Editors' Suggestion

Quantum key Distribution with a Hand-Held Sender Unit

Gwenaelle Vest,[1] Peter Freiwang,[1,2] Jannik Luhn,[1] Tobias Vogl,[1,3,4] Markus Rau,[1] Lukas Knips,[1,2,5,*] Wenjamin Rosenfeld,[1,2] and Harald Weinfurter[1,2,5,†]

[1] *Ludwig-Maximilians-Universität, München 80799, Germany*
[2] *Munich Center for Quantum Science and Technology (MCQST), München 80799, Germany*
[3] *University of Cambridge, Cambridge CB3 0HE, United Kingdom*
[4] *Friedrich-Schiller-Universität Jena, Jena 07745, Germany*
[5] *Max-Planck-Institut für Quantenoptik, Garching 85748, Germany*

(Received 24 August 2020; revised 21 April 2022; accepted 9 June 2022; published 25 August 2022)

Quantum key distribution (QKD) is a crucial component for truly secure communication, which enables the leakage of information due to eavesdropper attacks to be analyzed. Although impressive progress was made in the field of long-distance implementations, user-oriented applications involving short-distance links have mostly remained overlooked. Recent technological advances in integrated photonics now enable developments towards QKD also for existing hand-held communication platforms. In this work we report on the design and evaluation of a hand-held free-space QKD system including a micro-optics-based sender unit. This system implements the BB84 protocol employing polarization-encoded faint laser pulses at a rate of 100 MHz. Unidirectional beam tracking and live reference-frame alignment systems at the receiver side enable a stable operation over tens of seconds when aiming the portable transmitter to the receiver input by hand from a distance of about half a meter. The user-friendliness of our system was confirmed by successful key exchanges performed by different untrained users with an average link efficiency of about 20% relative to the case of the transmitter being stationarily mounted and aligned. In these tests we achieve an average quantum bit error ratio (QBER) of 2.4% and asymptotic secret key rates ranging from 4.0 kbps to 15.3 kbps. Given its compactness, the versatile sender optics is also well suited for integration into other free-space communication systems enabling QKD over any distance.

DOI: 10.1103/PhysRevApplied.18.024067

I. INTRODUCTION

Quantum key distribution (QKD) [1–6] enables the exchange of a secret cryptographic key between two authenticated parties with the security based on fundamental physical laws. Over the years QKD has evolved from an initial laboratory experiment [7] into a mature technology and fiber-based systems are already commercially available. By extending the range of secure point-to-point fiber [8–10] and free-space links [11,12] an essential step towards large-scale quantum networks has been achieved. More recently a satellite-to-ground key exchange has been demonstrated on a global scale [13,14], and a trusted-node based link was set up connecting Chinese cities over a distance of 2000 km [5,15].

Yet, QKD has also a remarkable potential for secure short-distance communication tasks, e.g., for secure cardless payments [16], safe connected homes [17], or user access to a quantum network [18]. In these scenarios, a mobile device storing sensitive data could exchange keys with any static node within the network. The resulting keys could be consumed immediately to securely upload content or be earmarked for later use. Such applications, however, require user-friendly QKD sender units which are ideally already integrated into daily use mobile devices such as mobile phones, tablets, or laptops.

The developments in the field of integrated optics and microelectronics have opened up new possibilities for the miniaturization of QKD hardware. Such technological advances have led to the demonstration of miniaturized components [19] and short-range free-space QKD optical links in static [16,20,21] as well as in a hand-held [22] configuration. Based on highly integrated, on-chip QKD components [23–29], the capabilities for generating key material at an impressive rate in a full encryption scheme

*lukas.knips@mpq.mpg.de
†h.w@lmu.de

have been reported [30]. Despite this great technological progress, all QKD hardware so far is only suited for standalone operation and still lacks integrability into portable communication devices.

In this work we combine these technological advances in miniaturizing all optical and electronic components for a hand-held QKD transmitter module. We detail its design and evaluate its performance in a realistic, fully hand-held free-space key exchange based on the BB84 protocol over a distance of about half a meter. Our micro-optics module generates attenuated laser pulses ($\lambda = 850$ nm) with four different polarizations at a repetition rate of 100 MHz. A visible beacon laser ($\lambda = 680$ nm), overlapped with the QKD beam path, provides visual feedback during the aiming procedure and enables efficient unidirectional beam tracking by the receiver station as well as synchronization. In the current version, a smartphone placed on top of the transmitter communicates its orientation to establish a shared reference frame for polarization analysis of the detected QKD signals. The achieved user-friendliness and technological readiness of our system highlight the potential of the approach as well as its prospects for deployment in virtually all free-space scenarios.

II. MINIATURE SENDER UNIT

A. Design

The present work focuses on integrating a QKD transmitter unit within hand-held host systems such as smartphones. This requires a very compact optical architecture with low power consumption implementing a simple protocol with preferably only a small number of active components. We thus chose the BB84 protocol with polarization encoding which can be realized with standard laser sources and passive components only.

The four polarization states are generated by four laser diodes, respectively, and in order to erase any information about the location of the source, the output of the diodes is overlapped by a waveguide chip into one spatial mode. This architecture achieves a high mechanical and thermal stability and requires less than 2×2 mm^2 transversally and 35 mm in longitudinal direction [31]. The operating wavelength of 850 nm provides high transmission through the atmosphere for free-space applications and a wide availability of inexpensive, high-efficiency single-photon detectors operating at noncryogenic temperatures.

The optical module [Fig. 1(a)] was put together with the electronics board into an aluminum case. The layout of the QKD sender module is shown in Fig. 1(b) (for details on components and assembly, see Appendix A 1). As light sources we employ an array of four single-mode vertical-cavity surface-emitting lasers (VCSELs) with a spacing of 250 μm. The VCSELs are operated in the strong modulation regime, yielding low background optical pulses with a duration of only 200 ps at 100 MHz repetition rate. Under strong and short carrier injection, transient effects lead to a low degree of polarization (DOP < 0.5), allowing for generation of the four BB84 states (H, V, $+45$, -45) by using polarization filters. For this purpose, we fabricated four gold wire-grid polarizers [32,33] matching the 250 μm pitch of the lasers and exhibiting extinction ratios better than 1000 : 1 [34]. The spatial overlap of the polarized beams is ensured by three directional couplers integrated in a low-birefringence aluminoborosilicate waveguide chip manufactured via femtosecond laser writing [35–37].

