Fully autocompensating high-dimensional quantum cryptography by quantum degenerate four-wave mixing

Jesús Liñares,* Xesús Prieto-Blanco, Daniel Balado, and Gabriel M. Carral
Quantum Materials and Photonics Research Group, Optics Area, Department of Applied Physics, Faculty of Physics and Faculty of Optics and Optometry, Universidade de Santiago de Compostela, Campus Vida s/n, E-15782 Santiago de Compostela, Galicia, Spain

(Received 29 September 2020; revised 12 March 2021; accepted 12 March 2021; published 12 April 2021)

We present a communication system based on quantum degenerate four-wave mixing for achieving fully autocompensating high-dimensional quantum cryptography. We prove that random phase shifts and couplings (cross-talking) among $2N$ optical modes (spatial and polarization modes), represented by arbitrary SU($2N$) transformations and due to mechanical and thermal perturbations, imperfections, and so on, are autocompensated after a single round trip between Alice and Bob. Bob uses a source of single photons or, alternatively, attenuated coherent states and thus autocompensated 1-qudit states are received by Bob for using them with high-dimensional quantum key distribution (QKD) protocols that provide larger secret key rates for large N. A security study is also presented for this autocompensating quantum cryptography system, where it is found that the secure key rate increases with respect to nonautocompensated links for decoy-state QKD in the case of collective attacks. This plug-and-play system can be used in both optical fiber and free-space communication systems.

DOI: 10.1103/PhysRevA.103.043710

I. INTRODUCTION

Quantum cryptography is based on the properties of quantum mechanics that allows to obtain, among others, secure quantum key distribution (QKD) protocols. One of them is the seminal so-called BB84 protocol [1] in which four quantum single-photon states and two bases are used. These states are excited in two simple polarization modes. On the other hand, space division multiplexing has been proposed to further increase the data bandwidth in optical fiber communications [2,3], and accordingly, high interest has arisen in new optical fibers such as few-mode fibers (FMFs) and multicore fibers (MCFs) with a relatively high number of spatial modes. Likewise, optical satellite communications, and in general free-space optical communications, based on spatial modes, such as those carrying orbital angular momentum, constitute a promising communications technology [4]. Thus, by using spatial optical modes a high-dimensional QKD (HD-QKD) can be implemented, and thus the interest in the development of quantum cryptography in both the mentioned new optical fibers and in free space has also remarkably increased in the last few years. Note that HD-QKD provides larger quantum bit error rates (QBERs) and secret key rates for large N, as proved theoretically and experimentally for a high-dimensional analog of the BB84 protocol [5,6].

Different optical systems have been proposed to implement QKD cryptography in both optical fibers and free space; such systems can use different kinds of modes, for instance, polarization modes in monomode optical fibers [7,8] and free space [9], collinear spatial modes in FMFs [10] and free space [11], and spatial codirectional modes in MCFs [12–14]. However, one of the most important drawbacks is that all guided modes in optical fibers and beam modes in free-space modes are needed to be kept stable over long propagation distances along the optical fibers or the atmosphere. Modes undergo instability because light, in its propagation along optical fibers or in free space, finds small spatial and polarization perturbations and imperfections, or slow temporal perturbations due to thermal, mechanical, and even geometrical factors such as curvatures and torsions. This gives rise to random modal coupling (modal cross-talking) which, together with random intermodal phases, causes instability of both modes and quantum states. The main consequence is an increase of error rates which makes much more difficult the error correction and eavesdropper detection. To overcome this drawback, specific (partial) autocompensating techniques have been proposed in quantum communication systems. Such techniques are based on placing the optical source at Bob. Therefore, the light travels to Alice a distance L, where a phase modulation is introduced (choice of the quantum states), and goes back to Bob where after the round trip a well-defined state is obtained; that is, on the way back all perturbations undergone on the way out to Alice are compensated. Accordingly, we can consider that a perturbation is slow if it does not change while light goes back and forth (distance $2L$). For example, if a perturbation does not change for a time $\tau_p = 10$ ms, then light, in an optical fiber, travels a round-trip distance of about $2L = 2000$ km. We must stress that thermal perturbation are still much longer than 10 ms. Examples of partial autocompensating techniques are polarization autocompensating quantum cryptography with 1-qubit states excited in polarization modes [7,15], or more recently with 1-qudit states excited in spatial modes acquiring random relative phases and polarization [16,17].

*Corresponding author: suso.linares.beiras@usc.es

However, to our knowledge, a fully autocompensating solution has not been proposed, that is, when the mentioned perturbations give rise to unpredictable modal coupling among optical modes (spatial and polarization modes) and therefore the quantum states (1-qudits) undergo general SU($2N$) transformations (the case of random relative phases and random polarization are only particular cases) which must be compensated. In this work we use a high-dimensional QKD protocol analog of the BB84 one (HD-QKD-BB84), that is, with two mutually unbiased bases (MUBs), and prove that full autocompensation is achieved by using a method based on quantum degenerate four-wave mixing (DFWM) which for coherent states becomes an optical phase conjugation. The method is valid for both free-space optical communication and optical fiber communications where spatial and polarization modal couplings are not negligible. In a most formal way, by using DFWM we compensate for unwanted effects in 1-qudit states caused by an arbitrary number q of unpredictable unitary transformations SU($2N$), where $2N$ is the number of spatial modes with two polarizations. For the sake of expositional convenience we present a detailed study of MCFs which can in turn be formally applied to both FMFs and free-space optical communications. Input multimode single-photon states can be used or, alternatively, coherent states which are attenuated on their way back up to a single-photon level (weak coherent states), so that 1-qudit states are produced. This attenuation can be made by using a variable attenuator or the DFWM itself. In this case, decoy states [18] have also to be generated for security purposes, as usual. In fact, by considering decoy-state QKD and in the case of collective attacks, a security analysis is presented by calculating secret key rates as a function of the link length.

The paper is organized as follows. In Sec. II the physical implementation of a quantum DFWM device intended for autocompensation is presented. In Sec. III the autocompensation theory by using DFWM is shown for a general multimode case although sections for particular perturbations are introduced, that is, spatial perturbations, spatial and birefringent (polarization) perturbations, and finally any perturbation represented by a general unitary transformation SU($2N$). In Sec. IV an optical fiber setup for physical implementation of A-HD-QKD is presented and the different photonic devices are described, particularly generation and detection devices of quantum states, together with a study of security by calculating both the QBER, due to an intercept-resend attack (a phase-remapping one) for different dimensions N, and the secret key rate as a function of the link length and the link perturbation error. In Sec. V conclusions are presented.

