

High-Dimensional Quantum Key Distribution via Full Core-Mode Encoding over Deployed Multicore Fibers

G. H. dos Santos^{1,2,*} K. B. Sawada^{1,2,*} N. Villalba^{1,2} C. Jara^{1,2} N. Guerrero^{1,2} C. Melo³ M. H. Magiotto⁴
D. Martinez^{5,6} G. B. Xavier⁷ J. Cariño⁸ G. Saavedra³ E. S. Gómez¹ S. P. Walborn^{1,2} and G. Lima^{1,2,†}

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

²*Millennium Institute for Research in Optics, Universidad de Concepción, 160-C Concepción, Chile*

³*Departamento de Ingeniería Eléctrica, Universidad de Concepción, 160-C Concepción, Chile*

⁴*Instituto de Física, Universidade Federal de Goiás, Goiânia, Goiás 74.690-900, Brazil*

⁵*University of Vienna, Faculty of Physics, Vienna Center for Quantum Science and Technology (VCQ), 1090 Vienna, Austria*

⁶*Christian Doppler Laboratory for Photonics Quantum Computer, Faculty of Physics, University of Vienna, 1090 Vienna, Austria*

⁷*Institutionen för Systemteknik, Linköpings Universitet, 581 83, Linköping, Sweden*

⁸*Departamento de Ingeniería Eléctrica, Universidad Católica de la Santísima Concepción, Concepción, Chile*



(Received 2 June 2026; revised 13 August 2026; accepted 10 September 2026; published 19 October 2026)

Quantum key distribution (QKD) provides information-theoretic security rooted in quantum physics, while high-dimensional (HD) encoding increases both noise tolerance and secret-key yield. Multicore fibers (MCFs), a leading platform for next-generation telecom networks, are a natural substrate for HD-QKD. Field demonstrations over deployed MCFs have so far relied on a hybrid qudit encoding strategy that combines two path (core modes) with the time-bin photonic degree of freedom, rather than exploiting the full set of available core modes. Although practical, this current approach incurs intrinsic efficiency penalties that grow with dimension. Encoding a qudit in the full set of core modes removes these penalties, but it requires the coherent control of all cores at once and has so far been restricted to laboratory settings. Here we implement a four-dimensional ($d = 4$) QKD protocol that directly exploits the full set of core modes of a four-core MCF, operating over an installed MCF network across the Universidad de Concepción campus under continuous environmental perturbations. We further benchmark the scheme using superconducting nanowire detectors at 10 dB channel loss, achieving a composable finite-key rate of $R = 6.19 \times 10^{-3}$ bits/pulse, the highest per-pulse rate reported to date for deployed HD-QKD at comparable loss. This result establishes core-mode encoding as a viable architecture for realistic, high-rate quantum-secure communications.

DOI: 10.1103/y779-t6ry

I. INTRODUCTION

Quantum key distribution (QKD) is among the most mature quantum technologies, offering information-theoretically secure key exchange whose security rests on the laws of quantum mechanics rather than on computational assumptions [1–4]. The looming prospect of cryptographically relevant quantum computers, capable

of breaking widely deployed public-key schemes via Shor's algorithm [5,6], has intensified efforts to move QKD out of the laboratory and into real communication infrastructure. Conventional QKD encodes one bit per photon in a two-dimensional (qubit) Hilbert space. High-dimensional QKD (HD-QKD), in which each photon constitutes a qudit carrying information in a d -dimensional space ($d > 2$), offers two interrelated advantages [7,8]: the tolerable error-rate threshold increases with d , improving noise robustness, and more than one secret bit can in principle be extracted per detected photon. A qudit is drawn from an alphabet of d symbols, so each detected photon carries up to $\log_2 d$ bits instead of one [7,9,10], and this is why the key yield per detection grows with the dimension. The noise tolerance grows for a related reason. An eavesdropper must guess in which of the d symbols the photon was prepared,

*These authors equally contributed to this work.

†Contact author: glima@udec.cl

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International license](#). Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

and a wrong guess sends the photon to one of $d - 1$ possible errors rather than to a single one [7,11]. The information she gains therefore buys her a larger disturbance as d increases on the quantum states, and the QBER at which the key rate vanishes rises accordingly.

Among the physical platforms for HD-QKD, multicore fibers (MCFs) are uniquely suited to field operation [12]. An MCF is an optical fiber in which several independent single-mode cores share a common cladding. MCFs are the leading platform for space-division multiplexing (SDM) [13,14] and are already part of deployed high-capacity telecom infrastructure [15–20]. The same property that makes MCFs attractive for classical SDM also makes them a natural physical substrate for HD-QKD: an MCF with d cores supplies a d -dimensional path (core) mode basis, with each core mode corresponding to one logical state $|k\rangle$. Coherent superpositions of all cores modes realize a d -dimensional qudit [21,22]. Because all cores share a common cladding, the differential phase drift between them is orders of magnitude slower than independent single-mode fibers of the same length [23], which helps to keep the qudit superposition phase-stable across the link. This property also holds true for long installed MCFs as it was demonstrated recently in Ref. [24]. State preparation and measurements are then performed by $d \times d$ multiport beam splitters, which can be fabricated with low insertion loss directly in MCFs [25].

Alternative approaches have combined path with a second encoding degree of freedom, most commonly time-bin, to build a higher-dimensional Hilbert space from a smaller number of cores. Following this route, Zahidy *et al.* [26] recently demonstrated a hybrid $d = 4$ QKD system on a 52 km installed MCF in L'Aquila, using two of the four cores available. The reported composable finite-key rate was 51.5 kbps at 22 dB of channel loss. Hybrid encodings of this kind are more robust to perturbations, since fewer core modes have to be kept coherent simultaneously, but they pay efficiency costs on both sides of the link. At the transmitter, each qudit spans multiple pulse slots, so the qudit generation rate is necessarily below the available laser clock rate. At the receiver, projecting onto time-bin superposition states requires Franson-like interferometers that discard a fraction of the detected photons per measurement, compounding with channel and detector loss [27]. Pure path encoding eliminates both limitations, at the cost of requiring simultaneous coherent control of d core modes, a requirement that has so far been met only in laboratory settings [21,22]. The encoding itself is therefore not new: what has been missing is the demonstration that the coherence of all d core modes can be maintained on an installed fiber, where temperature swings, mechanical stress and vibrations act on the link during the whole session.

In this work, a four-dimensional core-mode encoded HD-QKD protocol is demonstrated over an installed multicore fiber campus network at the Universidad de

Concepción, Chile. The deployed links connect laboratories across separate campus buildings over distances of approximately 200 m and 1.3 km, using permanently installed fibers that are fully exposed to real-world environmental perturbations throughout operation. To the authors' knowledge, this represents the first field deployment of a core encoded $d = 4$ HD-QKD system over a fully installed MCF network under uncontrolled operational conditions, establishing an important benchmark for realistic high-dimensional quantum communication. Furthermore, using superconducting nanowire single-photon detectors (SNSPDs) at 10 dB of channel loss, the system achieves a composable finite-key rate of $R = 6.19 \times 10^{-3}$ bits/pulse, or 12.4 kbps at the 2 MHz clock rate used here, the highest per-pulse finite-key rate reported to date for HD-QKD at comparable attenuation, surpassing the previous best time-bin implementation of 3.1×10^{-3} bits/pulse [28] by nearly a factor of two.

II. SECRET KEY RATE ESTIMATION

A. Decoy-state method

In general, QKD systems use weak coherent pulses (WCPs) rather than ideal single-photon sources. WCPs follow a Poissonian photon-number distribution, which makes them vulnerable to photon-number-splitting attacks [29]. The decoy-state method addresses this vulnerability by requiring Alice to randomly vary the mean photon number of each pulse among: (i) a signal mean photon number μ , and (ii) m decoy mean photon numbers with $\nu_1 > \dots > \nu_m$, while $\mu > \nu_1$. Randomization is an essential step to keep the protocol secure [30], but it enters the analysis as an assumption rather than as a measured quantity. For the secret key calculation only the sending probabilities and the corresponding mean photon numbers are used. Statistical differences between the gains and error rates observed for these pulses allow one to bound the contribution of true single-photon pulses for secret key generation, without which the key cannot be proven to be secure [29,31].

In the asymptotic limit of infinite pulses sent, the secret-key rate is given by [29,31]

$$R_\infty \geq q[Q_0 \log_2 d - Q_\mu H_d(E_\mu) f(E_\mu) + Q_1 [\log_2 d - H_d(e_1)]], \quad (1)$$

where d is the system dimension. Q_0 is the vacuum gain, Q_μ and E_μ are the gain and QBER of the signal state, and the function

$$H_d(x) = -x \log_2 \frac{x}{d-1} - (1-x) \log_2 (1-x) \quad (2)$$

is the generalized Shannon entropy for d -dimensional systems. The parameter $f(E_\mu)$ is the error-correction

inefficiency, Q_1 and e_1 are the gain and error rate of the single-photon pulses, and q is determined by the communication protocol. For the efficient BB84 protocol used here, $q = p_z^2$, where p_z is the probability that both Alice and Bob independently choose $\mathcal{Z}$ basis (used exclusively for key generation).

The quantities Q_0 , Q_1 , and e_1 cannot be measured directly, since Bob's detectors are not photon-number resolving. Nonetheless, they can be inferred indirectly from experimental data. In the practical and widely used case of two decoy states (a weak decoy of intensity ν and a vacuum decoy), one obtains $Q_0 = e^{-\mu} Y_0$, where Y_0 is the yield of the vacuum states, together with a lower bound Q_1^L on the single-photon gain and an upper bound e_1^U on the single-photon error rate, both written in terms of the measured gains and QBERs [29]. The explicit expressions are given in Appendix A.

Substituting these bounds into Eq. (1), one obtains that the lower bound of the secret key rate is given by [29,31]

$$R_\infty \geq q[Q_0 \log_2 d - Q_\mu H_d(E_\mu) f(E_\mu) + Q_1^L [\log_2 d - H_d(e_1^U)]] \quad (3)$$

B. Finite-key analysis

The asymptotic rate of Eq. (3) assumes an infinite number of transmitted signals. In any real implementation, only a finite number N of pulses is exchanged, and the observed quantities Q_μ , E_μ , Q_ν , E_ν are subject to statistical fluctuations. Finite-key analysis produces rigorous bounds on these quantities [31,32].

