Check for updates

ARTICLE   OPEN

Tools for the performance optimization of single-photon quantum key distribution

Timm Kupko[1], Martin von Helversen[1], Lucas Rickert[1], Jan-Hindrik Schulze[1], André Strittmatter[1,2], Manuel Gschrey[1], Sven Rodt[1], Stephan Reitzenstein[1] and Tobias Heindel [1 ✉]

Quantum light sources emitting triggered single photons or entangled photon pairs have the potential to boost the performance of quantum key distribution (QKD) systems. Proof-of-principle experiments affirmed these prospects, but further efforts are necessary to push this field beyond its current status. In this work, we show that temporal filtering of single-photon pulses enables a performance optimization of QKD systems implemented with realistic quantum light sources, both in experiment and simulations. To this end, we analyze the influence of temporal filtering of sub-Poissonian single-photon pulses on the expected secret key fraction, the quantum bit error ratio, and the tolerable channel losses. For this purpose, we developed a basic QKD testbed comprising a triggered solid-state single-photon source and a receiver module designed for four-state polarization coding via the BB84 protocol. Furthermore, we demonstrate real-time security monitoring by analyzing the photon statistics, in terms of $g^{(2)}(0)$, inside the quantum channel by correlating the photon flux recorded at the four ports of our receiver. Our findings are useful for the certification of QKD and can be applied and further extended for the optimization of various implementations of quantum communication based on sub-Poissonian quantum light sources, including measurement-device-independent schemes of QKD as well as quantum repeaters. Our work represents an important contribution towards the development of QKD-secured communication networks based on quantum light sources.

INTRODUCTION

Privacy in communication is an increasingly important challenge in our information-driven society[1]. The concepts gathered in the field of quantum communication[2–4] represent solutions to this challenge and enable information theoretical secure communication. Quantum key distribution (QKD) for instance enables the tap-proof encryption of data, by exploiting quantum properties of light[5,6]. The respective quantum light sources ideally required for QKD, however, had been impossible to fabricate with sufficient brightness and quality for a long time. Most implementations of QKD are therefore still implemented with weak coherent pulses (WCPs), i.e. attenuated lasers, requiring so-called decoy-state protocols[7,8]. During the last decade, however, tremendous progress has been made in the fabrication of quantum light sources. Single-photon sources (SPSs) based on epitaxial semiconductor quantum dots (QDs) nowadays can be triggered at GHz clock rates under pulsed-optical[9] and -electrical[10,11] excitation, feature high degrees of photon indistinguishability[12,13], large photon extraction efficiencies[11,14,15], and to date achieve the highest single-photon purity in terms of $g^{(2)}(0)$ compared to any other single-photon emitter[16,17]. The advancement of deterministic fabrication technologies had particular large impact on these developments, as summarized in a recent review article[18]. Despite this immense progress, only few proof-of-concept QKD experiments have been reported based on optically[19–25] and electrically[26,27] operated SPSs. These experiments affirmed the potential sub-Poissonian light sources offer for QKD. To push the field of sub-Poissonian QKD to a new level, however, further efforts need to be undertaken. In particular, practical methods for the security analysis and certification as well as measures to improve the performance of QKD systems for a given quantum light source

need to be developed. While Waks et al. discussed security aspects of QKD with sub-Poissonian light sources from a theoretical viewpoint[28], experimental studies on this important topic are still missing.

In this work, we perform a detailed analysis on the influence of temporal filtering of single-photon pulses on the performance of QKD systems implemented with sub-Poissonian light sources. For this purpose we set up a basic QKD testbed comprising a QD-based SPS and a receiver module designed for four-state polarization coding via the BB84 protocol. Using this Bob module in combination with our SPS, we determine the sifted key fraction, the quantum bit error ratio (QBER) caused by the receiver, and the $g^{(2)}(0)$ of the single-photon pulses inside the quantum channel, to finally extract the secure key rate expected in full implementations of QKD. As the temporal filtering of single-photon pulses differently affects these parameters, a performance optimization of QKD systems implemented with a quantum light source is possible. We show that optimal performance for a given SPS can be achieved by carefully setting Bob's acceptance time windows, depending on the pulse shape and noise level. This can be either used to maximize the secure key rate for a given channel loss or to extend the maximally tolerable loss, i.e. the achievable communication distance. In addition, we demonstrate real-time security monitoring by analyzing the suppression of multiphoton emission events, i.e. $g^{(2)}(0)$ of the single-photon pulses inside the quantum channel during key generation. Finally, we generalize our findings by employing simulations with synthetic pulse shapes, providing predictions for different SPSs and detectors. We consider the results presented in this work an important contribution towards the development of QKD-secured communication networks based on quantum light sources. Importantly, our approach can be easily applied and further extended for the optimization of any

[1]Institut für Festkörperphysik, Technische Universität Berlin, 10623 Berlin, Germany. [2]Present address: Institut für Experimentelle Physik, Otto-von-Guericke Universität Magdeburg, 39106 Magdeburg, Germany. ✉email: tobias.heindel@tu-berlin.de

implementation of quantum communication based on triggered sub-Poissonian quantum light sources.

RESULTS

QKD testbed

The QKD testbed used for our experiments is illustrated in Fig. 1a. On transmitter side, Alice is represented by a triggered SPS, comprising a single preselected QD embedded in a deterministically fabricated microlens[29] providing enhanced photon collection efficiency (see Methods section "Single-Photon Source"). As depicted in Fig. 1b this device emits single photons at an emission wavelength of 918 nm with low multiphoton emission probability reflected in an antibunching of $g^{(2)}(0) = 0.089 \pm 0.002$. The nonideal $g^{(2)}(0)$ is a consequence of the simple excitation scheme (p-shell excitation) used in our present work, and can be further improved using strict resonant pumping of the quantum emitter. The polarization state of the emitted photons is set by a high-extinction-ratio linear-film polarizer and a lambda-half waveplate, respectively, preparing single-photon pulses in horizontal (H), vertical (V), diagonal (D), and antidiagonal (A) polarization. On receiver side, Bob comprises a four-state polarization analyzer with passive basis choice. Single-photon counting modules based on silicon avalanche photon diodes, time-tagging electronics and a custom-made control software is used for polarization-resolved single-photon detection, data acquisition, and postprocessing. The Bob module is integrated into a portable 19-inch rackbox presented in Fig. 1c (see Methods section "Receiver Module"). In the following, we investigate the performance of this QKD testbed assuming an implementation of the BB84 protocol by analyzing the achievable QBER, single-photon purity $g^{(2)}(0)$ and secret key rate.

