High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers

G. Cañas,[1,2,3] N. Vera,[1,2,3] J. Cariñe,[2,3,4] P. González,[1,2,3] J. Cardenas,[2,4] P. W. R. Connolly,[1,2,3,*] A. Przysiezna,[5] E. S. Gómez,[1,2,3] M. Figueroa,[2,4] G. Vallone,[6,7] P. Villoresi,[6,7] T. Ferreira da Silva,[8] G. B. Xavier,[2,3,4] and G. Lima[1,2,3,†]

[1]*Departamento de Física, Universidad de Concepción, 160-C Concepción, Chile*

[2]*Center for Optics and Photonics, Universidad de Concepción, 160-C Concepción, Chile*

[3]*Millenium Science Initiative, Nucleus for Advanced Optics, Universidad de Concepción, 160-C Concepción, Chile*

[4]*Departamento de Ingeniería Eléctrica, Universidad de Concepción, 160-C Concepción, Chile*

[5]*Institute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-308 Gdańsk, Poland*

[6]*Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova 35131, Italy*

[7]*Istituto di Fotonica e Nanotecnologie, Consiglio Nazionale delle Ricerche, Padova 35131, Italy*

[8]*Optical Metrology Division, National Institute of Metrology, Quality and Technology, 25250-020, Duque de Caxias, Rio de Janeiro, Brazil*

(Received 20 March 2017; published 18 August 2017)

Multiplexing is a strategy to augment the transmission capacity of a communication system. It consists of combining multiple signals over the same data channel and it has been very successful in classical communications. However, the use of enhanced channels has only reached limited practicality in quantum communications (QC) as it requires the manipulation of quantum systems of higher dimensions. Considerable effort is being made towards QC using high-dimensional quantum systems encoded into the transverse momentum of single photons, but so far no approach has been proven to be fully compatible with the existing telecommunication fibers. Here we overcome such a challenge and demonstrate a secure high-dimensional decoy-state quantum key distribution session over a 300-m-long multicore optical fiber. The high-dimensional quantum states are defined in terms of the transverse core modes available for the photon transmission over the fiber, and theoretical analyses show that positive secret key rates can be achieved through metropolitan distances.

DOI: 10.1103/PhysRevA.96.022317

I. INTRODUCTION

Over the last decades we have witnessed the advances of telecommunication technologies by experiencing a huge increase in our capacity to send or download data. This has been vastly based on the development of new techniques to multiplex information in different degrees of freedom of light transmitted over an optical fiber, which have allowed their information capacity to be increased around tenfold every four years [1]. Analogously, in quantum communications (QC), the use of high-dimensional quantum systems allows for more information to be transmitted between the communicating parties [2–5]. Fortunately, it turns out that such systems can be created by also exploring the degrees of freedom of faint light pulses and, therefore, most of the multiplexing strategies developed for classical telecommunications are to some extent connected to the implementation of high-dimensional secure QC.

Experimental high-dimensional quantum cryptography is still in its infancy, but secure communications based on the use of high-dimensional quantum systems encoded into the transverse momentum of single photons has been the subject of many recent experimental efforts [6–10], and theoretical analyses [5,11–16]. The motivation comes from the versatility it provides since it can be used to define an infinite-dimensional Hilbert space in terms of the orbital angular momentum (OAM) of Laguerre-Gaussian modes [17], or also in terms of the number of linear transverse modes available for photon transmission [18]. OAM-encoded quantum systems are suitable for communication over free-space links due to their resilience against atmospheric turbulence [19], while on the other hand, path-encoded states are suitable for communications systems based on waveguide integrated circuits [20]. However, no research so far has accomplished a secure QC session while propagating such quantum states over the available telecommunication optical fibers, thus severely limiting real-world applications.

Here we take a major step to overcoming this challenge and demonstrate a secure high-dimensional quantum key distribution (HD-QKD) session between two parties communicating over a 300-m-long telecommunication optical fiber, whose security is guaranteed by resorting to the decoy-state method [21–23]. Our technique is built upon multicore optical fibers, now used in classical telecommunications for space-division multiplexing [1]. In our scheme we are able to coherently propagate quantum signals over the entire multicore fiber, thus, allowing high-fidelity transmission of four-dimensional quantum systems that are encoded into the four core modes available in the fiber. Using a standard InGaAs gated single-photon detector, with a detection efficiency of 6% and a dark count probability of 2.25×10^{-7}, we obtain a secret key bit generation rate per pulse of $(4.31 \pm 1.19) \times 10^{-6}$. This is equivalent to the generation of approximately 15 secret bits per hour at the system current clock rate of 1 KHz. We prove the HD-QKD session to be highly stable, maintaining an overall quantum bit error rate (QBER) of $(10.25 \pm 0.6)\%$ over more than 20 hours of continuous operation. The decoy-state analysis also shows that our technique enables a positive secret key rate over metropolitan distances.

*Current address: Physics Department, David Brewster Building, Heriot-Watt University, Edinburgh EH14 4AS, Scotland.

†glima@udec.cl

Compared to conventional qubit-based QKD over a single spatial mode, our results reflect that HD-QKD is still in a very early stage of development. Nonetheless, it is in this context that this work becomes relevant. It proves the viability of transmitting with high-fidelity high-dimensional BB84 QKD states encoded into the transverse momentum of single-photons, and also paves the way for future research on the use of multicore fibers for HD quantum cryptography. As we discuss in the concluding remarks and Appendix C, there are new technological developments on solid-state devices compatible with multicore fibers, which shall allow for much faster and longer distance HD-QKD schemes in the near future.