The two regimes are used here for different purposes, and we keep them separate throughout. The asymptotic key rate is a figure of merit to compare different possible hardware and channel configurations. The finite-key rate is the important value for real-world operation, and we use it for a like-for-like comparison of our work with other literature reported results.

For the finite-key analysis we follow the approach of Zhang *et al.* [32], adapted to d -dimensional systems. A key feature of this method is that it does not assume a Gaussian profile for the statistical fluctuations of the observed quantities, which is critical for high-quality QKD implementations. In the low-QBER regime the block-wise QBER distribution is strongly asymmetric, and a symmetric Gaussian fit corrupts the finite-key bounds in both directions. The measured distributions, and the asymmetry itself, are presented in Sec. V.

Another interesting property of the method is that it does not rely on the standard Chernoff-Hoeffding approach [31]. Instead, it makes use of the full Chernoff bound when estimating statistical fluctuations. In practice, the usual Chernoff-Hoeffding treatment simplifies this bound into a convenient exponential form, which introduces additional

looseness in the resulting estimates. By retaining the full expression, the method captures more accurately the relation between the observed counts and the underlying probabilities, leading to tighter confidence intervals for the estimated parameters.

According to the two-decoy finite-key method of Zhang *et al.* [32], with Chernoff-based inverse bounds and random sampling, a secret key of length K that is ϵ_{sec} -secure and ϵ_{cor} -correct satisfies [31,32]

$$K \geq \left[M_0^{zL} \log_2 d - M_\mu H_d(E_\mu) f(E_\mu) + M_1^{zL} (\log_2 d - H_d(e_1^U)) - 6 \log_2 \frac{21}{\epsilon_{\text{sec}}} - \log_2 \frac{2}{\epsilon_{\text{cor}}} \right], \quad (4)$$

where $R = K/N$, and M_a is the number of detections from pulses of type a (for signal: $a = \mu$; weak decoy: $a = \nu$; vacuum: $a = 0$). ϵ_{cor} quantifies the probability that Alice and Bob obtain different final secret keys after error correction and verification, while ϵ_{sec} quantifies Eve's possible information about the final key. A protocol is considered secure when both probabilities are sufficiently small.

The bounds entering Eq. (4) are obtained in four steps. Inverse Chernoff bounds are applied to the observed counts to bound the expected gains of the signal, weak-decoy and vacuum WCPs. The standard decoy-state relations then give a lower bound on the single-photon detections in the $\mathcal{Z}$ basis across all WCPs, which a symmetric Chernoff bound restricts to the signal WCPs, and an analogous chain is followed for the vacuum contribution. Finally, the single-photon error rate measured in the $\mathcal{X}$ basis is converted into an upper bound on the phase-error rate in the $\mathcal{Z}$ basis by a random-sampling argument. The complete derivation, adapted here to d -dimensional systems so that the interested reader can reproduce it, is given in Appendix C.

The resulting bounds M_1^{zL} , M_0^{zL} , and e_1^U are substituted into Eq. (4) to obtain the composable secret key length, with the security and correctness parameters $\epsilon_{\text{sec}} = 3.80 \times 10^{-8}$ and $\epsilon_{\text{cor}} = 1.00 \times 10^{-15}$.

These values follow the composable security framework of Refs. [31–33] and the convention that both parameters be kept below the failure probability of the classical primitives used in post-processing. We take $\epsilon_{\text{cor}} = 10^{-15}$, the usual choice for the error-verification hash, and we let the secrecy parameter scale with the key length as $\epsilon_{\text{sec}} = 10^{-15} \times K$, so that the security per key bit is fixed regardless of the block size. With a key length of $K = 3.80 \times 10^7$, one gets that $\epsilon_{\text{sec}} = 3.80 \times 10^{-8}$. The failure probability of each individual statistical estimation is set to $\epsilon = 10^{-10}$, and the $6 \log_2(21/\epsilon_{\text{sec}})$ term in Eq. (4) already accounts for their

composition. The protocol is then $(\epsilon_{\text{cor}} + \epsilon_{\text{sec}})$ -secure, as detailed in Appendix C.

III. EXPERIMENTAL SETUP

The HD-QKD system consists of a prepare-and-measure apparatus, where transmitter and receiver are connected through a field-deployed MCF network as illustrated in Fig. 1. Four-dimensional quantum states

are encoded in the core modes of a four-core MCF. Throughout the text we call these states *ququarts*: the logical basis states $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ are associated with the four cores [see the inset of Fig. 1(a)]. The setup is a large fiber interferometer based on different MCF technologies. Superpositions of the logical states are created using a four-core MCF multipoint beam splitter (4C-MBS) at Alice. These are then transmitted through the installed MCF network to Bob, where the four modes interfere at a

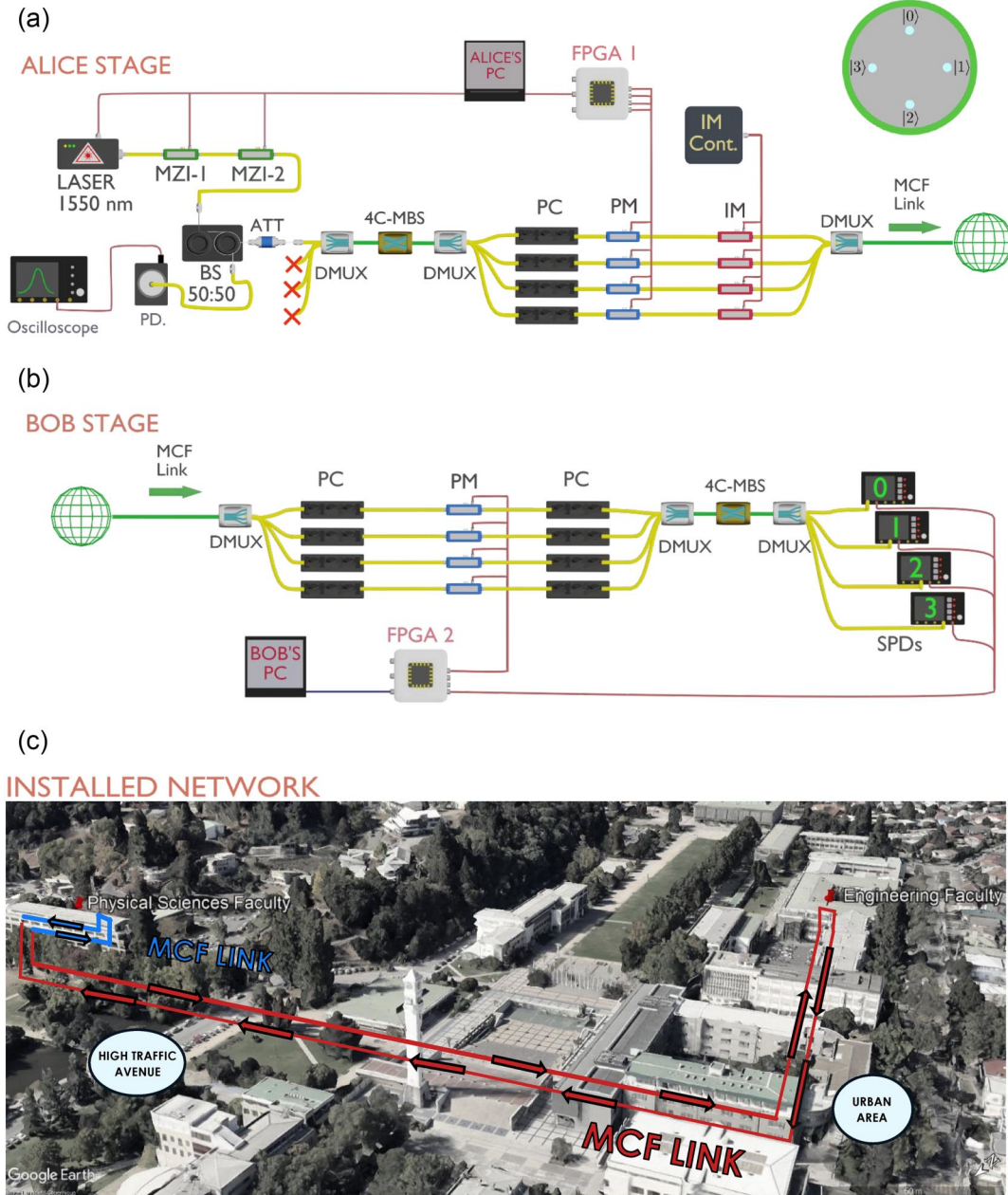


FIG. 1. Schematic of the core-encoded four-dimensional QKD system and network. Alice (a) prepares ququart states; Bob (b) measures them in two different bases. (c) The states are transmitted through different links of an MCF network installed over the campus of the Universidad de Concepción, Chile. PC: polarization controller; PM: phase modulator; IM: intensity modulator; Att: optical attenuator; MCF: multicore fiber; MUX/DMUX: MCF multiplexer/demultiplexer; 4 C-MBS: four-core multipoint beam splitter; SPD: single-photon detector.

second 4 C-MBS. The HD-QKD protocol is implemented using the phase-coding scheme, where Alice controls the initial phase between the core modes and Bob the final ones [3,4]. In the following sub-sections we describe each stage of the system in details.

A. Alice: State preparation

Alice's preparation stage, controlled by a field-programmable gate array (FPGA) electronics, begins with a continuous-wave telecom laser at 1550 nm [see Fig. 1(a)]. The laser output is carved into 5 ns pulses at a repetition rate of 2 MHz by two cascaded Mach-Zehnder interferometers (MZIs) driven by the FPGA. A tap coupler diverts a small fraction of the output to a photodetector and oscilloscope for real-time power and pulse monitoring. The main arm proceeds to an optical attenuator (Att) that fine adjusts the pulse intensity. Phase-drifts and different voltage levels are then used on MZI-2 to properly generate the WCPs required on the two-decoy QKD method.

