ARTICLE Open Access

# Time-bin encoded quantum key distribution over 120 km with a telecom quantum dot source

Jipeng Wang[1], Joscha Hanel[1], Zenghui Jiang[1], Raphael Joos[2], Michael Jetter[2], Eddy Patrick Rugeramigabo[1], Simone Luca Portalupi[2], Peter Michler[2], Xiao-Yu Cao[3], Hua-Lei Yin[3,4], Lei Shan[5], Jingzhong Yang[1]✉, Michael Zopf[1,6] and Fei Ding[1,6]

**Abstract**

Quantum key distribution (QKD) with deterministic single photon sources has been demonstrated over intercity fiber and free-space channels. The previous implementations relied mainly on polarization encoding schemes, which are susceptible to birefringence, polarization-mode dispersion and polarization-dependent loss in practical fiber networks. In contrast, time-bin encoding offers inherent robustness and has been widely adopted in mature QKD systems using weak coherent laser pulses. However, its feasibility in conjunction with a deterministic single-photon source has not yet been experimentally demonstrated. In this work, we construct a time-bin encoded QKD system employing a high-brightness quantum dot (QD) single-photon source operating at telecom wavelength. Our proof-of-concept experiment successfully demonstrates the possibility of secure key distribution over fiber link of 120 km, while maintaining extraordinary long-term stability over 6 h of continuous operation, that is highest secure key rate among the time-bin QKDs based on single-photon sources. This work provides the first experimental validation of integrating a QD single-photon source with time-bin encoding in a telecom-band QKD system. This development signifies a substantial advancement in the establishment of a robust and scalable QKD network based on solid-state single-photon technology.

## Introduction

Quantum key distribution (QKD) offers a practical approach to realize physical-level confidentiality for the sharing of secret keys in a communication network[1–4]. Since the first BB84 protocol[5], significant progress has been made to bridge the gap between the theoretically unconditional security and practical implementation[6–8]. Among the proposed methods, the decoy-state protocol plays a crucial role in practical QKD systems[9–12]. Using weak coherent pulses (WCPs) in the decoy-state protocol enables a secure and cost-effective implementation. As a result, it has been widely adopted in national and commercial QKD networks[13–18]. Despite its success, the performance of decoy-state QKD with WCPs as approximations to ideal single-photons remains fundamentally constrained. The probability of true single-photon emission is upper-bounded by the Poisson statistics of WCPs[19–21], and additional modulation processes required to implement the decoy protocol may introduce complexity and side-channel vulnerabilities[22–25]. These limitations have motivated the pursuit of genuine single-photon sources (SPSs) for QKD.

Semiconductor quantum dots (QDs) embedded in nanophotonic structures offer on-demand, high-purity single-photon emission with high efficiency[26–28]. Recent works have demonstrated the feasibility of using QDs as SPSs in QKD systems, both over fiber[29–36] and free-space[37–39] channels. In particular, telecom-band QDs with Purcell enhancement[40] can provide high-brightness photons suitable for intercity fiber communication[41], making them promising candidates for integration into practical QKD systems. Most existing QD-based QKD demonstrations rely on polarization encoding[35,42,43], but such schemes are highly sensitive to polarization-mode

Correspondence: Jingzhong Yang (jingzhong.yang@fkp.uni-hannover.de)
[1]Institut für Festkörperphysik, Leibniz Universität Hannover, Appelstraße 2, 30167 Hannover, Germany
[2]Institut für Halbleiteroptik und Funktionelle Grenzflächen, Center for Integrated Quantum Science and Technology (IQST) and SCoPE, University of Stuttgart, Allmandring 3, 70569 Stuttgart, Germany
Full list of author information is available at the end of the article

© The Author(s) 2026
**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

dispersion (PMD) and birefringence in optical fibers[44–48]. This makes QKD systems vulnerable to changes in the practical quantum channel caused by environmental factors, such as turbulence, temperature and vibrations. This necessitates active compensation. In contrast, time-bin encoding, where qubits are encoded in the temporal position of single photons, offers intrinsic stability against such channel fluctuations even without any complex compensation protocols[49,50]. While time-bin encoding has been widely demonstrated using coherent-state or entangled-photon sources[51–56], its implementation with deterministic QD-based SPSs remains largely unexplored.

Pioneering studies have utilized QDs for phase-encoding QKD[29,31], where asymmetric Mach–Zehnder interferometers (AMZIs) are used to create time-bin-like phase states. However, in those cases, the time-bin is not directly employed for key generation, and long-term stability tests are lacking. Entanglement-based QKD systems have also been explored[57–63], but they require complex state preparation techniques and are less practical for compact deployments. To date, there has been no demonstration of a QKD system employing genuine time-bin-encoding with deterministic single photons from QDs, especially at long distances.

In this work, we present a self-stabilized, time-bin encoded QKD system based on a deterministic telecom-wavelength QD source. This source, involving an epitaxial InGaAs/GaAs QD embedded in a circular Bragg grating photonic structure has been previously reported with a high-brightness single-photon emissions[40]. To minimize system complexity and loss, we adopt a single phase modulator for preparing three quantum states: two time-bin basis states ($|Z_0\rangle$, $|Z_1\rangle$) and one phase-basis state ($|X_0\rangle$), assuming $|X_0\rangle$ shares the same error rate as $|X_1\rangle$ in the conventional BB84 protocol[52,64].The system is operated continuously for 6 h, highlighting the intrinsic robustness of the time-bin scheme enabled by the system including the Sagnac interferometer (SNI), active feedback control, etc. Finally, we achieved a secure key bits (SKBs) per pulse of $2 \times 10^{-7}$ over a 120 km fiber spool. This result confirms the feasibility of integrating QD single-photon sources into stable and field-deployable time-bin QKD systems, marking an important step toward scalable, quantum-secure communication networks.

## Results

### Overview of the experimental scheme

The three time-bin states of the polarized single photons are generated using an AMZI configuration involving a SNI. In this configuration, the input beam splitter of the standard AMZI is replaced with a fiber-based optical circulator (Cir), as shown in the left panel of Fig. 1a, so that the single photons are first guided into the SNI passing through $BS_1$. In the SNI structure, a $LiNbO_3$ phase modulator (PM, Rofea Optoelectronics, ROF-PM-UV) is intentionally placed in an unbalanced position. Single photons arriving at the PM along the clockwise (↻) path at the time $t_0 + \Delta$ experience an additional time delay of $\Delta$ (half of the single-photon repetition period), compared to those arriving along the counterclockwise (↺) path at the time $t_0$.

In this experiment, we intentionally setup $\Delta$ to 6.5 ns as shown in Fig. 1b, considering the excitation repetition rate for the single photons is $f_{rep} = 75.947$ MHz. A correlation between the phase and the time of the photons arriving at the PM can be created by applying a sequence of two voltages to the PM within each single-photon period $\left(1/f_{rep} \approx 13.17 \text{ ns}\right)$. Within a single-photon period, a random voltage in the set $\{0, V_\pi, V_{\pi/2}\}$ is first applied to the PM at $t_0$ for the first time slot, until no voltage is applied from $t_0 + \Delta$ onwards for the second time slot. A random phase difference, $\theta_1$, can therefore be actively determined for each single photon between the ↻ and ↺ paths. Subsequent single-photon interference at $BS_1$ leads to a superposition of the path state[65],

$$|\Phi\rangle_{SNI} = \left(-\sin\frac{\theta_1}{2}\cdot|S\rangle_{AMZI_1} + \cos\frac{\theta_1}{2}\cdot|L\rangle_{AMZI_1}\right) \tag{1}$$

The states $|S\rangle$ and $|L\rangle$ represent the quantum states of the short and long paths that the photons chose between the $BS_1$ and $BS_2$. The single photons with the state $|L\rangle$ enter the green path of the $AMZI_1$ and go through the Cir (through port 2 → 3) in Fig. 1a, giving a time delay of $\Delta_1$ in comparison with the state $|S\rangle$. This results in the equal time separation between the early $|e\rangle$ and late $|l\rangle$ photons after the $AMZI_1$. Assuming the transmitted and reflected single photons from the output port of $BS_2$ corresponds to the $|L\rangle$ and $|S\rangle$ single-photon states, the time-bin state of a photon from $AMZI_1$ is,

$$|\Psi\rangle_c = \frac{1}{\sqrt{2}}e^{i\frac{\theta_1}{2}}\left(\sin\frac{\theta_1}{2}\cdot|e\rangle + i\cos\frac{\theta_1}{2}\cdot|l\rangle\right) \tag{2}$$

with $1/\sqrt{2}$ indicating the amplitude of state from one port, and $i$ the phase shift of $\pi/2$ for the $|S\rangle$-state photons upon reflection relative to transmission at $BS_2$. In this work, a single output port is used for key transmission. Figure 1c shows the sketch of correlation histograms between the single-photon triggering signals and the three time-bin states $|Z_0\rangle = |l\rangle$, $|Z_1\rangle = |e\rangle$ and $|X_0\rangle = 1/\sqrt{2}(|e\rangle + i|l\rangle)$, corresponding to the voltage levels of $\{0, V_\pi, V_{\pi/2}\}$ shown in Fig. 1b, respectively. Within a single-photon period, three time windows $\{W_1, W_2, W_3\}$ are defined each with a range of $\Delta_1 = 4.3$ ns. Coincidences that occur solely in $W_1$ and $W_2$ indicate the presence of the $|e\rangle$ and $|l\rangle$ photons, respectively. The probabilities of