II. QUANTUM FOUR-WAVE MIXING FOR AUTOCOMPENSATING CRYPTOGRAHY

First of all, we present the physical implementation of a particular quantum DFWM device intended for achieving autocompensation, that is, for compensating unpredictable unitary transformations SU($2N$), as commented above. DFWM is a well-known nonlinear optical quantum effect [19]. It involves the mutual interaction of four different waves of the same frequency through a nonlinear medium [20,21] which gives rise to interesting classical optical effects such as

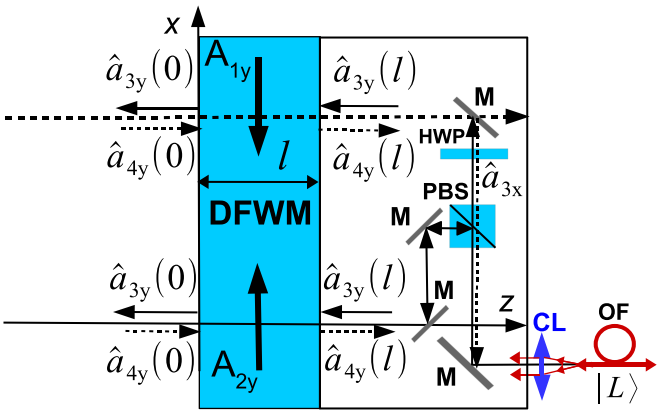

FIG. 1. Quantum DFWM device with two pump waves A_{1y} and A_{2y} and an input state $|L\rangle$ emerging from an optical fiber (OF) along $-z$. Optical fiber modes are collimated by a lens (CL) and redirected by mirrors (M). The PBS separates polarizations, and horizontal or x polarization becomes vertical or y polarization by using a HWP rotated $\pi/4$. Finally, the nonlinear medium implements a quantum degenerate four-wave mixing process.

amplified reflection, phase conjugation, and so on. In this work we have to adapt the DFWM device to obtain an autocompensating operation. We show the sketch of our DFWM device in Fig. 1. Let us consider an input spatial multimode optical quantum state $|L\rangle$ propagating along the $-z$ direction with frequency ω. Such a state emerges from an optical fiber (OF) and is directed by means of mirrors to the DFWM device. First of all, a collimating lens (CL) is inserted after the OF for collimating the optical fiber modes $\mathbf{e}_j(x,y)$, $j = 1,\ldots,N$. This CL is not strictly necessary but helps to understand much better the physical process. After the collimating lens, a polarizing beam-splitter (PBS) separates horizontal and vertical polarization modes (x and y modes). The linear x-polarization mode is rotated $\pi/2$ by means of a half-wave plate $\mathrm{HWP}_{\pi/4}$ (HWP rotated $\pi/4$). Finally, light reaches a third-order nonlinear material of length l in which there are two strong vertically polarized counterpropagating intense pump modes (strong coherent states) of frequency ω and amplitudes A_{1y} and A_{2y}. A possible isotropic nonlinear material for implementing DFWM can be CS_2 [21] with linear index n, which would contribute to vertical polarization with the term $\chi^{(3)}_{yyyy}$ of the third-order nonlinear tensor. For the moment, let us consider that $|L\rangle$ is a single-mode state excited in the incident mode 3 coming from an OF and with an associated optical field operator $\hat{E}_{3y} \propto (e^{-ik_o z}e^{-i\omega t}\hat{a}_{3y} + \mathrm{H.c.})$, where $\hat{a}_{3y}$ is an absorption operator. When $|L\rangle$ interacts with the nonlinear material then a fourth mode (reflected mode 4) arises, with an associated field operator $\hat{E}_{4y} \propto (e^{ik_o z}e^{-i\omega t}\hat{a}_{4y} + \mathrm{H.c.})$. We are interested in the quantum states propagating along the z direction in modes 3 and 4 (idler and signal modes) after nonlinear interaction, that is, in spatial propagation not in temporal evolution (Hamiltonian operator) [22]. Therefore, for spatial nonlinear coupling is convenient to use the momentum operator describing the quantum mode interaction [21–23],

$$\hat{M}_I = \int \chi^{(3)}_{yyyy} E_{1y} E_{2y} \hat{E}_{3y} \hat{E}_{4y}\, dx\, dy\, dt, \tag{1}$$

where the intense pump waves 1 and 2 can be treated classically and modes 3 and 4 in a quantum way, that is,

$$E_{\binom{1y}{2y}} = A_{\binom{1y}{2y}}\, e^{\mp ik_o nx}\, e^{-i\omega t} + \text{c.c.}, \tag{2}$$

$$\hat{E}_{\binom{3y}{4y}} = \sqrt{\hbar\omega}\, \mathrm{e}_j^{\binom{3}{4}}(x,y)\, \hat{a}_{\binom{3y}{4y}}\, e^{\mp ik_o nz}\, e^{-i\omega t} + \text{H.c.}, \tag{3}$$

where e_j is a jth normalized spatial mode of the OF with x or y polarization. As these modes are collimated by the CL then $\mathrm{e}_j^{(3)} \approx \mathrm{e}_j^{(4)}$. By inserting the above pump waves and field operators into Eq. (1) and performing the temporal integrations, the following operator is found:

$$\hat{M}_I = \hbar\chi_{\text{eff}} A_{1y} A_{2y} \hat{a}_{3y}^\dagger \hat{a}_{4y}^\dagger + \text{H.c.}, \tag{4}$$

where χ_{eff} is an effective nonlinear susceptibility which groups together all physical constants, and $\hat{a}_{3y}^\dagger$, $\hat{a}_{4y}^\dagger$ are emission operators. From the operator $\hat{M}_I$ the spatial Heisenberg equations [22] can be obtained,

$$-i\hbar \frac{\partial \hat{a}_{my}}{\partial z} = [\hat{a}_{my}, \hat{M}_I], \tag{5}$$

