Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution

Vagniluca, Ilaria; Da Lio, Beatrice; Rusca, Davide; Cozzolino, Daniele; Ding, Yunhong; Zbinden, Hugo; Zavatta, Alessandro; Oxenløwe, Leif K.; Bacco, Davide

How to cite

VAGNILUCA, Ilaria et al. Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution. In: Physical Review Applied, 2020, vol. 14, p. 014051. doi: 10.1103/PhysRevApplied.14.014051

This publication URL: https://archive-ouverte.unige.ch/unige:140301

Publication DOI: 10.1103/PhysRevApplied.14.014051

Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution

Ilaria Vagniluca,[1,2] Beatrice Da Lio,[3] Davide Rusca,[4] Daniele Cozzolino,[3] Yunhong Ding,[3] Hugo Zbinden,[4] Alessandro Zavatta,[1,5] Leif K. Oxenløwe,[3] and Davide Bacco[3,*]

[1] *Istituto Nazionale di Ottica (INO-CNR), Largo E. Fermi 6, 50125 Florence, Italy*

[2] *Department of Physics "Ettore Pancini", University of Naples "Federico II", Via Cinthia 21, 80126 Naples, Italy*

[3] *CoE SPOC, DTU Fotonik, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark*

[4] *Group of Applied Physics, Université de Genève, Chemin de Pinchat 22, 1211 Geneva 4, Switzerland*

[5] *LENS and Department of Physics, University of Florence, 50019 Sesto Fiorentino, Italy*

(Received 20 December 2019; revised 21 February 2020; accepted 6 April 2020; published 17 July 2020)

High-dimensional quantum key distribution (QKD) allows achievement of information-theoretic secure communications, providing high key-generation rates, which cannot, in principle, be obtained by QKD protocols with binary encoding. Nonetheless, the amount of experimental resources needed increases as the quantum states to be detected belong to a larger Hilbert space, thus raising the costs of practical high-dimensional systems. Here, we present an alternative scheme for fiber-based four-dimensional QKD, with time and phase encoding and one-decoy state technique. Quantum state transmission is tested over different channel lengths up to 145 km of standard single-mode fiber, evaluating the enhancement of the secret key rate in comparison to the three-state two-dimensional BB84 protocol, which is tested with the same experimental setup. Our scheme allows measurement of the four-dimensional states with a simplified and compact receiver, where only two single-photon detectors are necessary, thus making it a cost-effective solution for practical and fiber-based QKD.

DOI: 10.1103/PhysRevApplied.14.014051

I. INTRODUCTION

As the constant advancement in quantum computing is threatening the security of current cryptographic systems, our society needs an alternative technology to safely transmit sensitive data and confidential information [1]. A quantum-proof solution to safely deliver our cryptographic keys is quantum key distribution (QKD), which exploits quantum states of light as safeguarded bit carriers over untrusted communication channels [2–5]. In well-established QKD protocols such as the BB84 [2], each bit of the key is carried by a single photon, which is prepared in order to span a set of different quantum states belonging to a two-dimensional Hilbert space, i.e., qubits. High-dimensional QKD protocols were introduced more recently [6,7], proving how $n = \log_2(d) > 1$ bits of information can be safely encrypted on each single photon, by preparing an enlarged set of states belonging to a d-dimensional Hilbert space. Such states are called qudits. The higher information capacity of qudits allows for an optimized exploitation of the photon budget at the transmitter; at the same time it also mitigates the issue of saturation in the receiver's single-photon detectors. Moreover, using high-dimensional states improves the robustness to the noise affecting the communication, allowing for a higher threshold value of the quantum bit error rate (QBER). The result is an increase in the secret key rate achievable by high-dimensional QKD, as compared with standard QKD protocols with binary encoding ($d = 2$), at least until the overall losses are low enough to keep negligible the random dark counts at the receiver [8–10].

Although there are many degrees of freedom to be exploited to send more than one bit per photon [11–15], time-bin and time-energy encoding are the ones more suitable for single-mode fiber propagation, and thus more compatible with the already existing and widespread fiber networks [16–23]. Recent demonstrations of one-way fiber-based QKD include the record-breaking key rate of 26.2 Mbit/s at 4-dB channel loss [19], achieved with a four-dimensional time-bin protocol with two decoy states, which is proven to be robust against the most general (or coherent) attacks as well as finite-size effects. However, the apparent gain in the key rate comes with a cost, as the

*dabac@fotonik.dtu.dk

preparation and measurement of high-dimensional states require a larger amount of experimental resources, especially at the receiver, who has to project the incoming qudits on two unbiased bases of d orthogonal states. For instance, to perform the time-bin protocol presented in Ref. [19], at least three cascaded interferometers and five single-photon detectors are necessary to measure the four-dimensional states (actually three more detectors were added in the cited work, in order to reduce saturation effects in the first basis measurements). On the other hand, a simpler receiver with only two single-photon detectors is sufficient in many of the binary-encoded protocols with the same level of security, such as the BB84 [21,24,25].