First, we investigate the limit our Bob module introduces to the total QBER expected in a full implementation of QKD. For this purpose, we record the photon arrival time distribution at the four detection channels of Bob for all four possible input-polarizations of the SPS. The corresponding experimental data are shown in Fig. 1d in a 4×4 matrix representation, where the distributions within one row are normalized to the peak maximum of the curve in the respective diagonal element. Ideally, for a given input polarization (e.g. H) of one basis (H-V), one would expect only detection events in the respective channel at Bob's side (H), while the channel with orthogonal polarization (V) should be empty. Detection events in the other basis (D-A) should be equally distributed, due to the statistically random projection of the photons polarization. From the measured matrix in Fig. 1d this appears to be well reproduced in the experiment. A closer look in Fig. 1d (right panel), however, reveals the presence of erroneous detection events, by displaying the arrival time probability distributions for both polarizations of the target basis each normalized to the number of events in the given channel. In this representation, contributions of noise and optical imperfections can already be qualitatively distinguished. Correlated events in the wrong channel originate from state discrimination imperfections caused by optical imperfections of Bob (e.g. finite extinction ratios of polarizing beamsplitters and retardance deviations of waveplates), while uncorrelated background events stem from detector dark counts. The resulting QBER_{Bob} reads

$$\text{QBER}_{\text{Bob}} = \underbrace{\frac{qp_{\text{signal}}}{p_{\text{click}}}}_{\text{optical imperfections}} + \underbrace{\frac{p_{\text{dc}}/2}{p_{\text{click}}}}_{\text{dark counts}}, \tag{1}$$

where q denotes the error contributions due to Bob's optical
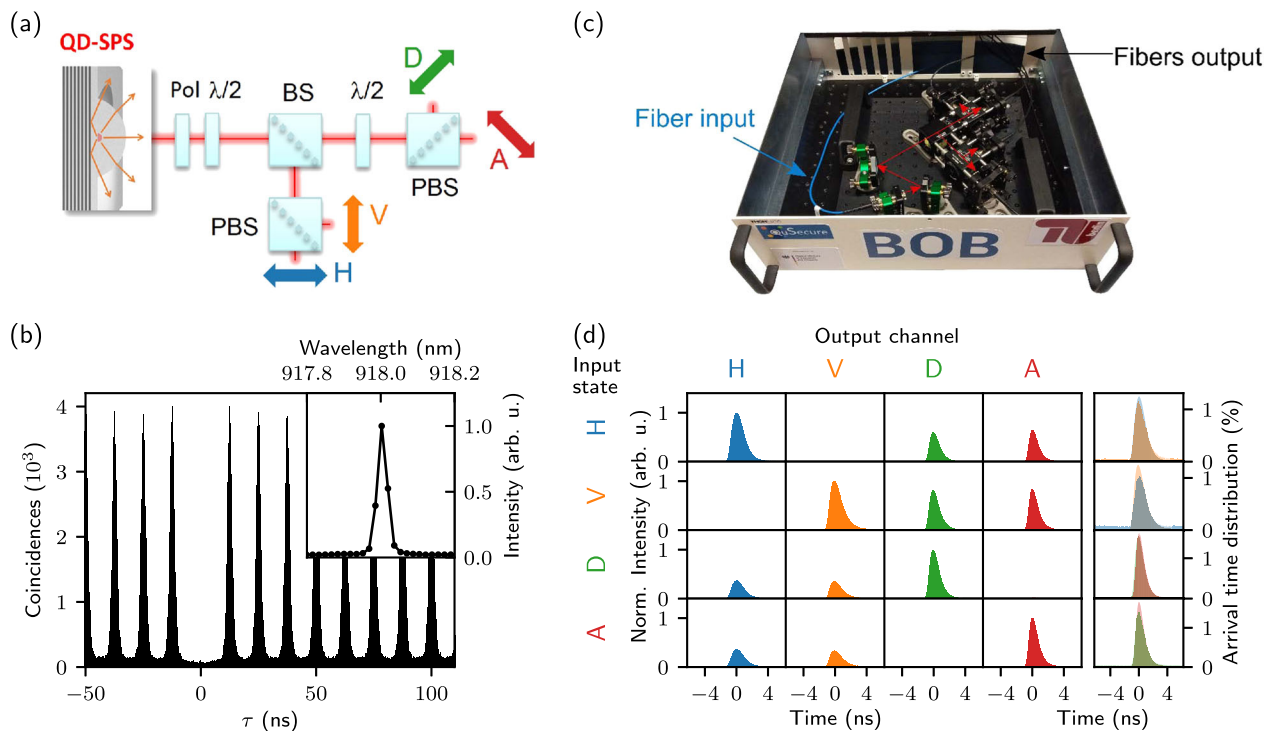
Fig. 1 BB84-QKD testbed using a triggered solid-state single-photon source (SPS) and polarization coding. a The transmitter (Alice) sends single-photon pulses with fixed polarization (H, V, D, and A) to the receiver module (Bob), comprising a four-state polarization analyzer. **b** Photon-autocorrelation measurement of the emission of the optically triggered SPS. Inset: Emission spectrum of the SPS, comprising a preselected quantum dot embedded in a photonic microlens (solid line is a guide to the eye). **c** Picture of the Bob module integrated in a 19-inch rackbox. **d** Measured photon arrival time distributions at the four detection channels of Bob for single-photon input-polarizations of H, V, D, and A. Measurement data in the left 4×4 matrix are normalized to the maximum of the respective input state. The right panel shows for each row of the matrix the two data sets of the target basis polarization (e.g. HH and HV) normalized to the number of events in a given channel, revealing erroneous detection events due to optical imperfections in Bob.
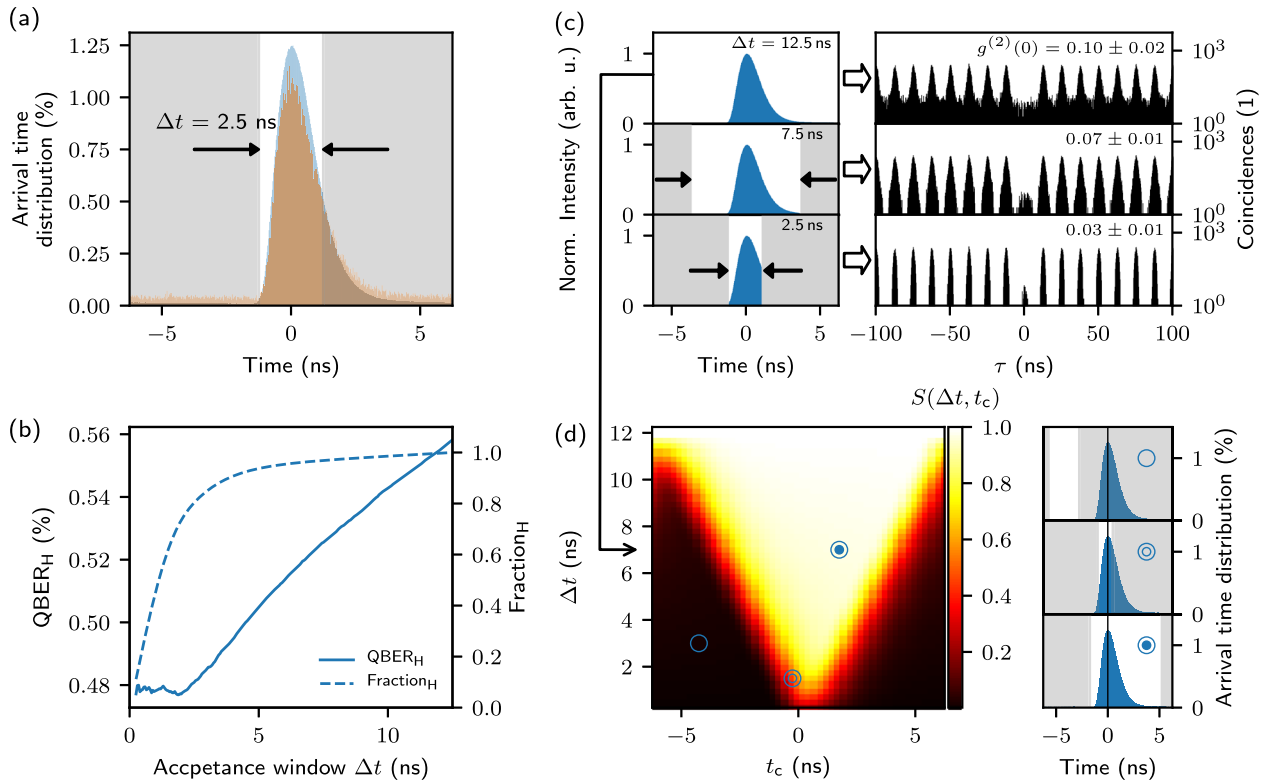
Fig. 2 The effect of temporal filtering on key parameters of QKD (exemplary shown for H input polarization). a Photon arrival time probability distributions of H-polarized photons detected in the H-channel (blue) and H-polarized photons detected in the V-channel (orange). Applying temporal filtering, noise due to detector dark counts can be reduced. **b** QBER and sifted key fraction F as a function of the acceptance time window width Δt for fixed window center t_c. **c** Impact of the temporal filtering on the $g^{(2)}(0)$. Each correlation histogram $g^{(2)}(\tau)$ is calculated from the raw recorded time-tags of all four detection channels after applying the temporal filter to the data for an evaluation time of 360 s. The unfiltered histogram was used to calculate the first data point in Fig. 4d. **d** Expected secret key rate fraction $S(\Delta t, t_c)$ as a function of the temporal width Δt and the center t_c of the acceptance time window. For the analysis, the QBER and the sifted key fraction were considered in a two-dimensional parameter space ($\Delta t, t_c$) (see Supplementary Note 3), while $g^{(2)}(0)$ was fixed to its unfiltered value (cf. discussion in main text).