where $m = 3, 4$. Let us denote the input operators as $\hat{a}_{3y}(l) \equiv \hat{a}_{o3}$ and $\hat{a}_{4y}(0) \equiv \hat{a}_{o4}$, and the output operators as $\hat{a}_{3y}(0) \equiv \hat{a}_3$, associated to the optical mode transmitted along the system, and $\hat{a}_{4y}(l) \equiv \hat{a}_4$, associated to the reflected optical mode (see Fig. 1). As mentioned, there are two pump waves with very large amplitudes A_{1y} and A_{2y} and initial phases equal to zero. Then the nonlinear interaction strength is given by a coupling coefficient $\kappa = \chi_{eff}|A_{1y}||A_{2y}|$; therefore, the nonlinear interaction is parametrically governed by $|A_{1y}||A_{2y}|$, that is, the efficiency of the process is governed by pumping. It is easy to check that the solutions of the spatial Heisenberg equations obtained by inserting Eq. (4) into Eq. (5) provide the well-known operator transformations [19,21]

$$\hat{a}_{3y}(l) \equiv \hat{a}_{o3} = \sec(\kappa l)\, \hat{a}_3 + i \tan(\kappa l)\, \hat{a}_4^\dagger, \tag{6}$$

$$\hat{a}_{4y}(0) \equiv \hat{a}_{o4} = \sec(\kappa l)\, \hat{a}_4 + i \tan(\kappa l)\, \hat{a}_3^\dagger. \tag{7}$$

Quantum mechanically these results show that a degenerate four-wave mixing produces the transformation $\hat{a}_{o3} \propto \hat{a}_4^\dagger$, that is, an Hermitian conjugation of the absorption operator $\hat{a}_{o3}$, and in a certain sense we can say that a quantum optical phase conjugation is obtained. In fact, absorption and emission operators can be written as a function of a phase operator $\hat{e}^{i\Phi}$ and an amplitude operator $\hat{g}$ [19], that is, $\hat{a} = \hat{g}\hat{e}^{i\Phi}$ and $\hat{a}^\dagger = \hat{e}^{-i\Phi}\hat{g}$, with $\hat{g} \equiv (\hat{n}+1)^{1/2}$, $\hat{e}^{-i\Phi} \equiv (\hat{e}^{i\Phi})^\dagger$, where $\hat{n} = \hat{a}^\dagger\hat{a}$ is the number operator. Therefore, Eq. (6) implements an Hermitian conjugation of the phase operator of the reflected mode, which can be rewritten as

$$\hat{g}_{o3}\hat{e}^{i\Phi_{o3}} = s\, \hat{g}_3 \hat{e}^{i\Phi_3} + it\, \hat{e}^{-i\Phi_4}\hat{g}_4, \tag{8}$$

where $s = \sec(\kappa l)$ and $t = \tan(\kappa l)$. It is well known that this Hermitian conjugation of the phase operator becomes an optical phase conjugation for a quasiclassical state. That is, let us consider a coherent state $|L\rangle = |\alpha_3 0_4\rangle$ excited in an optical fiber mode; then by taking into account the complex displacement operator and using Eq. (6) the output state can be rewritten as follows:

$$|L\rangle = e^{\alpha\hat{a}_{o3}^\dagger - \alpha^\star \hat{a}_{o3}}\, |00\rangle \rightarrow |L_c\rangle = |s\alpha\rangle\, |\text{-}it\alpha^\star\rangle. \tag{9}$$

We have obtained a transmitted state $|s\alpha\rangle$ and a reflected state $|\text{-}it\alpha^\star\rangle$. Note that the reflected coherent state has been conjugated, that is, the DFWM is an optical phase conjugator. Let us recall, however, that we are interested in multimode coherent states, that is, $|L\rangle = |\alpha_1 \cdots \alpha_N\rangle$ excited in N optical modes (denoted by subscript indices $1, \ldots, N$). Therefore, the DFWM produces the multimode coherent state

$$|L_c\rangle = (|s\alpha_1\rangle\, |\text{-}it\alpha_1^\star\rangle) \cdots (|s\alpha_N\rangle\, |\text{-}it\alpha_N^\star\rangle). \tag{10}$$

We must indicate that the N incident modes have excited N reflected modes $(|\text{-}it\alpha_1^\star\rangle) \cdots \text{-}it\alpha_N^\star\rangle)$ and N transmitted modes $(|s\alpha_1\rangle \cdots (|s\alpha_N\rangle)$. Note that reflected modes acquire conjugated factors $\alpha^\star$. It is interesting to stress that Alice can attenuate the reflected state by changing the pumping (parametric attenuation), that is, $\tan(\kappa l) \approx \kappa l \equiv \gamma \ll 1$, and $\sec(\kappa l) \approx 1$; then we can rewrite $|L_c\rangle \approx (|\alpha_1\rangle \cdots |\alpha_N\rangle)\, (|\text{-}i\gamma\alpha_1^\star\rangle) \cdots (\, |\text{-}i\gamma\alpha_N^\star\rangle)$. Next, we recall the single-photon approximation of a coherent state excited in a j mode, that is, $|-i\gamma\alpha_j^\star\rangle \approx |0_j\rangle - i\gamma\alpha_j^\star|1_j\rangle$. Therefore. the state given by Eq. (10) can be rewritten as follows (single-photon approximation):

$$|L_c \approx |\alpha_1\rangle \cdots |\alpha_N\rangle \{|0_1 \cdots 0_N\rangle - i\gamma \sum_j \alpha_j^\star |0 \cdots 1_j \cdots 0\rangle\}, \tag{11}$$

where terms γ^2 are neglected, that is, the reflected state is a single-photon state (actually a 1-qudit) obtained from a weak coherent state. Obviously by changing γ Alice can produce decoy states.

On the other hand, a source of single photons can be also used; that is, we can generate an input 1-qudit state $|L_o\rangle = \sum_j c_j |1_{3j}\rangle$, with, $j = 1, \ldots, N$, and subscript index $3j$ indicating that the jth mode is incident on the DFWM device. Now, the total momentum operator is given by

$$\hat{M}_I = \hbar\kappa \sum_j (\hat{a}_{3j}^\dagger \hat{a}_{4j}^\dagger + \text{H.c.}). \tag{12}$$

The state after DFWM can be calculated as $|L_c\rangle = \exp\{(i/\hbar)\hat{M}_I l\}|L_o\rangle$; therefore, for $\gamma = \kappa l \ll 1$, the above incident 1-qudit becomes the following state:

$$|L_c\rangle \approx \sum_j c_j |1_{3j} 0_{4j}\rangle - i\gamma\sqrt{2} c_j |2_{3j} 1_{4j}\rangle + \cdots. \tag{13}$$

Note that in this case the DFWM does not produce conjugation of the probability amplitudes c_j of the single-photon state excited in each one of the reflected modes $4j$; however, it produces a stimulated single-photon state. Obviously, we also have spontaneous emission of single-photon states but their efficiency is much lower due to the nature of spontaneous emission that is distributed in a large number of modes [24].