In this work we present an alternative scheme for four-dimensional QKD with time-bin encoding, which allows implementation of a simplified and more compact receiver, where only two single-photon detectors are necessary for measuring all the quantum states. The security of this protocol against general attacks is demonstrated in a finite-key scenario, when a simple and efficient one-decoy state method is implemented. Qudit exchange is tested over different fiber channels up to 145 km of length, corresponding to 31.5 dB of transmission loss. In addition to this, in order to evaluate the improved performances of our protocol, we also test a two-dimensional BB84 scheme over the same channel lengths, by employing mostly the same experimental setup. It is to be noted that both QKD systems employ two single-photon detectors, i.e., our proposal is cost effective. This method allows us to make a fair and rational comparison between the two time-bin protocols with $d = 2$ and $d = 4$. In the following sections, we describe the two protocols and we report the security analysis of our QKD scheme. We then show the experimental setup of the transmitter and the receiver. Finally, our results are presented and discussed in the last section of the paper.

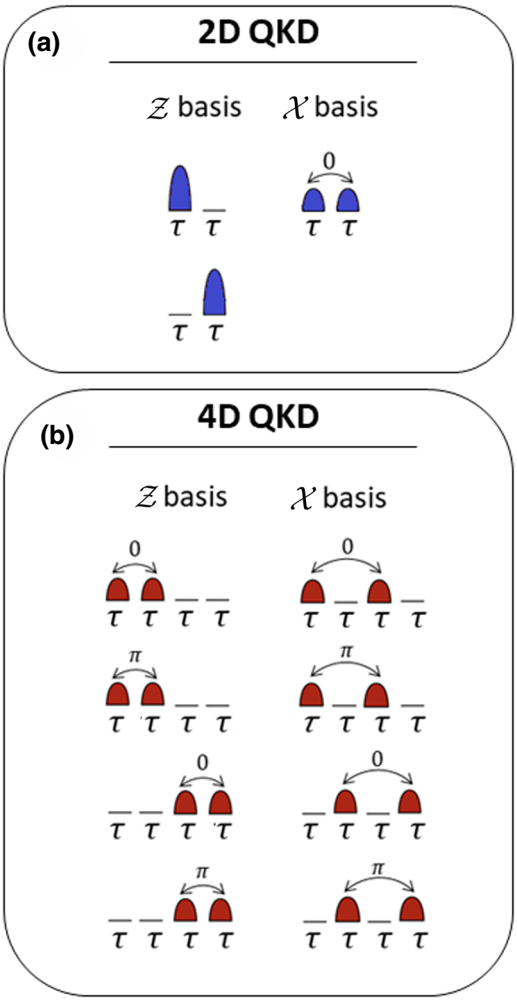

FIG. 1. Quantum states involved in the two QKD protocols. The three states belonging to the two-dimensional BB84 (a) and the eight states belonging to the four-dimensional protocol (b). τ is the time-bin duration, while 0 and π specify the relative phase between the different time bins occupied by the photon.

II. PROTOCOLS

Figure 1 schematically depicts the quantum states and mutually unbiased bases belonging to the two different QKD schemes that are performed in this work. The two- and four-dimensional protocols that we implement are the three-state time-bin BB84 and one of its possible generalizations in four dimensions, respectively. Both schemes are secure against general eavesdropping attacks that are addressed to the transmission channel, as we discuss later for a finite-key analysis. Defining τ as the bin duration, each qubit and qudit has a time span of two and four bins, respectively. In both cases, quantum states of the $\mathcal{Z}$ basis are adopted for key bits' encoding, while the $\mathcal{X}$ basis is implemented only for security checking. In the three-state BB84 [21], quantum states belonging to the $\mathcal{Z}$ basis differ for the time bin occupied by the photon and only one bit, corresponding to early or late bin occupation, is encoded on each state. The third state is the superposition of the two $\mathcal{Z}$ basis states with 0 relative phase, while the other orthogonal state in the $\mathcal{X}$ basis (with π relative phase) is not prepared, thus making this protocol a simplified version of the original four-state BB84. Here, the projection on the $\mathcal{Z}$ basis is made at the receiver by measuring the photon arrival time with a single-photon detector, while the $\mathcal{X}$ basis is measured by monitoring, with another single-photon detector, one of the two outputs of a Mach-Zehnder interferometer with a delay equal to τ. Whenever weak coherent pulses are prepared instead of single photons (as in our case), an efficient one-decoy scheme can be implemented in order to avoid photon-number splitting attacks [26–28]. The secret key length ℓ_{2D} per privacy amplification block is then given by the