II. IMPLEMENTATION AND RESULTS

By far the most widely used QKD protocol is BB84, which requires a prepare-and-measure scheme [24]. The BB84 QKD session consists of Alice (the transmitter) randomly encoding bits of information onto single photons and then sending them to Bob (the receiver) over an optical fiber or a free-space link. Alice's encoding procedure randomly chooses between states from two mutually unbiased bases (MUBs), and Bob independently also randomly chooses states between the same two MUBs to perform a projective measurement on each photon [2]. The four-dimensional BB84 QKD session requires that Alice and Bob prepare eight states spanning two MUBs. These states will be denoted by $|\varphi_i^{(j)}\rangle$, where $i = 1,2,3,4$ refers to the ith state of the jth MUB, with $j = 1,2$. The states of the first MUB are defined by $\langle\varphi_1^{(1)}| = \frac{1}{2}[1,1,1,1]$, $\langle\varphi_2^{(1)}| = \frac{1}{2}[1,-1,1,-1]$, $\langle\varphi_3^{(1)}| = \frac{1}{2}[1,1,-1,-1]$, and $\langle\varphi_4^{(1)}| = \frac{1}{2}[1,-1,-1,1]$. The second MUB states are $\langle\varphi_1^{(2)}| = \frac{1}{2}[1,1,1,-1]$, $\langle\varphi_2^{(2)}| = \frac{1}{2}[1,1,-1,1]$, $\langle\varphi_3^{(2)}| = \frac{1}{2}[1,-1,1,1]$, and $\langle\varphi_4^{(2)}| = \frac{1}{2}[-1,1,1,1]$. They are written on the basis of the four core modes shown in Fig. 1.

One major problem in QKD implementations is the fact that practical single-photon sources are not available, such that attenuated lasers producing weak coherent states must be used. The main issue when using these sources is that an eavesdropper may perform the so-called "photon-number splitting" attack on pulses that contain more than one photon [25]. The solution to this problem is the decoy-state method [21–23], where Alice and Bob can estimate more precisely the fraction of detected single-photon pulses and determine whether an eavesdropper is present. Due to its relatively straightforward implementation, the decoy-state method has been widely used [26–32]. In our implementation we use its generalization for the HD-QKD BB84 protocol [5,11]. We employ an attenuated telecom distributed feedback laser, whose emission wavelength is 1546.32 nm, as our light source (Fig. 1). The laser operates in continuous wave mode and is externally modulated by a Mach-Zehnder electrooptical modulator (MZ), generating 500-ps-wide optical pulses. A calibrated optical attenuator (ATT) is used to set the desired average photon number per pulse, μ, at Alice's output. In our work, the highest average photon number per pulsed adopted was $\mu = 0.27$. In this case, pulses containing only one photon are the vast majority of the nonnull pulses generated (∼90%). The repetition frequency for the optical pulses is set to 1 kHz in this first demonstration. Nonetheless, much faster clock rates

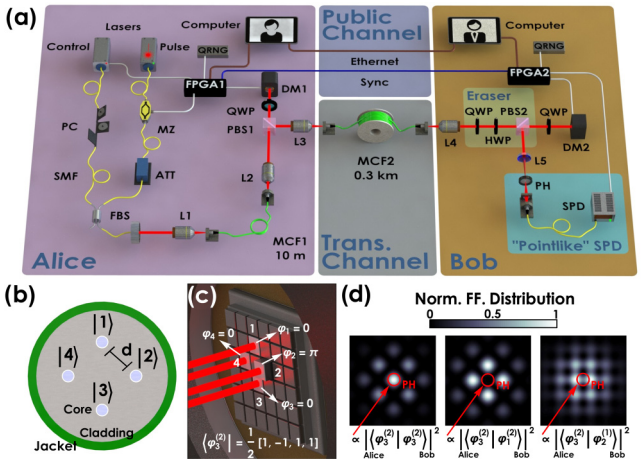

FIG. 1. (a) Experimental setup: Alice encodes the four-dimensional BB84 QKD states using a deformable mirror (DM1). The communication link consists of a 300-m-long four-core multicore fiber. Bob uses a deformable mirror (DM2) and a SPD to implement his measurements. See main text. (b) The multicore fiber's cross section. (c) The deformable mirror is composed of a 6 × 6 mirror matrix. Light coming from each MCF's core is mapped to an individual mirror. As an example, in (c) cores $|1\rangle$, $|3\rangle$, and $|4\rangle$ have a relative phase of 0 applied, while $|2\rangle$ has a π relative phase shift. (d) Simulated FF distribution with the pinhole area indicated by red circle. The first case is when Bob's projection is performed on the same state as the one Alice sent. It displays constructive interference. The second case is with an orthogonal projection, leading to no detection. The last case is when Alice and Bob use different MUBs. HWP (QWP): half (quarter) wave plate. PBS: polarizing beamsplitter.

can be obtained as we discuss in the concluding remarks. Last, note that since the period between consecutive pulses is longer than the coherence time of the laser (∼0.1 μs), there is no need of active phase randomization of the pulses to avoid security loopholes [33].