III. DFWM AUTOCOMPENSATION THEORY

First of all and for the sake of expositional convenience, we provisionally assume that polarization is maintained under propagation (Sec. III A); in fact, we must recall that in the atmosphere and special optical fibers polarization can be maintained. Accordingly, spatial perturbations are considered and therefore there will only be coupling among N spatial modes with the same linear polarization. In Sec. III B we

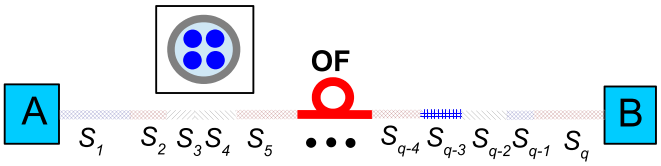

FIG. 2. Optical fiber with an arbitrary number q of mode perturbations represented by unitary transformations S_k, with $k = 1, \ldots, q$. Inset shows an example of a MCF with four spatial modes (four cores); that is, S_k would be 4×4 matrices.

will include polarization couplings, and finally, in Sec. III C arbitrary SU(N) perturbations are considered, which include, for instance, N-dimensional rotations. We must also stress that the general results that we are going to obtain in this section are also valid for collinear modes of FMF and free-space optical modes.

A. Spatial autocompensation

Let us consider, for example, codirectional modes of a MCF with N modes (cores) whose propagation constants are β_{oi}, $i = 1, \ldots, N$, and with associated absorption operators $\hat{a}_i$. The quantum state reaching the Bob system from the Alice system will be an unpredictable quantum state, and, as a consequence, modal coupling prevents us from implementing any QKD protocol. Next, we show how to overcome this drawback by using DFWM. Let us consider a perturbation $P_s(x, y)$ that induces modal coupling and can be considered as z invariant along a distance d; then the spatial Heisenberg equation describing modal coupling among N complex optical field operator modes $\hat{E}_i \propto \hat{a}_i$ can be written as follows [23]:

$$-i\hbar\frac{\partial \hat{a}_i}{\partial z} = \hbar\{\beta_i \sum_{j=1}^{N} \delta_{ij}\hat{a}_j + \sum_{j\neq i}^{N} \kappa_{ij}\hat{a}_j\} \equiv \hbar \sum_{j=1}^{N} C_{ij}\hat{a}_j, \quad (14)$$

where $\beta_i = \beta_{oi} + \kappa_{ii}$ are the perturbed propagation constants due to (random) modal self-coupling (κ_{ii}), and κ_{ij} are (random) modal coupling coefficients due to cross coupling. From a most fundamental point of view, an arbitrary coupling coefficient of spatial modes i, j is given by

$$\kappa_{ij} = \int \mathrm{e}_i(x, y)P_s(x, y)\mathrm{e}_j(x, y)\, dx\, dy, \quad (15)$$

where $\mathrm{e}_{(i,j)}(x, y)$ are the mode amplitudes. Note that $\kappa_{ij} = \kappa_{ji}$ and then $[C_{ij}] \equiv C$ is a symmetric matrix. Therefore, by using the algebraic properties of symmetric matrices, the formal matrix solution $[S_{ij}] \equiv S = \exp\{iCz\} = \mathbb{I} + izC - z^2C^2/2! + \cdots$ of the differential equation given by Eq. (14) is a symmetric matrix, that is, $S_{ij} = S_{ji}$. Moreover, modal coupling is a unitary transformation; therefore, $[S_{ij}]^{-1} = [S_{ji}]^\star = [S_{ij}]^\star$.

In general, we will have an arbitrary number q of perturbations between Alice and Bob along the optical fiber, such as shown in Fig. 2 which can be z invariant in distances d_k, $k = 1, \ldots, q$. The inset shows an example of MCF with four cores, that is, four spatial modes. Accordingly, if we have a quantum source in system B for QKD (single-photon states or coherent states) the total effect along the z direction from system B (Bob) to system A (Alice) can be represented by the total matrix $M = S_1 \cdots S_q$. We must stress that this matrix acts on the quantum fields. Next, according to the result given by Eq. (9) for the reflection modes, the matrix M becomes $M^\star = S_1^\star \cdots S_q^\star$ at Alice. Next, the quantum state is propagated back to system B; therefore, we have to use a reflected coordinate system which is defined, without loss of generality, by $(-x)y(-z)$ with respect to the incident coordinate system xyz. The coupling coefficients κ_{ij} are invariant under the transformation $x \to -x$ and consequently the matrices C are also invariant. Now, the total matrix for the way back is $M_b = S_q \cdots S_1$, which can be rewritten as $M_b = M^t$, with superscript index t indicating transpose. Therefore, once the light has traveled the path back and forth, the total coupling matrix is $S_q \cdots S_1 S_1^\star \cdots S_q^\star = \mathbb{I}$, or in an algebraic compact form, $M^t M^\star = MM^\star = \mathbb{I} = M^{-1}M$. We must recall that we have assumed slow temporal perturbations; that is, the time t_p during which the disturbance is considered to be unchanged is much longer than the time t_{AB} it takes for light to travel back and forth between A and B. In short, the unpredictable modal coupling has been removed, and therefore, if Bob launches a multimode coherent state $|L\rangle = |\alpha_{B31} \cdots \alpha_{B3N}\rangle = |\alpha_1 \cdots \alpha_N\rangle$ undergoing modal coupling along an OF or in the atmosphere, the state after the DFWM and traveling its way back has the form given by Eq. (10), and accordingly, we recover the initial state except for π phases and conjugations.