imperfections, p_{signal} is the probability to observe a signal event, p_{dc} the probability for a dark count event, and p_{click} the overall probability for a click[28]. Furthermore, the distributions of photons projected in the wrong basis, i.e. D photons detected in the H channel and vice versa, are not equally distributed as ideally expected. Instead, the probability to detect an H (V) photon in the D (A) basis is higher compared to the case of detecting D (A) photons in the H (V) basis. This is a result of a detection efficiency mismatch across the four detection channels, which is caused by slightly varying transmission losses in the optical paths and different quantum efficiencies of the detector modules. Please note that the detection efficiency mismatch is important to consider in the security analysis of full implementations of QKD, as it leads to a reduced tolerable QBER[30].

Performance optimization via temporal filtering
In the following, we analyze the impact of the temporal filtering of the raw sifted key on the performance of our single-photon QKD testbed. Experimentally, the error contribution in the H-channel is calculated via $QBER_H(\Delta t, t_c) = N_V/(N_H + N_V)$, where N_H and N_V denote the number of clicks in H and V polarization, respectively, detected within an acceptance time window of width Δt centered at time t_c. Note here that we calculate the QBER by its definition using all events recorded in the respective acceptance time window, while it has to be carefully estimated in full implementations using subsets of bits[31]. Restricting the acceptance time window, the signal-to-noise ratio can be enhanced, as noise due to detector dark counts can be filtered effectively[27,32]. Figure 2a

exemplarily illustrates the measured photon arrival time probability distributions at both detectors of the H-V basis (H-polarized single-photon input) together with an acceptance time window $\Delta t = 2.5$ ns centered at the pulse maximum ($t_c = 0$ ns). Evaluating $QBER_H(\Delta t, t_c)$ by applying a temporal filter to the recorded time-tags, the QBER and the fraction F of the sifted and filtered photon detection events can be extracted as a function of Δt (see Fig. 2b). Restricting the acceptance time window Δt leads first of all to a reduction of the sifted key, as portions of the overall signal are discarded. At the same time the contribution of detector dark counts is reduced, leading to a decrease of $QBER_H$ towards small Δt. Below $\Delta t = 1.7$ ns the $QBER_H$ saturates and we observe minimal values around 0.48% limited by optical imperfections inside the receiver. This value can be further improved, e.g. by using polarization beamsplitters based on Wollaston prisms enabling higher extinction ratios compared to beamsplitter cubes with dielectric coating. Note that the global minimum in $QBER_H$ at $\Delta t = 0.05$ ns is not taken into account, due to the vanishing sifted key. The remaining three channels of the Bob module show similar behavior (see Supplementary Note 1). Note that the single-photon pulses at Bob need to be synchronized carefully for both channels of one basis to achieve optimum performance (see Methods section "Postprocessing").

Next, the photon statistics needs to be taken into account in the security analysis for sub-Poissonian quantum light sources. The multiphoton probability p_m inside the quantum channel is governed by $g^{(2)}(0)$ and the mean photon number per pulse μ Alice couples to the quantum channel[28]: $p_m \leq 1/2\mu^2 g^{(2)}(0)$. In our

QKD testbed we obtain the photon autocorrelation $g^{(2)}(\tau)$ by directly correlating the temporally filtered time-tags recorded at all four detection channels of Bob (see Methods section "Postprocessing"). Please note, that this apporach is different from reports, where postselected values of $g^{(2)}(0)$ are generated by the temporal filtering of $g^{(2)}(\tau)$ after performing the correlation measurement[17,33]. The resulting $g^{(2)}(\tau)$ histograms are exemplary shown in Fig. 2c for the case of three different acceptance time windows. Narrowing the temporal filter, the antibunching improves from 0.104 ± 0.017 at $\Delta t = 12.50$ ns to 0.032 ± 0.007 at $\Delta t = 2.5$ ns (see Supplementary Note 2 for further analysis). This trend is explained by the temporal filtering of two-photon emission events due to a finite probability for the re-excitation of the quantum emitter outside the acceptance time window. This effect can be used in principle to further enhance the security and the performance of QKD systems based on realistic sub-Poissonian light sources. To benefit from the temporal filtering of $g^{(2)}(0)$ at Bob, however, an active gating (e.g. via an amplitude modulator) or at least monitoring of $g^{(2)}(0)$ at Alice's side would be necessary, due to possible photon number splitting attacks outside the acceptance time window. This is an interesting perspective not considered in previous work. Due to the experimentally more demanding implementation, however, we use the $g^{(2)}(0)$ as obtained from the time-tags of the complete repetition period from now on.

