anant. This grant is enabled by the National Science Foundation under Award Numbers 1741707 (EFRI ACQUIRE), 1919355 and 1936375 (QII-TAQS), and 2137984 (QuIC-TAQS). This study is supported by the Army Research Office Multidisciplinary University Research Initiative (W911NF-21-2-0214),

Author contributions

K -C C developed the idea. K -C C, X C, and M C S conducted the measurements. K-C C, and M C S performed data analysis and security calculations. K-C C, and Z Z performed theoretical calculations. M C S, Z Z, and C W W supported and discussed the studies. K-C C, M C S, X C, and C W W prepared the manuscript. C W W supervised the project.

Appendix

A.1 Measured cross-correlation between Alice and Bob at 21 and 50 km fiber distances

As described in the main text, here we present all of the measured cross-correlation functions (T_1T_2, T_1F_2, F_1T_2, and F_1F_2) between Alice and Bob at 21 and 50 km fiber distances. Similar to the main text figure 1(b), we connect ± 10 000 ps nm^{-1} dispersion emulator (compensator) modules after compensating chromatic dispersions of fiber spools at 21 and 50 km. In figure A1(a), the FWHMs of matched time-frequency MUB are observed to be 170.99 and 235.63 ps, and those of unmatched MUB is 19.86 and 19.90 ns, respectively. We report measured cross-correlations between Alice and Bob, using all combinations of time-frequency pairs at 50 km fiber distance, as shown in figure A1(b). The FWHMs of matched MUB are observed to be 167.16 and 228.09 ps, and those of unmatched MUB are 19.73 and 19.69 ns, respectively. All the FWHM of time-frequency correlation peaks increase slightly compared to the noiseless condition in main text figure 1(b) due to the imperfect nonlocal dispersion cancelations after 21 and 50 km fiber distributions. For both fiber distances, the asymmetric profile of correlation peaks in T_1F_2, F_1T_2, and F_1F_2 comes from the slightly mismatched dispersion between ± 10 000 ps nm^{-1} dispersion emulator (compensator) modules, and the cutoff of T_1F_2 correlation peak around 15 ns appears because the limitation of the passband of Bob's −10 000 ps nm^{-1} DCM. Using the measurement values of T_1T_2 and F_1F_2 basis, we extract Eve's Holevo