The attenuated pulses enter an initial MCF through a spatial demultiplexer (DMUX), which is a commercial fan-in/fan-out device that maps each core of a MCF to an individual single-mode fiber. The pulses are then sent to a 4 C-MBS [25], which splits the input equally across all four cores. The output cores of the 4 C-MBS are coupled back to four single mode fibers (SMFs) using another DMUX in the reverse order. The SMFs are connected to a set of four phase modulators (PMs), one for each SMF. With the 4 C-MBS and PMs, Alice can create an equal-amplitude core-encoded qudit superposition. The entire single-mode fiber section is only ≈ 5 m long and is covered on isolation materials such that their contribution to the interferometer's drifts is negligible. The generated qudits are then given by

$$|\Psi\rangle = \frac{1}{2}(e^{i\phi_0^A}|0\rangle + e^{i\phi_1^A}|1\rangle + e^{i\phi_2^A}|2\rangle + e^{i\phi_3^A}|3\rangle), \quad (5)$$

where ϕ_k^A is the phase applied by the PM acting on core $k \in \{0, 1, 2, 3\}$. By choosing the set of phases $\{\phi_k^A\}$ properly, Alice prepares one of eight qudit states (given in Fig. 7 in Appendix D.), corresponding to one of two mutually unbiased bases $\mathcal{Z}$ or $\mathcal{X}$, as required by the HD-BB84 protocol. By design, neither $\mathcal{Z}$ nor $\mathcal{X}$ coincides with the core (logical) basis. Rather, both are composed of superposition states, such that fast PMs can toggle between them. In each path a polarization controller (PC) aligns the optical field to the acceptance axis of each PM. The four PMs are independently driven by the FPGA to apply individual phases to each core. Intensity modulators (IM) in each arm are used for aligning purposes before each QKD session. Finally, a DMUX couples the four paths back into MCFs for transmission over the installed MCF network.

B. Bob: Measurement system

At Bob's station, a DMUX is used to separate light from the four cores into another isolated ~ 5 m-long section of independent SMFs, which are each connected to a PC, PM and second PC [see Fig. 1(b)]. The first set of PCs aligns the polarization in each SMF to the acceptance axis of the corresponding PM. The PMs then apply one of two fixed phase patterns to select the measurement basis: $\vec{\Phi}_{\mathcal{Z}}^B = \{0, 0, 0, 0\}$ for the $\mathcal{Z}$ basis, or $\vec{\Phi}_{\mathcal{X}}^B = \{\pi, 0, 0, 0\}$ for the $\mathcal{X}$ basis. The second set of PCs finely tunes the polarization to ensure mode indistinguishability at the 4 C-MBS. The four paths are routed through compact DMUX stages before and after the 4 C-MBS, as in Alice's stage. Each output port of the 4 C-MBS is monitored by a single-photon detector (SPD) to conclude the measurement procedure.

The resulting measurement basis states follow from the transfer matrix of the 4 C-MBS [25] and are written explicitly in Appendix D, Eq. (D1). Projection onto state $|\psi_k\rangle$ is associated to the SPD in core mode k .

For the QKD experiment, two detector technologies were employed. We first used InGaAs avalanche photodiode SPDs to characterize the network links and to test the QKD system operating with this low-cost technology, demonstrating that the system remains viable with more commercially accessible hardware. In this case, Bob's mean detection efficiency is limited to $\sim 7.5\%$. We then used modern SNSPDs, with mean detection efficiency of $\sim 85\%$, to define the practical performance bound attainable by the system, setting its finite-key generation rate benchmark. Bob's FPGA synchronizes the detection gate windows with Alice's pulsed laser and controls Bob's PMs.

Regarding the detector parameters relevant to the protocol, the dark-count probabilities per detection gate are 3.81×10^{-6} for the InGaAs SPDs and 1.35×10^{-5} for the SNSPDs, and these are the values entering the key-rate estimation. Afterpulsing, dead time and timing jitter play no role in our operating regime: with the laser at 2 MHz and weak pulses, successive detections in a given detector are separated by times far longer than the scale of these parameters, and the timing jitter of both technologies is well below the 5 ns pulse width.

C. MCF network

The QKD system was tested on a multicore fiber network installed across the campus of the Universidad de Concepción. The network employs custom-fabricated cables, each one containing two Fibercore SM-4C1500 four-core homogeneous MCFs. Each multicore fiber has four identical cores of diameter 8 μm arranged in a square geometry with a center-to-center pitch of 50 μm (nominal) within a cladding of 124 ± 1 μm diameter, and a mode field diameter of 7.4–8.5 μm at 1550 nm. Each core

supports single-mode propagation in the telecom C and L bands, with a nominal attenuation of 0.2 dB/km. Inter-core crosstalk, which could in principle couple the core modes during propagation, is negligible in this system. Characterizations of deployed four-core fibers of this class report crosstalk below -50 dB/km [26], and ultra-low-crosstalk designs reach total values below -70 dB after tens of kilometers [34]. For our longest link this bounds the crosstalk-induced error probability at the 10^{-4} level, more than two orders of magnitude below the measured QBERs, and consistently no crosstalk was detected in our fibers above the sensitivity of our measurement apparatus.

The campus network is arranged in a star topology, with a central laboratory serving as the hub that interconnects three peripheral laboratories [see Fig. 1(c)] [19]. The main laboratory, which houses Alice's and Bob's apparatus, is located on the second floor of the Faculty of Physical and Mathematical Sciences. The hub resides on the same floor of the building, separated from the main laboratory by several tens of meters of MCF that constitute the first deployed link. From the hub, a vertical link rises through the building to a third laboratory on the sixth floor, while a second link extends across the university campus to reach a fourth laboratory in the Faculty of Engineering. Together, these three fiber spans form the physical backbone of the network and define the set of point-to-point channels available to the QKD system. Three distinct operating round-trip configurations are implemented over this infrastructure and are referenced throughout the paper by

- (i) *BtB* (back-to-back): Alice is connected directly to Bob through three 5 m patchcords (15 m of total fiber), entirely within the main laboratory. This configuration serves as the reference baseline.
- (ii) *P6* (sixth-floor link): Alice's output is routed from the second floor through the internal building infrastructure to the laboratory on the sixth floor and back, yielding a round-trip length of approximately 200 m.
- (iii) *PtE* (Physics-to-Engineering link): Alice's output is routed out of the main building, through the underground fiber infrastructure that crosses the campus plaza, into the laboratory at the Faculty of Engineering, and back, yielding a round-trip length of approximately 1300 m.

The round-trip configuration of each link is realized over a pair of 4-core MCFs: one MCF carries the encoded states from Alice toward the remote laboratory, while the second returns them to the main laboratory, where Bob's measurement apparatus is located. Further details of these links are given in Table I.

As is typical of testbed networks, where the physical configuration is frequently reconfigured and reconnected, the channel loss is dominated by fiber-to-fiber connections and splices rather than by intrinsic fiber propagation. For the PtE link, the bare fiber contributes only ≈ 0.13 dB of

TABLE I. Channel configurations of the deployed network. For each link we report the total measured attenuation η_L (averaged over the four MCF cores) and the round-trip optical length L . The last column gives the equivalent length of MCF (assuming 0.2 dB/km) that would yield the same attenuation in the absence of connectors and splices.

Link	η_L (dB)	L (m)	Eff. MCF (km)
BtB	2.16	15	10.8
P6	9.36	200	46.8
PtE	10.70	1300	53.5

the total 10.70 dB; the remaining ≈ 10.6 dB arises from stress-related core misalignment from butt-coupled MCF connectors, fusion splices, and DMUXs. As a result, η_L is essentially uncorrelated with L : the P6 link (200 m) and PtE link (1300 m) have nearly the same total attenuation. Nonetheless, the PtE cable traverses a road, a parking lot, and a pedestrian plaza with substantial daytime activity, producing a noisier and more variable differential-phase environment than the P6 link.

IV. MEASUREMENT PROCEDURE AND NETWORK CHARACTERIZATION

A. Polarization stability

Polarization stability of the installed links is critical. Independent polarization evolution along the different cores of the MCF would compromise the coherent propagation of the core modes used by the QKD protocol. To prevent this, the polarization state of each core is manually aligned prior to every QKD run. At Alice's station, the PCs are adjusted to match the acceptance axis of her PMs. At Bob's station, the first set of PCs is aligned with the acceptance axis of his PMs, while the second set is tuned for polarization-mode indistinguishability at the 4 C-MBS. Once this initial alignment is completed, the PCs remain static and no active polarization stabilization is employed such that slow environmental perturbations are allowed to act freely on the channel. Representative polarization-stability measurements for the BtB and PtE links are shown in Fig. 2. In both cases, the polarization state remains essentially constant for more than two hours, confirming that the in-laboratory and outside-plant environments are sufficiently stable on this timescale. This window comfortably exceeds the time required to initialize and complete the QKD sessions reported below, eliminating the need for active polarization control. These measurements also identify what governs the practical operation of the system: the relative phase between the cores, characterized in the next sub-section, drifts orders of magnitude faster than the polarization, and is therefore the quantity that dictates the operating cycle of the protocol. Since the polarization of short deployed links remains at acceptable levels for several hours, and residual drift over

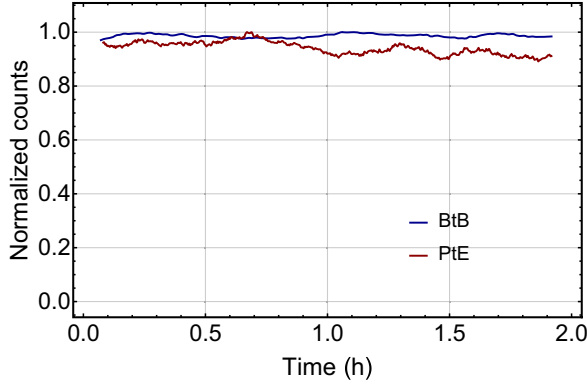


FIG. 2. Polarization stability of the deployed links. Normalized single-photon count rate, integrated in 100 ms bins, recorded with a fixed polarization analyzer for the back-to-back (BtB) configuration and the installed Physics-to-Engineering (PtE) link. After an initial manual alignment, no active polarization control is applied. The count rate remains stable over more than two hours in both settings, demonstrating that environmental drifts in the laboratory and across the deployed campus link are slow compared with the duration of a typical QKD session.

longer spans can be followed with standard polarization tracking, polarization is not a limiting factor for an active implementation of path-coded HD-QKD over multicore fibers.