Exploiting temporal filtering as discussed above, the overall performance of a QKD implementation based on SPSs can be optimized as we will demonstrate in the following. For this purpose, a trade-off needs to be found between low QBER on the one hand and high sifted key fractions on the other hand. In addition, a symmetric temporal filter as chosen above is not sufficient in general, due to the asymmetry in the photon arrival time distribution of the single-photon pulses. To this end, we perform a two-dimensional (2D) analysis by varying the temporal width Δt and the center t_c of the acceptance time window. The 2D analysis is performed for the $\text{QBER}_H(\Delta t, t_c)$ and the sifted fraction $F_H(\Delta t, t_c)$ (see Supplementary Note 3). From these quantities, we finally extract the normalized secret key rate $S(\Delta t, t_c)$ expected in a full implementation of BB84-QKD according to[28]

$$S = \frac{p_{\text{click}}}{2}\left(\beta\tau(e) - f(e)h(e)\right). \tag{2}$$

Here, the factor 1/2 stems from the sifting procedure for symmetric basis choice encoding, p_{click} is the probability to observe a click at the detectors, e the QBER, β the fraction of the detection events caused by single photons, $\tau(e)$ the compression function accounting for Eve's possible attacks, $h(e)$ the binary Shannon-entropy, and $f(e)$ the error correction efficiency[28]. The expected back-to-back secret key rate calculated from Eq. (2) is presented in Fig. 2d. A small Δt leads to a small QBER but also to a small sifted fraction. An acceptance window within a region governed by noise does not allow for a secret key distribution at all. The optimal value for our specific experiment does only need to discard a small part of the signal. Depending on the length of the single-photon pulses and the detector noise level, however, temporal filtering can have a crucial impact on the resulting back-to-back secure key, as demonstrated in simulations discussed further below.

The secure communication distance achievable with a given QKD system is of superior importance. Based on the secret key analysis performed in Fig. 2d, we calculated the rate-loss dependencies accounting for our experimental conditions (see Methods section "Estimation of expected secret key rates"). Figure 3 illustrates the expected secret key per pulse as a function of the losses inside the quantum channel for different temporal filters. In the low-loss regime (<20 dB) optimum back-to-back performance is achieved for our SPS by using the full acceptance time window ($\Delta t = 12.5$ ns), as already discussed above. The maximal tolerable
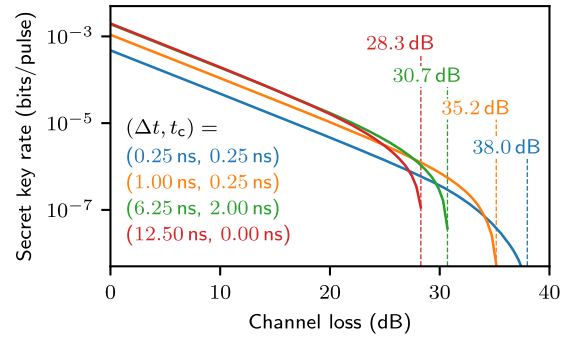
Fig. 3 Optimization of single-photon QKD exploiting temporal filtering of realistic quantum light sources. Rate-loss diagram considering our experimental data from Fig. 2d for different values of Δt and t_c. Choosing optimized settings for the acceptance time window ($\Delta t = 1$ ns, $t_c = 0.25$ ns), the tolerable loss inside the quantum channel can be enhanced by 24% in case of our SPS.

loss, however, is limited to 28.3 dB in this case. In the asymptotic case, the range could in principle be extended indefinitely by applying an asymptotic small temporal filtering and therefore enhancing the signal-to-noise ratio (SNR). In practice this is not possible. First, there is the finite temporal resolution of realistic device. The smallest possible time window in our system is lower bounded by the 1 ps digitization of the time tags. Second, the reduction in sifted key by further and further narrowing the width of the acceptance time window renders the system impractical as well due to finite size effects which would require impractical acquisition times. The reduction to $\Delta t = 1$ ns enhances the tolerable losses to 35.2 dB by decreasing the sifted fraction to 55%. A further reduction down to $\Delta t = 0.25$ ns, already below the detector timing resolution, further enhances the tolerable losses to 38.0 dB but reduces the sifted fraction further down to 24% (see also Fig. 2b). Therefore, for our system the achievable maximal tolerable loss inside the quantum channel can be enhanced to 35.2 dB for an optimized filter setting ($\Delta t = 1.00$ ns, $t_c = 0.25$ ns). This corresponds to a QKD range extension of 24% enabled by the improvement in signal-to-noise ratio due to the temporal filtering (see Supplementary Note 2). This transmission range extension could be even further enhanced by exploiting the temporal filtering and monitoring of $g^{(2)}(0)$ on Alice's side, as discussed with Fig. 2c. Assuming an SPS of similar performance with an emission wavelength of 1310 nm and 1550 nm, respectively, extensions for the secure communication distance by 22.2 km (to a distance of 113.4 km) and 40.4 km (to a distance of 206.8 km) are expected, for state-of-the-art single-mode fiber (Corning SMF28-ULL) with 0.31 dB/km and 0.17 dB/km at 1310 nm and 1550 nm, respectively. The extrapolated values compare favorably with the best experimental value of 120 km reported in ref.[34] for single-photon QKD in the telecom C-band. Importantly, the optimization routine presented above can be adapted and extended for many other applications in quantum communication employing realistic triggered quantum light sources, including future implementations of multi-user quantum networks based on measurement-device-independent QKD[35,36] or multi-dimensional memory-based quantum repeaters[37].