Finally, the signal pulses are superimposed with a bright, visible 680 nm beacon laser using a dichroic beamsplitter cube and collimated with a small aspheric lens ($f = 4.9$ mm). The beacon light helps the user to aim at the receiver, and allows for efficient beam tracking (see Sec. III). A modulation of this beam (100 MHz) ensures an accurate synchronization with the receiver.

The assembled optical module has a size of $35 \times 20 \times 8$ mm^3 where the large lateral extension is mainly determined by the footprint of the electric connector and of the printed circuit board (PCB, 20×6 mm^2) onto which the VCSEL array is mounted, as well as by the width of the glass chip containing the multiple photonic circuits. The control electronics, implemented on a single PCB ($96 \times 60 \times 18$ mm^3), includes four laser drivers and pulse generators together with a field-programmable gate array (FPGA). The latter enables communication with a PC or a smartphone for controlling the device parameters. For this proof-of-principle demonstration the sequence of random bits determining the state to be sent was generated by a pseudorandom number generator (Java SecureRandom class) and uploaded to the FPGA. With a current storage capacity of 131056×2 bits, the random pattern was then repeated periodically every 1.3 ms. The physical size of the device can surely be reduced during industrialization while the random numbers ideally have to be produced in real time by a quantum random number generator.

B. Characterization of the sender unit

The polarization states emerging from the sender were characterized by complete state tomography in order to evaluate their quality. Figure 1(c) shows the results as red dots on the Poincaré sphere, which come close to the desired set of states up to a rotation resulting from birefringence in the waveguide chip (see Appendix A 2 for details). This rotation can be almost fully compensated by a set of external half- and quarter-waveplates for all four states simultaneously. A very good agreement between the simulation (not shown) and the experimentally achieved compensation (Fig. 1(c), blue dots) was observed. Alice's compensated states resulted in a source-related quantum bit error ratio (QBER) $e_{\text{source}} = 1.5\%$. Furthermore, the tomographic measurements (see Appendix Table II) also allow to determine how well the basis states are mutually

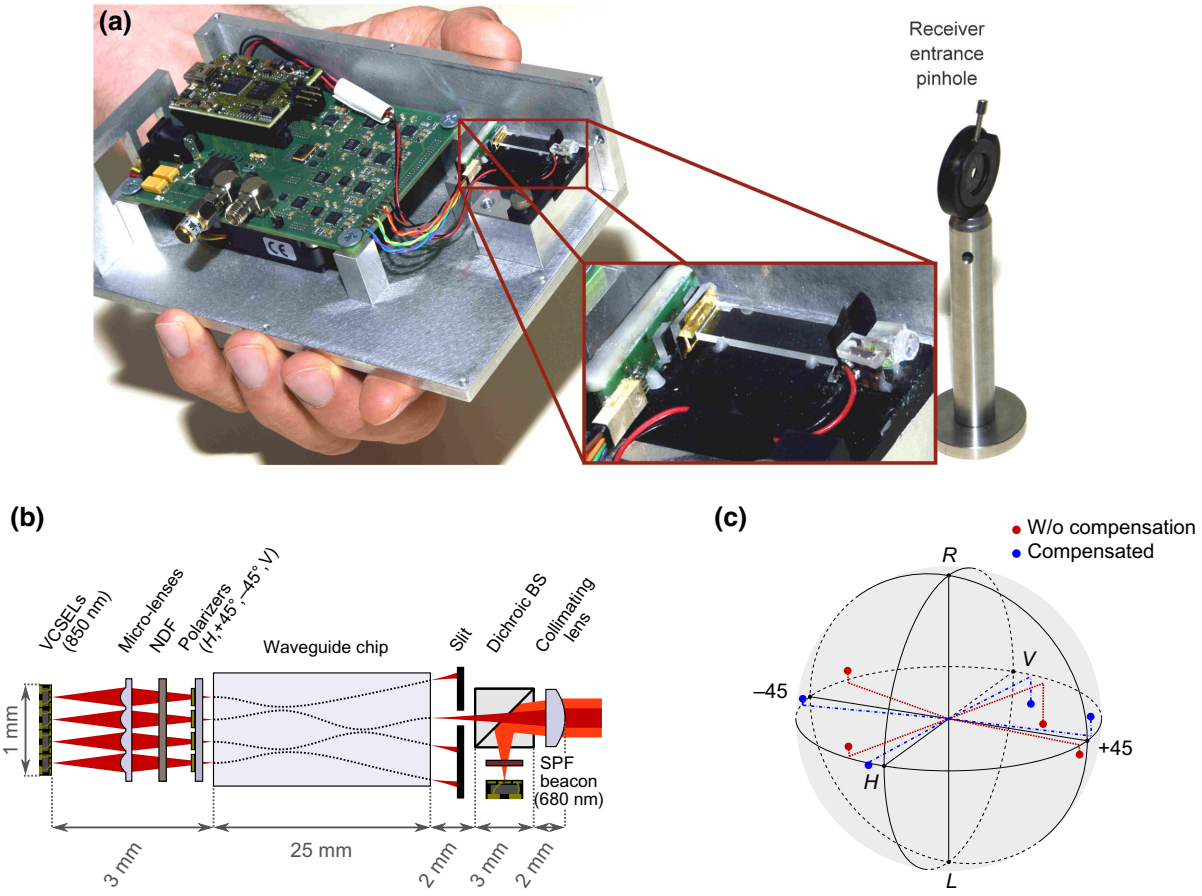

FIG. 1. The hand-held transmitter unit. (a) Mobile transmitter unit featuring a micro-optical bench (inset) with a size of 30 × 6.5 × 5 mm^3 (together with PCB and connector 35 × 20 × 8 mm^3) for generating BB84 states and its dedicated electronics. The surrounding case has a size of 15.5 × 9 × 5 cm^3. (b) Schematic of the optics architecture. Pulses centered around 850 nm and exhibiting a low degree of polarization are produced at 100 MHz rate by an array of four vertical-cavity surface-emitting lasers (VCSELs). The pulses are attenuated by a neutral density filter (NDF), polarized by an array of wire-grid polarizers and coupled into a low-birefringence waveguide chip containing three directional couplers. A micro-lens array enables here a coupling efficiency of about 20%. The desired output of the waveguide is selected by a thin slit. An additional beacon laser ($\lambda = 680$ nm) is spectrally filtered by a short-pass filter (SPF) to reduce background emission and overlapped with the 850 nm signal using a miniature beamsplitter to provide visual feedback during the aiming procedure and to allow for synchronization as well as efficient beam tracking on the receiver's side. (c) Polarization states as measured by quantum tomography at the output of the transmitter unit (red) and after compensation by the set of waveplates in the receiver (blue).