following formula:

$$\ell_{2D} \leq D_0^{\mathcal{Z}} + D_1^{\mathcal{Z}}\Big[1 - h\big(\phi_{\mathcal{Z}}\big)\Big] - \lambda_{EC} - 6\log_2(19/\epsilon_{sec}) - \log_2(2/\epsilon_{corr}), \quad (1)$$

where $D_0^{\mathcal{Z}}$ and $D_1^{\mathcal{Z}}$ are the lower bounds of vacuum events and single-photon events in the $\mathcal{Z}$ basis, $h(\cdot)$ is the binary entropy function, $\phi_{\mathcal{Z}}$ is the upper bound on the phase error rate and λ_{EC} is the number of bits that are publicly announced during error correction, while ϵ_{sec} and ϵ_{corr} are the secrecy and correctness parameters [29].

The direct generalization in four dimensions of the time-bin BB84 is the protocol presented in Ref. [19], where the four qudits belonging to the $\mathcal{Z}$ basis differ only for the time bin, which is individually occupied among the four bins available, and each state of the $\mathcal{X}$ basis is a superposition of all the four bins, combined with different relative phases. In that case, the projection on the $\mathcal{Z}$ basis is made simply with a detector measuring the time of arrival of the photons, as for the two-dimensional protocol. On the other hand, the projection on the mutually unbiased $\mathcal{X}$ basis requires a more complicated setup, with at least a cascade of three interferometers and four detectors (as reported in Refs. [19] and [30]) or even more complex solutions (as discussed in Ref. [31]).

In our alternative scheme we exploit two more convenient four-dimensional bases, which are depicted in Fig. 1(b). Here, we have two time bins combined for each state in both bases, and the four states that are defined on consecutive bins are employed for key encoding in the $\mathcal{Z}$ basis. Qudits belonging to the same basis are orthogonal to each other and the two bases are mutually unbiased, since the general relation

$$\left|\langle z_n|x_m\rangle\right|^2 = \frac{1}{d} \quad (2)$$

is still satisfied for all $|z_n\rangle$ and $|x_m\rangle$ states belonging to $\mathcal{Z}$ and $\mathcal{X}$ basis, respectively, $(n, m = 0, \ldots, d-1)$. For this scheme, the projection on the $\mathcal{Z}$ basis is made with one single τ-delayed interferometer, while the projection on the $\mathcal{X}$ basis requires a single 2τ-delayed interferometer. This makes it possible to hugely simplify the experimental setup at the receiver side, in comparison to Ref. [19], as we further describe in the following section.

The secret key length ℓ_{4D} per privacy amplification block is given by

$$\ell_{4D} \leq 2D_0^{\mathcal{Z}} + D_1^{\mathcal{Z}}\Big[2 - H\big(\phi_{\mathcal{Z}}\big)\Big] - \lambda_{EC} - 6\log_2(19/\epsilon_{sec}) - \log_2(2/\epsilon_{corr}), \quad (3)$$

where $H(x) := -x\log_2(x/3) - (1-x)\log_2(1-x)$ is the Shannon entropy in a four-dimensional Hilbert space. The lower and upper bounds on the single-photon events in the equation above are obtained by using the one-decoy technique appearing in Ref. [28], modified for the four-dimensional QKD protocol. The difference between the original one-decoy protocol [28] and the one presented here is the method to find the upper bound to the vacuum events, $D_0^{\mathcal{Z},u}$. In the four-dimensional QKD each basis measurement has four possible outputs, meaning that the probability of error due to a vacuum event is 3/4. By exploiting this fact, the vacuum events can be bounded by the total number of errors $m_{\mathcal{Z},k}$ in the $\mathcal{Z}$ basis corresponding to the decoy intensity k. By correcting the estimated quantities using the finite-key technique presented in Ref. [28], the upper bound to the vacuum events is given by the following expression:

$$D_0^{\mathcal{Z}} \leq D_0^{\mathcal{Z},u} := \frac{4}{3}\left[\tau_0\frac{e^k}{p_k}\left(m_{\mathcal{Z},k} + \sqrt{\frac{m_{\mathcal{Z}}}{2}\log\frac{1}{\varepsilon_2}}\right) + \sqrt{\frac{n_{\mathcal{Z}}}{2}\log\frac{1}{\varepsilon_1}}\right], \quad (4)$$

where $\tau_0 = \sum_{k\in\kappa} p_k e^{-k}$ is the total probability to send the vacuum state, p_k is the probability to prepare the decoy state of intensity k, $n_{\mathcal{Z}}$ and $m_{\mathcal{Z}}$ are, respectively, the total number of detections and the total number of errors in the $\mathcal{Z}$ basis.