By taking into account the transformation of a coherent state we have just proven that autocompensation is obtained; nevertheless, for the sake of completeness, it is worth explicitly deriving the transformations between the input operators corresponding to the optical modes at Bob, that is, $\hat{a}_{Bo3j}$, and the final operators at Bob after a round trip, that is, $\hat{a}_{B4j}$, in order to give a formal quantum proof. Moreover, such transformations facilitate the study of any quantum state. We start by considering the transformation of input operators up to the DFWM device is given by

$$\begin{pmatrix} \hat{a}_{o31} \\ \vdots \\ \hat{a}_{o3N} \end{pmatrix} = S_1 \cdots S_q \begin{pmatrix} \hat{a}_{B31} \\ \vdots \\ \hat{a}_{B3N} \end{pmatrix} = M \begin{pmatrix} \hat{a}_{B31} \\ \vdots \\ \hat{a}_{B3N} \end{pmatrix}, \quad (16)$$

and by taking into account the quantum transformation implemented by DFWM and given by Eq. (6) we write

$$\begin{pmatrix} s\hat{a}_{31} + it\hat{a}_{41}^\dagger \\ \vdots \\ s\hat{a}_{3N} + it\hat{a}_{4N}^\dagger \end{pmatrix} = S_1 \cdots S_q \begin{pmatrix} \hat{a}_{B31} \\ \vdots \\ \hat{a}_{B3N} \end{pmatrix}. \quad (17)$$

Next, the relation between the operators $\hat{a}_{4j}$ at the Alice system and $\hat{a}_{B4j}$ at the Bob system, after the return trip from Alice and through the q symmetric perturbations, is given by

$$\begin{pmatrix} \hat{a}_{B41} \\ \vdots \\ \hat{a}_{B4N} \end{pmatrix} = S_q \cdots S_1 \begin{pmatrix} \hat{a}_{41} \\ \vdots \\ \hat{a}_{4N} \end{pmatrix}. \quad (18)$$

Therefore, by inserting this equation into Eq. (17) the following total transformation is obtained:

$$\begin{pmatrix} \hat{a}_{B31} \\ \vdots \\ \hat{a}_{B3N} \end{pmatrix} = sM^{-1} \begin{pmatrix} \hat{a}_{31} \\ \vdots \\ \hat{a}_{3N} \end{pmatrix} + it\,(M^{-1}M) \begin{pmatrix} \hat{a}_{B41}^\dagger \\ \vdots \\ \hat{a}_{B4N}^\dagger \end{pmatrix}, \quad (19)$$

where $M^{-1} = S_q^\star \cdots S_1^\star$ (recall that $S_k, k = 1, \ldots, q$, are symmetric matrices). Note that the factor $(M^{-1}M) = \mathbb{I}$ of the vector formed by the operators $\hat{a}^\dagger_{B4j}$ is just the one obtained above by matrix calculation; therefore, the operators of reflected modes are Hermitian conjugate, as expected. Now, we can rewrite Eq. (19) for each mode j as follows:

$$\hat{a}_{B3j} = s \sum_i m_{ij} \hat{a}_{3i} + it \hat{a}^\dagger_{B4j}, \tag{20}$$

where m_{ij} are the matrix elements of M^{-1}. By defining new operators $\hat{a}_{A3j} = \sum_i m_{ij} \hat{a}_{3i}$, we obtain a new momentum operator for the optical system,

$$\hat{M} = \sum_j \hat{M}_j = \hbar\kappa \sum_j (\hat{a}^\dagger_{A3j} \hat{a}^\dagger_{B4j} + \text{H.c.}). \tag{21}$$

Now, the quantum states given by Eqs. (10) and (13) can explicitly be calculated. First of all, let us consider a single-mode coherent state $|L_o\rangle = |\alpha_k\rangle$ excited in the kth mode. By taking into account Eqs. (19) and (20) the state becomes

$$|L_c\rangle = |sm_{1k}\alpha_j\rangle \cdots |sm_{Nk}\alpha_k\rangle |\text{-}it\alpha_k^\star\rangle. \tag{22}$$

That is, we have obtained a transmitted coherent state $|sm_{1k}\alpha_j\rangle \cdots |sm_{Nk}\alpha_k\rangle$ and the reflected single-mode coherent state $|\text{-}it\alpha_k^\star\rangle$. This kind of state will be of great interest in an optical system for implementing this autocompensating quantum cryptography, as shown later. Therefore, if we consider the incident multimode state $|\alpha_1\rangle \cdots |\alpha_N\rangle$, then the output state will be

$$|L_c\rangle = |\alpha_1'\rangle \cdots |\alpha_N'\rangle | - it\alpha_1^\star\rangle \cdots | - it\alpha_N^\star\rangle, \tag{23}$$

where α_j', with $j = 1, \ldots, N$, are unpredictable values due to the matrix M^{-1} representing the perturbations of the optical fiber. However, we must recall that the transmitted state $|\alpha_1'\rangle \cdots |\alpha_N'\rangle$ is not relevant for our purposes.

On the other hand, we can consider a single-photon state excited in the kth mode, that is, $|L_o\rangle = |1_k\rangle$. Now, by taking into account the momentum operator given by Eq. (21), the output state is approximately given by

$$|L\rangle \approx |1_{3k}0_{4k}\rangle - i\gamma \left(\sum_{i=1}^{N} m_{ik}^\star \sqrt{2}\, |2_{3i}\rangle \right) |1_{B4k}\rangle + \cdots . \tag{24}$$

In this case the two-photon state $|2_{3i}\rangle$ at the Alice system can be detected in any transmitted mode $3i$, but the single-photon state is recovered again in the kth mode (now the reflected kth mode) and with a well-defined complex probability amplitude; that is, couplings and phases have been compensated thanks to the Hermitian conjugation implemented by DFWM. Expressions for 1-qudit states can be obtained in a straightforward way.

B. Spatial and birefringent autocompensation

As commented, we also have to remove unpredictable polarization modal coupling together with the above spatial modal coupling; that is, we have to achieve autocompensation with spatial and polarization modes. First of all, we characterize the matrix transformation produced by an arbitrary coupling between linearly polarized spatial modes (e.g., LP modes). Since there are $2N$ modes (N spatial modes with two polarizations), we introduce, for the sake of expositional convenience, the new subscript indices $i, j = \{1H, 1V, 2H, 2V, \ldots, NH, NV\}$, with $H \equiv x$, $V \equiv y$. Note that in this case we will have $2N$ transmitted modes and $2N$ reflected modes. As in the above (scalar) case, the coupling matrix $[C_{ij}] \equiv C$ is also a complex symmetric matrix. However, when considering backward propagation, this matrix gets modified because, as discussed, the incident coordinate system xyz becomes $(-x)y(-z)$ under reflection. Indeed, an arbitrary coupling coefficient of spatial modes m, n with different polarization H, V is given by