conjugated using the so called preparation quality [38]

$$q = -\log_2\left[\max_{\{\psi_{H,V},\psi_{\pm 45^\circ}\}}\left(|\langle\psi_{H,V}|\psi_{\pm 45^\circ}\rangle|^2\right)\right]. \qquad (1)$$

For our sender module, the maximum of the four products to be calculated is found for $|\langle\psi_V|\psi_{+45^\circ}\rangle|^2$ resulting in the reduced value $q = 0.75$ ($q_{\text{ideal}} = 1.0$) mainly because of an angle misalignment in the production of the polarizers. In addition, imperfections due to the polarization-dependent loss (PDL) in the waveguide chip and other optical components of the sender contribute to the preparation quality.

Finally, we have investigated the robustness of our implementation to side-channel attacks [39,40], which would become possible due to residual distinguishability in any other degree of freedom besides the polarization (see Appendix A 1). Our high-speed electronics featuring delay lines with 5 ps resolution, together with the fast optical response of the VCSELs allow us to achieve excellent temporal overlap of the pulses, whereas the optimized design of the waveguide results in essentially perfect spatial overlap. We observed a spectral distinguishability of the four off-the-shelf VCSELs due to fabrication imperfections, however, for our proof-of-principle demonstration we accept this open side channel. When commercializing such systems in the future, this could be avoided, e.g., by proper selection of the diodes prior to the assembly of the module [39], by the use of microelectromechanical system (MEMS)-tunable structures [41,42] or by spectral filtering once the spectra of the four diodes start overlapping.

III. FREE-SPACE RECEIVER WITH REAL-TIME ALIGNMENT CAPABILITIES

Our free-space receiver (Fig. 2) includes a standard polarization analysis unit (PAU) capable of analyzing Alice's states and featuring several extensions strongly simplifying the operation during a hand-held key exchange. In particular, a dynamic alignment system compensates for beam wander due to user's hand movements and thereby ensures a stable optical link with the hand-held platform. Furthermore, it provides an additional audio feedback to the user allowing the transmission to be maximized. Finally, an active reference frame alignment compensates for varying rotations of the sender during operation.

A. Polarization analysis

The PAU of the BB84 receiver device (see Fig. 2) consists of a 50:50 beamsplitter for the passive basis choice, two polarizing beamsplitters and four actively quenched, fiber-coupled avalanche photodiodes (APDs, *SPCM-AQ4C*, Perkin Elmer) with a specified detection efficiency $\eta \approx 38\%$. Here, one has to take into account the birefringent phases of the involved optical components (gold and dichroic mirrors) leading to a rotation of the incoming polarization states. This was analyzed separately by performing a state tomography of well-defined input states directly at the entrance of the PAU. With this and the knowledge of the polarization states sent by the transmitter (Sec. II B) a unitary transformation which minimizes the detected QBER can be calculated and implemented by a set of motorized waveplates $(\lambda/4, \lambda/4, \lambda/2)$. Full compatibility with any transmitter unit thus could be achieved by, e.g., communicating the sender characteristics prior to the key exchange.

B. Reference-frame alignment

A well-known challenge for moving platforms is that the transmitter and the receiver in general do not share the same reference frame. This problem can be overcome by using intrinsically rotation-invariant states [43], reference-frame-independent protocols tolerating slow rotations [44], calibration of the channel using strong classical light [45], or using information extracted from the signal itself [46]. Following our quest towards a practical system under the conditions where only the sender reference frame may tilt (stationary receiver), we use a motorized half-waveplate in front of the receiver to perform a dynamic rotation of Alice's states according to the current orientation of the sender unit. The changes in the tilt of the user's hand are retrieved from the attitude sensor of a smartphone placed on top of the transmitter. Changes exceeding the specified resolution of the sensor (1°) are sent to the receiver over WLAN with a refresh rate of about 10 Hz.

C. Beam tracking

It was recently shown that the pointing angle of the input beam with respect to the optical axis of a free-space PAU opens a receiver side-channel and thus is a critical security factor [40,47]. The probability to detect each of the four BB84 states may indeed vary with the angle of incidence, which could be exploited by an eavesdropper. In order to avoid this potential side-channel we employed a spatial filter. It restricts the possible incidence angles into the PAU to maximally $\pm 0.08^\circ$ and thereby guarantees equal coupling efficiency into all four detectors. To enable hand-held operation in spite of this significant restriction we implemented a beam steering system which extends the acceptance range for the sender to $\pm 3^\circ$. For this purpose, the beacon beam is split off the quantum signals using a dichroic mirror and its pointing angle is retrieved using a quadrant photodiode. The error signal is fed to a voice coil mirror featuring a bandwidth of about 800 Hz.

IV. QUANTUM KEY DISTRIBUTION

The performance of the whole system was first evaluated with the sender unit being mounted about 30 cm away from the entrance iris of the receiver. This allows the determination of the essential security parameters, such as the mean photon number μ and the overall transmission T through the quantum channel and the receiver to the detectors. In particular, for a given transmission there exists an optimal μ maximizing the secure key rate. For the free-space channel of 30 cm in air at our working wavelength we could safely assume negligible absorption. Losses occur when coupling into the receiver due to absorption by optical elements and spectral filters, as well as coupling through the spatial mode filter and into the fibers of the detectors. The resulting transmission was measured for the case of optimal alignment and amounted to $T_{\mathrm{Bob}} = 40.9\%$ (Appendix B). In the hand-held case the transmission was generally lower, we define the relative hand-held efficiency $\xi \in [0, 1]$ such that $T(t) = \xi(t) \cdot T_{\mathrm{Bob}}$.

To initiate the key exchange, a PC uploads the parameters for the laser diodes as well as the random bit sequence (131k $\times$ 2 bits) to the FPGA which then starts the sequence of attenuated pulses. Detection events are recorded by a time-tagging unit of Bob's PAU and correlated to the bit sequence sent by Alice to distill a raw key.