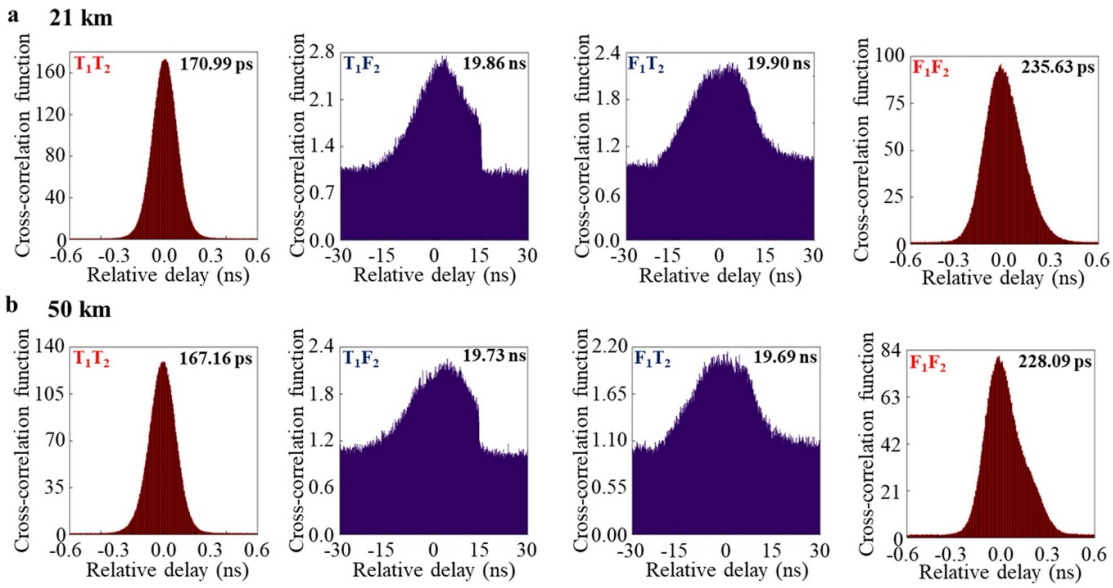

Figure A1. Measured cross-correlation between Alice and Bob at 21 and 50 km fiber distances. (a) Measured cross-correlations between Alice and Bob, using all possible combination of time-frequency pairs at 21 km fiber distance. The FWHMs of matched MUB are observed to be 170.99 and 235.63 ps, and those of unmatched MUB are 19.86 and 19.90 ns, respectively. (b) Measured cross-correlations between Alice and Bob, using all possible combination of time-frequency pairs at 50 km fiber distance. The FWHMs of matched MUB are observed to be 167.16 and 228.09 ps, and those of unmatched MUB are 19.73 and 19.69 ns, respectively. All the FWHM of time-frequency correlation peaks increase slightly compared to noiseless condition in main text figure 1(b) due to imperfect nonlocal dispersion cancelations after 21 and 50 km fiber distributions. For both fiber distances, the asymmetrical shape observed in correlation peaks for T_1F_2, F_1T_2, and F_1F_2 results from the slight discrepancy in dispersion between $\pm 10\,000$ ps nm^{-1} dispersion emulator (compensator) modules. Additionally, the cutoff of T_1F_2 correlation peak at approximate 15 ns is due to the limitations of Bob's $-10\,000$ ps nm^{-1} DCM passband.

information after 21 and 50 km fiber distributions by calculating the time-frequency covariance matrix [12, 42].

A.2 High-dimensional key throughput and PIE versus encoded bits/photon with different quantum channel losses

In figure A2, we present the high-dimensional key throughput and PIE versus different bits/photon encoding of energy-time entangled sources at 21 and 50 km fiber distances. To be consistent with the results in the main text, here we choose a time-bin size of 100 ps, and include same finite-key effects for all the data analysis in figures A2 and A3. In figure A2(a), for a 21 km fiber distribution, the maximum measured SKR (raw key rate) and secure PIE are 0.66 Mbits s^{-1} (0.83 Mbits s^{-1}), 2.65 (3.04) bits/coincidences with 8 and 6 bits/photon encoding, respectively. The QBER at 8 and 6 bits/photon encoding are 42.31% and 28.23%, respectively. In figure A2(b), at 50 km fiber distance, we measured maximized SKR (raw key rate) and secure PIE of 0.24 (0.30) Mbits s^{-1}, 2.39 (2.72) bits/coincidences, with 8 and 6 bits/photon encoding, respectively. The QBER at 8 and 6 bits/photon encoding are 43.10% and 30.03%, respectively. We can see that as the loss of quantum channel increases, the QBER in corresponding bits/photon encoding also increases. As the time frame extends, the secure PIE diminishes due to the increasing detection of accidental photons. The error bars are based on the standard deviation of three QKD sessions for each data set.

Then, we report the high-dimensional key throughput and PIE versus different bits/photon encoding of energy-time entangled source under 18, 31, and 39 dB quantum channel loss in figure A3. Figure A3(a) shows the maximum measured SKR (raw key rate) and secure PIE with 18 dB transmission loss are 38.33 kbits s^{-1} (51.87 kbits s^{-1}), 1.70 (1.99) bits/coincidences with 7 and 5 bits/photon encoding, respectively. The QBER at 7 and 5 bits/photon encoding are 42.54% and 27.79%, respectively. In figure A3(b), at 31 dB channel loss, we measured maximized SKR (raw key rate) and secure PIE of 1.80 (2.35) kbits s^{-1}, 1.19 (1.51) bits/coincidences, with 6 and 5 bits/photon encoding, respectively. The QBER at 6 and 5 bits/photon encoding are 39.21% and 32.43%, respectively. Finally, in figure A3(c), under 39 dB transmission loss, we measured maximized SKR (raw key rate) and secure PIE of 0.30 (0.39) kbits s^{-1}, 1.10 (1.35) bits/coincidences, with 5 bits/photon encoding. The QBER at 5 bits/photon encoding is 34.46%. Note that for all the secure PIE and SKR presented in this appendix, the finite-key effects have been considered.