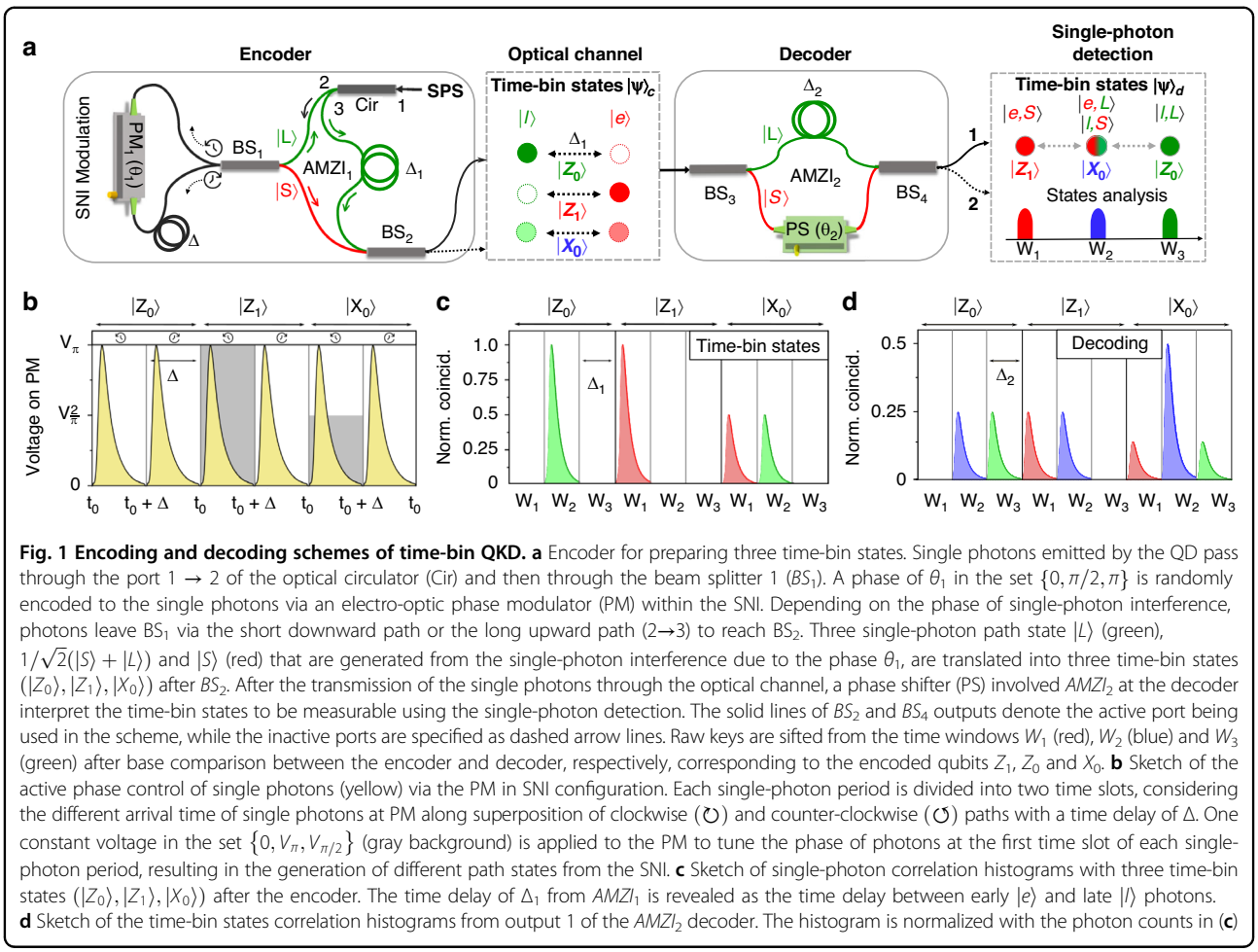


**Fig. 1 Encoding and decoding schemes of time-bin QKD. a** Encoder for preparing three time-bin states. Single photons emitted by the QD pass through the port 1 → 2 of the optical circulator (Cir) and then through the beam splitter 1 ($BS_1$). A phase of $\theta_1$ in the set $\{0, \pi/2, \pi\}$ is randomly encoded to the single photons via an electro-optic phase modulator (PM) within the SNI. Depending on the phase of single-photon interference, photons leave $BS_1$ via the short downward path or the long upward path (2→3) to reach $BS_2$. Three single-photon path state $|L\rangle$ (green), $1/\sqrt{2}(|S\rangle + |L\rangle)$ and $|S\rangle$ (red) that are generated from the single-photon interference due to the phase $\theta_1$, are translated into three time-bin states $(|Z_0\rangle, |Z_1\rangle, |X_0\rangle)$ after $BS_2$. After the transmission of the single photons through the optical channel, a phase shifter (PS) involved $AMZI_2$ at the decoder interpret the time-bin states to be measurable using the single-photon detection. The solid lines of $BS_2$ and $BS_4$ outputs denote the active port being used in the scheme, while the inactive ports are specified as dashed arrow lines. Raw keys are sifted from the time windows $W_1$ (red), $W_2$ (blue) and $W_3$ (green) after base comparison between the encoder and decoder, respectively, corresponding to the encoded qubits $Z_1$, $Z_0$ and $X_0$. **b** Sketch of the active phase control of single photons (yellow) via the PM in SNI configuration. Each single-photon period is divided into two time slots, considering the different arrival time of single photons at PM along superposition of clockwise (↻) and counter-clockwise (↺) paths with a time delay of Δ. One constant voltage in the set $\{0, V_\pi, V_{\pi/2}\}$ (gray background) is applied to the PM to tune the phase of photons at the first time slot of each single-photon period, resulting in the generation of different path states from the SNI. **c** Sketch of single-photon correlation histograms with three time-bin states $(|Z_0\rangle, |Z_1\rangle, |X_0\rangle)$ after the encoder. The time delay of $\Delta_1$ from $AMZI_1$ is revealed as the time delay between early $|e\rangle$ and late $|l\rangle$ photons. **d** Sketch of the time-bin states correlation histograms from output 1 of the $AMZI_2$ decoder. The histogram is normalized with the photon counts in (**c**)

50% for each $W_1$ and $W_2$ suggests the successfully encoded of $|X_0\rangle$ state.

To decode the time-bin states, an AMZI with an internal time delay of $\Delta_2 = \Delta_1$ and a phase shifter (PS, Luna Innovation, FPS-001) is employed. For simplicity, we ignore the global phase induced by the quantum channel in between the encoder and decoder, and exemplifying the phase $\theta_2 = \pi/2$ from the PS. Then the single-photon state from output 1 of the $AMZI_2$ can be expressed as follows,

$$\begin{aligned}|\Psi\rangle_d &= R_{AMZI_2} \cdot |\Psi\rangle_c \\ &= \tfrac{1}{2\sqrt{2}} e^{i\frac{\theta_1}{2}} \big(-i \sin\tfrac{\theta_1}{2} |e\rangle|S\rangle_{AMZI_2} + \sin\tfrac{\theta_1}{2} |e\rangle|L\rangle_{AMZI_2} \\ &\quad + \cos\tfrac{\theta_1}{2} |l\rangle|S\rangle_{AMZI_2} + i\cos\tfrac{\theta_1}{2} |l\rangle|L\rangle_{AMZI_2}\big)\end{aligned} \tag{3}$$

where the $R_{AMZI_2}$ is operation gate of $AMZI_2$ for the single-photon state (see details in the methods). Here we assume that the phase shift of $\pi/2$ is applied to single-photon states, when the $AMZI_2$ short path and active output port corresponds to the reflected photons from the $BS_3$ and $BS_4$, respectively. Figure 1d represents the detection of a single photon at a set of given time windows $\{W_1, W_2, W_3\}$ of output 1 corresponding to three cases,

- $W_1$: The early photon goes through the short path $|e, S\rangle$;
- $W_2$: The early photon goes through the long path $|e, L\rangle$ or the late photon goes through the short path $|l, S\rangle$;
- $W_3$: The late photon goes through the long path $|l, L\rangle$;

In the Eq. (3), the first term indicates the global phase induced by PM. Meanwhile, the square of the coefficient for each term within the parentheses denotes the probability of each detected state. The sketch of correlation histograms in Fig. 1d illustrates the detection probability distribution of the above cases at output 1 of $BS_4$ when the phase $\theta_1$, encoded by the PM, is set to $\{0, V_\pi, V_{\pi/2}\}$. The $|Z_0\rangle$ state with late photonic qubits leads to photon detection at either $W_2$ or $W_3$, but only the photon in $W_3$ denote the $Z_0$ decoding basis. Likewise, early photonic qubits in $|Z_1\rangle$ states can be measured at $W_1$ or $W_2$ while the $W_1$ is the $|Z_1\rangle$ basis. For the encoded $|X_0\rangle$ qubits, when $\theta_1 = V_{\pi/2}$, the decoding basis is $W_2$ measured from output 1. This basis can be switched with that

for $|X_1\rangle = 1/\sqrt{2}(|e\rangle - i|l\rangle)$, by controlling the phase difference of paths $\theta_2$ of $AMZI_2$.