A. Static configuration

With the sender module mounted and aligned, we observed for a mean photon number $\mu = 0.042$ [48], a raw key rate (overall detection rate before sifting, 1.5 ns time window per pulse applied) of $R_{\mathrm{raw}} = 649.5$ kbps, and a QBER of $e = 2.1\%$. The QBER mainly results from imperfect preparation of polarization states and a background contribution by emission of the VCSELs below

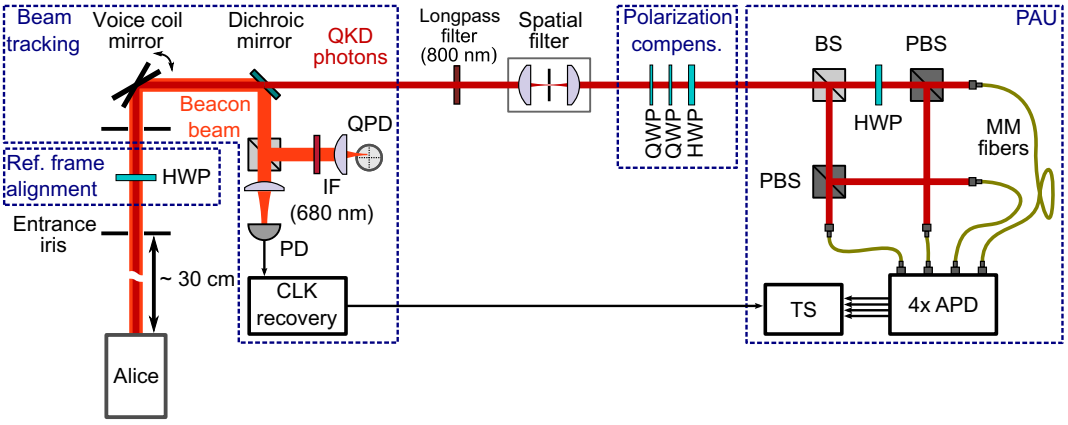

FIG. 2. Architecture of the free-space receiver. A polarization analysis unit (PAU) discriminates between four BB84 states. Prior to the spectral and spatial filtering of the attenuated pulses, a motorized half-waveplate (HWP) rotates the reference frame of the PAU depending on the sender unit's orientation. The latter is recorded by a smartphone placed on top of the sender unit and transmitted over a wireless local area network (WLAN). Polarization rotations occurring in the sender and receiver are compensated by a set of motorized waveplates. Beam tracking is performed on the beacon laser using a quadrant photodiode (QPD) and an electrically driven voice coil mirror. The beacon is additionally modulated at 50 MHz allowing for clock recovery with a fast photodiode. PD: photodiode; BS: beamsplitter; PBS: polarizing beamsplitter; MM: multimode fiber; APD: avalanche photodiode; TS: time-tagging (timestamp) unit.

threshold. The contribution of the beacon laser and detector dark counts was as small as 0.075%. With the high transmission observed here, the simple GLLP [49] scheme is still very efficient. To evaluate the final extractable secure key rate R_{sec} we also account for imperfect preparation of the quantum states using the preparation quality q [Eq. (1)], resulting in

$$R_{\mathrm{sec}} = R_{\mathrm{sift}}\Bigg[(1-\Delta)\left(q - H_2\left(\frac{e}{1-\Delta}\right)\right) - f\,(e)\cdot H_2(e)\Bigg], \tag{2}$$

where R_{sift} is the key rate after the basis reconciliation (sifting), $\Delta = 1-(1+\mu)e^{-\mu}/T\cdot\eta\cdot(1-e^{-\mu})$ the fraction of "tagged" pulses, η the detector efficiency, H_2 the binary entropy, and T is the overall transmission (in the static case $T = T_{\mathrm{Bob}}$). Assuming an error correction efficiency $f\,(e) = 1.22$, we obtained $R_{\mathrm{sec}} = 103.2$ kbps (without considering finite key effects).

B. Hand-held operation

The hand-held QKD tests were performed by four untrained users with two attempts each. The user removed the sender unit from its pedestal and aimed at the receiver entrance iris with the help of the visible beacon laser. Acoustic feedback informed the user about the quality of the aiming, where a low (high) pitch sound corresponded to a small (big) deviation from optimal pointing, respectively. Evidently, it is possible for a person to aim well at a point. Thus, no additional pointing hardware is required in the sender. The small fluctuations due to unsteady hands are compensated by the receiver tracking system.

In order to take the fluctuating transmission into account, additional post-processing steps had to be included in the data analysis [50–53]. The method used here is based on defining a certain transmission threshold value T_{thr} (corresponding to a link efficiency threshold ξ_{thr}) and discarding detection events where the transmission is too low. For the accepted events we conservatively assume T_{thr} as the transmission value for the evaluation of R_{sec} via Eq. (2). For each time bin k (of 10 ms) we then obtain a raw key rate

$$R_{\mathrm{raw}}(k,\xi_{\mathrm{thr}}) = \begin{cases} R_{\mathrm{raw}}(k) & \text{for } \xi(k) \geq \xi_{\mathrm{thr}}, \\ 0 & \text{for } \xi(k) < \xi_{\mathrm{thr}}. \end{cases}$$

There is an optimal T_{thr} because a low threshold level requires a high shrinkage of the key during privacy amplification, also due to a typically higher QBER, whereas a high threshold leads to discarding a large amount of data and thus a lower raw key rate. As it turned out, this value did not vary much for the different trials and could be defined in advance for a practical application.

Figure 3 shows traces of the raw key rate together with its corresponding QBER for two trials of different users. In order to also evaluate the time required to establish the connection with the receiver, we started to record detection events while the transmitter was still attached to the mount (but not necessarily optimally aligned as in Sec. IV A). The drop in transmission corresponds to the moment where the user picked up the sender, and the following period of low rate is due to the initial pointing attempt. On average

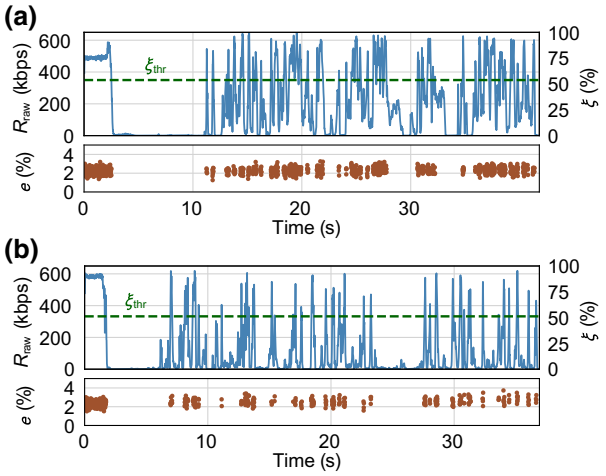

FIG. 3. Raw key rate R_{raw}, relative hand-held efficiency ξ and QBER e obtained in realistic key exchanges for two different untrained users (a) and (b) over a distance of about 30 cm. The rates are calculated for time bins of 10 ms. The threshold level ξ_{thr} is represented by a dashed green line.