$$\kappa_{mHnV} = \int \mathrm{e}_{mH}(x, y) P_v(x, y) \mathrm{e}_{nV}(x, y)\, dx\, dy, \tag{25}$$

where $P_v(x, y)$ is an arbitrary perturbation producing polarization (vector) modal coupling. Obviously, under reflection (back path) we have $\mathrm{e}_{nH}(x, y) \to -\mathrm{e}_{nH}(x, y)$; then $\kappa_{ij} \equiv \kappa_{mHnV} \to -\kappa_{mHnV} \equiv -\kappa_{ij}$. Note that for the same polarization the coupling coefficient is positive (or zero) under reflection. Therefore, the coupling matrix $[B_{ij}] \equiv B$ under reflection can be written as follows:

$$B = (I_N \otimes \sigma_z)\, C\, (I_N \otimes \sigma_z) \equiv DCD, \tag{26}$$

with I_N the N-dimensional identity matrix, $\otimes$ the tensor product, and σ_z the third Pauli matrix. Next, by taking into account that $DD = (I_N \otimes \sigma_z)(I_N \otimes \sigma_z) = I_{2N}$ (where I_{2N} is the identity matrix $2N \times 2N$), it is easy to check that the transformation matrix produced by the perturbation $P_v(x, y)$, that is, the formal matrix solution $[R_{ij}] \equiv R = \exp\{iBz\}$, can be written by using the Taylor expansion of an exponential function as follows:

$$R = (I_N \otimes \sigma_z)\, S\, (I_N \otimes \sigma_z) \equiv DSD, \tag{27}$$

where $S = \exp\{iCz\}$. Note that matrix R (transformation of the absorption operators $\hat{a}_{jH}, \hat{a}_{jV}$) is also symmetric. On the other hand, it is easy to check that the $\text{HWP}_{\pi/4}$ introduces a phase π between the H mode and the V mode of every spatial mode on its way back. Therefore, after the DFWM device, when polarization modes are recombined in the PBS (see Fig. 1), the matrix $D = I_N \otimes \sigma_z$ is implemented. Consequently, for the general case of q random couplings, we obtain, after the path back to Bob, the total matrix

$$M_T = R_q \cdots R_1 D S_1^\star \cdots S_q^\star = D, \tag{28}$$

where we have taken into account the following relationships: $R_k = DS_kD$, $DD = I_{2N}$, and $S_kS_k^\star = I_{2N}$, $k = 1, \ldots, q$. In short, symmetric spatial perturbations together with polarization perturbations have been removed. The main consequence of this result is that a polarization-independent HD-QKD device can be used because initial polarization will be restored. Likewise, a quantum study, similar to the one made at the end of the previous section, can be also made; however, no new physical results are obtained.

C. SU(2N) autocompensation

The above results have made clear the autocompensation of symmetric unitary coupling transformations. Now, we generalize the above results for nonsymmetric unitary coupling transformations, for example, polarization rotation due to

optical activity, $2N \times 2N$ abstract rotations, and so on, that is, perturbations represented by general SU($2N$) matrices. In order to prove this assertion we must take into account that all unitary transformation SU($2N$) can be factorized as an ordered product of SU(2) transformations of subspaces i, j [25–27]. Thus, by proving autocompensation by DFWM of an arbitrary SU(2) transformation the case SU($2N$) is also proven. A general SU(2) transformation S can be represented by

$$S = \begin{pmatrix} \cos\theta & i\sin\theta e^{-i\phi} \\ i\sin\theta e^{i\phi} & \cos\theta \end{pmatrix} \equiv Z(\phi)X(\theta)Z(-\phi) \qquad (29)$$

with $Z(\pm\phi) = \mathrm{diag}(1, e^{\pm i\phi})$ the matrix of a phase retarder $\pm\phi$ generated by the Pauli matrix σ_z, and $X(\theta)$ a matrix whose generator is the Pauli matrix σ_x, with elements $X_{11}(\theta) = X_{22}(\theta) = \cos\theta$, and $X_{12}(\theta) = X_{21}(\theta) = i\sin\theta$. By considering that we are in a polarization two-mode subspace, it is easy to check that the matrix T obtained by reflection is characterized by the changes $\phi, \theta \to -\phi, -\theta$; then $T = D_2 S^t D_2$, where $D_2 = \sigma_z$. Therefore, after the DFWM device and by taking into account the action of the $\mathrm{HWP}_{\pi/4}$, shown in Fig. 1, can be represented by the matrix D_2, we obtain the following result:

$$T D_2 S^\star = D_2 S^t D_2 D_2 S^\star = D_2 S^t S^\star = D_2, \qquad (30)$$

and consequently autocompensation is again achieved. Rigorously, a general SU(2) matrix requires an additional matrix corresponding to an α-phase retarder, that is, $U = Z(\alpha)S$; however, a retarder $Z(\alpha)$ is also autocompensated, as proven above. We must also stress that similar results are found for spatial two-mode subspace. Thus, for vertical polarization the matrix $-I_2$ is obtained, and for the horizontal one the identity matrix is I_2. Likewise, topological phases due to helical paths, torsions, and so on of an OF can be also autocompensated because such phases also correspond to unitary transformations (rotations and so on) [28]. In short, a multimode coherent state $|L\rangle = |\alpha_{1H}\alpha_{1V}\cdots\alpha_{NH}\alpha_{NV}\rangle$ (or multimode single-photon state) coming from Bob becomes a predictable reflected multimode coherent state (or single-photon state). Thus, by using the factorization of SU($2N$) [25–27] along with the above results, the state

$$|L_c\rangle = |L'\rangle|-it\alpha_{1H}\, it\alpha_{1V} - \cdots - it\alpha_{NH}\, it\alpha_{NV}\rangle \qquad (31)$$

is obtained, where $|L'\rangle = |\alpha'_1\rangle\cdots|\alpha'_N\rangle$ is the transmitted state. Therefore, we have proved that the DFWM device has canceled a number q of unpredictable perturbations represented by SU($2N$) transformations and thus A-HD-QKD can be implemented.

IV. PHYSICAL IMPLEMENTATION OF A-HD-QKD

By taking into account the results obtained in the previous sections we can implement an autocompensating optical system for A-HD-QKD BB84 quantum cryptography in optical fibers. Such a system is shown in the sketch of Fig. 3 where the main photonic devices are indicated.