B. Phase stabilization and data acquisition

In our phase-coding QKD scheme, information is encoded in the relative phases across the four core modes. Random phase fluctuations between different cores must therefore be compensated before each key-generation window. Although the common cladding of the MCF suppresses differential phase drift between cores [23], residual stochastic phases $\delta\phi_k(t)$ remain, driven primarily by temperature and mechanical perturbations along the link. This can be seen in Fig. 3(a) where we prepare the first state given in Fig. 7, and let the PtE MCF link evolve freely while monitoring the photon state evolution using quantum tomography [35,36]. The integration time for recording the single counts is 100 ms, and each tomography takes ~ 400 ms to be concluded. Thus, Fig. 3(a) spans a total time of 20 s of channel evolution. The slow phase drifts can be seen as random rotations on the states prepared by Alice, which leads to errors in Bob's measurement outcomes and thus an increased QBER in a QKD session. Importantly, we find that these phases are stable over periods of at least 100 ms, which is the key property that makes a 100 ms acquisition window viable. This can be seen in Fig. 3(b), where the tomographies are now performed during the time window of 100 ms after the same Alice's state has been prepared. A procedure has been repeated 50 times. In this case, high overall fidelities and purities are obtained for the reconstructed states with

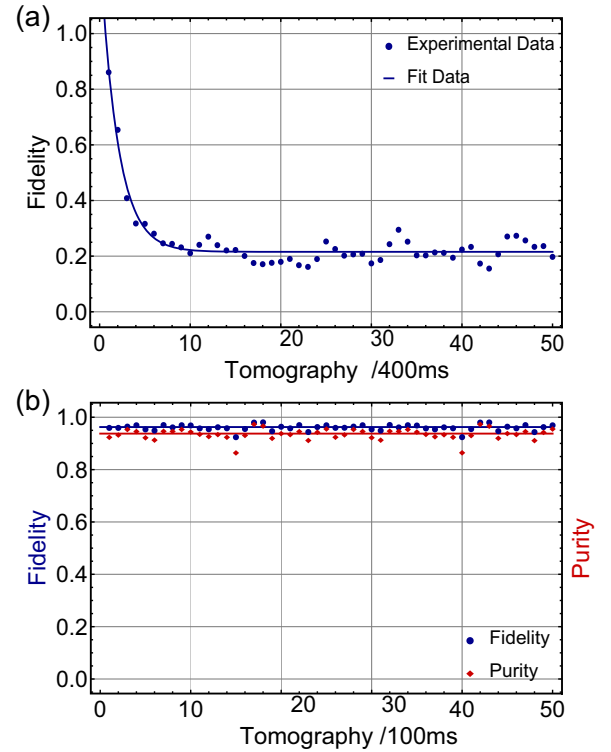


FIG. 3. Characterization of the PtE MCF link. (a) Free evolution of the transmitted state over ~ 20 s, reconstructed via sequential quantum state tomography (for the first input state defined in Fig. 7). Each projector is integrated for 100 ms, and a full tomographic reconstruction is completed in ~ 400 ms. The slow phase drifts induced by thermal and mechanical perturbations can be seen as unitary rotations of the prepared state, progressively degrading its overlap with the target. (b) Tomographic reconstructions acquired within a single 100 ms interval following the preparation of the same input state, repeated over 50 independent realizations. The reconstructed states exhibit a mean fidelity of $\bar{F} = 0.96 \pm 0.01$ with respect to the target one and a mean purity of $\bar{P} = 0.94 \pm 0.02$, demonstrating that the residual stochastic phases $\delta\phi_k(t)$ remain stationary over 100 ms. Thus, 100 ms is an operational acquisition window, which was then employed in the QKD protocol.

a mean value of $\bar{F} = 0.96 \pm 0.01$ and $\bar{P} = 0.94 \pm 0.02$, respectively.

Once a viable operational detection time is identified, it is necessary to ensure that Alice's states and Bob's measurements remain properly implemented over time despite slow phase fluctuations along the MCF. For this, we employ a calibration procedure based on Alice's phase modulators. Prior to each measurement session, the modulators are biased so that, at the input of Bob's 4 C-MBS, the effective relative phases among the four cores are nulled up to a global phase. Specifically, assuming that $\delta\phi_k(t)$ represents the stochastic phase accumulated on core k during propagation, and by denoting α_k as the compensation phase applied by Alice's modulator on that core, the condition for perfect constructive interference at

detector D_0 , corresponding to core mode 0, is

$$[\alpha_k + \delta\phi_k(t)] - [\alpha_0 + \delta\phi_0(t)] \equiv 0 \pmod{2\pi}. \quad (6)$$

Note that α_0 does not need to be zero: the equation constrains only the phase differences between cores, leaving a free global phase α_0 that has no physical consequence for the interference. So, in our experiment we use a perturb-and-observe algorithm to modify Alice's PM phases, presented in detail at [37], which finds the set $\{\alpha_k\}$ satisfying Eq. (6), and that maximizes the count rate at D_0 when sending the state $\{0, 0, 0, 0\}$. The fraction F_e of photons detected at $D_{j \neq 0}$ thus provides a direct, real-time indicator of phase imperfection in the channel. We define the threshold T as the maximum allowable for this erroneous count rate. Thus, phase calibration is performed until $F_e \leq T$, at which point the system begins the protocol procedure (run phase). During the run phase, Alice's total phase on core k is $\alpha_k + \phi_k^A$, where $\phi_k^A \in \{0, \pi\}$ is one of the phases required to encode a chosen QKD state. The compensation phases $\{\alpha_k\}$ are held fixed throughout the run window and updated again only in the next Adjust phase. After each run window (of 100 ms), the system checks the relation $F_e \leq T$, if satisfied, another run phase is performed. If not, the system returns to adjust the phases. Figure 3(b) constitutes also an example of the resulting alignment, where a QKD protocol state is prepared and measured over time while considering $T = 5\%$.

The relevant question is whether the relative drifts remain stationary for a long enough period of time to accumulate one acquisition block. Two arguments suggest that this may remain the case at metropolitan distances. The first is the field characterization of deployed MCFs discussed in Ref. [24], which showed phase coherence over links of up to 25 km. The second argument is provided by a phenomenological model in which each fiber core's relative phase is treated as an independent random walk (Wiener process). In this case, since the predicted stability times remain comparable to those observed experimentally, decreasing from approximately 100 ms at 1 km to 20 ms at 100 km, the model suggests that successful QKD operation should remain feasible across a wide range of metropolitan-scale fiber link distances. Note, however, that in this model the variance grows in time at a rate set by a single phase-diffusion coefficient. This simplified description assumes a stationary diffusion coefficient and therefore does not capture time-dependent environmental perturbations, such as thermal variations or mechanical shocks, which may modify the phase dynamics of a deployed fiber. Accordingly, the extrapolation to longer distances should be interpreted as an indicative estimate rather than as a quantitative prediction for a specific deployed link.

V. QKD RESULTS AND DISCUSSION

A. QBER distributions and threshold analysis

We initially investigated the statistical distribution of the QBER and its dependence on the threshold T , in order to properly characterize optimal operation conditions for secret key generation. Figure 4 shows the QBER distributions for the PtE link as a function of the threshold T , varied from 5% to 15%. We focus on the PtE link because it represents the more demanding scenario: its longer cross-campus route is subject to higher environmental noise, resulting in a broader QBER distribution than the P6 loop under comparable thresholds. The histograms display the asymmetric, bounded character anticipated previously: the hard boundary at zero suppresses the low side, the peak is shifted away from the mean, and a longer right tail extends toward larger errors. This asymmetry is most pronounced at tight thresholds, where the distribution is pushed against the lower boundary, but remains visible across the entire range of T explored. A symmetric Gaussian fit is manifestly inadequate in this regime, as it would overestimate the probability of near-zero QBER and underestimate the upper-tail fluctuations. This justifies the use of the Zhang *et al.* analysis [32], which makes no Gaussian assumption on the statistics of the observed quantities.

The solid lines in Fig. 4 are fits to a Beta distribution, with the fit function and the fitted parameters given in Appendix B. The fraction of 100 ms windows whose QBER lies below the $d = 4$ security bound falls from 89.6% at $T = 5\%$ to 70.5% at $T = 15\%$, while the number of recorded windows grows from 289 to 3688.

The dependence of the distribution on T illustrates the trade-off inherent to the phase-stabilization algorithm: a

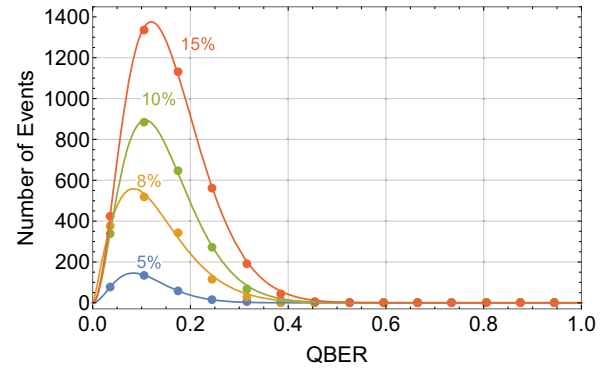


FIG. 4. Distributions of the QBER measured in 100 ms windows on the PtE link, for threshold values T ranging from 5% to 15%. Each histogram is fit with a Beta distribution (solid lines), which captures the asymmetric, bounded character of the data: the hard boundary at zero suppresses the low side, the peak is shifted away from the mean, and a longer right tail extends toward larger errors. As T is tightened, the distribution narrows and shifts toward $\text{QBER} \approx 0$, at the cost of a reduced duty cycle (fewer accepted windows).

tighter threshold selects lower-error windows but increases the re-adjustment frequency, thereby reducing the duty cycle ($\mathcal{D}$). The threshold of each session is therefore chosen to maximize the total secret key produced per unit of time, the product $\mathcal{D} \times R$, rather than either factor alone. The optimum is link- and detector-specific, since the detector noise sets the lowest QBER that can be reached, and the mapping of the QBER distribution against T in Fig. 4 is what allows each configuration to be operated in its optimized regime. The parameter that determines whether a positive key rate is achievable at all, and therefore sets the maximum operating distance, is the mean QBER: at the security boundary (QBER = 18.93% for $d = 4$) the key rate vanishes regardless of how many windows are accepted. Reducing the QBER is thus the primary mechanism for extending range.

B. Secret key rates over the MCF network

This work reports two main results. The first, presented in this sub-section, is a four-dimensional QKD session based on pure core-mode encoding over an installed MCF network under uncontrolled real-world perturbations, which establishes core-mode HD-QKD as viable under field conditions and sets a quantitative reference for the design of future MCF-based quantum networks. The second, presented in the next sub-section, is a composable finite-key rate of 6.19×10^{-3} bits/pulse obtained with SNSPDs at 10 dB of channel loss, the highest per-pulse rate reported to date for HD-QKD at comparable attenuation, which shows that hybrid encodings can be avoided without compromising the secret-key rate.