the initial pointing took 8.5 s. We set the average photon number per pulse to $\mu = 0.042$, a value supporting a good key generation performance despite the different handling capabilities (shaking) of the users. The results are presented in Appendix C and show secret key rates between 4.0 kbps and 15.3 kbps, with an average value of 7.1 kbps and a mean QBER of 2.4%. We evaluated for each trial the link efficiency $\xi_{link} = 1/k_{link} \sum_k \xi(k)$ for the time intervals between first successful pointing and until the respective trial was stopped (corresponding to k_{link} time bins). Averaging over all trials we obtain a value as high as $\bar{\xi}_{link} = 21.1\%$ confirming the capabilities of our beam steering system.

The secret key rates could be further increased in the future by implementing a decoy protocol [54,55], an extension providing full security against photon-number splitting attacks even for a higher mean photon number per pulse. Although our current driver electronics equipment does not support this functionality, we were still able to conduct an analysis by extracting the relevant parameters from an additional experimental hand-held dataset. This dataset of seven key exchanges with three different users was obtained for a significantly higher $\mu = 0.153$ which would be allowed by the decoy protocol. There we measured an average QBER of 1.6%, close to the source intrinsic error of the transmitter unit of 1.5%, thus confirming the quality of our automatic reference-frame alignment. To estimate the possible performance, we use the formalism introduced in Ref. [56] for a protocol employing two decoy states (vacuum + weak decoy state). Assuming a fraction of 97% for signal pulses and a mean photon number for the weak decoy state of $\nu = 0.077$ would allow for an increased secret key rate with an average value exceeding 100 kbps. For a practical application it is also important that the key extraction can be performed with a mobile platform within a reasonable time. Preliminary tests with a smartphone showed sufficient processing capabilities even for on-the-fly data processing for the range of detection rates and QBER observed in this work.

V. CONCLUSION AND OUTLOOK

We have developed a micro-optics based QKD transmitter unit and assembled a prototype which features a very small footprint. The architecture is optimized for BB84-like protocols with weak polarized laser pulses at a wavelength of 850 nm and operates at 100 MHz repetition rate. The QKD beam is overlapped with a visible beacon laser facilitating both the beam tracking on the receiver's side, as well as clock synchronization between the two parties. Several untrained users tested our integrated hand-held transmitter unit and obtained on average a key generation rate of 7.1 kbps.

Further measurements have shown that the secret key rate can be increased by more than one order of magnitude. Equipping the sender electronics with such decoy capabilities should lead to only an insignificant increase of form factor and power consumption.

The ability to generate subnanosecond pulses, assuming that the electronics and single-photon detectors can also be upgraded to such speeds, suggests that the optoelectronics platform is suitable even for gigahertz operation. This will put the key rates into the Mbit/s range thereby enabling to exchange a significant amount of key during a short time.

Owing to its compact architecture, the presented transmitter unit could easily be integrated in other existing optical communication systems. It could provide secure key exchange for a variety of applications such as free-space links in urban areas, drones and high-attitude platforms or even small low-Earth orbit satellites enabling global secure communication.

ACKNOWLEDGMENTS

The authors thank G. Corrielli, A. Crespi, and R. Osellame at the Politecnico di Milano for the design and fabrication of the waveguide array, VI-Systems GmbH for providing the single-mode VCSELs, and A. Baliuka and M. Auer for helpful discussions. This project was funded by the excellence cluster Nano-Initiative Munich (NIM), Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC-2111 – 390814868, by EU project OpenQKD, and by BMBF Projects QUBE, QUBE-II, and DE-QOR.

APPENDIX A: OPTICAL TRANSMITTER UNIT

1. Components and architecture

a. VCSELs

The VCSEL array used in the prototype was fabricated by VI-Systems GmbH as a single chip (1×0.25 mm^2) and features four VCSELs with a low threshold ($I_b = 0.4$ mA) as well as transverse and longitudinal single-mode emission around 850 nm. Each laser is operated in the strong modulation regime, i.e., the diodes are biased below threshold and switched on for a short time period by an intense radiofrequency pulse. These conditions ensure the generation of bright, phase-randomized 200 ps long pulses with low background emission in the off state. The temporal overlap of the pulses originating from different channels was retrieved from a time-difference histogram [see Fig. 4(a)], where the arrival time of the attenuated pulse was measured with an avalanche photodiode featuring a jitter of 30 ps and a time-to-digital converter with a resolution of about 80 ps. The spectrum of these pulses was taken with a grating-based spectrometer with a resolution of 125 pm [Fig. 4(b)]. The observed spectral mismatch of the different laser diodes is less than 0.7 nm, but has to be further reduced by using selected or tunable diodes. Clearly, for hardware such as our sender module the open spectral side channel has to be closed but was accepted for this proof-of-principle experiment.

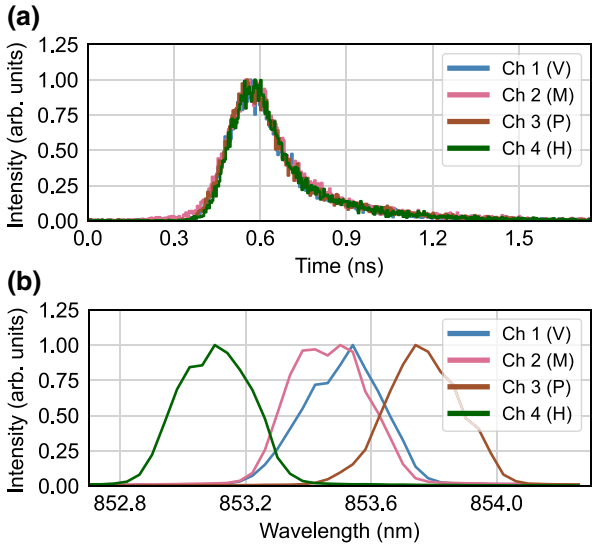

FIG. 4. Temporal and spectral properties of Alice's output pulses. (a) Time-difference histogram of the photons with respect to the 100 MHz clock showing the temporal shape of the optical pulses generated by the four channels. Precise synchronization of the channels and individual tailoring of the pulse parameters result in a high temporal overlap. (b) Spectrum obtained with a grating-based spectrometer with single-photon sensitivity featuring a resolution of 125 pm. Evidently, to avoid the spectral side-channel, selected or tunable diodes have to be used for secure applications.