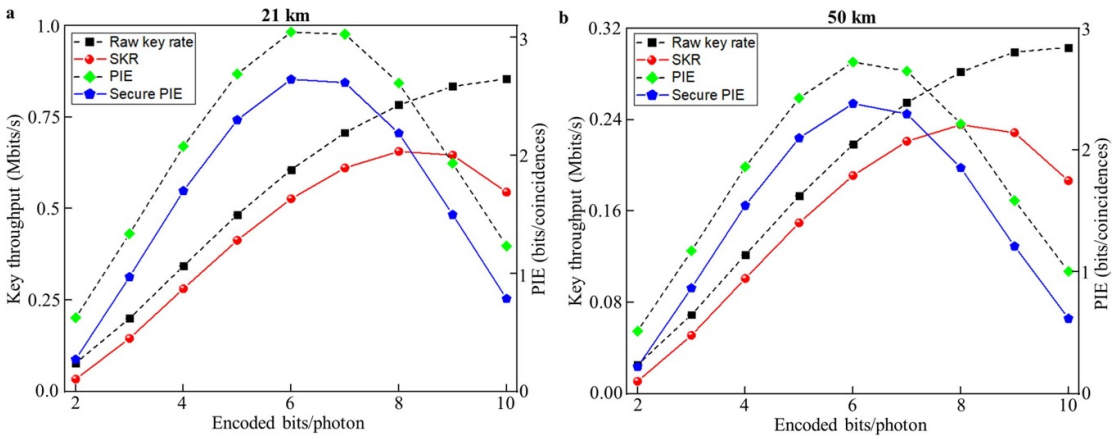

Figure A2. High-dimensional time-bin QKD with various encoded bits/photon at 21 and 50 km fiber distances. (a) Including the finite-key effects, the maximum measured SKR (raw key rate) and secure PIE at 21 km are 0.66 Mbits s^{-1} (0.83 Mbits s^{-1}), 2.65 (3.04) bits/coincidences with 8 and 6 bits/photon encoding, respectively. The QBER at 8 and 6 bits/photon encoding are 42.31% and 28.23%, respectively. (b) At 50 km fiber distance, we measured maximized SKR (raw key rate) and secure PIE of 0.24 (0.30) Mbits s^{-1}, 2.39 (2.72) bits/coincidences, with 8 and 6 bits/photon encoding and finite-key effects, respectively. The QBER at 8 and 6 bits/photon encoding are 43.10% and 30.03%, respectively. As the time frame extends, the secure PIE diminishes due to the increasing detection of accidental photons. The error bars are based on the standard deviation of three QKD sessions for each data set.