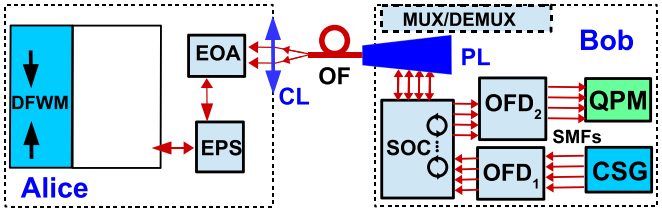

FIG. 3. Basic optical fiber setup for autocompensating HD-QKD by OPC (see Sec. IV A for description).

A. Optical fiber setup for A-HD-QKD

We follow the optical configuration shown in Fig. 3. The first device is a coherent states generator (CSG) located in the Bob system, which generates multimode coherent states $|L\rangle = |\alpha_{1H}\alpha_{1V}\cdots\alpha_{NH}\alpha_{NV}\rangle$ excited in $2N$ optical modes which can be coupled to $2N$ single-mode fibers (SMFs) by an integrated device described in Sec. IV B. SMFs are drawn with red arrows in the Bob system. In particular we choose $\alpha_{1H} = \cdots = \alpha_{NV} = \alpha$, and thus we can obtain, from the single-photon components of the weak coherent states (single-photon level), quantum states belonging to MUBs. Next, a first set of optical fiber delayers OFD_1 [29] produces modal delays τ_j $(j = 1, \ldots, 2N)$; that is, we use a time demultiplexing mechanism, or in other words, we have a multimode coherent state formed by the tensor product of delayed single-mode coherent states, $|L\rangle = |\alpha_{\tau_1}\alpha_{\tau_2}\cdots\alpha_{\tau_{2N-1}}\alpha_{\tau_{2N}}\rangle$. These delays will allow Alice to introduce phases in each mode. Afterwards, a set of optical circulators (SOC) for optical fibers [30] launches the state towards the Alice system through a MCF. The coupling between $2N$ SMFs and the MCF can be achieved by means of a photonic lantern [31]. We must indicate that a spatial multiplexing-demultiplexing (mux-demux) device is also needed if collinear propagation is required as in the case of a FMF or free space. Different spatial multiplexing devices can be implemented according to the kind of collinear modes used [32,33], although photonic lanterns between SMFs and FMFs can be also used for multiplexing purposes [31]. Note that for a MCF the mux-demux device is not required (codirectional modes).

After propagation along the OF each jth delayed single-mode coherent state (excited in each core of a MCF) becomes an unpredictable multimode coherent state due to modal coupling. Such a state reaches the DFWM device described in detail in Fig. 1 and explained above. Note in Fig. 3 that now we have placed a standard bulk electro-optic phase shifter (EPS) such as a Pockels cell crystal, and a bulk variable electro-optic attenuator (EOA) [16] in the off position between the DFWM device and the CL-OF. To a good approximation, the CL converts the optical modes in nonuniform plane modes; therefore, bulk optics can be used in the Alice system. At this point, we must stress that after the DFWM device the reflected state has to be coupled again to the OF; however, the DFWM device implements by itself this transverse modal coupling to the OF (analogous to the well-known image restoration by optical phase conjugation [19–21]), although different systems can be used to optimize this coupling, for example, as in our case, by means of a CL. Next, the reflected state in the DFWM device goes through

the EPS which introduces global phases φ_j on the mentioned multimode coherent states, and the EOA attenuates the state up to the single-photon level. Note that at the Bob system each of these multimode single-photon states will become again a jth delayed one-mode single photon due to DFWM, that is, due to autocompensation. The purpose of the EOA is not only to attenuate but also to increase the security of the system, i.e., the attenuation of the EOA can be electronically controlled, enabling the production of different attenuated pulses: signal and decoy states against different attacks of an eavesdropper Eve, as in the photon-number-splitting attack, although we must indicate that modal coupling is also a defense against attacks along the line. Moreover, it is interesting to underline that different attenuated states can be also obtained by modulating the pump intensity, that is, by a parametric attenuation. Therefore, the Alice system generates 1-qudit states which propagate along the OF up to the Bob system and thus the modal coupling and relative phases are fully removed. Next, the SOC sends the 1-qudit state to the second set of delayers OFD_2 which cancels the delays τ_j between states $|1_j\rangle$ of the 1-qudit. In short, by taking into account the state given by Eq. (31) with $\alpha_{H1} = \cdots = \alpha_{VN} = \alpha$ and phases $\varphi_{jH}, \varphi_{jV}$ introduced by Alice, the (attenuated) normalized quantum state reaching the Bob system is given by

$$|L_c\rangle \approx -i\gamma'\alpha\left\{\sum_{j=1}^{N} e^{i\varphi_{jH}}|1_{B4jH}\rangle - e^{i\varphi_{jV}}|1_{B4jV}\rangle\right\}, \qquad (32)$$

with $\gamma' = \eta\kappa l$, where η is the attenuation factor introduced by the EOA or parametric attenuation. These states are chosen with values of φ_{jH} and φ_{jV} for defining two $2N$-dimensional MUBs [6] for QKD.

B. Generation and detection of quantum states

As commented, the initial state generated in the CSG is converted to a quantum state belonging to a MUB at the Alice system, and finally reaches a quantum projective measurer (QPM) at the Bob system. Since both CSG and QPM are relevant devices it is worth showing here a possible physical implementation of them. One of the advantages of optical fibers in general and MCFs in particular is their high compatibility with integrated optical components. Each core of a MCF can be connected to a channel guide of an integrated circuit, for instance, by a lantern coupler; therefore, the generation and measurement of quantum states can be made on chip.