As with conventional QKDs using BB84 protocol, raw keys are sifted from the measured events according to shared basis information between users. In the time-bin-based QKD scheme, the decoder will gains the sifted keys by checking its measured results (the position of the detected event in time) based on the shared basis information from the encoder. For example, a '0' key will be sifted when the decoder learns the Z basis commonly used by the encoder and the photon is measured in $W_3$ (Fig. 1d). In analogy to the $|Z_0\rangle$ qubit, the raw keys '1' and '0' will be sifted when the common bases $|Z_1\rangle$ and $|X_0\rangle$ are revealed and the photons are detected within $W_1$ and $W_2$, respectively. In the following text, the bases of the $\{Z_0, Z_1, X_0\}$ are colored green, red and blue, to indicate the correlation with the time windows set that result in the sifted keys. For Fig. 1d, note that for $|Z_0\rangle$ and $|Z_1\rangle$, the same histograms will be measured at output 2, from which the other half of keys at the Z basis can be extracted from the time windows $W_3$ and $W_1$, respectively. However, due to the constructive interference $(\theta_2 = \pi/2)$, the $|X_0\rangle$ state can be analyzed directly using the detected event located within $W_2$ of output 1 (destructive interference pattern with the $W_2$ from output 2).

## Experimental setup

Figure 2 shows a sketch of the experimental setup for time-bin QKD using telecom single photons from an InGaAs/GaAs QD involved in a circular Bragg grating photonic device reported in the previous work[40]. In this QKD system, Alice, acting as the sender, encrypts the time-bin states using single photons that are transmitted through the fiber spool to the receiver, Bob. Bob then performs decryption for the single-photon time-bin states. At Alice side, the sample is loaded in a cryostat (Attodry 1100) at a temperature of 3.57 K. A pulsed laser with a repetition rate of $f_{rep} = 75.947$ MHz synchronized with an arbitrary wave-function generator (AWG, Active Technologies, AWG5064) is used to excite the p-shell of the positive trion state of the QD. The single photon emissions with a central wavelength of 1560.6 nm (Fig. 2b) is collected by an objective with the numerical aperture of 0.7. The total decay time is extracted by fitting the time-resolved QD emission in a three-level system and is found to be $\tau = 1018$ ps, while the count drops to 1% up to ~4 ns. Taking into account the three time windows necessary for discriminating the time-bin states, we therefore apply the repetition rate $f_{rep} = 75.947$ MHz (corresponding to a window size of 4.3 ns for each). In a time-bin QKD system with a semiconductor single-photon source, employing the photonic resonant structure can reduce the lifetime and compromise the inherent limit of the repetition rates.

The encrypted raw time-bin key rate after a sequence of optical components and encoder is measured from the output of Alice ~162 kHz, involving the detection efficiency of $\eta_D = 74\%$. This corresponds to average photon number per pulse of $\langle n\rangle \approx 2.89\times 10^{-3}$ coupled to the quantum channel. To evaluate the influence of the single-photon purity on QKD, we performed an autocorrelation measurement using a Hanbury Brown and Twiss setup and extract a blinking-corrected $g^2(0) = 0.85\%$ from the histogram (Fig. 2c) without any temporal filter applied to the coincidence count integration $\left(\tau = 1/f_{rep}\right)$. Therefore, it is estimated that the upper bound of the multi-photon probability with a single-photon source is $p_m \leq \langle n\rangle^2 \cdot g^2(0)/2$. At short quantum channel length, the secure key rate (SKR) of QKD drops linearly with the quantum channel loss (logrithem scale), while the multi-photon probability limits the maximum tolerable loss significantly in the high-loss (long-distance) regime. In practical QKD, properly attenuating the single-photon rate can extend the MTL by compromising the raw key rate $\langle n\rangle$ and the multiphoton portion $p_m$ (detailed calculation in the Methods section).

Before the time-bin encoder, the single photons are first polarized by an in-line fiber polarizer (ILFP) to align their polarization with the axis of the fiber optics, i.e., PM. In the SNI configuration, the phase control with the PM is implemented by an AWG that delivers squared modulation signals in pair with a clock rate locked to the excitation laser. Three voltage gaps $\{0, 1.6\text{ V}, 3.2\text{ V}\}$ corresponding to $\left\{0, V_{\frac{\pi}{2}}, V_{\pi}\right\}$ within each pair are applied to PM over the first time slot to generate the three time-bin states. In the actual experiment, a 16-bit repeating sequence with these random voltages are applied to the PM for the states of $\{X_0, Z_1, Z_0, X_0, Z_0, Z_1, X_0, Z_1, Z_0, X_0, Z_0, Z_1, X_0, Z_0, Z_1, Z_1\}$. This leads to a basis choice ratio of 5/16 and 11/16 for X and Z basis, respectively, and number of bits $\{5, 6, 5\}$ for $\{Z_0, Z_1, X_0\}$. It has been demonstrated that the asymmetric basis ratio in the BB84 protocol can improve the SKR[30]. The encrypted single photons are then sent to the receiver setup through the variable-length fiber spools. Similar to the transmitter at Alice, the receiver at Bob uses an ILFP to ensure the alignment of the photon's polarization with the axis of the fiber optics in the decoder. A fiber polarization controller is placed in front to compensate the polarization drift from the fiber channel. Additionally, a programmable power source (PPS, Siglent Technologies, SPD3303) controls the PS in the decoder to actively stabilize the phase between the $AMZI_2$'s arms by minimizing the quantum bit error rate (QBER) of the system. Eventually, the arrival times of the single photons are registered by a superconducting nanowire single-photon detector (SNSPD), followed by a time-to-digital converter synchronized with the AWG. The measured system dark

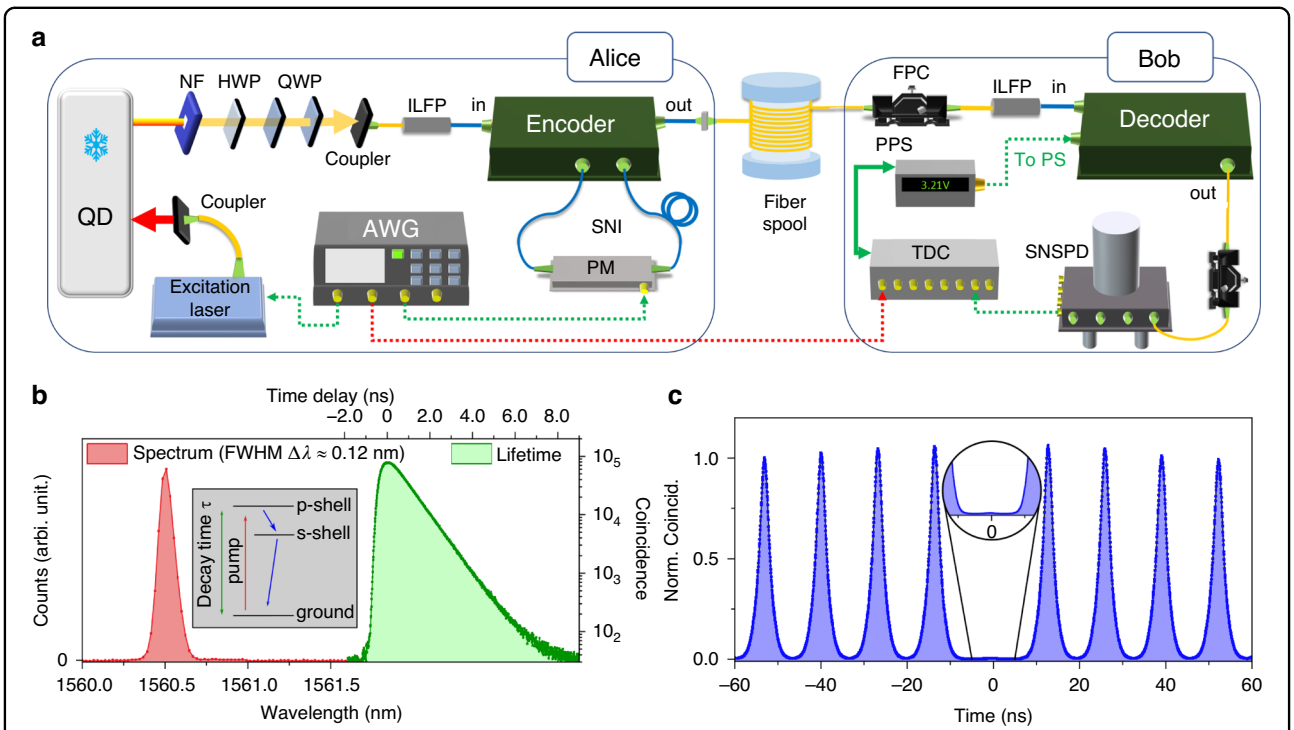


**Fig. 2 Experimental setups and source characteristics. a** Fiber-coupled excitation pulse laser, triggered by the arbitrary wave-function generator (AWG), transmits through a BS (R:T = 98.5:1.5) and is used to excite the telecom QD loaded in the cryostat. The emitted single photons collected by the objective are obtained by filtering out the laser using a notch filter. Then, single photons are coupled to the in-line fiber polarizer (ILFP), through a series of free-space half- and quarter- waveplates (HWP and QWP) for the polarization control. The PM inside the encoder is synchronized with the excitation laser via the AWG, and randomly generate three single-photon time-bin states. The time-bin qubits are decrypted at the receiver setup from Bob, which consists of a decoder, superconducting nanowire single-photon detector (SNSPD), and a time-to-digital converter (TDC). The excitation laser and PM at Alice are synchronized with the TDC at Bob via the AWG, which distributes electronic triggering signals through electrical cables. FPC, fiber polarization controller; PPS, programmable power source. **b** The photoluminescence spectrum and time-resolved lifetime histogram (logarithm scale) of the single-photon emissions from the QD. The inset shows the decay process of the p-shell excitation within the QD band structure. **c** Normalized second-order autocorrelation histogram for the single photons from the trion state emissions with the inset showing the zoomed-in view of the central peak

count rate is $d = \sim 100$ cts/s, resulting in the dark count probability $p_{dc} = d \cdot \tau$. This reduces the SKR and MTL, and is calculated in the Methods section.