III. EXPERIMENTAL SETUP

The experimental setup of the two QKD schemes performed is illustrated in Fig. 2. The transmitter (Alice) is very similar in both cases: a train of weak coherent pulses is prepared from a cw laser emitting at1550 nm, by means of sequential intensity modulators (IM). We employ two cascaded IMs in order to optimize the pulse carving, while a third one is used for implementing the one-decoy state technique. A phase modulator (PM) modulates the relative phase between the time bins, necessary for qudit preparation. Finally, a variable optical attenuator (VOA) is used to reach the single-photon level before sending the pulses into the fiber channel. All the optical modulators at the transmitter side are driven with a field programmable gate array (FPGA). For carving the cw laser we use a custom sequence of electrical pulses (of about 150 ps of width), which already includes Alice's state and basis choice. The time-bin duration is $\tau = 840$ ps, resulting in a qubit rate of about 595 MHz and a qudit rate of approximately 297.5 MHz. A pseudo random binary sequence (PRBS) of $2^{12} - 1$ symbols and a symbol width of $d \cdot \tau$ (with $d = 2$ or 4 depending on the protocol) is used to drive the third IM, in order to send the two different intensity levels corresponding to signal (μ_1) and decoy (μ_2) states. With this configuration, the probability to send μ_1 or μ_2 is fixed to

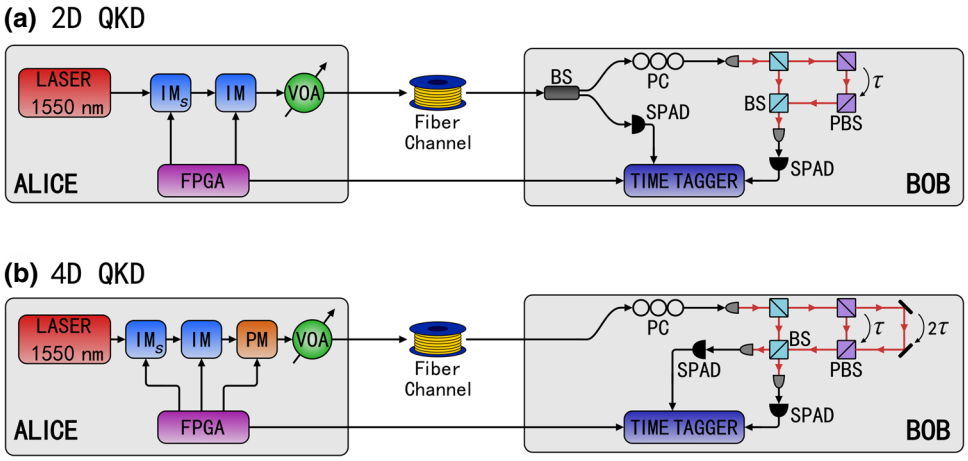

FIG. 2. Experimental setup for the two QKD schemes. Transmitter (Alice) and receiver (Bob) employed to test the three-state BB84 (a) and the four-dimensional protocol (b). Black lines represent fiber optic and electrical cables while red lines stand for free-space propagation. The same setup is employed to test both protocols, thus the three-state BB84 is performed by using one of the two overlapping interferometers that are shown in (b). IM, intensity modulator; PM, phase modulator; VOA, variable optical attenuator; FPGA, field programmable gate array; PC, polarization controller; BS, beam splitter; PBS, polarizing beam splitter; SPAD, single-photon avalanche detector. τ and 2τ are the delays in time corresponding to the two overlapped interferometers at the receiver side.

50% (for both qubits and qudit preparation) and can not be optimized for each different channel loss. To prepare the qudits, another PRBS of $2^{12}-1$ symbols and a symbol width equal to τ is used to drive the PM. Please notice that the phase randomization of quantum states (required to guarantee the security of the decoy-state method) can be easily performed with another phase modulator, or by employing a pulsed laser source working in gain-switching mode [21,32]. At the receiver side (Bob) two overlapping free-space interferometers are installed, as shown in Fig. 2(b). The short arm is in common, while the long arm is selected between two different paths (with delay equal to τ and 2τ) by means of two polarizing beam splitters (PBS). Light with vertical polarization is reflected by the PBS and follows the τ delay line, while horizontally polarized light is transmitted by the PBS and follows the 2τ delay line. To perform our measurements, the polarization of quantum pulses entering Bob's station is manually adjusted with a fiber-based polarization controller (PC). The overall loss of the τ-delayed and 2τ-delayed interferometer is 2.3 dB and 2.5 dB, respectively, due to imperfect beam splitting and fiber coupling at the detectors. Additional losses of about 9.2 dB are due to the detection efficiency (20%) and timing resolution (200 ps) of the single-photon avalanche detectors (SPADs). The detectors' dead time is 20 μs, therefore their click rate saturates when it approaches the value of 50 kHz.