To assess the robustness of our SPS against transmission losses, we further analyzed its device performance in our QKD testbed in terms of the mean photon number per pulse μ (i.e. its efficiency) into the quantum channel. As derived in ref.[28], a critical value $\mu_c = \sqrt{2p_{\text{dc}}/g^{(2)}(0)}$ can be estimated above which a sub-Poissonian light source with a given $g^{(2)}(0)$ is able to achieve the same maximally tolerable loss as the same source but with unity efficiency ($\mu = 1$). Based on our experimental results from Fig. 2d, we estimated $\mu_c = 0.0053$ for the maximal width of the acceptance

time window corresponding to a tolerable loss of $T_{min} = 33.2$ dB (see also Fig. 3). The experimental mean photon number per pulse $\mu = 0.0043$ our SPS delivers into the quantum channel (cf. Methods) therefore deviates by only 18% from this critical value, leading to a slightly reduced maximal tolerable loss (cf. Fig. 3). Also note that the μ achieved in our QKD testbed is comparable to previous implementations of single-photon QKD by Waks et al. with $\mu = 0.007$[19], although we do not reach the performance of more recent implementation by Takemoto et al.[34] with $\mu = 0.05$. The considerations above show that the requirements for maximum robustness against transmission losses can be fulfilled by relatively modest improvements of our source efficiency. To outperform WCP-based implementations with sub-Poissonian light sources, however, a simple estimation leads to the requirement $\mu > 0.3$ (see Methods section "Comparison of Device Performance"). The value $\mu > 0.3$ thereby is a pessimistic upper bound, which is further reduced if the QBER is not negligible. Also, finding tighter bounds for the multiphoton emission probability as a function of $g^{(2)}(0)$ will give a tighter bound on μ. Recent experimental progress showed that this efficiency threshold is within reach using state-of-the-art deterministically fabricated solid-state quantum light sources[38]. In addition, numerically optimized designs for directly fiber-coupled quantum light sources have recently been reported by our group[39], showing prospects to achieve this high performance also at telecom wavelengths.

Real-time photon statistics monitoring

In future QKD-secured networks implemented with quantum light sources, $g^{(2)}(0)$ inside the quantum channel needs to be monitored in real time to enable secret key distillation. Until now, most reports on single-photon QKD measured $g^{(2)}(0)$ separately and independently from the key generation process, using for instance a Hanbury–Brown and Twiss setup on Alice's side. Applying our approach for the optimization via temporal filtering presented above, we are able to monitor $g^{(2)}(0)$ in real-time and for each block used for secret key distillation. For this purpose, we conducted a proof-of-principle experiment by recording time-tags over a period of 90 min with fixed input polarization H of our SPS. Based on the recorded events, we first analyze the confidence of determining $g^{(2)}(0)$ from our data. If the evaluation accumulation time is too short, the $g^{(2)}(0)$ may be over- or underestimated. In the case of an overestimation this leads to reduced performance, while the case of overestimation could lead to information leakage compromising the security. Figure 4a depicts the $g^{(2)}(0)$ of our SPS evaluated via Bob together with the corresponding sifted block size as a function of the accumulation time. As expected, the error decreases with increasing accumulation time. The value of $g^{(2)}(0)$ converges to $g^{(2)}(0) = 0.089 \pm 0.002$ for accumulation times approaching the entire measurement period. Figure 4b, c additionally show the count rates of the four detection channels and the extracted $QBER_H$ during the 90-min measurement period confirming stable conditions for the photon collection efficiency. Interestingly, a closer look at Fig. 4a reveals that the extracted $g^{(2)}(0)$ does not perfectly match the converged value (within its error) for certain ranges of accumulation times. This behavior could be related to slight changes of the properties of Alice (i.e. the SPS itself or the experimental setup) over time, which are important to consider for full implementations of quantum communication. Next, we demonstrate real-time monitoring of $g^{(2)}(0)$ inside the quantum channel evaluating the time-tags from Bob. Comparison with Fig. 4a reveals that for 10 s of accumulation time, the obtained $g^{(2)}(0)$ is close to the converged value but the uncertainty is far too large (43%). For 60 s the error margin is significantly reduced to 16% and the block size should already be enough to allow for a secret key distillation incorporating finite-key size effects[40]. Choosing 360 s
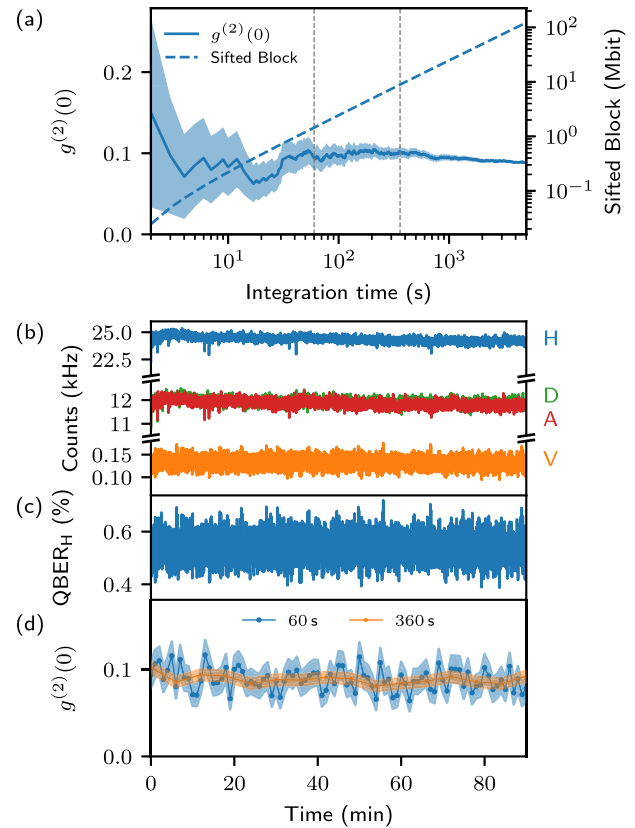

Fig. 4 **Real-time security monitoring for single-photon QKD. a** Antibunching $g^{(2)}(0)$ of our SPS evaluated via correlating the time-tags of all four detection channels in overlapping blocks for different accumulation times compared with the corresponding length of the sifted block. **b** Clicks recorded in all four detection channels of Bob for H-polarized single photons as input. **c** $QBER_H$ calculated from the data in **b**. **d** Antibunching $g^{(2)}(0)$ of our SPS evaluated via correlating the time-tags of all four detection channels in nonoverlapping blocks of 60 s (blue) and 360 s (orange) length (cf. markers in **a**).

accumulation time, the uncertainty is further reduced to 6% and the sifted block size would already allow secret key distillation by neglecting finite-key size effects. Figure 4c presents the time traces of $g^{(2)}(0)$ for two different choices of the accumulation time of 60 s and 360 s (cf. markers in Fig. 4a) corresponding to sifted block sizes of 1.47 Mbit, and 8.93 Mbit at the first measurement point. The real-time monitoring of $g^{(2)}(0)$ presented above, previously only been used for coherent and bunched light sources[41,42], enables us to perform a reliable security analysis in future QKD experiments, by taking into account the photon statistics of single-photon pulses used for secret key distillation. In addition, the ability to monitor the photon statistics in real time allows for reacting on changes in the source itself or on various types of attacks, if $g^{(2)}(0)$ is additionally monitored on Alice side. In case of photon number splitting attacks, for instance, an eavesdropper would artificially reduce $g^{(2)}(0)$ inside the quantum channel, which could be detected comparing $g^{(2)}_{Alice}(0)$ and $g^{(2)}_{Bob}(0)$. Moreover, any attack where the eavesdropper uses a light source with photon statistics different from the one of the QKD implementation could easily be detected.