## Evaluation of the QKD performance

As the figure-of-merit for QKDs, the SKR ($R_{secure}$) from the three time-bin states, is emulated in the finite-key regime with the multiplicative Chernoff bound[30],

$$R_{secure} = \left\lfloor \underline{N}^{Z}_{R,nmp}\left(1 - h\left(\overline{\phi}_Z\right)\right) - \lambda_{EC} - 2\log_2\frac{1}{2\varepsilon_{PA}} - \log_2\frac{2}{\varepsilon_{cor}} \right\rfloor / N_{sum} \tag{4}$$

In this process, the raw keys on the Z basis are post-processed to create secure keys after error correction and privacy amplification, while the raw keys from the X basis are shared publicly to analyze the system QBER. $\underline{N}^{Z}_{nmp}$ denotes the lower bound of the received raw key rate on the Z basis, excluding the noisy bit rates caused by multi-photon emission that can be estimated based on second-order correlation $g^{(2)}(0)$. As it is impossible to obtain the QBER on the Z basis in the actual QKD, the upper bound of the phase error that is translated from the QBER on the X basis is employed. This is involved in, $h(\cdot)$ the binary Shannon entropy, accounting for eavesdropper's attack on the quantum raw keys. $\lambda_{EC}$ is the lower bound of information leakage during the error correction. $\epsilon_{PA}$ and $\epsilon_{cor}$ are the security parameter over the error verification, and failure probability of privacy amplification, respectively. In the finite-key regime, which closely resembles a practical scenario, the quantum keys are sent in blocks, with $N_{sum}$ specifying the size of the key block sent from the encoder. Details about the system parameters and the calculation model are provided in the Methods section.

The QBERs are extracted from the histograms as presented in Fig. 3a, in which the number of raw keys bits and error bits are counted. The decoder first measures the 16 histograms corresponding to the time-bin states repeatedly sent by the encoder. The QBER for each basis is calculated using the ratio of the integrated photon

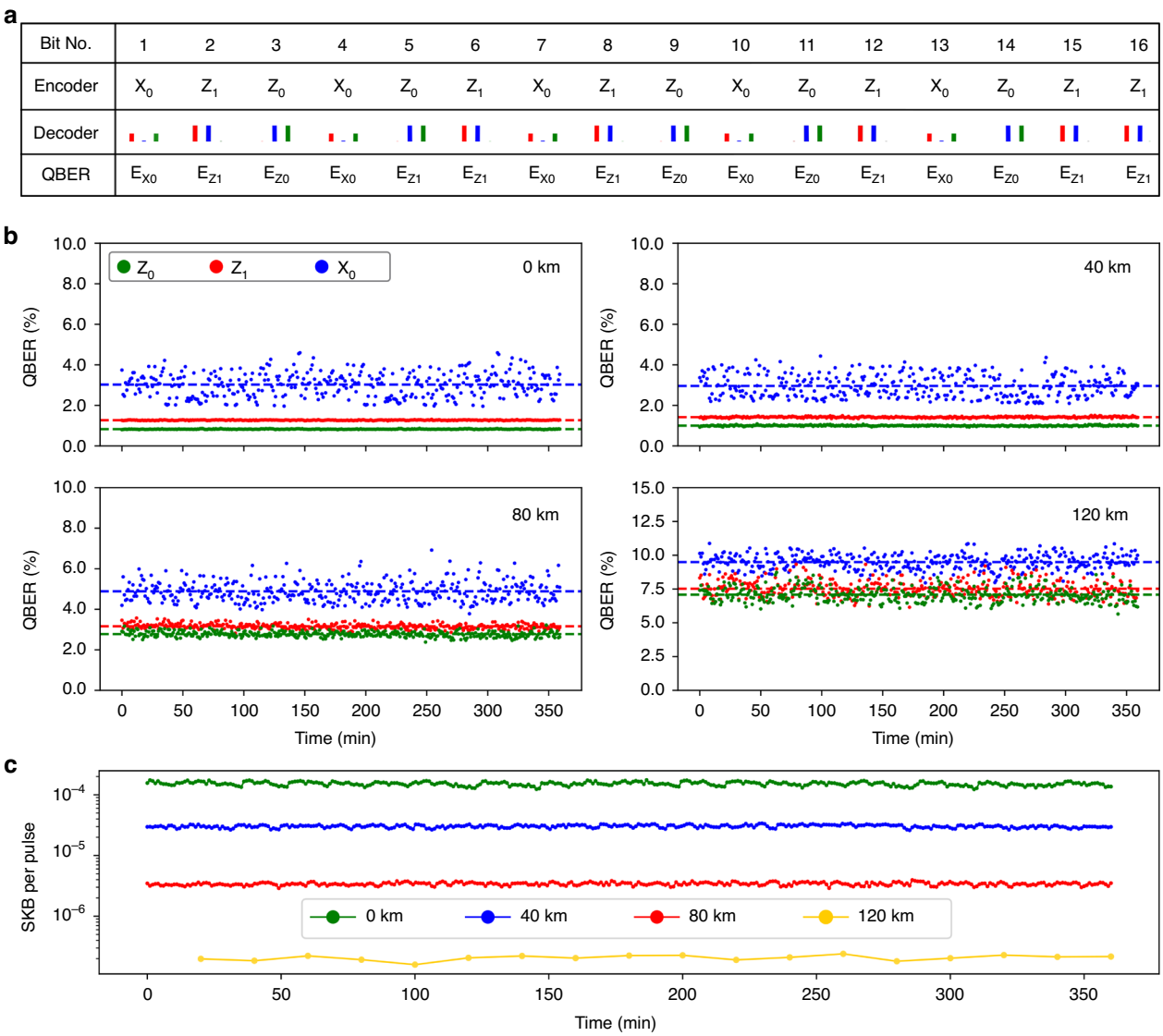


**Fig. 3 Time-dependent QKD performance at various transmission distances. a** Schematic of QBER extraction with the bases comparison of statistical data. The time windows $\{W1, W2, W3\}$ are indicated by the red, blue, and green columns, respectively. The height of each columns denotes the probability of detecting photons within a given time window when specific states are encoded. **b** Time-dependent QBER for different fiber spool lengths of 0 km, 40 km, 80 km, and 120 km. Each data point represents 1 min of measurement time. The dashed lines indicate the average QBERs on the bases over the 6 h. **c** Secure key bits (SKBs) per pulse as a function of measurement time for the different fiber spool lengths ranging from 0 km to 120 km. For the spool lengths of 0 km, 40 km, and 80 km, an acquisition time of 1 min $(N_{sum} = 4.56\times 10^9)$ is used in the finite key analysis. For the 120 km transmission distance, an acquisition time of 20 min $(N_{sum} = 9.12\times 10^{10})$ is used

counts at the two perpendicular bases. For instance, the QBER for encoded $E_{Z_1}$ is calculated as $N_{Z_0}/N_{Z_0}+N_{Z_1}$, where $\{N_{Z_0}, N_{Z_1}\}$ are the integrated photon counts within each 4.3 ns time windows $\{W3, W1\}$ of the histograms (Bit no. 2, 5, 8, 12, 15, 16). Same calculation algorithm applies to $E_{Z_0}$, which is $N_{Z_1}/N_{Z_0}+N_{Z_1}$ with $\{N_{Z_0}, N_{Z_1}\}$ counted within the time window $\{W3, W1\}$ from the corresponding histograms (Bit no. 3, 5, 9, 11, 14). However, determining $E_{X_0}$ is relatively challenging due to the absence of one more detector channel of $AMZI_2$ for the $N_{X_0}$ and $N_{X_1}$ at the same time. We adjust PS phase to be $-\pi/2$ while sending the $|X_0\rangle$, such that theoretically there is no correlation peak within the $W_2$ window from the $|X_0\rangle$ state due to the destructive interference. Then, we regard the detected error qubits as $N_{X_1}$ similar to four-state BB84 protocol, and assume the QBER of $|X_0\rangle$ state to be $E_{X_0} = N_1/N_{Z_0}+N_{Z_1}$, as the splitting ratio between X- and Z- basis at the decoder is 1/2 resulting in $N_{X_0}+N_{X_1} = N_{Z_0}+N_{Z_1}$ (Bit no. 1, 4, 7, 10, 13). For the measurement of $E_{X_0}$, the phase difference between the paths