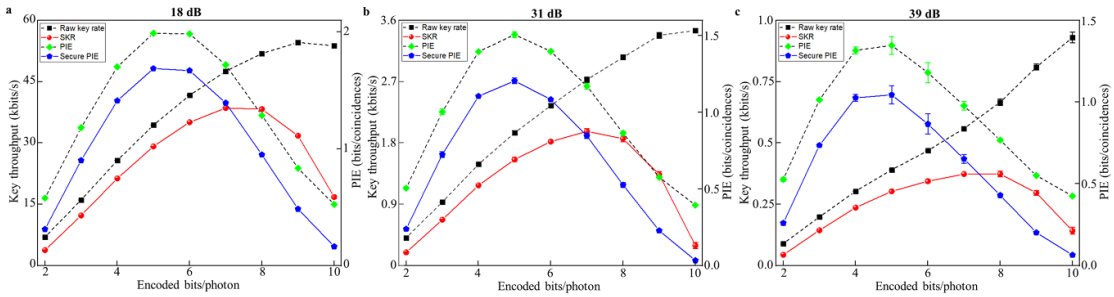

Figure A3. High-dimensional key throughput and PIE with various encoded bits/photon under higher quantum channel losses. (a) With the finite-key effects, the maximum measured SKR (raw key rate) and secure PIE with 18 dB transmission loss are 38.33 kbits s^{-1} (51.87 kbits s^{-1}), 1.70 (1.99) bits/coincidences with 7 and 5 bits/photon encoding, respectively. The QBER at 7 and 5 bits/photon encoding are 42.54% and 27.79%, respectively. (b) At 31 dB channel loss, we measured maximized SKR (raw key rate) and secure PIE (PIE) of 1.80 (2.35) kbits s^{-1}, 1.19 (1.51) bits/coincidences, with 6 and 5 bits/photon encoding and finite-key effects, respectively. The QBER at 6 and 5 bits/photon encoding are 39.21% and 32.43%, respectively. (c) Under 39 dB transmission loss, we measured maximized SKR (raw key rate) and secure PIE of 0.30 (0.39) kbits s^{-1}, 1.10 (1.35) bits/coincidences, with 5 bits/photon encoding in finite-key regime. The QBER at 5 bits/photon encoding is 34.46%. For variable attenuations, the increasing error bars in key throughput and PIE is resulting from the increasing noise in a quantum channel. The error bars are based on the standard deviation of three QKD sessions for each data set.

For variable attenuations, the increasing error bars in key throughput and PIE result from the increasing noise in a quantum channel. The error bars are based on the standard deviation of three QKD sessions for each data set. For QBER analysis, we can see that in same bits/photon encoding, the QBER increases with higher quantum channel losses. By using our photon-efficient energy-time entangled qudit-based QKD protocol, at 50 km fiber link, including finite-key effects, we measured maximized SKR (raw key rate) and secure PIE of 0.24 (0.30) Mbits s^{-1}, 2.39 (2.72) bits/coincidences, respectively. Our results show that under a high loss regime of 39 dB, our entangled source and qudit QKD protocol can preserve its high-dimensional nature and deliver several hundreds of secret keys per second with PIE over 1 bits/coincidences. These results closely match the theoretical upper bound limit of SKR of energy-time entanglement-based high-dimensional QKD protocols [12, 59], and outperform recent state-of-the-art qubit QKD protocols using standard single-photon detectors [25, 26, 66–69].

ORCID iDs

Kai-Chi Chang https://orcid.org/0000-0002-2562-0009
Murat Can Sarihan https://orcid.org/0000-0003-3800-7980
Xiang Cheng https://orcid.org/0000-0003-4632-8477

Zheshen Zhang https://orcid.org/0000-0002-8668-8162
Chee Wei Wong https://orcid.org/0000-0001-7652-7720