b. Nano wire-grid polarizers

The geometry of the subwavelength nanowire gratings was carefully optimized using finite-difference time-domain simulations [34]. A gold film deposited onto a thin glass substrate was milled by a focused gallium ion beam. The choice of this manufacturing technique is motivated by its high etching resolution, crucial for the observation of extinction ratios above 30 dB (Table I), and by its capability to precisely control the relative orientation of the polarizers. Small polarization effects occurring within the waveguide chip could be determined beforehand and thus be precompensated by fabricating polarizers with certain linear polarizations, in order to obtain output states as close as possible to the states required for the BB84 protocol. The wire-grid polarizers feature a transmission of about 9% for the selected polarization, whereas the orthogonal polarization component is strongly reflected. As the VCSELs are sensitive to optical feedback, we placed a thin neutral density filter with a transmission of approximately 8% between the VCSEL array and the polarizers in order to avoid polarized retro-injection.

c. Waveguide chip

The three directional waveguide couplers ensuring the spatial mode overlap (see Fig. 5) of the four polarized beams were implemented in a aluminoborosilicate chip by femtosecond laser writing [35–37] by the Politecnico di Milano [57]. The low intrinsic birefringence ($\Delta n = 7 \times 10^{-5}$) of the waveguides introduces a global shift as small as 3π over the length of the chip. The polarization dependence of the coupling ratios was minimized by engineering a 3D layout [58] of the couplers [59] resulting in only small changes in the relative angles between the input polarization states after propagation through the waveguide. See Appendix A 2 for characterization of the resulting output states.

d. Collimating optics

For overlapping the signal and the beacon light a $3.5 \times 3.5 \times 3$ mm^3 dichroic beamsplitter from a commercial DVD player was used. The transmission for the 850 nm signal exceeds 99.8%, whereas the reflection amounts to 50% for the 680 nm beacon beam. The aspheric lens collimating both beams has a diameter of 3 mm and a focal

TABLE I. Extinction ratios (ERs) of the employed wire-grid polarizers at 850 nm, differences are due to variation of the grid parameters [34].

	H	$+45$	-45	V
ER	1800:1	1620:1	1200:1	1150:1

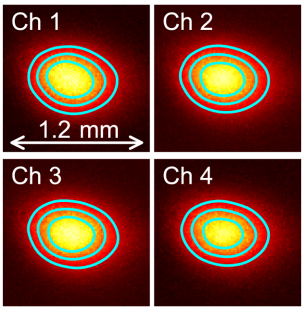

FIG. 5. Spatial mode distribution of the four output states of the sender unit. The pictures were taken with an EMCCD camera at a distance of about 50 cm from the sender's output aperture. The cyan contour lines of relative optical intensity are shown for facilitating visual comparison of the distributions.

length of 4.9 mm. This optics is well-suited for short-distance operation and maintains a compact architecture. Key exchanges over longer distances could be performed by combining the miniature sender unit with a telescope or with optical terminals of other free-space communication systems.

e. Micro-optics assembly

The careful characterization of the micro-optics components was followed by their precise positioning on the anodized aluminum micro-optical bench using a custom-made vacuum gripper mounted onto a standard six-axis stage. Repeated stacking and gluing of the components using a ultraviolet (UV) curing adhesive ensured a good mechanical stability of the optical setup. The distance between the optical parts was precisely controlled by an optimal combination of silica spacers whose thicknesses were selected according to Zemax simulations to achieve a high coupling efficiency. After the assembly we observed a rather uniform coupling efficiency close to 20% across the VCSEL array. The current prototype has a size of $35 \times 20 \times 8$ mm^3, although a size of $30 \times 3 \times 3$ mm^3 seems feasible by exploiting more suitable assembly techniques, a tighter cutting of the waveguide glass substrate and especially by reducing the size of the connector and of the printed circuit board (PCB) down to the minimal required area.

f. Compatibility with high volume manufacturing

Most of the elements (VCSELs, micro-lenses, spacers, filter, beamsplitter, and lens) are commercially available, and the few custom-made elements require only standard fabrication processes and could in principle be also manufactured in large series. For instance, the wire-grid polarizers have been fabricated using focused ion beam (FIB) milling, whereas other groups have demonstrated successful manufacturing of these elements using nanoimprint [60] or UV lithography [61,62]. In the case of femtosecond laser writing, the scanning speed can be as large as a few centimeters per second, and is thus viable for high-volume fabrication.

TABLE II. Tomographic data. (a) Complete tomography of the sender's output states measured with an additional arrangement of a polarizer, quarter waveplate, and an APD. The average degree of polarization (DOP) is 0.990 and the preparation quality [Eq. (1)] $q = 0.75$. (b) Partial tomography of the sender's states as measured by the receiver without compensation. The modulus of the third Stokes parameter S_3^* is calculated from S_1, S_2 with the assumption of unity DOP, reasonably confirmed by the complete tomography of the sender (a) beforehand. The sign is inferred from the polarization transformation within the receiver known from additional measurements. (c) Partial tomography of the sender's states as measured by the receiver with optimal compensation.