To perform the two-dimensional protocol, the receiver passively selects his basis with a beam splitter (BS), as shown in Fig. 2(a). One SPAD measures the time of arrival while the other SPAD monitors an output of the τ-delayed interferometer. A time-tagging unit, which is synchronized with Alice's FPGA via a classical channel, collects the electrical outputs from the two SPADs and finally transmits the acquired data to Bob's computer. The polarization of free-space light is kept aligned with the vertical direction while testing the three-state BB84. Please notice that, to perform this protocol, the two PBS can be replaced with two standard mirrors, which make unnecessary the polarization controlling. However, here both protocols are tested with the same experimental setup, thus one of the two overlapping interferometers of the four-dimensional scheme [shown in Fig. 2(b)] is employed to also perform the three-state BB84.

In order to test the four-dimensional protocol, both outputs of the interferometers are monitored with the two SPADs, and basis selection at the receiver is made by manually switching the polarization between the two directions [Fig. 2(b)]. This means that only one of the two four-dimensional bases is prepared and measured at a time and therefore, no real-time basis choice is performed for the four-dimensional protocol during this experiment (on the other hand, the three-state BB84 is tested with real-time basis choice at both the transmitter and the receiver sides). The interference of four-dimensional states is observed in the second and fourth time bins for the $\mathcal{Z}$ basis measurements, and in the third and fourth time bins for the $\mathcal{X}$ basis measurements. The receiver can uniquely determine the output of his projection by observing the time bin and the detector at which the click occurs. It is to be noted that, even though the observed time bins at the detection output are correlated with the polarization of incoming light, this does not represent an advantage for the eavesdropper, who is still unable to control the detection efficiency in

Bob's measurement bases without being noticed. Anyway, adding a polarizer in front of Bob's setup would definitely filter out any component of residual light in the wrong polarization.

IV. RESULTS AND DISCUSSION

The two QKD schemes are tested over different channel lengths of standard single-mode fiber. The experimental parameters and results are summarized in Table I. For each transmission channel we experimentally set, at the transmitter side, the optimal values for the mean photon number of signal and decoy states (μ_1 and μ_2), that are previously estimated in order to maximize the secret key rate achievable by each protocol. As already mentioned, the probability to send μ_1 or μ_2 is fixed to 50% in our experimental setup.

For the three-state BB84 we use a pulse sequence on the FPGA consisting of 90% of $\mathcal{Z}$ basis states, thus the basis choice at the transmitter is $p_{\mathcal{Z}}^{\text{Alice}} = 0.9$ for all channel lengths. At the receiver side we set $p_{\mathcal{Z}}^{\text{Bob}}$ equal to 0.5 or 0.9 (see Table I), depending on the splitting ratio of the BS that is selected in order to maximize the secret key rate (SKR). For the four-dimensional protocol we test only one basis at a time, thus the probabilities $p_{\mathcal{Z}}^{\text{Alice}}$, $p_{\mathcal{Z}}^{\text{Bob}}$ are numerically set during the evaluation of the final SKR. We fix $p_{\mathcal{Z}}^{\text{Alice}} = 0.9$ as for the two-dimensional protocol, and again we select $p_{\mathcal{Z}}^{\text{Bob}}$ from two different values (0.7 or 0.5, see Table I) in order to get the highest SKR at each channel length.

From the acquired data we evaluate the quantum bit error rate in the $\mathcal{Z}$ basis (QBER) and in the $\mathcal{X}$ basis, which gives the upper bound on the phase error rate ($\phi_{\mathcal{Z}}$). Notice that with this terminology (the same as that adopted in most of the previous works) we always refer to the symbol-error rate, which exactly matches the bit error rate only in the two-dimensional case. These data are plotted in Fig. 3 for both protocols. As expected, the error rates appear to increase with the channel loss, due to the random noise counts, which become more and more significant as we leave the saturation regime of the single-photon detectors. Noise counts include the detectors' dark counts, the background photons entering in the fibers, and also the imperfect modulation of light pulses at the transmitter side. The QBER is lower for the two-dimensional protocol, since measuring only the arrival time of weak pulses is generally more straightforward than also measuring their phase, which requires the interference to be maximized and stabilized. On the other hand, $\phi_{\mathcal{Z}}$ is lower in the four-dimensional case, since here the photons are collected simultaneously from both outputs of each interferomenter. This configuration, where both outputs are monitored at the same time, practically results in a more stable optimization of interference during the acquisition. As a consequence, the measurement of relative phase exhibits less noise, as compared with