References

[1] Xu F, Ma X, Zhang Q, Lo H K and Pan J W 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002
[2] Vernam G S 1926 Cipher printing telegraph systems: for secret wire and radio telegraphic communications *J. AIEE* **45** 109
[3] Shannon C E 1949 *Bell Syst. Tech. J.* **28** 656
[4] Zapatero V, Van Leent T, Arnon-Friedman R, Liu W-Z, Zhang Q, Weinfurter H and Curty M 2023 Advances in device-independent quantum key distribution *npj Quantum Inf.* **9** 10
[5] 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] Marcikic I, De Riedmatten H, Tittel W, Zbinden H, Legré M and Gisin N 2004 Distribution of time-bin entangled qubits over 50 km of optical fiber *Phys. Rev. Lett.* **93** 180502
[7] Inagaki T, Matsuda N, Tadanaga O, Asobe M and Takesue H 2013 Entanglement distribution over 300 km of fiber *Opt. Express* **21** 23241
[8] Aktas D, Fedrici B, Kaiser F, Lunghi T, Labonté L and Tanzilli S 2016 Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography *Laser Photon. Rev.* **10** 451
[9] Ecker S *et al* 2019 Overcoming noise in entanglement distribution *Phys. Rev.* X **9** 041042
[10] Chang K-C *et al* 2021 648 Hilbert space dimensionality in a biphoton frequency comb: entanglement of formation and Schmidt mode decomposition *npj Quantum Inf.* **7** 48
[11] 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
[12] 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
[13] 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
[14] Nunn J, Wright L J, Söller C, Zhang L, Walmsley I A and Smith B J 2013 Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion *Opt. Express* **21** 15959
[15] Mirhosseini M, Magaña-Loaiza O S, O'Sullivan M N, Rodenburg B, Malik M, Lavery M P, Padgett M J, Gauthier D J and Boyd R W 2015 High-dimensional quantum cryptography with twisted light *New J. Phys.* **17** 033033
[16] Zhong T *et al* 2015 Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding *New J. Phys.* **17** 022002
[17] Islam N T, Lim C C W, Cahall C, Kim J and Gauthier D J 2017 Provably secure and high-rate quantum key distribution with time-bin qudits *Sci. Adv.* **3** e1701491
[18] Lee C, Bunandar D, Zhang Z, Steinbrecher G R, Dixon P B, 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
[19] Pirandola S, Eisert J, Weedbrook C, Furusawa A and Braunstein S L 2015 Advances in quantum teleportation *Nat. Photon.* **9** 641
[20] Sangouard N, Simon C, De Riedmatten H and Gisin N 2011 Quantum repeaters based on atomic ensembles and linear optics *Rev. Mod. Phys.* **83** 33
[21] Azuma K, Tamaki K and Lo H K 2015 All-photonic quantum repeaters *Nat. Commun.* **6** 6787
[22] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 Bell nonlocality *Rev. Mod. Phys.* **86** 419
[23] Uola R, Costa A C, Nguyen H C and Gühne O 2020 Quantum steering *Rev. Mod. Phys.* **92** 015001
[24] Bunandar D *et al* 2018 Metropolitan quantum key distribution with silicon photonics *Phys. Rev.* X **8** 021009
[25] Wengerowsky S *et al* 2019 Entanglement distribution over a 96-km-long submarine optical fiber *Proc. Natl Acad. Sci.* **116** 6684
[26] Wengerowsky S *et al* 2020 Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre *npj Quantum Inf.* **6** 5
[27] Zhang L, Silberhorn C and Walmsley I A 2008 Secure quantum key distribution using continuous variables of single photons *Phys. Rev. Lett.* **100** 110504
[28] Etcheverry S, Cañas G, Gómez E S, Nogueira W A T, Saavedra C, Xavier G B and Lima G 2013 Quantum key distribution session with 16-dimensional photonic states *Sci. Rep.* **3** 2316
[29] Cañas G *et al* 2017 High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers *Phys. Rev.* A **96** 022317
[30] Ding Y, Bacco D, Dalgaard K, Cai X, Zhou X, Rottwitt K and Oxenløwe L K 2017 High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits *npj Quantum Inf.* **3** 25
[31] Bacco D *et al* 2019 *Commun. Phys.* **2** 140
[32] Xavier G B and Lima G 2020 Quantum information processing with space-division multiplexing optical fibres *Commun. Phys.* **3** 9
[33] Lio B D, Cozzolino D, Biagi N, Ding Y, Rottwitt K, Zavatta A, Bacco D and Oxenløwe L K 2021 Path-encoded high-dimensional quantum communication over a 2-km multicore fiber *Npj Quantum Inf.* **7** 63
[34] Doda M, Huber M, Murta G, Pivoluska M, Plesch M and Vlachou C 2021 Quantum key distribution overcoming extreme noise: simultaneous subspace coding using high-dimensional entanglement *Phys. Rev. Appl.* **15** 034003
[35] Sit A *et al* 2017 High-dimensional intracity quantum cryptography with structured photons *Optica* **4** 1006
[36] Cozzolino D *et al* 2019 Orbital angular momentum states enabling fiber-based high-dimensional quantum communication *Phys. Rev. Appl.* **11** 064058
[37] Wang F X, Chen W, Yin Z Q, Wang S, Guo G C and Han Z F 2019 Characterizing high-quality high-dimensional quantum key distribution by state mapping between different degrees of freedom *Phys. Rev. Appl.* **11** 024070
[38] Otte E, Nape I, Rosales-Guzmán C, Denz C, Forbes A and Ndagano B 2020 High-dimensional cryptography with spatial modes of light: tutorial *J. Opt. Soc. Am.* B **37** A309
[39] Wang Q K, Wang F X, Liu J, Chen W, Han Z F, Forbes A and Wang J 2021 High-dimensional quantum cryptography with hybrid orbital-angular-momentum states through 25 km of ring-core fiber: a proof-of-concept demonstration *Phys. Rev. Appl.* **15** 064034