(a)

	H	V	$+45°$	$-45°$
S_1	0.944	−0.868	0.197	−0.326
S_2	−0.300	0.367	0.969	−0.918
S_3	0.120	−0.292	0.011	0.162

(b)

	H	V	$+45°$	$-45°$
S_1	0.938	−0.855	0.102	−0.234
S_2	−0.134	0.094	0.926	−0.858
S_3^*	0.319	−0.509	−0.362	0.457

(c)

	H	V	$+45°$	$-45°$
S_1	0.949	−0.971	−0.091	−0.007
S_2	0.004	0.068	0.982	−0.990
S_3^*	0.314	0.228	0.163	0.137

2. Analysis of the polarization states

The Stokes components of the polarization states were reconstructed by quantum state tomography entailing successive measurements in three different bases $\{H, V\}$,$\{\pm 45°\}$ and $\{R, L\}$:

$$S_1 = \frac{I_H - I_V}{I_H + I_V},$$
$$S_2 = \frac{I_{+45°} - I_{-45°}}{I_{+45°} + I_{-45°}},$$
$$S_3 = \frac{I_R - I_L}{I_R + I_L}.$$

Owing to the angle misalignment during the production of the polarizers, the sender output states [Table II(a)] are, on the one hand, jointly rotated and, on the other hand, also not perfectly mutually conjugated. Although the former can be compensated for at the receiver, the latter is accounted for during privacy amplification [Eq. (2)] by the

TABLE III. Hand-held measurements obtained for different users at a mean photon number $\mu = 0.042$. Here ξ_{link} represents the link efficiency, i.e., the ratio between the average rates observed in the hand-held case during link time and the rate in the static configuration, ξ_{thr} is the link efficiency threshold used for accepting data, R^*_{raw} the raw key rate after the time and threshold filtering, and R_{sec} the calculated asymptotic secure key rate according to Eq. (2).

User	Time (s)	Aiming (s)	ξ_{link} (%)	ξ_{thr} (%)	QBER (%)	R^*_{raw} (kbps)	R_{sec} (kbps)
1	30.5	8.0	34.5	53.8	2.3	140.3	15.3
2	31.0	4.0	13.9	51.2	2.6	43.9	4.0
3	33.0	17.0	20.6	51.2	2.2	76.1	8.4
4	40.5	6.0	19.0	45.2	2.6	69.3	5.3
1	33.5	9.5	16.9	60.7	2.4	46.3	5.4
2	41.0	6.0	20.5	62.0	2.3	41.3	5.0
3	61.0	10.0	20.2	52.9	2.3	68.6	7.2
4	39.5	7.5	23.3	61.9	2.5	59.6	6.4
Average	38.8	8.5	21.1	54.9	2.4	68.2	7.1

preparation quality q [Eq. (1)]. Tables II(b) and II(c) detail the states detected by the receiver before and after compensation of possibly rotated states of the sender and further rotations due to birefringent components in the receiver using a set of waveplates before the PAU. This simplifies the sender significantly, whereas the receiver can easily adopt to different transmitter polarization state orientations by communicating the respective tomographic data at the begin of a key exchange.

APPENDIX B: METHODS

1. Measurement of the transmission

The transmission through the receiver is defined by $T_{\text{Bob}} = I_{\text{PAU}*}/I_{\text{PAU}}$ determined by taking the ratio of two count rates where $I_{\text{PAU}*}$ is the average count rate of the light output by the Alice module (static configuration, pulsed mode) detected by the four APDs of the PAU, whereas I_{PAU} is obtained by coupling the light from the output of the Alice module into a multimode fiber (coupling efficiency of 83.3%) connected to one of the PAU APDs. These measurements were performed for each of the four output polarizations and then averaged resulting in $T_{\text{Bob}} = 40.9\%$.

2. Determination of the mean photon number

In order to determine the mean photon number μ we directly measured the count rate at the receiver. From this number (at a given repetition rate) μ can be extracted by using the receiver transmission, the specified efficiency of the detectors ($\eta = 38\%$) and accounting for the slightly polarization-dependent transmission and reflection coefficients, respectively, of the beamsplitter in the PAU as well as the corrections of nonlinearity of the detectors at high count rates.

APPENDIX C: HAND-HELD KEY EXCHANGE DATA

Table III lists the hand-held key exchange data.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Proc. IEEE Int. Conf. Comput., Syst. Signal Process., 175 (1984).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[4] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Inf. **2**, 16025 (2016).

[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).

[6] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, J. Cryptol. **5**, 3 (1992).

[8] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics **7**, 378 (2013).

[9] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[10] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[11] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Experimental demonstration of free-space decoy-state quantum key distribution over 144 km, Phys. Rev. Lett. **98**, 010504 (2007).

[12] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, Air-to-ground quantum communication, Nat. Photonics **7**, 382 (2013).

[13] S.-K. Liao, *et al.*, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).