The attenuated pulses are used by Alice to encode the required high-dimensional quantum states. For this purpose they are initially coupled into a 10-m-long multicore fiber (MCF1), composed of four single-mode cores, by means of a 10× objective lens (L1) [See Figs. 1(a) and 1(b)]. The core mode field diameter is 8.5 μm and the cores are separated by $d = 36.25\,\mu$m to ensure that cross-talk effects are negligible. All cores of the fiber are equally illuminated. Thus, the probability amplitudes for the photon transmission by each core are equally weighted. Contrary to standard fiber arrays, the cores of multicore fibers lie within the same cladding, ensuring that random phase-fluctuations induced by thermal and mechanical stress are strongly suppressed. Therefore, the state of the photons transmitted over the MCF1 is a coherent superposition given by $|\Psi\rangle = \frac{1}{2}\sum_1^4 e^{i\phi_l}|l\rangle$, where $|l\rangle$ denotes the state of the photon transmitted by the lth transverse core mode, and ϕ_l is the relative phase acquired during the propagation over the lth core. This is the fiducial state which is then used to prepare the required ones for the four-dimensional BB84 QKD session. This is done by imaging the output face of MCF1 onto a deformable mirror (DM1) by means of a second 10× objective lens (L2). The 10× magnification factor is chosen such that the image of each

core is formed at different mirrors, as shown schematically in Fig. 1(c). Each mirror's longitudinal position can be set individually. By defining different offset positions for the four mirrors, the residual phases ϕ_l are compensated and the first state $|\varphi_1^{(1)}\rangle$ prepared. The other QKD states are generated with the mirrors at positions that correspond to phase-shifts $\varphi_l = \pi$.

The attenuated pulses are then coupled to a 300-m-long multicore fiber (MCF2), comprising the transmission channel. After transmission through MCF2, the photon is detected at Bob's station for state analysis. Bob's detection scheme is similar to the one used by Alice. The output face of MCF2 is magnified at a second deformable mirror (DM2) and the relative-phase of each core is addressed individually by four independent mirrors. To define a common shared referential frame, like in fiber-based polarization schemes, Bob first defines the offset positions of the four mirrors for detecting the state $|\varphi_1^{(1)}\rangle$, when Alice is also sending such state. Thus, compensating residual phase-shifts ϕ_l' acquired over MCF2. By placing one "pointlike" single-photon detector (SPD) at the DM2's far-field (FF) plane, and properly adjusting the mirrors longitudinal positions to set phase-shifts, Bob can detect any state $|\varphi_i^{(j)}\rangle$ required for the four-dimensional BB84 QKD session. In our case the "pointlike" SPD is composed of a pinhole (PH) fixed at the center of the FF plane of a lens L5 ($f_{L5} = 7.5$ cm), a single-mode fiber, and an InGaAs avalanche detector. The probability of photon detection at the center of the FF plane C_s is proportional to the overlap between the generated and detected states (see Refs. [8,34] and Fig. 1(d)). Note that the use of the "single detector scheme" for the implementation of the four-dimensional QKD is just for sake of practicability to demonstrate the viability of multicore fibers for secure HD-QC. It does not represent a limiting issue of the presented technique as we discuss in the concluding remarks. Lastly, for the sake of completeness, we show in Appendix A that this single detector four-dimensional BB84 scheme can still outperforms some traditional qubit based approaches.

The multicore fiber is intrinsically robust against random-phase fluctuations. Nonetheless for long multicore fibers, like MCF2, slowly varying phase-drifts can still be observed. This effect deteriorates the referential frame shared by Alice and Bob, resulting in a mean QKD state fidelity ($\bar{F} \equiv 1 - \mathrm{QBER}$) that varies over time. The typical behavior observed is shown in Fig. 2(a). This renders HD-QKD over long multicore fibers not practical if not addressed. To overcome this problem we developed a control system. It checks the shared referential of Alice and Bob over time intervals of 30 s and the control routine is initialized if the QBER surpasses a defined threshold value. During the control procedure the QKD session, explained next, is interrupted. The control system is composed of a laser that is multiplexed into the multicore fibers and two field-programmable gate arrays (FPGA1 and FPGA2) electronic modules that actively control the deformable mirrors. Based on a custom designed closed-loop maximum-power-point-tracking algorithm, the control system varies the offset positions of all the active mirrors used on the QKD session until the recorded QBER is below our threshold of 12%. Then, it is turned off and the QKD session restarts. The resulting effect of the control system is shown into Fig. 2(a). It allows the stabilization of the shared referential frame,

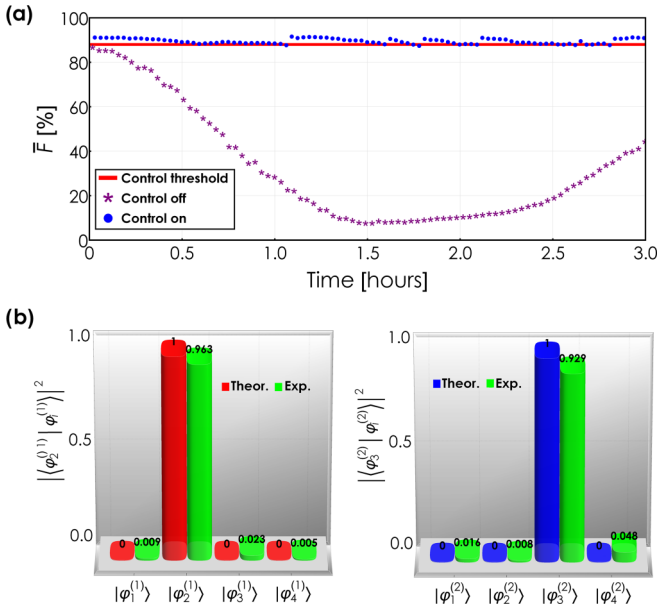

FIG. 2. (a) Mean QKD fidelity of the four-dimensional BB84 states transmitted through the 300-m-long multicore fiber. With the control system off, the fidelity slowly degrades. With the control on, the fidelity remains above the threshold, enabling stable QKD sessions. (b) Two examples of measured fidelities after 1.08 hours, for the states $|\varphi_2^{(1)}\rangle$ and $|\varphi_3^{(2)}\rangle$.