Figure 5 summarizes asymptotic secret key rates obtained with InGaAs SPD operating at $T = 5\%$, and for SNSPDs operating with $T = 3\%$ (corresponding to the lowest T achievable of each technology). All the experimental data recorded and used to calculate such secret key rates are explicitly given in Appendix E.

For the InGaAs SPDs, lower key rates are obtained as expected. Nonetheless, since we are interested in testing the limits of the system, it is interesting to see that a more commercial version of this QKD system can operate up to 14 dB of channel losses. In the ideal case, this is equivalent to the attenuation obtained over ~ 70 km of modern multicore fibers. For the experimental data at 14 dB of channel losses, we obtain a secret key rate per pulse of $8.62 \times 10^{-6} \pm 7.63 \times 10^{-5}$, which corresponds to 17 bits/s at the 2 MHz clock used here. In this investigation we worked with a clock rate set to 2 MHz because: (i) this already allows one to determine with good precision the most relevant parameter of a QKD system, which arguably is the secret key rate per pulse transmitted; and (ii) at low attenuation regime, it keeps the count rate well below the dead time and quenching period of the detectors, where the recorded gains would no longer be linear.

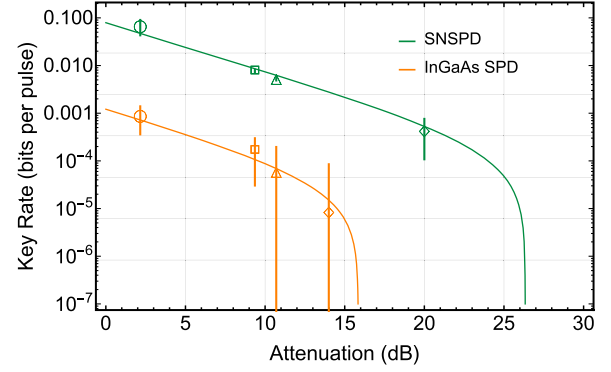


FIG. 5. Asymptotic key rate (bits/pulse) vs channel attenuation while using InGaAs SPDs and SNSPDs. Points: recorded experimental rates. Curve: asymptotic model. ($\circ$) represents the results for the BtB link; ($\square$) represents the results for the P6 link; ($\triangle$) represents the results for PtE link and; ($\diamond$) represents the results for channels with extra attenuation to test the viability for secret key generation with higher losses. The key generation values are given explicitly in Appendix E.

The asymptotic green curve modeling the results obtained with SNSPDs defines the secret key rate limits for our core-encoding QKD system. For instance, much higher losses are tolerated by the QKD system such that it could reach, in the ideal case, MCF propagation distances greater than 100 km. This is shown in Fig. 5, where we have been able to achieve positive secret key generation rates at 20 dB of artificial channel attenuation. The impact of detector technology on the core-encoding QKD system can be directly assessed over the deployed PtE link, for instance. With InGaAs SPDs, we measured a secret key rate of $R_\infty = 6.04 \times 10^{-5}$ bits per pulse, whereas SNSPDs yielded $R_\infty = 5.36 \times 10^{-3}$ bits per pulse, corresponding to an improvement of two orders of magnitude.

C. Finite-key rate benchmark

Now we study the core-encoded QKD performance while considering finite statistics in the key generation procedure. The asymptotic analysis based on the two-decoy method is relevant to define upper bounds on the QKD performance of the system. Nonetheless, it assumes an ideal situation where an infinite number of WCPs are sent to Bob, such that probabilities can be measured directly. In practice, however, only a finite number of WCPs can be sent, and the implemented measurements are subject to statistical fluctuations that must properly be modelled to guarantee the security of the generated key. Another interesting aspect of measuring the composable finite-key generation rate for the core-encoded QKD scheme is that this value can be used to directly compare our system against several modern QKD experiments that also rely on finite-key analysis.

Following the finite-key two-decoy-state protocol of Zhang *et al.* [32], we evaluate our finite-key rate

TABLE II. Experimental data recorded for the finite-key rate estimation. N : total pulses emitted; M_z : $\mathcal{Z}$ -basis detections; e_{det}^z , e_{det}^x : average QBERs in $\mathcal{Z}$ and $\mathcal{X}$; M_0^{zL} , M_1^{zL} : lower bounds on vacuum and single-photon detections; e_1^U : upper bound on single-photon error rate; $f(E_\mu)$: error-correction inefficiency; K : secret key length; R : secret-key fraction.

Quantity	Value
Loss (dB)	10
N	6.130×10^9
M_z	8.18×10^7
$M_{\mu z}$	80,904,263
$M_{\nu z}$	904,329
$M_{\mu x}$	677,165
$M_{\nu x}$	7640
M_{0z}	2082
$E_{\mu z} M_{\mu z}$	1,703,281
$E_{\nu x} M_{\nu x}$	252
$E_{0x} M_{0x}$	13
e_{det}^z	1.98%
e_{det}^x	2.85%
M_0^{zL}	54,842
M_1^{zL}	35,290,908
e_1^U	7.29%
$f(E_\mu)$	1.05
ϵ	10^{-10}
ϵ_{cor}	10^{-15}
ϵ_{sec}	3.8×10^{-8}
K	3.80×10^7
R	6.19×10^{-3}

benchmark at a channel attenuation of 10 dB, a typical reference loss level used to compare QKD systems. In our case, the finite-key session uses two-decoy settings optimized for Bob-side's loss of 5.7 dB, using SNSPDs with a detection efficiency of 85%. Table II summarizes the measured detection counts, error counts and the resulting finite-key bounds. Over $N = 6.13 \times 10^9$ emitted pulses, Bob registered $M_z = 8.18 \times 10^7$ detections in the $\mathcal{Z}$ basis. The detection error rates are $e_{\text{det}}^z = 1.98\%$ and $e_{\text{det}}^x = 2.85\%$. In Fig. 6, we show the QBER distribution, integrated over several blocks of 100 ms, for all the $M_z = 8.18 \times 10^7$ detections registered. As one can see, the QKD scheme works with the QBER distribution stably over the entire session, showing that phase-drift has been properly controlled by the stabilization algorithm. The finite-key rate obtained is

$$R_{\text{finite}}(10 \text{ dB}) = 6.19 \times 10^{-3} \text{ bits/pulse}, \quad (7)$$

corresponding to 12.4 kbps at the 2 MHz clock rate used here.

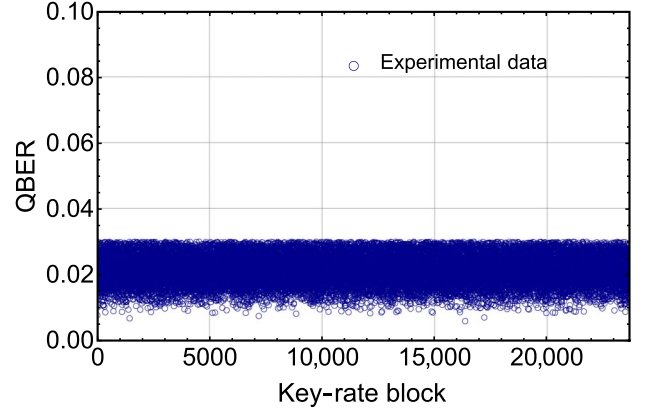


FIG. 6. QBER distribution, integrated over blocks of 100 ms, for the entire $M_z = 8.18 \times 10^7$ detections registered in the QKD session. The distribution center remains mainly within 1.5%–2.5%, with weak dependence on block counts, indicating that the spread is dominated by detector dark counts and timing jitter rather than phase drifts.

D. Comparison with previous works

Table III places the present work in the context of representative modern QKD demonstrations at a channel attenuation of 10 dB, a standard reference loss for cross-experiment comparisons. The comparison is made in bits per pulse because this removes the clock rate, which differs by orders of magnitude between these experiments and is a property of the electronics rather than of the encoding (Sec. VB). A central motivation for HD-QKD is the promise of higher noise tolerance and more information per detected photon relative to qubit-based schemes. Whether this theoretical advantage translates into competitive secret-key rates under field conditions has remained an open question, since practical HD implementations have historically incurred efficiency penalties that eroded the dimensional gain. The results reported here allow us to examine this question concretely.

Among HD-QKD demonstrations, the two most directly comparable results are Islam *et al.* [28], who report 3.1×10^{-3} bits/pulse using a $d = 4$ time-bin protocol over spooled SMF with SNSPDs, and Zahidy *et al.* [26], who deployed a $d = 4$ hybrid core + time-bin system over a 52 km installed MCF in L'Aquila. Our result of 6.19×10^{-3} bits/pulse surpasses Islam *et al.* by nearly a factor of two and Zahidy *et al.* by more than a factor of four. These gains are consistent with the elimination of the encoding penalties inherent to time-bin-based approaches.

Viewed against the broader QKD landscape, the significance of this result becomes even clearer. Li *et al.* [38] recently reported 8.9×10^{-3} bits/pulse using a $d = 2$ polarization protocol equipped with a high-speed integrated transmitter and multipixel SNSPDs. A highly engineered qubit system currently represents the state of the art in per-pulse key-generation rate. Our $d = 4$ QKD

TABLE III. Comparison with representative recent QKD demonstrations. See main text for details.

Reference	Dimension	Encoding	Loss (dB)	Rate (bits/pulse)
Zahidy <i>et al.</i> [26]	4	Core + time-bin	10	1.4×10^{-3} (finite) ^a
Islam <i>et al.</i> [28]	4	Time-bin	10	3.1×10^{-3} (finite) ^a
W. Li <i>et al.</i> [38]	2	Polarization	10	8.9×10^{-3} (finite) ^a
This work	4	Core modes	10	6.19×10^{-3} (finite)

^aThese values are directly reported or obtained from the experimental data fit at 10 dB of channel attenuation.

result reaches 6.19×10^{-3} bits/pulse (within a factor of 1.5) of that qubit benchmark. This proximity is notable: it suggests that, with the encoding efficiency recovered by the pure core-mode approach, the intrinsic advantages of HD encoding are no longer being fully absorbed by system overhead. While qubit QKD retains practical advantages in simplicity and absolute clock-rate scalability, the present result indicates that HD-QKD is reaching a regime of practical competitiveness, where its higher information capacity per photon can be meaningfully harvested in real-world deployments.