[14] S.-K. Liao, *et al.*, Satellite-relayed intercontinental quantum network, Phys. Rev. Lett. **120**, 030501 (2018).
[15] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, Large scale quantum key distribution: challenges and solutions, Opt. Express **26**, 24260 (2018).
[16] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, Low cost and compact quantum key distribution, New J. Phys. **8**, 249 (2006).
[17] O. Elmabrok and M. Razavi, Wireless quantum key distribution in indoor environments, J. Opt. Soc. Am. B **35**, 197 (2018).
[18] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, A quantum access network, Nature **501**, 69 (2013).
[19] Y. Li, S.-K. Liao, X.-L. Chen, W. Chen, K. Cheng, Y. Cao, H.-L. Yong, T. Wang, H.-Q. Yang, W.-Y. Liu, J. Yin, H. Liang, C.-Z. Peng, and J.-W. Pan, Space-bound optical source for satellite-ground decoy-state quantum key distribution, Opt. Express **22**, 27281 (2014).
[20] D. M. Benton, P. M. Gorman, P. R. Tapster, and D. M. Taylor, A compact free space quantum key distribution system capable of daylight operation, Opt. Commun. **283**, 2465 (2010).
[21] D. Lowndes, S. Frick, A. Hart, and J. Rarity, A low cost, short range quantum key distribution system, EPJ Quantum Technol. **8**, 15 (2021).
[22] H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, D. O'Brien, and D. Bitauld, Handheld free space quantum key distribution with dynamic motion compensation, Opt. Express **25**, 6784 (2017).
[23] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, Chip-based quantum key distribution, Nat. Commun. **8**, 13984 (2017).
[24] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, Silicon photonic transmitter for polarization-encoded quantum key distribution, Optica **3**, 1274 (2016).
[25] M. Ziebell, M. Persechino, N. Harris, C. Galland, D. Marris-Morini, L. Vivien, E. Diamanti, and P. Grangier, in *2015 European Conference on Lasers and Electro-Optics - European Quantum Electronics Conference* (Optical Society of America, 2015).
[26] A. Orieux and E. Diamanti, Recent advances on integrated quantum communications, J. Opt. **18**, 083002 (2016).
[27] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, Metropolitan quantum key distribution with silicon photonics, Phys. Rev. X **8**, 021009 (2018).
[28] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, High-speed measurement-device-independent quantum key distribution with integrated silicon photonics, Phys. Rev. X **10**, 031030 (2020).
[29] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics, npj Quantum Inf. **7**, 93 (2021).
[30] T. K. Paraïso, T. Roger, D. G. Marangon, I. D. Marco, M. Sanzaro, R. I. Woodward, J. F. Dynes, Z. Yuan, and A. J. Shields, A photonic integrated quantum secure communication system, Nat. Photonics **15**, 850 (2021).
[31] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, Design and evaluation of a handheld quantum key distribution sender module, IEEE J. Sel. Top. Quantum Electron. **21**, 131 (2015).
[32] G. R. Bird and M. Parrish Jr., The wire grid as a near-infrared polarizer, J. Opt. Soc. Am. **50**, 886 (1960).
[33] M. Guillaumée, L. A. Dunbar, C. Santschi, E. Grenet, R. Eckert, O. J. F. Martin, and R. P. Stanley, Polarization sensitive silicon photodiodes using nanostructured metallic grids, Appl. Phys. Lett. **94**, 193503 (2009).
[34] G. Mélen, W. Rosenfeld, and H. Weinfurter, Impact of the slit geometry on the performance of wire-grid polarisers, Opt. Express **23**, 32171 (2015).
[35] K. M. Davis, K. Miura, N. Sugimoto, and K. Hirao, Writing waveguides in glass with a femtosecond laser, Opt. Lett. **21**, 1729 (1996).
[36] R. R. Gattass and E. Mazur, Femtosecond laser micromachining in transparent materials, Nat. Photonics **2**, 219 (2008).
[37] G. D. Valle, R. Osellame, and P. Laporta, Micromachining of photonic devices by femtosecond laser pulses, J. Opt. A: Pure Appl. Opt. **11**, 13001 (2009).
[38] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).
[39] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, Information leakage via side channels in freespace BB84 quantum cryptography, New J. Phys. **11**, 065001 (2009).
[40] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, Spatial mode side channels in free-space QKD implementations, IEEE J. Sel. Top. Quantum Electron. **21**, 187 (2015).
[41] H. A. Davani, B. Kögel, P. Debernardi, C. Grasse, C. Gierl, K. Zogal, A. Haglund, J. Gustavsson, P. Westbergh, T. Gründl, P. Komissinskiy, T. Bitsch, L. Alff, F. Küppers, A. Larsson, M.-C. Amann, and P. Meissner, Polarization investigation of a tunable high-speed short-wavelength bulk-micromachined MEMS-VCSEL, Proc. SPIE **8276**, 82760T (2012).
[42] C. Gierl, T. Gründl, S. Paul, K. Zogal, M. T. Haidar, P. Meissner, M.-C. Amann, and F. Küppers, Temperature characteristics of surface micromachined MEMS-VCSEL with large tuning range, Opt. Express **22**, 13063 (2014).
[43] V. D'Ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, Complete experimental toolbox for alignment-free quantum communication, Nat. Commun. **3**, 961 (2012).
[44] P. Zhang, K. Aungskunsiri, E. Martin-Lopez, J. Wabnig, M. Lobino, R. W. Nock, J. Munns, D. Bonneau, P.

Jiang, H. W. Li, A. Laing, J. G. Rarity, A. O. Niskanen, M. G. Thompson, and J. L. O'Brien, Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client, Phys. Rev. Lett. **112**, 130501 (2014).

[45] G. B. Xavier, G. V. de Faria, T. F. da Silva, G. P. Temporão, and J. P. von der Weid, Active polarization control for quantum communication in long-distance optical fibers with shared telecom traffic, Microw. Opt. Technol. Lett. **53**, 2661 (2011).

[46] B. L. Higgins, J.-P. Bourgoin, and T. Jennewein, Practical polarization-frame alignment for quantum key distribution with single-photon-level resources (2020).

[47] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch, Phys. Rev. A **91**, 062301 (2015).

[48] For better comparability, in the static configuration we set μ to a value which was optimized and used for the hand-held case.

[49] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[50] A. A. Semenov and W. Vogel, Quantum light in the turbulent atmosphere, Phys. Rev. A **80**, 021802 (2009(R)).

[51] A. A. Semenov and W. Vogel, Entanglement transfer through the turbulent atmosphere, Phys. Rev. A **81**, 023835 (2010).

[52] C. Erven, B. Heim, E. Meyer-Scott, J. P. Bourgoin, R. Laflamme, and G. Weihs, and T. Jennewein, Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere, New J. Phys. **14**, 123018 (2012).

[53] G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villoresi, Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels, Phys. Rev. A **91**, 042320 (2015).

[54] Xiang-Bin Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[55] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[56] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[57] G. Mélen, T. Vogl, M. Rau, G. Corrielli, A. Crespi, R. Osellame, and H. Weinfurter, Integrated quantum key distribution sender unit for daily-life implementations, Adv. Photon. Quantum Comput., Memory, Commun. IX **9762**, 31 (2016).

[58] R. Heilmann, M. Gräfe, S. Nolte, and A. Szameit, Arbitrary photonic wave plate operations on chip: realizing Hadamard, Pauli-X, and rotation gates for polarisation qubits, Sci. Rep. **4**, 4118 (2014).

[59] L. Sansoni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi, and R. Osellame, Two-particle bosonic-fermionic quantum walk via integrated photonics, Phys. Rev. Lett. **108**, 010502 (2012).

[60] S.-W. Ahn, K.-D. Lee, J.-S. Kim, S. H. Kim, J.-D. Park, S.-H. Lee, and P.-W. Yoon, Fabrication of a 50 nm half-pitch wire grid polarizer using nanoimprint lithography, Nanotechnology **16**, 1874 (2005).

[61] I. Verrier, T. Kämpfe, F. Celle, A. Cazier, M. Guttmann, B. Matthis, J. Laukkanen, F. Lacour, C. Veillas, S. Reynaud, O. Parriaux, and Y. Jourlin, Wire-grid polarizer using galvanic growth technology: demonstration of a wide spectral and angular bandwidth component with high extinction ratio, Opt. Eng. **54**, 047105 (2015).

[62] X. Liu, X. Deng, P. Sciortino, M. Buonanno, F. Walters, R. Varghese, J. Bacon, L. Chen, N. O'Brien, and J. J. Wang, Large area, 38 nm half-pitch grating fabrication by using atomic spacer lithography from aluminum wire grids, Nano Lett. **6**, 2723 (2006).