critical for long-term QKD sessions. In Fig. 2(b) we show the fidelity for the states $|\varphi_2^{(1)}\rangle$ and $|\varphi_3^{(2)}\rangle$ at 1.08 hours. The mean fidelity is $\bar{F}_{1.08} = (92.05 \pm 0.03)\%$ and the fidelity of each state is $(96.31 \pm 0.03)\%$ and $(92.93 \pm 0.03)\%$, respectively. Note that at Alice's site polarizing optics are used to ensure no coupling between the polarization and the core modes. It is also important to consider that polarization drifts may occur over long fibers, such that the core modes get marked by different polarizations. Fortunately, this effect is compensated with a polarization filter to erase the which-path information (see Fig. 1).

The four-dimensional QKD session is also implemented by the FPGAs. Alice's FPGA1 generates a 1-kHz synchronization signal which is shared to Bob's FPGA2. Then, FPGA1 reads a number from an idQuantique quantum random number generator (QRNG), which determines whether MUB $j = 1$ or $j = 2$ will be used, and which of the $|\varphi_i^{(j)}\rangle$ states from that MUB will be created at the DM1. Bob's FPGA2 will receive the same sync pulse almost simultaneously as Alice generates it. He then also takes a number from his QRNG and chooses one of the two MUBs and one of the corresponding four states in which to project the incoming photon. A delayed version of the synchronization pulse is fed in the gated-mode single-photon detector (idQuantique id210), with the gate width adjusted to 0.85 ns. FPGA2 then checks whether there was a photon detection in the SPD for each sync pulse. Both FPGAs record the chosen MUB and states. The FPGAs compare the detected strings after basis reconciliation to calculate the QBER.

The secret key rate (R) as a function of the dimension d is given by $R \geqslant Q_0 \log_2 d + Q_1[\log_2 d - H_d(e_1)] -$

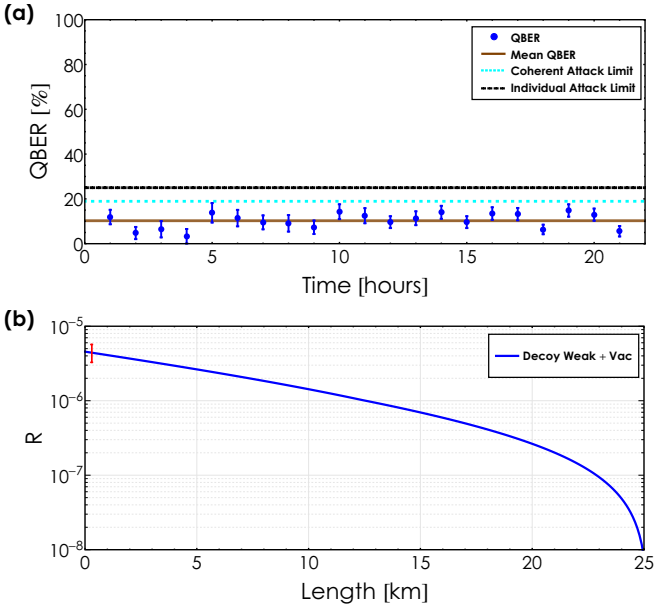

FIG. 3. (a) Measured QBER over time (blue dots). The brown line is the average QBER of 10.25%. The dashed black and cyan lines are the bounds to achieve positive key rate against individual (25%) and coherent (18.93%) attacks, respectively. (b) Secret key rate (R) as a function of distance for the weak decoy + vacuum protocol. The point is the actual key generation rate in our QKD session.

$Q_\mu H_d(E_\mu) f(E_\mu)$, where Q_0 and Q_1 are the gains of the vacuum and single photon states, respectively. Q_μ is the gain for an average μ photon number. $H_d(x) = -x\log_2[x/(d-1)] - (1-x)\log_2(1-x)$ is the d-dimension modified Shannon entropy of the QBER [11]. e_1 is the single-photon error rate, E_μ is the overall quantum bit error rate (QBER), and $f(E_\mu)$ is the inefficiency of the error correction function. Q_0, Q_μ, and E_μ can be directly measured, while Q_1 and e_1 must be estimated by the decoy state method [35].