**Table 1 SKB per pulse and QBERs over a range of fiber spool lengths**

| Distance (km) | $R_{secure}/f_{rep}$ | $R_{raw}/f_{rep}$ | $E_Z$ (%) | $\sigma_{Z_0}$ (%) | $\sigma_{Z_1}$ (%) | $E_{X_0}$ (%) | $\sigma_{X_0}$ (%) |
|---|---|---|---|---|---|---|---|
| 0 | $1.59 \times 10^{-4}$ | $2.23 \times 10^{-4}$ | 0.98% | 0.01% | 0.01% | 3.14% | 0.54% |
| 40 | $3.04 \times 10^{-5}$ | $4.33 \times 10^{-5}$ | 1.19% | 0.08% | 0.03% | 3.12% | 0.56% |
| 80 | $3.54 \times 10^{-6}$ | $6.87 \times 10^{-6}$ | 3.02% | 0.13% | 0.14% | 4.90% | 0.52% |
| 120 | $1.99 \times 10^{-7}$ | $1.34 \times 10^{-6}$ | 6.85% | 0.60% | 0.56% | 9.60% | 0.58% |

The QBER on Z-basis, $E_Z$, is the average value of $E_{Z_0}$ and $E_{Z_1}$. Acquisition times of 1 min and 20 min with the key blocks in the finite key regime are used for 0–80 km and 120 km, respectively

of $AMZI_2$ is dynamically stabilized by suppressing the photon counts $N_{X_1}$ within the time window $W_2$ to be the minimal.

To investigate the stability of the time-bin QKD system in terms of the QBER, SKBs per pulse $\left(R_{secure}/f_{rep}\right)$ at different quantum channel lengths, we implement the time-dependent measurement using the length-variable fiber spools (average loss of $\alpha = 0.1956$ dB km) connected between the transmitter and receiver setups. As shown in Fig. 3b, the mean and deviation of the QBERs at X basis are both relatively higher than Z basis. This is due to the limited visibility of interference at $AMZI_2$ (i.e., imperfect power splitting ratio of the BSs), as the accurate detection of the $|X_0\rangle$ requires high-quality single-photon interference at the $BS_4$. This is revealed by the higher misalignment probability of the optical setup on the X basis than the Z basis ($p_{misX} > p_{misZ}$), which contributes bit errors at a transmission distance of 0 km. We attribute the slightly higher QBERs of $|Z_1\rangle$ state compared to the $|Z_0\rangle$ state to the imperfect phase encoding of PM due to inaccurate targeting voltage (i.e., flatness uncertainty of the peak voltage). As represented in Fig. 1b, an ideal $|Z_0\rangle$ state can be generated without applying any voltage to the PM over a single-photon period. However, voltages $V_\pi$ and $V_{\frac{\pi}{2}}$ with time duration of $1/2f_{rep}$ is required to obtain $|Z_1\rangle$ and $|X_0\rangle$ state, respectively. The uncertainties in these voltages translates into the additional QBERs for the $|Z_1\rangle$ and $|X_0\rangle$ states. On the other hand, the QBER increases with the length of the optical fiber, since the system dark counts become more dominant with a decreased signal-to-noise ratio. Nevertheless, average QBERs below 11% are maintained at a transmission distance of 120 km, which is promising for a secure intercity-scale communication. Fiber-induced light dispersion causes an elongation of the single-photon pulses for ~ 265 ps at a transmission distance of 120 km considering the linewidth of the emitted single photon is $\Delta\lambda \approx 0.13$ nm[40]. This gives a negligible influence on the time-bin qubits, with a time separation of 4.3 ns. Figure 3c illustrates stable SKB per pulse over 6 h for different fiber spools, which is the ratio of $R_{secure}$ and $f_{rep}$. The average $E_{X_0}$ within the integration time is dynamically employed in the calculation of $R_{secure}$, while considering fixed values of the mean photon number per pulse $\langle n\rangle = 2.89\times 10^{-3}$ entering the quantum channel and $g^{(2)}(0) = 0.85\%$. The integrated finite blocks at a distance of 120 km are given a longer time of 20 min to ensure sufficient key length for a positive key rate.

Table 1 presents the statistics of the Gaussian distribution according to the results from Fig. 3. The extraction ratio of the $R_{secure}$ from the raw key rate $R_{raw}$ becomes lower with the enhanced transmission distance because of the increased QBER. With the case of the repetition rate $f_{rep} = 75.947$ MHz, the reachable SKR at the distance of 120 km is approx. 15 bits $s^{-1}$, which is still possible for the text message encryption. The standard deviation of the QBERs $\left(\sigma_{\{Z_0,Z_1,X_0\}}\right)$ on both the Z- and X-bases remains below 0.6% to be constant thanks to the effective phase compensation program and stable laboratory environment. Figure 4a presents the QBERs and the SKB per pulse as a function of the transmission distance. Apart from the experimental data points as illustrated in the table, we performed a simulation to determine the maximum tolerable distance for our time-bin QKD system, where the QBERs of $E_X$ and $E_Z$ on Z- and X-bases ($\phi^Z$ and $\phi^X$) are simulated as,

$$E_X = \frac{M_R^X}{\underline{N}_{R,nmp}^X} \quad E_Z = \frac{M_R^Z}{\underline{N}_{R,nmp}^Z} \tag{5}$$

where $M_R^{X,Z}$ and $\underline{N}_{R,nmp}^{X,Z}$ denote the number of error bits and lower bound of non-multiphoton fraction of received photons at $\{X, Z\}$ bases, respectively (see Methods for details). A maximum tolerable distance of 127 km is underestimated in the case that the QBER at X-basis approaches 11%, since keys from Z-basis with a lower QBER value are typically employed for the information encryption in practical QKDs.

## Discussion

In our experiment, a secure key rate of $1.99 \times 10^{-7}$ bit per pulse was achieved over a 120 km fiber spool using a total pulse block size of $N_{\text{sum}} = 10^{11}$, corresponding to an integration time of ~1300 s. This result demonstrates the feasibility of employing a deterministic, telecom-band QD single-photon source in a time-bin encoded QKD system under

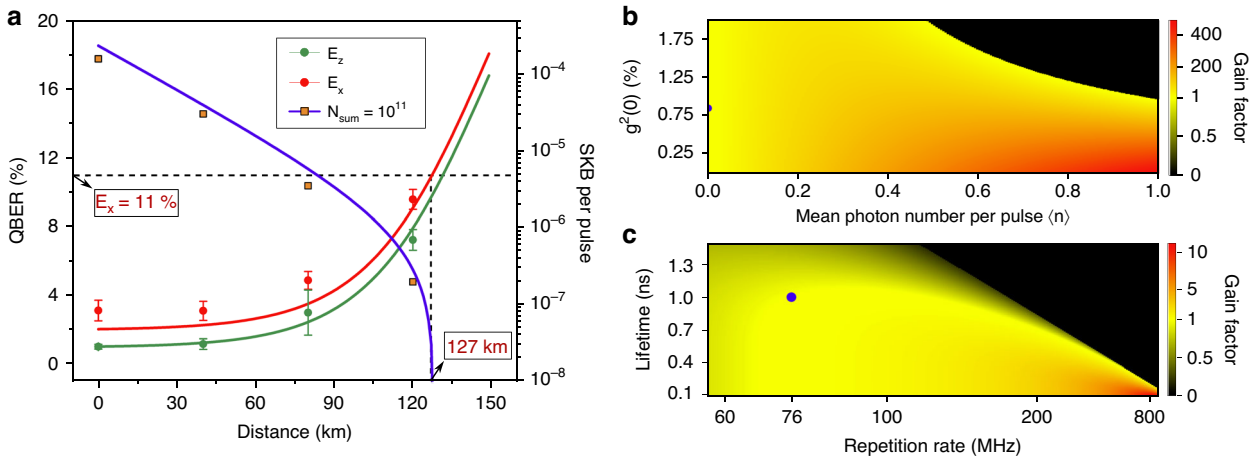


**Fig. 4 Time-bin QKD performance versus transmission distance and gain in secure key rate with improved source qualities. a** QBERs at the $|X\rangle$ and $|Z\rangle$ bases and SKB per pulse as a function of the secret key transmission distance. A received block size of $N_{sum} = 10^{11}$ is employed for the finite key analysis. **b** Gain of simulated SKR as a function of the mean photon number per pulse $\langle n\rangle$ and second order autocorrelation $g^{(2)}(0)$, compared with this experiment. **c** Gain of simulated SKR as a function of the repetition rate of the excitation laser and the QD lifetime, compared with this experiment. The blue circles indicate the parameters in the current time-bin QKD system

long-distance transmission and realistic conditions. Nevertheless, there remains considerable potential for further improvement in system performance, as discussed below:

1. Influence of source brightness and system loss. The mean photon number $\langle n\rangle$ is a critical parameter affecting the key rate. Increasing source brightness and reducing encoder loss can significantly enhance $\langle n\rangle$ compared to current experimental conditions. As shown in Fig. 4b, the SKR improves with larger $\langle n\rangle$. However, higher brightness increases sensitivity to multi-photon components, and a low $g^{(2)}(0)$ becomes increasingly important to preserve security. Poor single-photon purity (i.e., high $g^{(2)}(0)$) has a stronger negative impact at higher source brightness.
2. Repetition rate limitations imposed by QD lifetime and modulation structure. Compared with weak coherent laser pulses, QD sources typically exhibit longer radiative lifetimes. Therefore, increasing the system repetition rate leads to temporal overlap between ↻ and ↺ wave packets within the Sagnac interferometer (SNI). This overlap region exhibits the same phase and thus lacks modulation contrast, making it unusable for key generation. Additionally, at higher repetition rates, overlap between detection windows (W1, W2, and W3) may occur, resulting in photons from adjacent bits falling into incorrect time bins and increasing the quantum bit error rate (QBER). To further explain this point, we performed simulations based on a fitted model of the QD lifetime to explore the trade-off between repetition rate and temporal overlap, as shown in Fig. 4c. While higher repetition rates can theoretically enhance the key rate, they are only effective when the pulse lifetime is sufficiently short to prevent peak overlap. An optimal operating point must balance increased repetition with minimal temporal crosstalk.
3. Optical loss and visibilities in the encoding and decoding modules. The secure key rate is also constrained by the intrinsic loss in both Alice's and Bob's modules. Several components in the system can be optimized further, such as using lower-loss fiber devices and replacing standard fiber connectors with high-precision fusion splicing, thereby minimizing insertion loss and back-reflection. To further reduce the QBERs of the $|X_0\rangle$ state, AMZIs with high- and stable visibilities needs to be carefully optimized by employing ultra-balanced BSs and automate feedback phase shift control.
4. Detector performance and dark count suppression. The performance of the SNSPD plays a crucial role in system reliability. Although the detectors used in this work exhibit good efficiency and low dark count probability, further improvements are possible. Enhancing detector efficiency and reducing background counts through improved device fabrication and environmental isolation could boost the overall key rate.
5. Synchronization between encoder and decoder at remote sites. Synchronization between Alice and Bob is essential for a working QKD system to enable basis comparison using timing information. In our laboratory implementation, this is achieved by distribution of electronic clock signals. For a real-world point-to-point QKD system, various methods

have been proposed to realize synchronization without relying on additional hardware or external references such as GPS[66–70].

In summary, we have demonstrated the feasibility and long-term self-stability of a time-bin encoded QKD system based on a deterministic single-photon source at telecom wavelengths. Benefiting from a stable emission of high-brightness and pure telecom single photons[40], the system operates continuously for over 6 h at 120 km and achieves a highest finite-size key rate among the time-bin QKDs with single-photon sources. Our work identifies key advantages and also limitations of QD single photon sources for the generation of time-bin qubits. The results provide practical paths for optimization of all system components, therefore contributing to the realization of a robust and scalable quantum communication infrastructure based on solid-state single-photon emitters.

## Materials and methods

### Transformation of quantum states with the AMZI

For an asymmetric Mach–Zehnder interferometer (AMZI), consisting of two beam splitters and a phase shifter (fast axis along with H polarization of single photons) for one arm, the transformation matrix for the single-photon states before the $BS_4$ is,

$$\begin{aligned} R'_{AMZI} &= R_{PS} \otimes R_{BS_3} \\ &= \begin{pmatrix} e^{i\theta_2} 0 \\ 01 \end{pmatrix}_{PS} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} i1 \\ 1i \end{pmatrix}_{BS_3} \end{aligned} \tag{6}$$

where the $R_{BS}$, $R_{PS}$ are the transformation matrix for the BS and PS, respectively. Taking into account the single-photon state from the quantum channel is,

$$\begin{aligned} |\Psi\rangle_c &= \frac{1}{\sqrt{2}} e^{i\frac{\theta_1}{2}} \left(\sin\frac{\theta_1}{2} \cdot |e\rangle + i\cos\frac{\theta_1}{2} \cdot |l\rangle\right) \\ &= \frac{1}{\sqrt{2}} e^{i\frac{\theta_1}{2}} \cdot \begin{pmatrix} \sin\frac{\theta_1}{2} \\ i\cos\frac{\theta_1}{2} \end{pmatrix}_T \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}_P \end{aligned} \tag{7}$$

with the first two terms the time-bin states $T$ for the $|e\rangle$ and $|l\rangle$ photons from the quantum channel. The third term indicates the path states $P$ corresponding to $|S\rangle$ and $|L\rangle$ before $AMIZ_2$. The single-photon states before $BS_4$ is then,

$$\begin{aligned} |\Psi\rangle'_{AMZI_2} &= R'_{AMIZ} \cdot |\Psi\rangle_1 \\ &= \frac{1}{\sqrt{2}} e^{i\frac{\theta_1}{2}} \cdot \begin{pmatrix} \sin\frac{\theta_1}{2} \\ i\cos\frac{\theta_1}{2} \end{pmatrix}_T \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} ie^{i\theta_2} \\ 1 \end{pmatrix}_P \\ &= \frac{1}{2} e^{i\frac{\theta_1}{2}} \cdot \Big( i\sin\frac{\theta_1}{2} e^{i\theta_2} \cdot |e\rangle|S\rangle_{AMZI_2} \\ &\quad + \sin\frac{\theta_1}{2} \cdot |e\rangle|L\rangle_{AMZI_2} - \cos\frac{\theta_1}{2} e^{i\theta_2} \cdot |l\rangle|S\rangle_{AMZI_2} \\ &\quad + i\cos\frac{\theta_1}{2} \cdot |l\rangle|L\rangle_{AMZI_2} \Big) \end{aligned} \tag{8}$$

In our experiment, only one output port of $BS_4$ is used for the measurement. The final state from one port of the $AMZI_2$ can be written as follows, with a amplitude factor of $1/\sqrt{2}$ is applied considering the splitting probability of 50:50 with the BS. In addition, assuming that the output of $BS_4$ corresponds to photons from the short path, it leads to a phase shift of $\pi/2$ with the $|S\rangle$-state photons sigified by i.

$$\begin{aligned} |\Psi\rangle'_{AMZI_2} &\to |\Psi\rangle_d \\ &= \frac{1}{2\sqrt{2}} e^{i\frac{\theta_1}{2}} \cdot \Big( -\sin\frac{\theta_1}{2} e^{i\theta_2} \cdot |e\rangle|S\rangle_{AMZI_2} \\ &\quad + \sin\frac{\theta_1}{2} \cdot |e\rangle|L\rangle_{AMZI_2} - i\cos\frac{\theta_1}{2} e^{i\theta_2} \cdot |l\rangle|S\rangle_{AMZI_2} \\ &\quad + i\cos\frac{\theta_1}{2} \cdot |l\rangle|L\rangle_{AMZI_2} \Big) \end{aligned} \tag{9}$$

### Estimation of QBERs

In our time-bin QKD system, we estimate the QBERs and SKRs based on the calculation of click $p_{click}^{X,Z}$ and error $p_e^{X,Z}$ probability with the detected photons by SNSPD at $\{X, Z\}$ bases, taking into account of the system parameters such as mean photon number per pulse $\langle n\rangle$, $g^{(2)}(0)$, total system loss (incl. fiber spools) $\eta_{total}$, etc.

$$\begin{aligned} p_c^{X,Z} &= \sum_{n=0}^{\infty} p_n [1 - (1 - p_{dc})(1 - \eta_{total})^n] \\ p_e^{X,Z} &= p_0 p_{dc} + \sum_{n=1}^{\infty} p_n \left[1 - (1 - p_{dc})(1 - \eta_{total})^n\right] p_{mis} \end{aligned} \tag{10}$$

in which $p_{dc}$ is dark count probability equal to the multiplication of system dark counts $d$ and individual time window $\tau_W = 4.3$ ns. Here, the parameter $p_{mis}^{X,Z}$ is the error probability of the signal components due to imperfect state preparation, channel decoherence, and imperfect power splitting at decoder. This is given by the average QBER for an optical fiber length of 0 km in the experiment. The probability of n-photon emission $p_n$ is calculated as[30],

$$p_2 = \frac{\overline{n}^2 \cdot g^{(2)}(0)}{2} \quad p_1 = \overline{n} - 2p_2 \quad p_0 = 1 - p_1 - p_2 \tag{11}$$

with $\overline{n} = \langle n\rangle \cdot \eta_B \cdot \eta_D$ the average photon number per pulse after the detector. In the simulation of Fig. 4 about the QBER as a function of transmission distance, we employ the phase error rate to estimate the QBER in the finite key length regime,

$$E_X = \phi^Z = \frac{M_R^X}{\underline{N}_{R,nmp}^X} \quad E_Z = \phi^X = \frac{M_R^Z}{\underline{N}_{R,nmp}^Z} \tag{12}$$

in which $M_R^{X,Z}$ and $\underline{N}_{R,nmp}^X$ are calculated as,

$$\begin{aligned} M_R^{X,Z} &= N_{sum} \cdot p_{X,Z}^A \cdot p_{X,Z}^B \cdot p_e^{X,Z} \\ \underline{N}_{R,nmp}^X &= N_R^{X,Z} - \overline{N}_{sum,mp}^{X,Z} \\ &= N_{sum} \cdot p_{X,Z}^A \cdot p_{X,Z}^B \cdot p_c^{X,Z} - N_{sum} \cdot p_{X,Z}^A \cdot p_{X,Z}^B \cdot p_m \end{aligned} \tag{13}$$

$p_{X,Z}^{A,B}$ is the splitting ratio of the keys for the $\{X, Z\}$ bases at the encoder and decoder sites. $p_m$ is the the multi-photon emission probability of the source, which is equal

to $p_2$ in our case by only taking into account the multi-photon events up to two. $\overline{N}^{X,Z}_{sum,mp}$ denote the upper bound of the emitted photons from the encoder that is derived with the upper Chernoff bound and $N^{X,Z}_{sum,mp}$,

$$\overline{x} = (1+\delta_U)x^* \tag{14}$$

with $\delta^U = \frac{\beta+\sqrt{8\beta x^*+\beta^2}}{2x^*}$ and $\beta = -\log_e(\epsilon_{PE})$.