[40] Brendel J, Gisin N, Tittel W and Zbinden H 1999 Pulsed energy-time entangled twin-photon source for quantum communication *Phys. Rev. Lett.* **82** 2594
[41] Pasquinucci H B and Tittel W 2000 Quantum cryptography using larger alphabets *Phys. Rev.* A **61** 062308
[42] Lee C *et al* 2014 Entanglement-based quantum communication secured by nonlocal dispersion cancellation *Phys. Rev.* A **90** 062331
[43] Lukens J M, Islam N T, Lim C C W and Gauthier D J 2018 Reconfigurable generation and measurement of mutually unbiased bases for time-bin qudits *Appl. Phys. Lett.* **112** 111102
[44] Bouchard F, England D, Bustard P J, Heshami K and Sussman B 2022 Quantum communication with ultrafast time-bin qubits *PRX Quantum* **3** 010332
[45] Vagniluca I, Lio B D, Rusca D, Cozzolino D, Ding Y, Zbinden H, Zavatta A, Oxenløwe L K and Bacco D 2020 Efficient time-bin encoding for practical high-dimensional quantum key distribution *Phys. Rev. Appl.* **14** 014051
[46] Ikuta T, Akibue S, Yonezu Y, Honjo T, Takesue H and Inoue K 2022 Scalable implementation of $(d+1)$ mutually unbiased bases for d-dimensional quantum key distribution *Phys. Rev. Res.* **4** L042007
[47] 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
[48] Liu X *et al* 2020 An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution *APL Photon.* **5** 076104
[49] Liu X *et al* 2022 40-user fully connected entanglement-based quantum key distribution network without trusted node *PhotoniX* **3** 2
[50] Zhong T, Wong F N C, Restelli A and Bienfang J C 2012 Efficient single-spatial-mode periodically-poled $KTiOPO_4$ waveguide source for high-dimensional entanglement-based quantum key distribution *Opt. Express* **20** 26868
[51] Korzh B *et al* 2020 Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector *Nat. Photon.* **14** 250
[52] Marsili F *et al* 2013 Detecting single infrared photons with 93% system efficiency *Nat. Photon.* **7** 210
[53] Wengerowsky S, Koduru S, Steinlechner F, Hubel H and Ursin R 2018 An entanglement-based wavelength-multiplexed quantum communication network *Nature* **564** 225
[54] Joshi S K *et al* 2020 A trusted node-free eight-user metropolitan quantum communication network *Sci. Adv.* **6** eaba0959
[55] Appas F, Baboux F, Amanti M I, Lemaître A, Boitier F, Diamanti E and Ducci S 2021 Flexible entanglement-distribution network with an AlGaAs chip for secure communications *npj Quantum Inf.* **7** 118
[56] Kim J-H, Chae J-W, Jeong Y-C and Kim Y-H 2022 Quantum communication with time-bin entanglement over a wavelength-multiplexed fiber network *APL Photonics* **7** 016106
[57] Huang Z *et al* 2022 Experimental implementation of secure anonymous protocols on an eight-user quantum key distribution network *npj Quantum Inf.* **8** 25
[58] Solomons N R *et al* 2022 Scalable authentication and optimal flooding in a quantum network *PRX Quantum* **3** 020311
[59] Zhang Z, Mower J, Englund D, Wong F N C and Shapiro J H 2014 Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry *Phys. Rev. Lett.* **112** 120506