TABLE I. Experimental parameters and results. Here the values that we set at the transmitter and the receiver for each fiber channel are reprtoed, such as the mean photon number for signal and decoy states (μ_1, μ_2) and the probabilities to prepare and measure the $\mathcal{Z}$ basis ($p_{\mathcal{Z}}^{\text{Alice}}$, $p_{\mathcal{Z}}^{\text{Bob}}$). From the acquired data we measure the quantum bit error rate and the upper bound on the phase error rate ($\phi_{\mathcal{Z}}$) in the $\mathcal{Z}$ basis; then we evaluate the final secret key rate. The block size is fixed to 10^7 for all channel lengths. The state preparation rate (R) is 595 MHz for qubits and 297.5 MHz for qudits.

Transmission channel	Length loss	25 km 5.1 dB	65 km 14 dB	105 km 23 dB	145 km 31.5 dB
Two-dimensional	μ_1	0.07	0.12	0.26	0.31
three-state BB84	μ_2	0.03	0.06	0.14	0.15
protocol	$p_{\mathcal{Z}}^{\text{Alice}}$	0.9	0.9	0.9	0.9
($R = 595$ MHz)	$p_{\mathcal{Z}}^{\text{Bob}}$	0.5	0.9	0.5	0.5
	QBER	1.1%	1.1%	1.4%	2.3%
	$\phi_{\mathcal{Z}}$	6.6%	9.2%	8.9%	13.6%
	SKR	15 kbit/s	12 kbit/s	5.1 kbit/s	0.53 kbit/s
	SKR/R	2.6×10^{-5}	2.0×10^{-5}	8.7×10^{-6}	8.9×10^{-7}
Four-dimensional	μ_1	0.10	0.20	0.21	0.18
protocol	μ_2	0.05	0.10	0.10	0.08
	$p_{\mathcal{Z}}^{\text{Alice}}$	0.9	0.9	0.9	0.9
($R = 297.5$ Mhz)	$p_{\mathcal{Z}}^{\text{Bob}}$	0.7	0.7	0.7	0.5
	QBER	3.4%	3.4%	4.9%	7.9%
	$\phi_{\mathcal{Z}}$	3.9%	4.6%	5.7%	7.2%
	SKR	37 kbit/s	24 kbit/s	5.5 kbit/s	0.42 kbit/s
	SKR/R	1.2×10^{-4}	7.9×10^{-5}	1.8×10^{-5}	1.4×10^{-6}

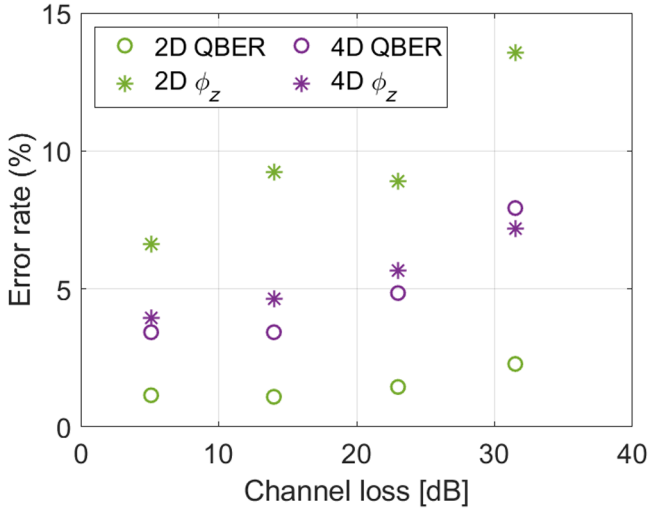

FIG. 3. Error rates measured for each protocol. Quantum bit error rate and upper bound on the phase error rate ($\phi_{\mathcal{Z}}$) experimentally measured for the two protocols, at the different channel losses.