VI. CONCLUSIONS

High-dimensional quantum key distribution has received growing attention as a technique to boost the secret-key rate per protocol round, with path-encoded implementations over multicore fibers emerging as a particularly promising route [3,12]. Here we have demonstrated a $d = 4$ HD-QKD protocol based on pure core-mode encoding over a deployed MCF campus network, operating under continuous and uncontrolled environmental perturbations. The system was characterized across three distinct network configurations, ranging from a back-to-back reference baseline to an installed cross-campus link spanning 1.3 km, and benchmarked using both commercially accessible InGaAs avalanche photodiode detectors and high-efficiency SNSPDs. A key advance of this implementation is that information is encoded across all four core modes of the MCF, rather than in a reduced core subspace supplemented by an auxiliary degree of freedom. This direct encoding eliminates the generation-rate penalty associated with time-bin schemes and the photon loss inherent to Franson-like measurement interferometers [27]. The use of low-loss multiport beam splitters fabricated directly in MCF [25] for both state preparation and measurement is central to this result, enabling high-fidelity qudit operations within the deployed network.

The experiment was performed under real-world conditions, including temperature variations, mechanical perturbations, and vehicle-induced vibrations along the cross-campus routes. Despite these perturbations, the common-cladding geometry of the MCF strongly suppresses differential phase drift between cores [23],

enabling operational integration times of 100 ms, and coherent qudit propagation with mean state fidelity $\bar{F} = 0.96 \pm 0.01$ over the longest deployed link. Positive asymptotic secret-key rates were obtained over all tested links and with both detector technologies, confirming viability across a range of operational scenarios.

To establish a composable finite-key benchmark and enable direct comparison with the broader QKD literature, a dedicated session was conducted at a reference channel attenuation of 10 dB using SNSPDs, yielding a finite-key rate of $R = 6.19 \times 10^{-3}$ bits/pulse and a total of 3.80×10^7 secret key bits from 6.13×10^9 emitted pulses. This is the highest per-pulse finite-key rate reported to date for HD-QKD, within a factor of 1.5 of the current state of the art in qubit QKD [38].

Moving to larger alphabets is not straightforward, since more cores bring higher inter-core crosstalk and more relative phases to stabilize. Even so, path coding in seven-core fibers has already been investigated, together with the corresponding multiport beam splitters [25]. An implementation along these lines would scale path coding in installed multicore networks to a larger alphabet.

Beyond QKD, the ability to prepare, transmit, and measure coherent spatial qudits in deployed multicore fibers is relevant for future metropolitan quantum networks based on space-division multiplexing [12] and for quantum communication exploiting high-dimensional spatial entanglement [39]. Our results thus establish core-mode encoding as a hardware-efficient and field-viable framework for high-dimensional quantum-secure communications.

ACKNOWLEDGMENTS

This research was funded by ANID Anillo Project No. ATE250003, Fondo Nacional de Desarrollo Científico y Tecnológico (FONDECYT) Grants No. 1260111, No. 1240746, No. 1240843, No. 1231940, ANID Millennium Science Initiative Program ICN17-012, ANID AC3E CIA 250006, and Wallenberg Center for Quantum Technologies (WACQT). D.M. gratefully acknowledges the support from the Austrian Federal Ministry of Labour and Economy, the National Foundation for Research, Technology, and the Christian Doppler Research Association.

DATA AVAILABILITY

There are no publicly available research data or software supporting this manuscript. Requests for further information or data should be sent to the authors.

APPENDIX A: ASYMPTOTIC TWO-DECOY BOUNDS

For the two-decoy configuration used in this work, a weak decoy of intensity ν and a vacuum decoy, a lower bound on the single-photon gain is given by [29]

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2} \left[Q_\nu e^\nu - \frac{\nu^2}{\mu^2} Q_\mu e^\mu - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right], \quad (\text{A1})$$

and the upper bound on the single-photon error rate by

$$e_1^U = \frac{E_\nu Q_\nu \mu e^\nu - \mu e_0 Y_0}{\nu Q_1^L e^\mu}, \quad (\text{A2})$$

where $e_0 = (d-1)/d$ is the probability of a random dark count in a detector that is not expected to fire when Alice's and Bob's bases are matched, and Q_ν and E_ν are the gain and QBER for the decoy state ν . Substituting Eqs. (A1) and (A2) into Eq. (1) of the main text yields Eq. (3).

APPENDIX B: BETA-DISTRIBUTION FITS OF THE QBER HISTOGRAMS

The histograms of the QBER measured in 100 ms windows on the PtE link (Fig. 4 of the main text) were fitted with the Beta probability density function

$$f(x; \alpha, \beta) = \frac{1}{B(\alpha, \beta)} x^{\alpha-1} (1-x)^{\beta-1}, \quad 0 < x < 1, \quad (\text{B1})$$

where α and β are the shape parameters and the Beta function $B(\alpha, \beta)$ normalizes the distribution. Being defined on a bounded support, this function reproduces the

TABLE IV. Shape parameters α and β obtained by fitting Eq. (B1) to the QBER histograms of Fig. 4, measured on the PtE link, and the variance $\alpha\beta/[(\alpha+\beta)^2(\alpha+\beta+1)]$ of the fitted distribution. N_w is the number of 100 ms windows recorded at each threshold, and the last column is the fraction of those windows whose QBER lies below the $d=4$ security bound, QBER = 18.93%.

T (%)	α	β	Var	N_w	QBER < 18.93%
5	3.18	24.99	0.003	289	89.62%
8	2.36	15.95	0.006	1390	84.24%
10	3.09	18.37	0.005	2223	77.87%
13	3.78	24.74	0.004	3566	79.98%
15	3.18	16.99	0.006	3688	70.50%

asymmetric character of the measured distributions. Table IV lists the fitted parameters for each threshold T , together with the variance of the fitted distribution, the number of recorded windows N_w and the fraction of windows whose QBER lies below the $d=4$ security bound. These statistics quantify the trade-off between window quality and duty cycle discussed in Sec. V.

APPENDIX C: FINITE-KEY PARAMETER ESTIMATION PROCEDURE

Here we present the complete procedure used to estimate the finite-key bounds M_1^{zL} , M_0^{zL} , and e_1^U appearing in Eq. (4) of the main text. The analysis follows the method of Zhang *et al.* [32] for the two-decoy finite-key protocol. We adapt the method to the high-dimensional case and extend it to obtain a finite-key correction for the bound M_0^{zL} .

1. Step 1: Inverse Chernoff bounds and Y_1^{*L}

For any experimentally observed count χ , the quantities $\mathbb{E}^L[\chi]$ and $\mathbb{E}^U[\chi]$ denote, respectively, lower and upper bounds on the expected value $\mathbb{E}[\chi]$ obtained using inverse Chernoff bounds. These bounds are given by

$$\mathbb{E}^L[\chi] = \frac{\chi}{1 + \delta^L}, \quad \mathbb{E}^U[\chi] = \frac{\chi}{1 - \delta^U}, \quad (\text{C1})$$

where δ^L and δ^U are obtained numerically from

$$\left[\frac{e^{\delta^L}}{(1 + \delta^L)^{1 + \delta^L}} \right]^{\chi/(1 + \delta^L)} = \frac{1}{2} \epsilon, \quad (\text{C2})$$

$$\left[\frac{e^{-\delta^U}}{(1 - \delta^U)^{1 - \delta^U}} \right]^{\chi/(1 - \delta^U)} = \frac{1}{2} \epsilon, \quad (\text{C3})$$

for a chosen failure probability $\epsilon = 10^{-10}$.

Using $\mathbb{E}[M_a]/N_a = \mathbb{E}[Q_a]$, where Q_a denotes the gain associated with WCPs of type a , the finite-key analog of the single-photon yield lower bound is

$$Y_1^{*L} = \frac{\mu}{\mu\nu - \nu^2} \left[\frac{\mathbb{E}^L[M_\nu]}{N_\nu} e^\nu - \frac{\nu^2 \mathbb{E}^U[M_\mu]}{\mu^2 N_\mu} e^\mu - \frac{\mu^2 - \nu^2}{\mu^2} \frac{\mathbb{E}^U[M_0]}{N_0} \right]. \quad (\text{C4})$$

The corresponding lower bound on the expected number of single-photon detections in the $\mathcal{Z}$ basis across all WCPs is then

$$M_1^{*zL} = Y_1^{*L} N p_z^2 (p_\mu e^{-\mu} \mu + p_\nu e^{-\nu} \nu). \quad (\text{C5})$$

2. Step 2: Lower bound M_1^{zL}

The quantity M_1^{*zL} provides a bound on the expected number of single-photon detections across all WCPs. To obtain the bound restricted to the signal WCP, the symmetric Chernoff bound is applied with $\bar{\chi} = \mathbb{E}[M_1^{zL}] = p_{1s} M_1^{*zL}$, where p_{1s} denotes the probability that a single-photon detection in the $\mathcal{Z}$ basis is from the signal WCP. This yields

$$M_1^{zL} = (1 - \delta)\bar{\chi}, \quad (\text{C6})$$

with

$$\delta = \frac{-\ln(\epsilon/2) + \sqrt{\ln(\epsilon/2)^2 - 8\ln(\epsilon/2)\bar{\chi}}}{\bar{\chi}}. \quad (\text{C7})$$

3. Step 3: Lower bound M_0^{zL}

An analogous inverse-Chernoff analysis is applied to the vacuum detections. This gives

$$Y_0^{*L} = \frac{\mathbb{E}^L[M_0]}{N_0}; \quad (\text{C8})$$

$$M_0^{*zL} = Y_0^{*L} N p_z^2 (p_\mu e^{-\mu} + p_\nu e^{-\nu} + p_v), \quad (\text{C9})$$

from which the bound on vacuum detections associated with the signal intensity is obtained as $M_0^{zL} = (1 - \delta)\bar{\chi}$ with $\bar{\chi} = p_{0s} M_0^{*zL}$, where p_{0s} denotes the probability that a vacuum detection in the $\mathcal{Z}$ basis came from the signal WCP.