### Calculation of SKR

The calculation of SKR in finite key regime based on the Chernoff bound has been discussed in the previous publications for the polarization-encoded QKDs[30,41],

$$R_{secure} = \lfloor \underline{N}^Z_{R,nmp}\left(1-h(\overline{\phi}_Z)\right) - \lambda_{EC} - 2\log_2\frac{1}{2\varepsilon_{PA}} - \log_2\frac{2}{\varepsilon_{cor}}\rfloor / N_{sum} \tag{15}$$

with $\overline{\phi}_Z$ calculated as,

$$\begin{gathered}\overline{\phi_Z} = \phi_Z + \gamma^U\left(N^X_{R,nmp}, N^Z_{R,nmp}, \phi_Z, \tfrac{\varepsilon_{sec}}{6}\right),\ \phi_Z = E_X = \frac{M^X_R}{\underline{N^X_{nmp}}} \\ \gamma^U(n,k,\lambda,\varepsilon') = \frac{1}{2+2\frac{A^2G}{(n+k)^2}}\left\{\frac{(1-2\lambda)AG}{n+k} + \sqrt{\frac{A^2G^2}{(n+k)^2} + 4\lambda(1-\lambda)G}\right\} \\ A = \max\{n,k\},\ G = \frac{n+k}{nk}\log_e\frac{n+k}{2\pi nk\lambda(1-\lambda)\varepsilon'^2}\end{gathered} \tag{16}$$

**Table 2 System parameters**

| Description | Parameter | Value |
|---|---|---|
| Repetition rate | $f_{rep}$ | 75.947 MHz |
| Average photon number per pulse before the quantum channel | $\langle n\rangle$ | $2.89 \times 10^{-3}$ |
| Second-order correlation | $g^{(2)}$ | 0.85% |
| Transmission efficiency of encoder and decoder | $\eta_A$, $\eta_B$ | 10.11%, 41.7% |
| Z-basis choice (Encoder) | $p^A_Z$ | 11/16 |
| X-basis choice (Encoder) | $p^A_X$ | 5/16 |
| Z- and X- basis choice (Decoder) | $p^B_X$ | 1/2 |
| Misalignment probability of Z-basis | $p_{misZ}$ | 1% |
| Misalignment probability of X-basis | $p_{misX}$ | 2% |
| Averaged fiber-spool loss | $\alpha$ | 0.1956 dB km$^{-1}$ |
| Detector efficiency | $\eta_D$ | 74% |
| Dead time | $\tau_{dt}$ | 35.8 ns |
| Time window of one bit | $\tau_W$ | 4.3 ns |
| Dark count probability | $p_{dc}$ | $1.33 \times 10^{-6}$ |
| Parameter estimation failure probability | $\epsilon_{PE}$ | $2 \times 10^{-10}/3$ |
| Error correction failure probability | $\epsilon_{EC}$ | $10^{-10}/6$ |
| Privacy amplification failure probability | $\epsilon_{PA}$ | $10^{-10}/6$ |
| Error verification failure probability | $\epsilon_{cor}$ | $10^{-15}$ |

$\lambda_{EC}$ is the estimation on the known leakage of information from the error correction process,

$$\lambda_{EC} = \left[n^Z_R(1-E_Z) - F^{-1}\left(\varepsilon_{cor}\cdot\left(1+\frac{1}{\sqrt{n^Z_R}}\right); n^Z_R, 1-E_Z\right) - 1\right] \tag{17}$$

where $E_Z = \frac{M^Z_R}{N^Z_R}$ is bit error rate of received Z basis count and $F^{-1}\left(\varepsilon_{cor}\left(1+\frac{1}{\sqrt{n^Z_R}}\right); n^Z_R, 1-E_Z\right)$ is the inverse of the cumulative distribution function of the binomial distribution. The simulation parameter is displayed in the following Table 2.

**Acknowledgements**

The authors thank Alessandro Fedrizzi and Frederik Brooke Barnes for the fruitful discussion about SKR simulation, Johann Dzeik for helping with the 3D-printing of encoder and decoder container, and Jialiang Wang for the experimental assistance. The authors gratefully acknowledge the funding by the German Federal Ministry of Education and Research (BMBF) within the project QR.X (16KISQ013 and 16KISQ015), QR.N (16KIS2188 and 16KIS2207), SQuaD (16KISQ117) and SemIQON (13N16291), and the European Research Council (MiNet GA101043851). We thank the project EQSOTIC within the QuantERA II Programme that has received funding support from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No. 101017733, and BMBF (No. 16KIS2060K), the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) via the Project 469373712, GRK2642, InterSync (GZ: INST 187/880-1 AOBJ: 683478), and under Germany's Excellence Strategy (EXC-2123) Quantum Frontiers (390837967).

**Author details**

[1]Institut für Festkörperphysik, Leibniz Universität Hannover, Appelstraße 2, 30167 Hannover, Germany. [2]Institut für Halbleiteroptik und Funktionelle Grenzflächen, Center for Integrated Quantum Science and Technology (IQST) and SCoPE, University of Stuttgart, Allmandring 3, 70569 Stuttgart, Germany. [3]National Laboratory of Solid State Microstructures and School of Physics, Collaborative Innovation Center of Advanced Microstructures, Nanjing University, 210093 Nanjing, China. [4]Department of Physics and Beijing Key Laboratory of Opto-electronic Functional Materials and Micro-nano Devices, Key Laboratory of Quantum State Construction and Manipulation (Ministry of Education), Renmin University of China, 100872 Beijing, China. [5]Information Materials and Intelligent Sensing Laboratory of Anhui Province, Institutes of Physical Science and Information Technology, Anhui University, 230601 Hefei, China. [6]Laboratorium für Nano- und Quantenengineering, Leibniz Universität Hannover, Schneiderberg 39, 30167 Hannover, Germany

**Author contributions**

J.P. Wang built encoder and decoder setup and carried out the QKD experiment (CRediT: Investigation), with help of J. Hanel and X.Y. Cao (CRediT: Methodology). Z.H. Jiang and J.Z. Yang implemented the optical characterization of the quantum dot sample (CRediT: Validation), with preliminary support from M. Jetter and R. Joos (CRediT: Resources). E.P. Rugeramigabo provided support with instrumentation and optical experiments (CRediT: Resources). J.P. Wang performed the data analysis (CRediT: Software). J.P. Wang, J.Z. Yang and F. Ding wrote the manuscript (CRediT: Formal analysis, Writing), with the help of S.L. Portalupi, M. Zopf and the other co-authors (CRediT: Project administration, Writing). F. Ding, M. Zopf and J.Z. Yang conceived and supervised the project (CRediT: Funding acquisition, Conceptualization, Supervision), with support from S. L. Portalupi and P. Michler (CRediT: Validation, Writing).

**Funding**

Open Access funding enabled and organized by Projekt DEAL.

**Data availability**

The data that support the plots within this paper and other findings of this study are available from the corresponding author upon reasonable request.

**Conflict of interest**

F.D. serves as an Editor for the Journal. No other author has reported any competing interests.