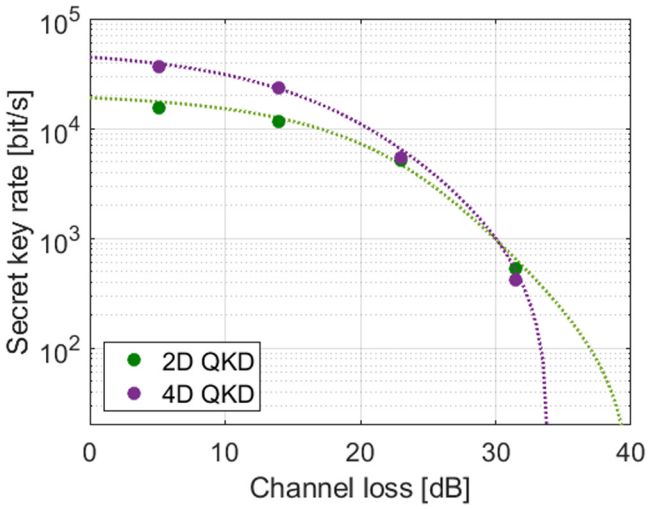

FIG. 4. Secret key rate as a function of channel loss. Each point represents the secret key rate evaluated from the experimental data. Dashed lines reproduce the simulated behavior of the secret key rate achievable by our setup, for the two QKD protocols.

the two-dimensional protocol, where only a single output of the interferometer is monitored during the acquisition. Moreover, since the measurement method of the two bases is the same in the four-dimensional case (involving both phase and time simultaneously), the values of the QBER and $\phi_{\mathcal{Z}}$ are more similar to each other, in comparison to the error rates of the two-dimensional protocol, where each basis is measured in a different way (involving only phase or only time separately). The value of $\phi_{\mathcal{Z}}$ also depends on the total amount of detections in each basis and is affected by the different setting of $p_{\mathcal{Z}}^{\mathrm{Bob}}$.

From Bob's detection data we compute the final SKR achievable in a finite-key scenario, by setting a block size of $n_{\mathcal{Z}} = 10^7$ in the $\mathcal{Z}$ basis, and a secrecy and correctness parameters of 10^{-9}. In Table I the secret fraction SKR/R is also reported, which estimates how many secret key bits can be extracted from each quantum state that is initially prepared. Our results, which are plotted in Fig. 4, show an enhancement of the SKR achievable by the four-dimensional protocol for the first two experimental points, for which the SKR is increased by a factor 2.4 and 2.0, respectively. For higher channel loss, the SKR decreases faster than in the three-state protocol, in agreement with the expected behavior, which is represented by the dashed lines in Fig. 4. Indeed, our experimental setup allows extraction of a secret key up to 39-dB channel loss with the three-state BB84, and up to 34 dB with the four-dimensional protocol. This is due to the fact that a random-noise count has $1 - 1/d$ probability to generate an error at the receiver, where d is the dimension of the encoding: the higher the Hilbert-space dimension, the more effective the random noise at the receiver is. On the other hand, the doubled information capacity and the enhanced resilience to state perturbations, make it possible to increase the SKR by more than a factor 2 in the saturation regime of the single-photon detectors. In addition, the secret fraction SKR/R is improved by the four-dimensional protocol for all the experimental points (as shown in Table I): fewer photons are necessary to deliver the same secret key. This means that if we prepare the qudits at the same rate as used for the qubits, we can increase the SKR for all of the four channel lengths.

V. CONCLUSIONS

In conclusion, we present a fiber-based four-dimensional QKD protocol with an efficient time and phase-encoding scheme, which has the advantage of requiring a very simple and compact setup at the receiver. This scheme is experimentally tested over different channel lengths, and its performances are compared with the three-state BB84, a well-established two-dimensional protocol, which is also tested in this work. Mostly the same experimental setup is employed to test the two protocols, including the same amount of single-photon detectors at the receiver, as well as the same time-bin duration (which resulted in a halved preparation rate of four-dimensional states at the transmitter). In this configuration, we demonstrate an enhancement of the secret key rate by a factor 2.4 in the saturation regime of the detectors, by testing only one four-dimensional basis at a time. In the future, we plan to perform a real-time basis choice at the receiver, by adding a polarization switcher (an off-the-shelf component for fiber-based telecommunications). This additional device introduces an extra loss at the receiver (of about

2 dB), which in any way is low enough to not affect the improved performances of our four-dimensional scheme in the saturation regime. Moreover, the effect of this extra loss can be easily balanced by reducing the other sources of loss at the receiver, or by optimizing all of the experimental parameters at the transmitter side (such as the basis choice and the decoy probabilities, which are both fixed during this experiment). Furthermore, our system can easily be modified to implement the two-decoy state technique, which is more resilient to noise. This allows us to optimize the protocol for each configuration of the experimental parameters, increasing the overall performance once more.

Our demonstration proves that high-dimensional quantum systems allow a notable improvement in the key generation process as compared with the binary-encoding case. At the same time, no extra expensive resources are necessary for the full implementation of such a system. Thus, our experiment paves the way towards a wider use of high-dimensional encoding in quantum communication.