4. Step 4: Upper bound e_1^U from $\mathcal{X}$ basis

Inverse Chernoff bounds applied to the error counts yield

$$e_1^U = \frac{\frac{\mathbb{E}^U[E_{0x} M_{0x}]}{N_{0x}} e^\nu - \frac{\mathbb{E}^L[E_{0x} M_{0x}]}{N_{0x}}}{Y_1^{*L} \nu}. \quad (\text{C10})$$

To relate this quantity to the phase-error rate in the $\mathcal{Z}$ basis, a random-sampling argument is used. The correction θ satisfying $e_1^U = e_1^{xU} + \theta$ is obtained numerically from

$$\epsilon = \frac{\sqrt{M_1^{*xL} + M_1^{zL}}}{\sqrt{e_1^{xU}(1 - e_1^{xU})M_1^{*xL} M_1^{zL}}} 2^{-(M_1^{*xL} + M_1^{zL})\epsilon(\theta)}, \quad (\text{C11})$$

where $\epsilon(\theta) = H_2(e_1^{xU} + \theta - q_x \theta) - q_x H_2(e_1^{xU}) - (1 - q_x) H_2(e_1^{xU} + \theta)$ and $q_x = M_1^{*xL} / (M_1^{*xL} + M_1^{zL})$.

Substituting the resulting bounds M_1^{zL} , M_0^{zL} , and e_1^U into Eq. (4) yields the composable secret key length K , guaranteeing ϵ_{sec} security and ϵ_{cor} correctness against general attacks.

In the case that the parameters $\epsilon_{\text{cor}}, \epsilon_{\text{sec}} > 0$, the protocol is said to be $(\epsilon_{\text{cor}} + \epsilon_{\text{sec}})$ -secure [33]. Correctness is satisfied if

$$\Pr[K_A \neq K_B] \leq \epsilon_{\text{cor}}, \quad (\text{C12})$$

where K_A and K_B denote the final secret keys held by Alice and Bob, respectively. Thus, the probability that Alice and Bob obtain different final keys is bounded by ϵ_{cor} . Secrecy is satisfied if

$$(1 - p_{\text{abort}}) \|\rho_{AE} - U_A \otimes \rho_E\|_{1/2} \leq \epsilon_{\text{sec}}, \quad (\text{C13})$$

where ρ_{AE} is the joint state of Alice's final key and Eve's system. U_A is the uniform mixture over all possible values of Alice's final key, and p_{abort} is the probability that the protocol aborts. This condition guarantees that, except with probability ϵ_{sec} , the final key is indistinguishable from an ideal uniform secret key independent of Eve's information.

In practical QKD implementations, the correctness parameter is commonly chosen as $\epsilon_{\text{cor}} = 10^{-15}$, while the secrecy parameter is typically taken to scale with the final secret-key length. Following the standard convention adopted in the literature, the secrecy contribution is therefore written as $\epsilon_{\text{sec}} = 10^{-15} \times K$, prior to the additional finite-key corrections introduced by the statistical estimation procedure.

APPENDIX D: FOUR-DIMENSIONAL BB84 QKD STATES AND BASIS

In Fig. 7 we give the explicit form of the states prepared by Alice and measured by Bob.

The four measurement basis states defined by Bob's 4 C-MBS are [25]

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{2} (e^{i\phi_0^B} |0\rangle + e^{i\phi_1^B} |1\rangle + e^{i\phi_2^B} |2\rangle + e^{i\phi_3^B} |3\rangle), \\ |\psi_1\rangle &= \frac{1}{2} (e^{i\phi_0^B} |0\rangle + e^{i\phi_1^B} |1\rangle - e^{i\phi_2^B} |2\rangle - e^{i\phi_3^B} |3\rangle), \\ |\psi_2\rangle &= \frac{1}{2} (e^{i\phi_0^B} |0\rangle - e^{i\phi_1^B} |1\rangle + e^{i\phi_2^B} |2\rangle - e^{i\phi_3^B} |3\rangle), \\ |\psi_3\rangle &= \frac{1}{2} (e^{i\phi_0^B} |0\rangle - e^{i\phi_1^B} |1\rangle - e^{i\phi_2^B} |2\rangle + e^{i\phi_3^B} |3\rangle), \end{aligned} \quad (\text{D1})$$

where ϕ_k^B is the phase applied by the second modulator in the core mode k .

APPENDIX E: RECORDED DATA USED IN THE ASYMPTOTIC KEY RATE CALCULATIONS

In Tables V and VI, we list the recorded data used to reproduce all the asymptotic key-rate calculations reported in the main text with the InGaAs SPDs and SNSPDs, respectively.

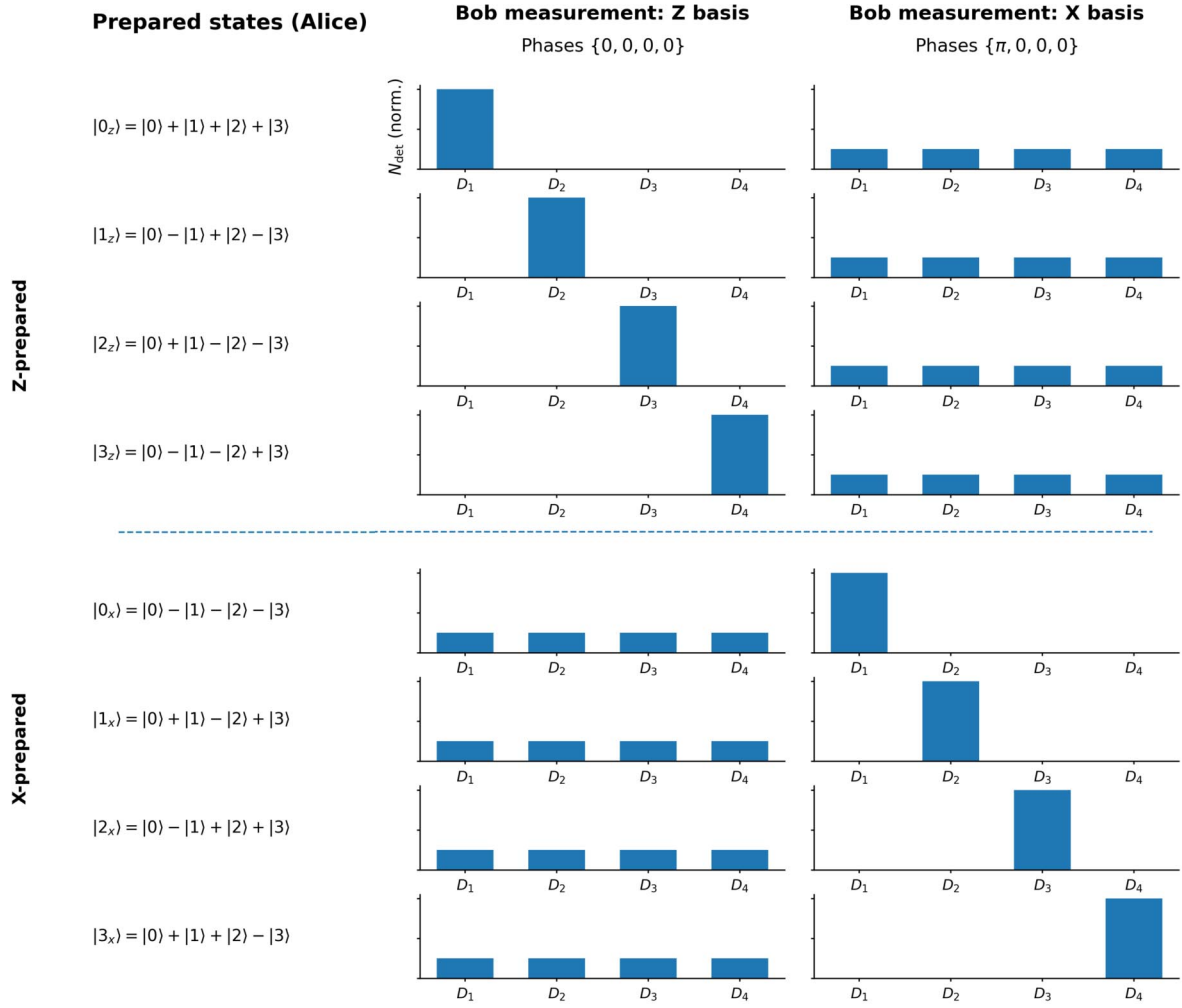


FIG. 7. Expected detection distribution for each prepared qudit state at Bob's four single-photon detectors ($D_1 - D_4$), for both the $\mathcal{Z}$ basis (center column, phase pattern $\{0, 0, 0, 0\}$) and the $\mathcal{X}$ basis (right column, phase pattern $\{\pi, 0, 0, 0\}$). Each row corresponds to one of the eight prepared states. A tall bar in detector D_k indicates high probability of detection at port k ; ideally one port dominates for each state, realizing the BB84 discrimination condition.

TABLE V. Recorded data used for the asymptotic calculations with the InGaAs SPDs. $P_{\text{dark}} = 3.81 \times 10^{-6} \pm 2.27 \times 10^{-6}$.

Quantity	BtB, 2.16 dB	P6, 9.36 dB	PtE, 10.70 dB	Sim., 14.0 dB
E_μ	0.1151 ± 0.0187	0.1195 ± 0.0179	0.1417 ± 0.0255	0.1639 ± 0.0350
Q_μ	$325.0 \times 10^{-5} \pm 5.2 \times 10^{-5}$	$57.1 \times 10^{-5} \pm 1.9 \times 10^{-5}$	$46.7 \times 10^{-5} \pm 1.9 \times 10^{-5}$	$17.8 \times 10^{-5} \pm 1.2 \times 10^{-5}$
μ	0.2673 ± 0.0069	0.2409 ± 0.0099	0.2658 ± 0.0124	0.2051 ± 0.0160
E_ν	0.1062 ± 0.0173	0.1402 ± 0.0237	0.1581 ± 0.0279	0.2687 ± 0.0513
Q_ν	$122.4 \times 10^{-5} \pm 3.3 \times 10^{-5}$	$23.3 \times 10^{-5} \pm 1.3 \times 10^{-5}$	$18.4 \times 10^{-5} \pm 1.3 \times 10^{-5}$	$68.6 \times 10^{-6} \pm 7.0 \times 10^{-6}$
ν	0.0997 ± 0.0034	0.0936 ± 0.0060	0.0992 ± 0.0081	0.0672 ± 0.0098
e_1^U	0.1108 ± 0.0234	0.1127 ± 0.0584	0.1233 ± 0.0752	0.1536 ± 0.2128
Q_1^L	$24.5 \times 10^{-4} \pm 1.9 \times 10^{-4}$	$43.4 \times 10^{-5} \pm 9.3 \times 10^{-5}$	$34.4 \times 10^{-5} \pm 9.2 \times 10^{-5}$	$13.4 \times 10^{-5} \pm 7.8 \times 10^{-5}$
R_∞	$8.77 \times 10^{-4} \pm 5.00 \times 10^{-4}$	$1.64 \times 10^{-4} \pm 1.40 \times 10^{-4}$	$6.04 \times 10^{-5} \pm 1.35 \times 10^{-4}$	$8.62 \times 10^{-6} \pm 7.63 \times 10^{-5}$

TABLE VI. Recorded data used for the asymptotic calculations with the SNSPDs. $P_{\text{dark}} = 13.50 \times 10^{-6} \pm 1.30 \times 10^{-6}$.