Simulations

To extend the scope of our approach for the performance optimization of single-photon QKD beyond the specific properties of our testbed, we additionally performed simulations on the secret key fraction expected for different SPSs and detectors. For
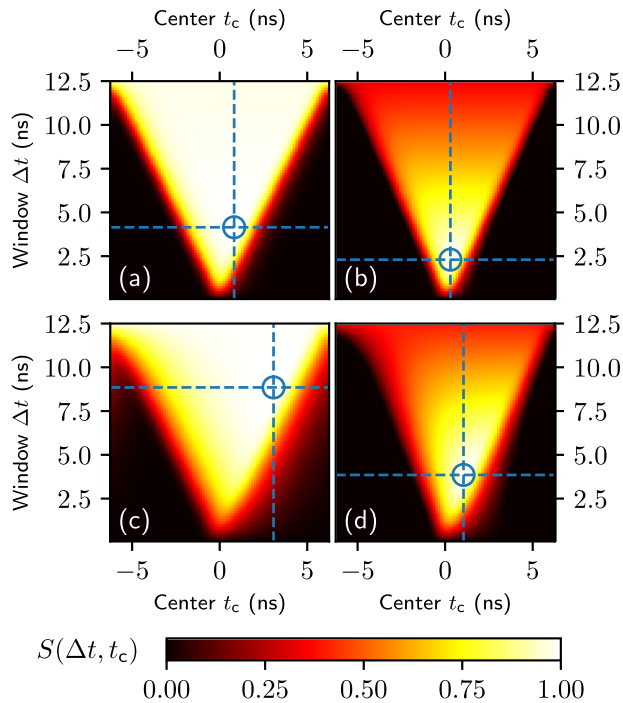
Fig. 5 Simulated back-to-back secret key rates achievable via temporal filtering for different pulse lengths and noise levels. a Low noise and long pulse; **b** high noise and short pulse; **c** low noise and long pulse, as well as **d** high noise and long pulse. Careful adjustment of the acceptance time windows results in a maximum in the secret key (see markers).

this purpose, we modeled the photon arrival time distributions of the single-photon pulses with a synthetic pulse shape and varied the decay time constant as well as the noise level (see Methods section "Simulations"). For the sake of clarity, we limit ourselves to four regimes: (1) low noise and short lifetime, (2) high noise and short lifetime, (3) low noise and long lifetime, and (4) high noise and long lifetime, with short and long referring to the clock-rate. The simulation results for the secret key fraction $S(\Delta t, t_c)$ are presented in a two-dimensional parameter space in Fig. 5, assuming an ideal SPS ($g^{(2)}(0) = 0$). In all four cases the temporal filtering enables one to find an optimal trade-off between sifted-key and QBER. Hence the secret key rate can be maximized by correctly choosing the settings of the temporal filter, resulting in a performance optimization of the QKD system. The gain in secret key rate compared to the case without applying a temporal filter is 2.5% in case (1), 184.5% in case (2), 6.0% in case (3), and 148.3% in case (4). Substantial improvements are achieved in the cases with high noise levels ((2) and (4)), corresponding to the regime of high transmission channel losses. Therefore, the optimization via temporal filtering becomes particularly important in long-distance QKD with noisy detectors. Using state-of-the-art super-conducting single-photon detectors[43], the noise can be drastically reduced[44]. Many practical QKD scenarios, however, will not be able to provide the infrastructure for liquid-helium or closed-cycle refrigerators required for these detectors to date.

DISCUSSION

We demonstrated that temporal filtering of single-photon pulses is a viable tool to optimize the performance of QKD implementations based on sub-Poissonian quantum light sources. Using a basic QKD testbed comprising a solid-state-based triggered SPS and a receiver module for four-state polarization coding, we

showed that carefully setting the acceptance time windows enables one to maximize the achievable back-to-back secure key rate or the maximally tolerable transmission loss inside the quantum channel. Our optimization routine is particular beneficial in the high loss regime characteristic for long-distance QKD. Additionally, we showed real-time security monitoring by evaluating the photon statistics of our SPS in terms of $g^{(2)}(0)$ during key generation.

The routines developed in our work with a basic BB84-QKD testbed are readily applicable for various implementations of quantum communication employing realistic quantum light sources, including measurement-device-independent QKD and quantum repeaters, and are useful for the certification of QKD[45]. Furthermore, the temporal filtering and real-time monitoring of sub-Poissonian light pulses opens up new possibilities for improving the performance taking detection flaws into account. Using SPSs for QKD, an attacker is forced to use an SPS as well. This in turn reduces the penalty on the achievable secret key rate taking detection flaws into account[30]. Even advanced nonlinear attacks influencing or even controlling the photon statistics inside the quantum channel can be detected, by additionally monitoring $g^{(2)}(0)$ on Alice's side. With respect to full implementations of QKD, further extensions are required, taking side-channel attacks[27,46] or finite-key effects[47–49] into account. As the temporal filtering reduces the amount of key material that can be generated, finite-key size effects are getting increasingly important. Finally, to compete with WCP-based QKD implementations and to enable long-distance single-photon QKD in optical fibers, the efficiency of quantum light sources operating at telecom wavelengths needs to be pushed further, e.g. by employing numerically optimized directly fiber-coupled devices[39].

METHODS

Single-photon source

The SPS on Alice's side comprises a single preselected InGaAs/GaAs QD embedded in a monolithic microlens above a bottom distributed Bragg reflector, both of which increase the photon collection efficiency from the QD. Details on the sample and its deterministic fabrication can be found elsewhere[29,50]. The SPS was mounted into a closed-cycle refrigerator integrated in a cryooptical table (Model attoDRY800, attocube systems AG) for operating the SPS at a temperature of 4.2 K. An aspheric lens (NA = 0.77) inside the cryostat collected the QD emission, which was optically triggered at 80 MHz repetition rate using quasi-resonant excitation into the QD's p-shell via a pulsed (2 ps pulse width) tunable laser system (picoEmerald, APE GmbH). Single-photon emission from the QD was spectrally filtered via an edge-pass filter and a monochromator coupled to a polarization maintaining single-mode fiber (PM 98-U25D) connected to the receiver module Bob. Here, the polarization of the single-photon pulses is set using a high-extinction-ratio linear-film polarizer followed by a lambda-half waveplate for aligning Alice's and Bob's polarization axes.