ACKNOWLEDGMENTS

This work is supported by the Center of Excellence, SPOC – Silicon Photonics for Optical Communications (Ref. DNRF123), by the EraNET Cofund Initiatives QuantERA within the European Union's Horizon 2020 research and innovation program Grant Agreement No. 731473 (project SQUARE), by the NATO Science for Peace and Security program under Grant No. G5485 and by the European Union's Horizon 2020 program under the Marie Skłodowska-Curie project QCALL (GA 675662).

D.B. and I.V. conceived the experiment. I.V., B.D.L., D.C., and D.B. carried out the experimental work. D.R. and B.D.L. carried out the theoretical analysis on the protocols. All authors contributed to the writing of the manuscript.

[1] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on Post-Quantum Cryptography* (US Department of Commerce, National Institute of Standards and Technology, 2016).

[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers Systems and Signal Processing* (IEEE, Los Alamitos, CA, 1984), p. 175.

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

[4] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Advances in quantum cryptography, arXiv:1906.01645 (2019).

[5] F. Xu, X. M. Zhang, H.-K. Lo, J.-W. Pan *et al.*, Quantum cryptography with realistic devices, arXiv:1903.09051 (2019).

[6] H. Bechmann-Pasquinucci and W. Tittel, Quantum cryptography using larger alphabets, Phys. Rev. A **61**, 062308 (2000).

[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 (2010).

[9] 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).

[10] D. Bacco, B. Da Lio, D. Cozzolino, F. Da Ros, X. Guo, Y. Ding, Y. Sasaki, K. Aikawa, S. Miki, H. Terai *et al.*, Boosting the secret key rate in a shared quantum and classical fibre communication system, Commun. Phys. **2**, 1 (2019).

[11] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, Experimental quantum cryptography with qutrits, New J. Phys. **8**, 75 (2006).

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

[13] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. Connolly, A. Przysiezna, E. Gómez, M. Figueroa, G. Vallone *et al.*, High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers, Phys. Rev. A **96**, 022317 (2017).

[14] 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).

[15] D. Cozzolino, D. Bacco, B. Da Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran *et al.*, Orbital Angular Momentum States Enabling Fiber-Based High-Dimensional Quantum Communication, Phys. Rev. Appl. **11**, 064058 (2019).

[16] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits *et al.*, Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding, New J. Phys. **17**, 022002 (2015).

[17] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. B. Dixon, F. N. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, High-rate field demonstration of large-alphabet quantum key distribution, arXiv:1611.01139 (2016).

[18] D. Bacco, J. B. Christensen, M. Castaneda, Y. Ding, S. Forchhammer, K. Rottwitt, and L. K. Oxenløwe, Two-dimensional distributed-phase-reference protocol for quantum key distribution, Sci. Rep. **6**, 36756 (2016).

[19] 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).

[20] T. Ikuta and H. Takesue, Four-dimensional entanglement distribution over 100 km, Sci. Rep. **8**, 817 (2018).

[21] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, and M.-J. Li *et al.*, Secure Quantum Key Distribution Over 421 km of Optical Fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[22] B. Da Lio, D. Bacco, D. Cozzolino, Y. Ding, K. Dalgaard, K. Rottwitt, and L. K. Oxenløwe, Experimental demonstration of the DPTS QKD protocol over a 170 km fiber link, Appl. Phys. Lett. **114**, 011101 (2019).

[23] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, Scalable high-rate, high-dimensional time-bin encoding quantum key distribution, Quantum Sci. Technol. **4**, 035008 (2019).

[24] A. Ruiz Alba Gaya, D. Calvo Díaz-Aldagalán, V. García Muñoz, A. Martínez García, A. Ocampo, W. Alexander, R. Chicue, J. Guillermo, J. Mora Almerich, and J. Capmany Francoy, in *Waves* (Instituto de Telecomunicaciones y Aplicaciones Multimedia (iTEAM), 2011), Vol. 1, p. 4.

[25] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Simple and high-speed polarization-based QKD, Appl. Phys. Lett. **112**, 051108 (2018).

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

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

[28] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, Finite-key analysis for the 1-decoy state QKD protocol, Appl. Phys. Lett. **112**, 171104 (2018).

[29] 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).

[30] N. T. Islam, C. Cahall, A. Aragoneses, A. Lezama, J. Kim, and D. J. Gauthier, Robust and Stable Delay Interferometers with Application to *d*-Dimensional Time-Frequency Quantum Key Distribution, Phys. Rev. Appl. **7**, 044010 (2017).

[31] T. Brougham and S. M. Barnett, Mutually unbiased measurements for high-dimensional time-bin–based photonic states, EPL (Europhys. Lett.) **104**, 30003 (2013).

[32] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Simple 2.5 GHz time-bin quantum key distribution, Appl. Phys. Lett. **112**, 171108 (2018).