In the experiment, we first performed a long-term automated measurement to demonstrate the stability achieved in our experiment by performing a BB84 QKD session over the 300 m of multicore fiber, while employing an average photon number per pulse $\mu = 0.27$. The results are shown in Fig. 3(a), where we have an average of 44.5 detections per hour, with an overall QBER of 10.25% (basically limited by optical mismatch and accidental counts). Then we performed a key exchange QKD section whose security is guaranteed by the practical vacuum + weak decoy protocol (see Appendix B for details). We employed a passive modulation of the decoy protocol with the value of $\mu = 0.2$ for the signal, and the decoy states defined by $\nu = 0.1$ and vacuum. The measured parameters used to calculate the key rate R at the distance of 300 m were $Q_\mu = (9.31 \pm 0.63) \times 10^{-6}$, $E_\mu = (10.8 \pm 1.4)\%$, $Q_\nu = (4.89 \pm 0.30) \times 10^{-6}$, $E_\nu = (9.0 \pm 1.3)\%$, $Y_0 = (2.06 \pm 0.23) \times 10^{-7}$, and $E_0 = (71.1 \pm 3.4)\%$. We obtain a secret key generation rate per pulse of $(4.31 \pm 1.19) \times 10^{-6}$, plotted as the red dot in Fig. 3(b). Our calculation returns a lower bound for the single-photon gain $Q_1^L = (6.96 \pm 1.30) \times 10^{-6}$ and an upper bound of the single-photon error rate $e_1^U = (7.53 \pm 2.20)\%$. Note that within the experimental errors, the obtained value of e_1^U is in accordance with the expected one of $e_{1_{\text{theo}}}^U = 9.70\%$. The blue curve in Fig. 3(b) represents the expected key rate as a function of the MCF based channel length in our actual experimental configuration (see Appendix B for details), showing its viability for parties separated by more than 20 km.

III. CONCLUSION

The presented technique has the potential to provide a transformative HD-QKD network. Recent engineering developments, compatible with MCFs, will allow our experiment to be translated to an operational system capable of outperforming qubit communication. For instance, the adopted bulk single detector scheme (responsible of 24.5 dB of losses due to the use of a pinhole) can now be replaced by a fully integrated and low-loss d detector scheme (see Appendix C). It is based on the recent development of a MCF multiport beamsplitter that is built using a new technique to cut and splice MCFs [36]. Thus, allowing HD-QKD over distances similar to the qubit-based approach. The HD-QKD clock repetition rate can also be increased to the limits achieved with qubit systems (>1 GHz), while providing more information per round. As shown in Appendix C, a new MCF demultiplexer [37] can be used to couple fast fiber-based phase-modulators [38] to each core mode, thus allowing faster encoding or decoding of the BB84 QKD high-dimensional states. In our case, the limitation of the 1-KHz rate was mainly due to the response time of the DMs. Lastly, note that the viability of using MCFs with silicon chips [39], to multiplex classical and quantum signals [40], and to propagate entangled states [41], highlights MCFs as a new tool for several QC tasks.

Quantum key distribution is the most successful protocol of QC with many different demonstrations performed across several distinct scenarios. The interest on QKD is only expected to grow and considerable effort is being made to increase QC's information content by using the transverse momentum of a single-photon [6–10]. In our work we demonstrate the first fiber-based automated and secure decoy-state HD-QKD session, which relies on four-dimensional systems encoded onto the transverse core modes available for the photon transmission over a 300-m-long multicore optical fiber. Our results set the stage for future implementations of high-dimensional QC over the telecommunication infrastructure.

ACKNOWLEDGMENTS

The authors thank Jan-Åke Larsson for valuable discussions. This work was supported by Fondecyt 1160400, Fondecyt 1150101, CONICYT PFB08-024, and Milenio RC130001. G.C. acknowledges support from Fondecyt 11150324. E.S.G. acknowledges support from Fondecyt 11150325. M.F. acknowledges support from Fondecyt 1151278. J.C. acknowledges support from Fondecyt 3170596. P.W.R.C. acknowledges University of Birmingham Careers Network. A.P. acknowledges NCN Grant No. 2014/14/M/ST2/00818. N.V. and P.G. acknowledge CONICYT.

G.C., N.V., and J.C. contributed equally to this work.

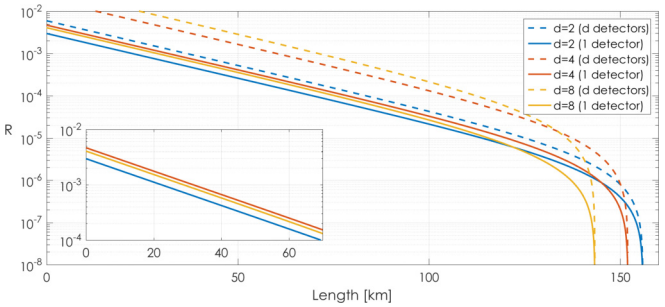

FIG. 4. Secret key rate for d-dimensional Hilbert spaces when considering a single-detector and a d-detector scheme configuration. Here we perform secret key rate simulations considering the infinite decoy case, while using as input parameters the experimental data from [42]. In the d-detector case, as expected, the rate increases for shorter distances and the cutoff point in the secret rate versus distance curve occurs for shorter distances, as d increases. In the single-detector case, the probability of correctly projecting the transmitted state onto itself decreases linearly with d, while the information gain per transmitted photon only increases with $O[\log(d)]$. Thus, the case of $d = 8$ always generates a lower secret key rate when compared to $d = 4$. Nonetheless, as shown on the inset, our implementation (i.e., the $d = 4$ case) is capable of beating the $d = 2$ case.