Receiver module

The receiver module Bob contains a four-state polarization analyzer with passive basis choice. Here, the stream of single-photon pulses is split by a nonpolarizing 50:50 beamsplitter (BS) followed by a polarizing beamsplitter (PBS) in the first output and a lambda-half waveplate combined with another PBS in the second output. Thus the four BB84 states (H-, V-, D-, and A-polarized photons) are routed in four different output ports, each comprising a fiber-collimator with attached optical multimode fiber (FG050LGA, Thorlabs GmbH). The photons are detected using four single-photon counting modules (COUNT-T100-FC, Laser Components GmbH) with a timing jitter between 500 ps and 600 ps. The single-photon detection events are converted to four streams of time-tags (1 ps digital resolution) using a time-to-digital converter (TDC) (quTag, qutools GmbH) synchronized to the excitation laser.

Postprocessing

To process the time-tags from the receiver module, a homemade software package was developed (based on LabVIEW and Rust), in order to extract the sifted key fraction, the QBER, and the antibunching value $g^{(2)}(0)$ as explained in the following. First, temporally filtered data sets were processed from the raw time-tags by discarding events outside the specified acceptance time windows of width Δt and center t_c. For this purpose, slight temporal delays within Bob had to be compensated using electronic delays build in the TDC electronics. This synchronization was achieved by minimizing the ratio $r = N_P/N_{\bar{P}}$ of the arrival time distributions for a given polarization basis P within the full temporal window of 12.5 ns. Note that this temporal synchronization is important for properly extracting $g^{(2)}(\tau)$ (see further below) as well as to reduce possible detection efficiency mismatches between channels affecting the performance of QKD systems[30]. Afterwards the parameters mentioned above were extracted from the temporally filtered data sets. The QBER was calculated from the photon arrival time distributions as well as the sifted key. The photon statistics $g^{(2)}(\tau)$ were evaluated in a $\Delta\tau = 250$ ns-wide delay window, by correlating the time-tags of the four detection channels at Bob. From the resulting $g^{(2)}(\tau)$ histograms, $g^{(2)}(0)$ was calculated via $g^{(2)}(0) = \frac{N_{\tau=0}}{N_{\tau\neq0}}$, where $N_{\tau=0}$ denotes the number of coincidences of the peak at zero time delay and $N_{\tau\neq0}$ the average number of coincidences of the side peaks. The standard error of $g^{(2)}(0)$ is deduced via Gaussian error propagation, taking into account $\sigma(N_{\tau=0}) = \sqrt{N_{\tau=0}}$ as well as the standard deviation of the areas from the side peaks. For illustrations in this work, a time-bin width of 25 ps and 250 ps were chosen for the photon arrival time distributions and $g^{(2)}(\tau)$ histograms, respectively.

Estimation of expected secret key rates

The expected loss-dependent secret key in Fig. 3 was calculated via Eq. (2) using estimated parameters extracted from our measurement data with the binary Shannon entropy $h(e) = -e\log_2(e) - (1-e)\log_2(1-e)$. The parameters used for the calculation stem from the long-term measurement for fixed H input polarization. The extraction from these data is described in the following for the mean photon number μ, the detection rate p_{click} and detector dark count probability p_{dc}. The mean photon number μ at Alice's output was calculated from the clock frequency of the excitation laser (80 MHz), the setup efficiency and the mean detector count rate on all four detectors during the measurement. This results in a mean photon number $\mu = 0.0043$. This already low value does not allow for much further optimization of μ as in ref. [28]. The detector dark counts were estimated by shielding the detectors from all incoming light, resulting in a cumulative dark count rate of below 100 Hz. For the unfiltered acceptance time window of 12.5 ns, this leads to $p_{dc} = 1.22 \times 10^{-6}$.

Comparison of device performance

While state-of-the-art point-to-point QKD systems employ WCPs or even light emitting diodes[51], the performance of QKD can in principle be further enhanced by using sub-Poissonian quantum light sources. In the following we estimate the threshold μ an SPS has to overcome in a given QKD-implementation to outperform a WCP source. One can show that for the case of an ideal implementation without errors nor noise and therefore neglecting the multiphoton emission events, the secret key rate S from Eq. (2) simplifies for SPSs and for WCPs alike to:

$$S_{ideal} = \eta_{sifting} f_{rep} T P(n=1). \tag{3}$$

Here, $\eta_{sifting}$ denotes the efficiency of the sifting procedure of the protocol, f_{rep} the repetition rate, T the transmission, and $P(n=1)$ the probability for single-photon emission. Note here that $\eta_{sifting}$ is 1/2 in case of BB84, but this efficiency can also become close to unity by choosing asymmetrical measurement bases[52]. For a given implementation of QKD, i.e. with the same $\eta_{sifting}$, f_{rep}, and T, the performance is ultimately bounded by the probability of single-photon emission $P(n=1)$ of Alice. Only single photons can be used for the secret key generation. Weak laser pulses following a Poisson photon number distribution are limited to $P(n=1)_{max}^{WCP} \leq 0.37$ with $\mu_{WCP} = 1$, whereby this case even ignores multiphoton events. Typical WCP experiments using mean photon numbers $\mu_{WCP} = 0.5$ [8] have an even lower value of $P(n=1) \simeq 0.3$. The upper bound for the multiphoton emission probability from[28] yields $P(n=1) \geq \mu - \mu^2 g^{(2)}(0)$. Therefore, to surpass the performance of a WCP-based QKD system at same $\eta_{sifting}$ and f_{rep}, Alice using an ideal SPS ($g^{(2)}(0) = 0$) must achieve $\mu > 0.3$ into the quantum channel. This efficiency is within reach using existing technologies as discussed in the main text.

Simulations

For the simulations the photon arrival time distributions of the single-photon pulses were modeled with synthetic pulse shapes using an exponential decay convoluted with a Gaussian of 500 ps width at half maximum, accounting for the temporal response function of the detection apparatus. Two types of QD-SPSs are considered: The first one resembles a QD with a radiative lifetime of 1.5 ns (long pulse) and the second one with a lifetime of 0.5 ns (short pulse). The optical imperfections in the second channel were modeled by the same distribution scaled to 1%. The finite signal-to-noise ratio (noise level) was considered by an uncorrelated offset of 0.01 per bin for low noise and 0.3 per bin for high noise, corresponding to signal-to-noise ratios of 392 and 13 in the input polarization channel. To account for effects arising from the overlap of consecutive pulses, a temporal window of 12.5 ns width was used from a train of three consecutive pulses.

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.