Received: 27 August 2025 Revised: 20 January 2026 Accepted: 21 January 2026
Published online: 25 February 2026

**References**

1. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
2. Li, H.-W. et al. Randomness determines practical security of BB84 quantum key distribution. *Sci. Rep.* **5**, 16200 (2015).
3. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133–165 (2005).
4. Scarani, V. & Renner, R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **100**, 200501 (2008).
5. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (1984).
6. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
7. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
8. Zhang, Q., Xu, F., Chen, Y.-A., Peng, C.-Z. & Pan, J.-W. Large scale quantum key distribution: challenges and solutions [invited]. *Opt. Express* **26**, 24260–24273 (2018).
9. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
10. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
11. Lim, C. C. W., Curty, M., Walenta, N., Xu, F. & Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **89**, 022307 (2014).
12. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
13. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
14. Ribezzo, D. et al. Deploying an inter-European quantum network. *Adv. Quantum Technol.* **6**, 2200061 (2023).
15. Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).
16. Cao, Y. et al. The evolution of quantum key distribution networks: on the road to the qinternet. *IEEE Commun. Surv. Tutor.* **24**, 839–894 (2022).
17. Paraïso, T. K. et al. A photonic integrated quantum secure communication system. *Nat. photonics* **15**, 850–856 (2021).
18. Oesterling, L., Hayford, D. & Friend, G. Comparison of commercial and next generation quantum key distribution: technologies for secure communication of information. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 156–161 (IEEE, 2012).
19. Bozzio, M. et al. Enhancing quantum cryptography with quantum dot single-photon sources. *npj Quantum Inf.* **8**, 104 (2022).
20. Wang, Q. et al. Experimental decoy-state quantum key distribution with a sub-Poissonian heralded single-photon source. *Phys. Rev. Lett.* **100**, 090501 (2008).
21. Pousa, R. G., Oi, D. K. L. & Jeffers, J. Comparison of non-decoy single-photon source and decoy weak coherent pulse in quantum key distribution. *arXiv* https://doi.org/10.48550/arXiv.2405.19963 (2024).
22. Yoshino, K. -i et al. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses. *npj Quantum Inf.* **4**, 8 (2018).
23. Huang, A. et al. Laser-seeding attack in quantum key distribution. *Phys. Rev. Appl.* **12**, 064043 (2019).
24. Huang, A., Sun, S.-H., Liu, Z. & Makarov, V. Quantum key distribution with distinguishable decoy states. *Phys. Rev. A* **98**, 012330 (2018).
25. Trefilov, D. et al. Intensity correlations in decoy-state BB84 quantum key distribution systems. Optica Quantum https://opg.optica.org/opticaq/fulltext.cfm?uri=opticaq-3-5-417 (2025).
26. Ding, F. Quantum dots get a bright upgrade. *Light Sci. Appl.* **13**, 267 (2024).
27. Rota, M. B. et al. A source of entangled photons based on a cavity-enhanced and strain-tuned GaAs quantum dot. *eLight* **4**, 13 (2024).
28. Yang, J. et al. Tunable quantum dots in monolithic Fabry-Perot microcavities for high-performance single-photon sources. *Light Sci. Appl.* **13**, 33 (2024).
29. Takemoto, K. et al. Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Sci. Rep.* **5**, 14383 (2015).
30. Morrison, C. L. et al. Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates. *Nat. Commun.* **14**, 3573 (2023).
31. Intallura, P. M. et al. Quantum communication using single photons from a semiconductor quantum dot emitting at a telecommunication wavelength. *J. Opt. A Pure Appl. Opt.* **11**, 054005 (2009).
32. Intallura, P. M. et al. Quantum key distribution using a triggered quantum dot source emitting near 1.3 μm. *Appl. Phys. Lett.* **91**, 161103 (2007).
33. Gao, T. et al. A quantum key distribution testbed using a plug&play telecom-wavelength single-photon source. *Appl. Phys. Rev.* **9**, 011412 (2022).
34. Schimpf, C. et al. Quantum cryptography with highly entangled photons from semiconductor quantum dots. *Sci. Adv.* **7**, eabe8905 (2021).
35. Zahidy, M. et al. Quantum key distribution using deterministic single-photon sources over a field-installed fibre link. *npj Quantum Inf.* **10**, 2 (2024).
36. Zhang, H. et al. Metropolitan quantum key distribution using a GaN-based room-temperature telecommunication single-photon source. *Phys. Rev. Appl.* **23**, 054022 (2025).
37. Basset, F. B. et al. Daylight entanglement-based quantum key distribution with a quantum dot source. *Quantum Sci. Technol.* **8**, 025002 (2023).
38. Rau, M. et al. Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources—a proof of principle experiment. *N. J. Phys.* **16**, 043003 (2014).
39. Samaner, C., Paçal, S., Mutlu, G., Uyanık, K. V. & Ateş, S. Free-space quantum key distribution with single photons from defects in hexagonal boron nitride. *Adv. Quantum Technol.* **5**, 2200059 (2022).
40. Nawrath, C. et al. Bright source of purcell-enhanced, triggered, single photons in the telecom C-band. *Adv. Quantum Technol.* **6**, 2300111 (2023).
41. Yang, J. et al. High-rate intercity quantum key distribution with a semiconductor single-photon source. *Light Sci. Appl.* **13**, 150 (2024).
42. Heindel, T. et al. Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range. *N. J. Phys.* **14**, 083001 (2012).
43. Al-Juboori, A. et al. Quantum key distribution using a quantum emitter in hexagonal boron nitride. *Adv. Quantum Technol.* **6**, 2300038 (2023).
44. Li, Y. et al. High-speed robust polarization modulation for quantum key distribution. *Opt. Lett.* **44**, 5262–5265 (2019).
45. Figer, D. F., Reimer, M. & Rotenberg, N. A detailed model for polarization mode dispersion in broadband polarization-encoded QKD. In *Photonics for Quantum*, vol. 13106 (SPIE, 2024).
46. Lucio-Martinez, I., Chan, P., Mo, X., Hosier, S. & Tittel, W. Proof-of-concept of real-world quantum key distribution with quantum frames. *N. J. Phys.* **11**, 095001 (2009).
47. Agnesi, C., Avesani, M., Stanco, A., Villoresi, P. & Vallone, G. All-fiber self-compensating polarization encoder for quantum key distribution. *Opt. Lett.* **44**, 2398–2401 (2019).
48. Ding, Y.-Y. et al. Polarization variations in installed fibers and their influence on quantum key distribution systems. *Opt. Express* **25**, 27923–27936 (2017).
49. Konteli, P. et al. Time-bin phase and polarization based QKD systems performance analysis over 16km aerial fibers. In *2025 30th OptoElectronics and Communications Conference (OECC) and 2025 International Conference on Photonics in Switching and Computing (PSC)*, 1–4 (IEEE, 2025).
50. Qiu, B.-Y. et al. 7 km free-space time-bin quantum key distribution. *Opt. Express* **33**, 35176–35184 (2025).
51. Yin, H.-L. et al. Experimental composable security decoy-state quantum key distribution using time-phase encoding. *Opt. Express* **28**, 29479–29485 (2020).
52. Boaron, A. et al. Simple 2.5 GHz time-bin quantum key distribution. *Appl. Phys. Lett.* **112**, 171108 (2018).

53. Tanaka, A. et al. High-speed quantum key distribution system for 1-mbps real-time key generation. *IEEE J. Quantum Electron.* **48**, 542–550 (2012).
54. Tang, Y.-L. et al. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113**, 190501 (2015).
55. Tang, B.-Y. et al. Free-running long-distance reference-frame-independent quantum key distribution. *npj Quantum Inf.* **8**, 117 (2022).
56. Jin, J. et al. Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel. *Opt. Express* **27**, 37214–37223 (2019).
57. Anderson, M. et al. Gigahertz-clocked teleportation of time-bin qubits with a quantum dot in the telecommunication C-band. *Phys. Rev. Appl.* **13**, 054052 (2020).
58. Yu, H. et al. Quantum key distribution implemented with d-level time-bin entangled photons. *Nat. Commun.* **16**, 171 (2025).
59. Fitzke, E. et al. Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding. *PRX Quantum* **3**, 020341 (2022).
60. Jayakumar, H. et al. Time-bin entangled photons from a quantum dot. *Nat. Commun.* **5**, 4251 (2014).
61. Chen, H. et al. Invited article: time-bin entangled photon pairs from Bragg-reflection waveguides. *APL Photonics* **3**, 080804 (2018).
62. Lee, J. P. et al. A quantum dot as a source of time-bin entangled multi-photon states. *Quantum Sci. Technol.* **4**, 025011 (2019).
63. Khodadad Kashi, A. & Kues, M. Frequency-bin-encoded entanglement-based quantum key distribution in a reconfigurable frequency-multiplexed network. *Light Sci. Appl.* **14**, 49 (2025).
64. Bacco, D. et al. Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area. *EPJ Quantum Technol.* **6**, 5 (2019).
65. Weihs, G. & Zeilinger, A. Photon statistics at beam-splitters: an essential tool in quantum information and teleportation. https://painterlab.caltech.edu/wp-content/uploads/2019/06/iqd_photon_stats_at_beamsplitters.pdf, https://api.semanticscholar.org/CorpusID:174794052 (2001).
66. Calderaro, L. et al. Fast and simple qubit-based synchronization for quantum key distribution. *Phys. Rev. Appl.* **13**, 054041 (2020).
67. Cochran, R. D. & Gauthier, D. J. Qubit-based clock synchronization for QKD systems using a Bayesian approach. *Entropy* **23**, 988 (2021).
68. Krause, J., Walenta, N., Hilt, J. & Freund, R. Clock-offset recovery with sublinear complexity enables synchronization on low-level hardware for quantum key distribution. *Phys. Rev. Appl.* **23**, 044015 (2025).
69. Spiess, C. & Steinlechner, F. Clock synchronization with pulsed single photon sources. *Quantum Sci. Technol.* **9**, 015019 (2023).
70. Zahidy, M. et al. Single-photon-based clock analysis and recovery in quantum key distribution. *AVS Quantum Sci.* **5**, 041403 (2023).