APPENDIX A: d DETECTOR VERSUS 1 DETECTOR QKD SCHEME

Similarly to classical communications, the use of higher dimensions to encode more information has interesting consequences. In the case of a HD-QKD, there are two approaches: a single-detector randomly placed at each possible output (the one done in this work), or having d detectors, one at each output. In the d detector case, as expected, the rate increases for shorter distances and the cutoff point in the secret rate versus distance curve occurs for shorter distances, as d increases (Fig. 4). This is due to the fact that for each detection round, the total dark count probability is higher, compared to the two-dimensional case, as there are d detectors. The single-detector case is more interesting, as can be also be seen in Fig. 4. In this case, the probability of correctly projecting the transmitted state onto itself decreases linearly with d, while the information gain per transmitted photon only increases with $O[\log(d)]$. Nonetheless, as shown on the inset of Fig. 4, our implementation (i.e., the $d = 4$ case) is capable of beating $d = 2$ for all distances until the dark count probability gets too strong at the cutoff point.

APPENDIX B: DECOY-STATE SECRET KEY GENERATION RATE PROBABILITY

Here we show how the secret key generation probability R of our HD-QKD system is derived using the decoy-state approach [21–23]. Our analysis follows the method of Ref. [35], and modifications are performed when necessary for dealing with the high-dimensional case. We also show how the key rate is estimated as a function of the distance.

The secret key generation probability for d-dimensional systems is given by [35,43]

$$R \geqslant Q_0 \log_2 d + Q_1[\log_2 d - H_d(e_1)] - Q_\mu H_d(E_\mu) f(E_\mu), \tag{B1}$$

where Q_0 and Q_1 are the gains of the vacuum and single-photon states, respectively. Q_μ is the overall gain (i.e., the probability of obtaining a detection when the signal state is sent), E_μ is the overall error rate, while e_1 is the error rate of the single-photon states. $H_d(x) = -x \log_2 [x/(d-1)] - (1-x)\log_2(1-x)$ is the d-dimensional modified Shannon entropy of the QBER [11]; $f(E_\mu)$ is the inefficiency of the error correction function. We employ $f(E_\mu) = 1.05$ [44] and consider the use of the efficient BB84 protocol [45].

The values of Q_μ and E_μ are directly obtained from the experimental data when Alice sends signal pulses. On the other hand, the parameters associated to single-photon pulses (Q_1 and e_1) and vacuum (Q_0) cannot be directly measured. They must be inferred through the use of a numerical approach based on the decoy-state technique [46]. A practical implementation of the decoy technique consists on using only one weak (with average photon flux $\nu < \mu$) and vacuum decoy states. Under this approach, Q_0 can be directly estimated as $Q_0 = e^{-\mu} Y_0$, where Y_0 is the measured yield of the vacuum states (i.e., the probability of detection measured when no photons are sent from Alice). On the other hand, a lower bound Q_1^L on Q_1, and an upper bound e_1^U of e_1, can be written as [35]

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left[Q_\nu e^\nu - \frac{\nu^2}{\mu^2} Q_\mu e^\mu - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right], \tag{B2}$$

and

$$e_1^U = (E_\nu Q_\nu \mu e^\nu - \mu e_0 Y_0)/\left(\nu Q_1^L e^\mu\right), \tag{B3}$$

with Q_ν and E_ν measured with the weak decoy state. These values are fed into Eq. (B1) to calculate the experimental secret key rate.

The same method can be exploited to derive the expected key rate as a function of the channel length. In this case the values of Q_μ, Q_ν, E_μ, and E_ν can be estimated by assuming the propagation in a lossy channel. When using a photon source modelled as an incoherent mixture of Fock states, given by the Poisson distribution $P_n = \mu^n e^{-\mu}/n!$, the overall gain and QBER values are computed through the summation over all possible states. Thus, $Q_\mu = \sum_{n=0}^{\infty} Y_n P_n$ and $E_\mu = (1/Q_\mu)\sum_{n=0}^{\infty} e_n Y_n P_n$. In the above expression Y_n is the n-photon yield, defined as the probability of detection at Bob's station when Alice sends an n-photon Fock state and

TABLE I. System parameters for estimation of the secret key generation probability as a function of transmission distance.

	Q_μ	E_μ	Q_1	e_1
d detectors	$Y_0 + 1 - e^{-\mu\eta}$	$\frac{e_0 Y_0 + e_{opt}(1-e^{-\mu\eta})}{Y_0 + 1 - e^{-\mu\eta}}$	$(Y_0 + \eta)\mu e^{-\mu}$	$\frac{e_0 Y_0 + e_{opt}\eta}{Y_0 + \eta}$
Single detector	$Y_0 + \frac{1-e^{-\mu\eta}}{d}$	$\frac{e_0 Y_0 d + e_{opt}(1-e^{-\mu\eta})}{Y_0 d + 1 - e^{-\mu\eta}}$	$(Y_0 + \frac{\eta}{d})\mu e^{-\mu}$	$\frac{e_0 Y_0 d + e_{opt}\eta}{Y_0 d + \eta}$

e_n is the corresponding error. The n-photon gain, $Q_n = Y_n P_n$, results from the product of the yield Y_n and the probability P_n of the state being produced by Alice.