REFERENCES

1. Acín, A. et al. The quantum technologies roadmap: a European community view. *New J. Phys.* **20**, 080201 (2018).
2. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
3. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8**, 595–604 (2014).
4. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2**, 16025 (2016).
5. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* 175–179 (IEEE Press, New York, 1984).
6. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
7. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
8. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
9. Schlehahn, A. et al. Single-photon emission at a rate of 143 MHz from a deterministic quantum-dot microlens triggered by a mode-locked vertical-external-cavity surface-emitting laser. *Appl. Phys. Lett.* **107**, 041105 (2015).
10. Hargart, F. et al. Electrically driven quantum dot single-photon source at 2 GHz excitation repetition rate with ultra-low emission time jitter. *Appl. Phys. Lett.* **102**, 011126 (2013).
11. Schlehahn, A. et al. An electrically driven cavity-enhanced source of indistinguishable photons with 61% overall efficiency. *APL Photon.* **1**, 011301 (2016).
12. Somaschi, N. et al. Near-optimal single-photon sources in the solid state. *Nat. Photon.* **10**, 340–345 (2016).
13. Wang, H. et al. Near-transform-limited single photons from an efficient solid-state quantum emitter. *Phys. Rev. Lett.* **116**, 213601 (2016).
14. Heindel, T. et al. Electrically driven quantum dot-micropillar single photon source with 34% overall efficiency. *Appl. Phys. Lett.* **96**, 011107 (2010).
15. Wang, H. et al. On-demand semiconductor source of entangled photons which simultaneously has high fidelity, efficiency, and indistinguishability. *Phys. Rev. Lett.* **122**, 113602 (2019).
16. Schweickert, L. et al. On-demand generation of background-free single photons from a solid-state source. *Appl. Phys. Lett.* **112**, 093106 (2018).
17. Hanschke, L. et al. Quantum dot single-photon sources with ultra-low multi-photon probability. *npj Quantum Inf.* **4**, 43 (2018).
18. Rodt, S., Reitzenstein, S. & Heindel, T. Deterministically fabricated solid-state quantum-light sources. *J. Phys. Condens. Matter* **32**, 153003 (2020).
19. Waks, E. et al. Secure communication: quantum cryptography with a photon turnstile. *Nature* **420**, 762–762 (2002).
20. Beveratos, A. et al. Single photon quantum cryptography. *Phys. Rev. Lett.* **89**, 187901 (2002).
21. Alléaume, R. et al. Experimental open-air quantum key distribution with a single-photon source. *New J. Phys.* **6**, 92 (2004).

22. 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).

23. Collins, R. J. et al. Quantum key distribution system in standard tele-communications fiber using a short wavelength single photon source. *J. Appl. Phys.* **107**, 073102 (2010).

24. Takemoto, K. et al. Transmission experiment of quantum keys over 50 km using high-performance quantum-dot single-photon source at 1.5 μm wavelength. *Appl. Phys. Express* **3**, 092802 (2010).

25. Leifgen, M. et al. Evaluation of nitrogen- and silicon-vacancy defect centres as single photon sources in quantum key distribution. *New J. Phys.* **16**, 023021 (2014).

26. Heindel, T. et al. Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range. *New J. Phys.* **14**, 083001 (2012).

27. Rau, M. et al. Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources proof of principle experiment. *New J. Phys.* **16**, 043003 (2014).

28. Waks, E., Santori, C. & Yamamoto, Y. Security aspects of quantum key distribution with sub-poisson light. *Phys. Rev. A* **66**, 042315 (2002).

29. Gschrey, M. et al. Highly indistinguishable photons from deterministic quantum-dot microlenses utilizing three-dimensional in situ electron-beam lithography. *Nat. Commun.* **6**, 7662 (2015).

30. Lydersen, L. & Skaar, J. Security of quantum key distribution with bit and basis dependent detector flaws. *Quantum Inf. Comput.* **10**, 60–76 (2010).

31. Gao, C., Jiang, D., Guo, Y. & Chen, L. Multi-matrix error estimation and reconciliation for quantum key distribution. *Opt. Express* **27**, 14545 (2019).

32. Ko, H. et al. Experimental filtering effect on the daylight operation of a free-space quantum key distribution. *Sci. Rep.* **8**, 14545 (2018).

33. Schöll, E. et al. Resonance fluorescence of GaAs quantum dots with near-unity photon indistinguishability. *Nano Lett.* **19**, 2404–2410 (2019).

34. 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).

35. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).

36. Braunstein, S. L. & Pirandola, S. Side-Channel-Free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).

37. Kuzmin, V. V., Vasilyev, D. V., Sangouard, N., Dür, W. & Muschik, C. A. Scalable repeater architectures for multi-party states. *npj Quantum Inf.* **5**, 115 (2019).

38. Wang, H. et al. Towards optimal single-photon sources from polarized microcavities. *Nat. Photon.* **13**, 770–775 (2019).

39. Rickert, L., Kupko, T., Rodt, S., Reitzenstein, S. & Heindel, T. Optimized designs for telecom-wavelength quantum light sources based on hybrid circular Bragg gratings. *Opt. Express* **27**, 36824 (2019).

40. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).

41. Dynes, J. F. et al. Testing the photon-number statistics of a quantum key distribution light source. *Opt. Express* **26**, 22733 (2018).

42. Kumazawa, M., Sasaki, T. & Koashi, M. Rigorous characterization method for photon-number statistics. *Opt. Express* **27**, 5297 (2019).

43. Zadeh, I. E. et al. Single-photon detectors combining high efficiency, high detection rates, and ultra-high timing resolution. *APL Photon.* **2**, 111301 (2017).

44. Boaron, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).

45. Tomita, A. Implementation security certification of decoy-BB84 quantum key distribution systems. *Adv. Quantum Technol.* **2**, 1900005 (2019).

46. Sajeed, S. et al. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Phys. Rev. A* **91**, 062301 (2015).

47. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).

48. Curty, M. et al. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 3732 (2014).

49. Zhang, Z., Zhao, Q., Razavi, M. & Ma, X. Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Phys. Rev. A* **95**, 012333 (2017).

50. Heindel, T., Rodt, S. & Reitzenstein, S. *Single-Photon Sources Based on Deterministic Quantum-Dot Microlenses* 199−232 (Springer International Publishing, Cham, 2017).

51. Xia, X.-X. et al. LED-based fiber quantum key distribution: toward low-cost applications. *Photon. Res.* **7**, 1169 (2019).

52. Lo, H.-K., Chau, H. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133–165 (2004).

AUTHOR CONTRIBUTIONS

T.K. designed and built the receiver module and the software used for the experiments. T.K. and M.v.H. ran the single-photon source, which was grown by J.-H.S. and A.S. and processed by M.G. and S.Rodt under the supervision of S.Reitzenstein. T.K. performed the experiments and analyzed the data, with input of L.R. and T.H. T.K. and T.H. wrote the manuscript with input from all authors. T.H. conceived the experiment and supervised the project.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information is available for this paper at https://doi.org/10.1038/s41534-020-0262-8.

Correspondence and requests for materials should be addressed to T.H.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.