[60] Wasak T, Szańkowski P, Wasilewski W and Banaszek K 2010 Entanglement-based signature of nonlocal dispersion cancellation *Phys. Rev.* A **82** 052120
[61] MacLean J P W, Donohue J M and Resch K J 2018 Direct characterization of ultrafast energy-time entangled photon pairs *Phys. Rev. Lett.* **120** 053601
[62] Li B, Hou F, Quan R, Dong R, You L, Li H, Xiang X, Liu T and Zhang S 2019 Nonlocality test of energy-time entanglement via nonlocal dispersion cancellation with nonlocal detection *Phys. Rev.* A **100** 053803
[63] Mei Y, Zhou Y, Zhang S, Li J, Liao K, Yan H, Zhu S L and Du S 2020 Einstein–Podolsky–Rosen energy-time entanglement of narrow-band biphotons *Phys. Rev. Lett.* **124** 010509
[64] Zhou H, Chandar V and Wornell G 2013 Low-density random matrices for secret key extraction *IEEE Int. Symp. Information Theory-Proc* p 2607
[65] Zhou H, Wang L and Wornell G 2013 Layered schemes for large-alphabet secret key distribution *Information Theory and Applications Workshop ITA-Conf. Proc.* p 1
[66] Zhang G *et al* 2019 An integrated silicon photonic chip platform for continuous-variable quantum key distribution *Nat. Photon.* **13** 839
[67] Liu H *et al* 2019 Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels *Phys. Rev. Lett.* **122** 160501
[68] Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S and Guo H 2020 Long-distance continuous-variable quantum key distribution over 202.81 km of fiber *Phys. Rev. Lett.* **125** 010502
[69] Wei K *et al* 2020 High-speed measurement-device-independent quantum key distribution with integrated silicon photonics *Phys. Rev.* X **10** 031030
[70] Franson J D 1992 Nonlocal cancellation of dispersion *Phys. Rev.* A **45** 3126
[71] Clausen C, Usmani I, Bussieres F, Sangouard N, Afzelius M, De Riedmatten H and Gisin N 2011 Quantum storage of photonic entanglement in a crystal *Nature* **469** 508
[72] Wiseman H M, Jones S J and Doherty A C 2007 Steering, entanglement, nonlocality, and the Einstein–Podolsky–Rosen paradox *Phys. Rev. Lett.* **98** 140402
[73] Branciard C, Cavalcanti E G, Walborn S P, Scarani V and Wiseman H M 2012 One-sided device-independent quantum key distribution: security, feasibility, and the connection with steering *Phys. Rev.* A **85** 010301
[74] Wang Y, Bao W S, Li H W, Zhou C and Li Y 2013 Finite-key analysis for one-sided device-independent quantum key distribution *Phys. Rev.* A **88** 052322
[75] Bao H Z, Bao W S, Wang Y, Chen R K, Ma H X, Zhou C and Li H W 2017 Time–energy high-dimensional one-side device-independent quantum key distribution *Chin. Phys.* B **26** 050302
[76] Niu M Y, Xu F, Shapiro J H and Furrer F 2016 Finite-key analysis for time-energy high-dimensional quantum key distribution *Phys. Rev.* A **94** 052323
[77] Gan Y H, Wang Y, Bao W S, Zhou C, Jiang M S and Li H W 2018 Finite-key analysis for high-dimensional quantum key distribution with intensity fluctuations *J. Phys. B: At. Mol. Opt. Phys.* **51** 245502