In a lossy channel the expected value of Y_n is $Y_n \approx Y_0 + \eta_n$, where Y_0 is the vacuum yield related to the dark count probability of the SPD (P_{dark}). The parameter $\eta_n = 1 - (1 - \eta)^n$ is related to the overall efficiency η of the channel given by the detector efficiency and the internal transmittance of Bob's apparatus ($\eta_{\text{SPD}} = 6.09\%$ and $\eta_{\text{Bob}} = 24.5$ dB respectively, corresponding to values of our implementation). The link transmittance is given by $10^{-\alpha L/10}$, with the attenuation coefficient represented by α [dB/km] and the transmission link length given by L [km]. In our case, the multicore fiber used (Fibercore) has $\alpha = 0.4$ dB/km. The error associated to the n-photon states can be estimated to be $e_n = (e_0 Y_0 + e_{\text{opt}} \eta_n)/Y_n$, where e_{opt} is due to the optical misalignment of the detection system and is estimated to be $e_{\text{opt}} = (9.64 \pm 0.98)\%$ in our case.

In a d-dimensional QKD system employing d outputs (one single-photon detector at each output), the yield of the vacuum states is $Y_0 = 1 - (1 - P_{\text{dark}})^d$ which, for small values of P_{dark}, increases linearly with the dimension $Y_0 \approx d P_{\text{dark}}$. The QBER associated to vacuum states is $e_0 = (d - 1)/d$, corresponding to the probability of a random dark count to occur in an SPD which is not expected to fire when Alice and Bob's bases are matched.

With one single-photon detector in the d-dimensional case, the vacuum yield is independent of the dimension and limited to $Y_0 = P_{\text{dark}}$. On the other hand, some nonvacuum states sent by Alice will not be measured by Bob, even in the case of compatible bases between Alice and Bob, and the overall efficiency is reduced to $\eta_n = [1 - (1 - \eta)^n]/d$.

The expected values of Q_μ and E_μ and the parameters associated to single-photon events, Q_1 and e_1 for a given overall channel efficiency η and a d-dimensional QKD system, are summarized in Table I for both single and d detector cases. The curve for the secret key rate as a function of the multicore fiber length, shown on Fig. 3 of the main text, is computed using the parameters of Table I into Eq. (B1).

APPENDIX C: IMPROVED *d* DETECTOR SCHEME

In our experiment, one of the main issue was the high losses introduced by the bulk single detector scheme. There are two reasons for this and they can now be avoided by using new engineered devices. The first cause of losses is the absence of a device, known as a multiport beamsplitter, capable of combining the four propagation core modes without resorting to diffraction. The other cause of losses is the absence of a second device capable of demultiplexing (DEMUX) each core of the fiber into individual single-mode fibers, requiring the use of only one detector at Bob stage.

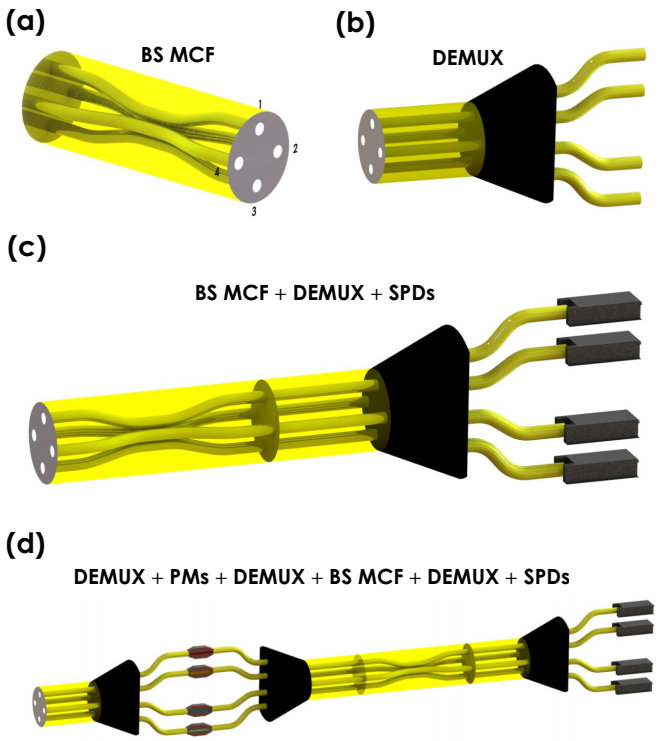

FIG. 5. Schematic setup of a d detector integrated detection scheme for HD-QKD based on MCFs. See text for details.

Nonetheless, recently, there have been the development of a MCF based multiport beamsplitter (BS MCF) that relies on a new technique to cut and splice multicore fibers [36]. Moreover, the fiber-producing Fibercore company has been able to develop the demux device required for our research, which is now available commercially [37]. The device allows the coupling of one detector to each core of the multicore fiber. These new devices are shown schematically in Figs. 5(a) and 5(b), respectively. The concatenation of the BS MCF device and the DEMUX will allow a d detector, low-loss, and waveguide coupled detection scheme for quantum cryptography in higher dimensions [Fig. 5(c)].

Lastly, note that by using extra DEMUX devices one can replace the deformable mirrors by much faster fiber-based phase modulators (PMs) [38], as shown schematically in Fig. 5(d). This allows faster encoding and decoding of the BB84 QKD high-dimensional states, since these PMs are capable to work up to a clock repetition rate of 30 GHz.

[1] D. J. Richardson, J. M. Fini, and L. E. Nelson, Space-division multiplexing in optical fibres, Nat. Photon. **7**, 354 (2013).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).
[3] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photon. **8**, 595 (2014).
[4] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, npj Quan. Infor. **2**, 16025 (2016).
[5] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d-Level Systems, Phys. Rev. Lett. **88**, 127902 (2002).