Quantity	BtB, 2.16 dB	P6, 9.36 dB	PtE, 10.70 dB	Sim., 20.0 dB
E_μ	0.0247 ± 0.0269	0.0510 ± 0.0015	0.0392 ± 0.0014	0.0447 ± 0.0059
Q_μ	$603.0 \times 10^{-4} \pm 7.5 \times 10^{-4}$	$1897.1 \times 10^{-5} \pm 2.1 \times 10^{-5}$	$1227.2 \times 10^{-5} \pm 1.5 \times 10^{-5}$	$1816.1 \times 10^{-6} \pm 7.9 \times 10^{-6}$
μ	0.8685 ± 0.0106	0.7296 ± 0.0073	0.6657 ± 0.0067	0.7807 ± 0.0089
E_ν	0.0603 ± 0.0129	0.0743 ± 0.0059	0.1320 ± 0.0104	0.3567 ± 0.0358
Q_ν	$189.5 \times 10^{-5} \pm 9.7 \times 10^{-5}$	$1187.0 \times 10^{-6} \pm 5.3 \times 10^{-6}$	$709.8 \times 10^{-5} \pm 5.8 \times 10^{-6}$	$137.8 \times 10^{-6} \pm 4.8 \times 10^{-6}$
ν	0.0134 ± 0.0007	0.0433 ± 0.0005	0.0341 ± 0.0005	0.0371 ± 0.0032
e_1^U	0.0411 ± 0.0146	0.0463 ± 0.0075	0.0870 ± 0.0135	0.1248 ± 0.0813
Q_1^L	0.0497 ± 0.0039	$90.4 \times 10^{-4} \pm 1.4 \times 10^{-4}$	$65.0 \times 10^{-4} \pm 1.4 \times 10^{-4}$	$8.1 \times 10^{-4} \pm 1.1 \times 10^{-4}$
R_∞	$5.96 \times 10^{-2} \pm 2.33 \times 10^{-2}$	$7.63 \times 10^{-3} \pm 5.01 \times 10^{-4}$	$5.36 \times 10^{-3} \pm 4.98 \times 10^{-4}$	$4.34 \times 10^{-4} \pm 3.26 \times 10^{-4}$

- [1] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
- [2] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, *Theor. Comput. Sci.* **560**, 7 (2014).
- [3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. 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).
- [4] 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).
- [5] P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994), pp. 124–134.
- [6] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, *SIAM J. Comput.* **26**, 1484 (1997).
- [7] 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).
- [8] L. Sheridan and V. Scarani, *Security proof for quantum key distribution using qudit systems*, *Phys. Rev. A* **82**, 030301(R) (2010).
- [9] H. Bechmann-Pasquinucci and W. Tittel, *Quantum cryptography using larger alphabets*, *Phys. Rev. A* **61**, 062308 (2000).
- [10] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, *High-dimensional quantum communication: Benefits, progress, and future challenges*, *Adv. Quantum Technol.* **2**, 1900038 (2019).
- [11] D. Bruß and C. Macchiavello, *Optimal eavesdropping in cryptography with three-dimensional quantum states*, *Phys. Rev. Lett.* **88**, 127901 (2002).
- [12] G. B. Xavier and G. Lima, *Quantum information processing with space-division multiplexing optical fibres*, *Commun. Phys.* **3**, 9 (2020).
- [13] D. J. Richardson, *Filling the light pipe*, *Science* **330**, 327 (2010).
- [14] D. J. Richardson, J. M. Fini, and L. E. Nelson, *Space-division multiplexing in optical fibres*, *Nat. Photonics* **7**, 354 (2013).
- [15] I. Morita, K. Igarashi, H. Takahashi, T. Tsuritani, and M. Suzuki, *Trans-oceanic class ultra-long-haul transmission using multi-core fiber*, *Opt. Express* **22**, 31761 (2014).
- [16] D. Soma, S. Beppu, Y. Wakayama, K. Igarashi, T. Tsuritani, I. Morita, and M. Suzuki, *10.16-peta-B/s dense SDM/WDM transmission over 6-mode 19-core fiber across the C + L band*, *J. Lightwave Technol.* **36**, 1375 (2018).
- [17] H. Takeshita, K. Nakamura, Y. Matsuo, T. Inoue, D. Masuda, T. Hiwatashi, K. Hosokawa, Y. Inada, and E. L. T. de Gabory, *Demonstration of uncoupled 4-core multicore fiber in submarine cable prototype with integrated multicore EDFA*, *J. Lightwave Technol.* **41**, 980 (2023).
- [18] Q. Wu *et al.*, *Integration of quantum key distribution and high-throughput classical communications in field-deployed multi-core fibers*, *Light:Sci. Appl.* **14**, 274 (2025).
- [19] C. Melo, M. Reyes F., D. Arroyo, E. S. Gómez, S. P. Walborn, G. Lima, M. Figueroa, J. Cariñe, and G. Saavedra, *All-fiber architecture for high speed core-selective switch for multicore fibers*, *Commun. Eng.* **4**, 77 (2025).
- [20] Y. Chen *et al.*, *High-capacity optical communication relayed by multi-core amplifier on deployed submarine seven-core fiber cable*, *Commun. Eng.* **5**, 108 (2026).
- [21] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysieszna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. F. da Silva, G. B. Xavier, and G. Lima, *High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers*, *Phys. Rev. A* **96**, 022317 (2017).
- [22] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, *High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits*, *npj Quantum Inf.* **3**, 25 (2017).
- [23] B. Da Lio, L. K. Oxenløwe, D. Bacco, D. Cozzolino, N. Biagi, T. N. Arge, E. Larsen, K. Rottwitt, Y. Ding, and A. Zavatta, *Stable transmission of high-dimensional quantum*

- states over a 2-km multicore fiber, *IEEE J. Sel. Top. Quantum Electron.* **26**, 1 (2020).
- [24] D. Bacco, N. Biagi, I. Vagniluca, T. Hayashi, A. Mecozzi, C. Antonelli, L. K. Oxenløwe, and A. Zavatta, *Characterization and stability measurement of deployed multicore fibers for quantum applications*, *Photonics Res.* **9**, 1992 (2021).
- [25] J. Cariñe, G. Cañas, P. Skrzypczyk, I. Šupić, N. Guerrero, T. García, L. Pereira, M. A. S. Prosser, G. B. Xavier, A. Delgado, S. P. Walborn, D. Cavalcanti, and G. Lima, *Multi-core fiber integrated multi-port beam splitters for quantum information processing*, *Optica* **7**, 542 (2020).
- [26] M. Zahidy, D. Ribezzo, C. De Lazzari, I. Vagniluca, N. Biagi, R. Müller, T. Occhipinti, L. K. Oxenløwe, M. Galili, T. Hayashi, D. Cassioli, A. Mecozzi, C. Antonelli, A. Zavatta, and D. Bacco, *Practical high-dimensional quantum key distribution protocol over deployed multicore fiber*, *Nat. Commun.* **15**, 1651 (2024).
- [27] A. Alarcón, J. Argillander, G. Lima, and G. B. Xavier, *Few-mode-fiber technology fine-tunes losses in quantum communication systems*, *Phys. Rev. Appl.* **16**, 034018 (2021).
- [28] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, *Provably secure and high-rate quantum key distribution with time-bin qudits*, *Sci. Adv.* **3**, e1701491 (2017).
- [29] H.-K. Lo, X. Ma, and K. Chen, *Decoy state quantum key distribution*, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [30] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, *Discrete-phase-randomized coherent state source and its application in quantum key distribution*, *New J. Phys.* **17**, 053014 (2015).
- [31] D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, *Security proof for a simplified Bennett-Brassard 1984 quantum-key-distribution protocol*, *Phys. Rev. A* **98**, 052336 (2018).
- [32] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, *Improved key-rate bounds for practical decoy-state quantum-key-distribution systems*, *Phys. Rev. A* **95**, 012333 (2017).
- [33] 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).
- [34] T. Hayashi, T. Taru, O. Shimakawa, T. Sasaki, and E. Sasaoka, *Design and fabrication of ultra-low crosstalk and low-loss multi-core fiber*, *Opt. Express* **19**, 16576 (2011).
- [35] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, *Measurement of qubits*, *Phys. Rev. A* **64**, 052312 (2001).
- [36] M. S. Kaznady and D. F. V. James, *Numerical strategies for quantum tomography: Alternatives to full optimization*, *Phys. Rev. A* **79**, 022109 (2009).
- [37] H. Abarzúa, C. Melo, S. E. Restrepo, S. Vergara, D. Sbarbaro, G. Cañas, G. Lima, G. Saavedra, and J. Cariñe, *Adaptive-step perturb-and-observe algorithm for multidimensional phase noise stabilization in fiber-based multi-arm Mach-Zehnder interferometers*, *Algorithms* **17**, 534 (2024).
- [38] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Q. Li, Y. Liu, Q. Zhang, C.-Z. Peng, L. You, F. Xu, and J.-W. Pan, *High-rate quantum key distribution exceeding 110 Mbs⁻¹*, *Nat. Photonics* **17**, 416 (2023).
- [39] E. S. Gómez, S. Gómez, I. Machuca, A. Cabello, S. Pádua, S. P. Walborn, and G. Lima, *Multidimensional entanglement generation with multicore optical fibers*, *Phys. Rev. Appl.* **15**, 034024 (2021).