[6] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. Souto Ribeiro, Quantum Key Distribution with Higher-Order Alphabets Using Spatially Encoded Qudits, Phys. Rev. Lett. **96**, 090501 (2006).

[7] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States, Phys. Rev. Lett. **98**, 060503 (2007).

[8] S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, Quantum key distribution session with 16-dimensional photonic states, Sci. Rep. **3**, 2316 (2013).

[9] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Ltkenhaus, and A. Forbes, Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, Phys. Rev. A **88**, 032305 (2013).

[10] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, High-dimensional quantum cryptography with twisted light, New J. Phys. **17**, 033033 (2015).

[11] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, Phys. Rev. A **82**, 030301 (2010).

[12] D. Bunandar, Z. Zhang, J. H. Shapiro, and D. R. Englund, Practical high-dimensional quantum key distribution with decoy states, Phys. Rev. A **91**, 022336 (2015).

[13] H. Bao, W. Bao, Y. Wang, C. Zhou, and R. Chen, Finite-key analysis of a practical decoy-state high-dimensional quantum key distribution, J. Phys. A **49**, 205301 (2016).

[14] H. Bao, W. Bao, Y. Wang, R. Chen, C. Zhou, M. Jiang, and H. Li, Detector-decoy high-dimensional quantum key distribution, Opt. Express **24**, 22159 (2016).

[15] M. Y. Niu, F. Xu, J. H. Shapiro, and F. Furrer, Finite-key analysis for time-energy high-dimensional quantum key distribution, Phys. Rev. A **94**, 052323 (2016).

[16] K. Brádler, M. Mirhosseini, R. Fickler, A. Broadbent, and R. Boyd, Finite-key security analysis for multilevel quantum key distribution, New J. Phys. **18**, 073030 (2016).

[17] J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial, Measuring the Orbital Angular Momentum of a Single Photon, Phys. Rev. Lett. **88**, 257901 (2002).

[18] L. Neves, G. Lima, J. G. Aguirre Gómez, C. H. Monken, C. Saavedra, and S. Pádua, Generation of Entangled States of Qudits using Twin Photons, Phys. Rev. Lett. **94**, 100501 (2005).

[19] B. Rodenburg, M. P. J. Lavery, M. Malik, M. N. O'Sullivan, M. Mirhosseini, D. J. Robertson, M. Padgett, and R. W. Boyd, Influence of atmospheric turbulence on states of light carrying orbital angular momentum, Opt. Lett. **37**, 3735 (2012).

[20] M. A. Ciampini, A. Orieux, S. Paesani, F. Sciarrino, G. Corrielli, A. Crespi, R. Ramponi, R. Osellame, and P. Mataloni, Path-polarization hyperentangled and cluster states of photons on a chip, Light Sci Appl. **5**, e16064 (2016).

[21] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[22] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

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

[24] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014); Original version in *Proceedings Of The IEEE International Conference On Computers, Systems And Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[25] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

[26] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Experimental Quantum Key Distribution with Decoy States, Phys. Rev. Lett. **96**, 070502 (2006).

[27] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding, Phys. Rev. Lett. **98**, 010505 (2007).

[28] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate, Opt. Express **16**, 18790 (2008).

[29] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Decoy-state quantum key distribution with polarized photons over 200 km, Opt. Express **18**, 8587 (2010).

[30] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Proof-of-principle demonstration of measurement- device-independent quantum key distribution using polarization qubits, Phys. Rev. A **88**, 052303 (2013).

[31] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **111**, 130502 (2013).

[32] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **112**, 190503 (2014).

[33] Y. Zhao, B. Qi, and H.-K. Lo, Experimental quantum key distribution with active phase randomization, Appl. Phys. Lett. **90**, 044106 (2007).

[34] G. Lima, L. Neves, R. Guzmn, E. S. Gmez, W. A. T. Nogueira, A. Delgado, A. Vargas, and C. Saavedra, Experimental quantum tomography of photonic qudits via mutually unbiased basis, Opt. Express **19**, 3542 (2011).

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

[36] L. Gan *et al.*, Spatial-division multiplexed Mach-Zehnder interferometers in heterogeneous multicore fiber for multiparameter measurement, IEEE Photon. J. **8**, 7800908 (2016).

[37] http://fibercore.com/product/fan-outs.

[38] http://eospace.com/phase-modulator.

[39] Y. Ding *et al.*, High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits, npj Quant. Infor. **3**, 25 (2017).

[40] J. F. Dynes *et al.*, Quantum key distribution over multicore fiber, Opt. Express **24**, 8081 (2016).

[41] H. J. Lee, S.-K. Choi, and H. S. Park, Experimental demonstration of high-dimensional photonic spatial entanglement between multi-core optical fibers, arXiv:1610.04359v1.

[42] C. Gobby, Z. L. Yuan, and A. J. Shields, Quantum key distribution over 122 km of standard telecom fiber, Appl. Phys. Lett. **84**, 3762 (2004).

[43] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[44] D. Elkouss, J. Martinez-Mateo, and V. Martin, Information reconciliation for quantum key distribution, Quant. Infor. Comput. **11**, 0226 (2011).

[45] H.-K. Lo, H. F. Chau, and M. Ardehali, Efficient quantum key distribution scheme and proof of its unconditional security, J. Cryptol. **18**, 133 (2005).

[46] F. Xu, H. Xu, and H.-K. Lo, Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 052333 (2014).