A CSG can be easily made with integrated devices by using concatenated 2×2 directional couplers; that is, each output of a coupler is connected to another coupler and so on [6,16]. Such couplers can be represented by matrices $X(\theta)$ such as the one presented in Eq. (29) where $\theta = \kappa d_c$ with κ a linear coupling coefficient and d_c the coupling distance. We start from a coherent state excited in H and V polarization modes, that is, $|L\rangle = |\beta_H\beta_V\rangle$, with $\beta_H = \beta_V = \beta$. This state can be obtained by using a PBS, and each mode is coupled to an input channel guide of an integrated device. Each channel guide is in turn connected to a first directional coupler $X(\pi/4)$ formed by two channel guides. Next, each channel guide of each coupler is in turn coupled to a new directional coupler $X(\pi/4)$ and so on. In short, each coherent state is coupled to concatenated directional couplers $X(\pi/4)$ and then a multimode state $|L'\rangle = |L'_H\rangle|L'_V\rangle$ is obtained, where $|L'_H\rangle = |\alpha\rangle|i\alpha\rangle|-\alpha\rangle\cdots|-i\alpha\rangle|-\alpha\rangle|i\alpha\rangle$ for modes $1,\ldots,N$, and $|L'_V\rangle = |\alpha\rangle|i\alpha\rangle|-\alpha\rangle\cdots|-i\alpha\rangle|-\alpha\rangle|i\alpha\rangle_V$, for modes $N+1,\ldots,2N$, where $\alpha = 2^{-m/2}\beta$, with $2^m = N$. The relative phases $\{\pm\pi/2,\pi\}$ can be easily canceled by using the EPS of the Alice system when the proper phases $\varphi_{1H},\ldots,\varphi_{NV}$ are introduced at the Alice system, then $|L'\rangle = |\alpha\rangle_1\cdots|\alpha\rangle_{2N}$. We must stress that the same procedure can be followed for single-photon states.

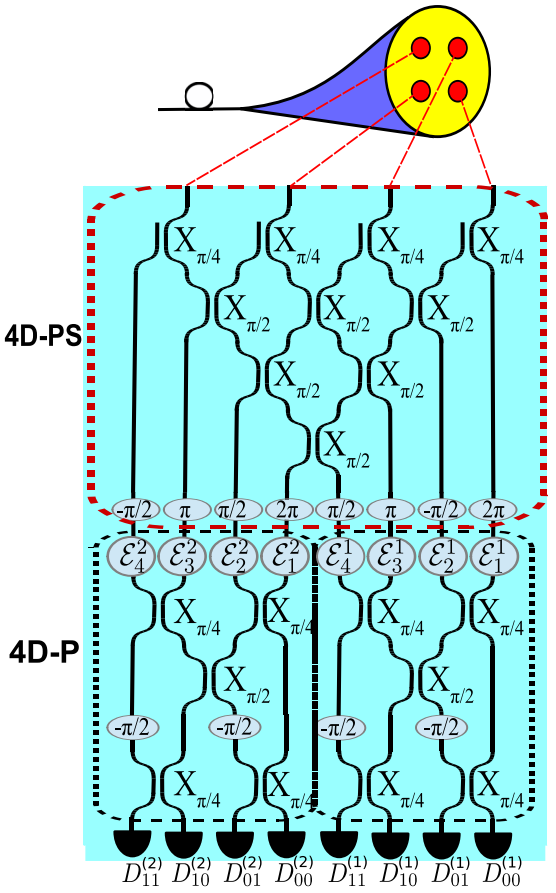

FIG. 4. Illustration of an integrated QPM device for $N = 4$ (for MCF with four cores) formed by $X_{\pi/4}$ and $X_{\pi/2}$ couplers and phase shifters (circles) that implement the random choice of a measure basis. It consists of a 4D passive splitter (4D-PS) and two 4D projectors (4D-P). Detectors D_{ab} measure the bits ab.

As to the QPM, passive integrated quantum projective meters, based on $X(\pi/4)$ and $X(\pi/2)$ couplers and phase shifters $Z(\phi)$, which randomly select bases of dimension $N = 2^m$ in MCFs, can be implemented [16]. For example, in Fig. 4 we show a passive on-chip device performing projective measurements in random bases for $N = 4$ and with two MUBs, that is, with eight 1-ququart states. Its generalization to N modes is straightforward. Recall that each core (for instance, the four cores of MCF shown in the inset of Fig. 2) is connected to one input channel waveguide. The QPM is formed by two devices, a passive splitter (4D-PS) and two projectors (4D-P) which implement measurements in two different bases. It is easy to check that passive splitters can be implemented

by couplers $X(\pi/4)$ and $X(\pi/2)$, where the matrix $X(\theta)$ is defined in Eq. (29). Therefore, if we have the single-photon state $|L\rangle = \sum_j c_j|1_j\rangle$, with $j = 1, \ldots, 4$ indicating the four input channel waveguides, then the passive splitter provides the state

$$|L_o\rangle = \frac{1}{\sqrt{2}}\left\{\sum_{j=1}^{4} c_j|1_j\rangle + \sum_{j=5}^{8} c_{j-4}|1_j\rangle\right\}. \tag{33}$$

That is, we have the same probability to measure the state $|L\rangle$ at the upper projector and at the lower one, or in other words, we implement a random choice of basis. The above state belongs to some MUB basis, and each basis has a projector defined by particular values of the phases ϵ_j as indicated in Fig. 4, that is, two projectors characterized by initial phases $\epsilon_1^1\epsilon_2^1\epsilon_3^1\epsilon_4^1$ and $\epsilon_1^2\epsilon_2^2\epsilon_3^2\epsilon_4^2$, respectively. As an example, let us consider the following basis for 1-ququart states written in matrix form, that is,

$$\mathcal{B}_1 = \frac{1}{2}\begin{pmatrix} 1 & i & i & -1 \\ i & -1 & 1 & i \\ -1 & i & i & 1 \\ -i & -1 & 1 & -i \end{pmatrix}, \tag{34}$$

where each row is a basis vector, that is, a 1-ququart state $\sum_{j=1}^{4} c_j|1_j\rangle$. Now, it is easy to check that the device with $\epsilon_1^1 = \epsilon_2^1 = \epsilon_3^1 = \epsilon_4^1 = 1$, indicated in Fig. 4, performs the transformation given by the above matrix, that is, implements a projector and therefore can make projective measurements. Note that the projector is factorized as a product of SU(2) transformations [26,27]. Therefore, if a 1-ququart reaches this projector we obtain a photon at the output of a channel guide j where it is detected. For example, the 1-ququart $(1/2)(|1_1\rangle + i|1_2\rangle + i|1_3\rangle - |1_4\rangle)$ becomes the state $|1_1\rangle$ which makes a click in detector $D_{00}^{(1)}$ (bit 00), the 1-ququart $(1/2)(i|1_1\rangle - |1_2\rangle + |1_3\rangle + i|1_4\rangle)$ becomes the state $|1_2\rangle$ which makes a click in detector $D_{01}^{(1)}$ (bit 01), and so on. However, we also have the 1-ququart $\sum_{j=5}^{8} c_{j-4}|1_j\rangle$. If it belongs to a second MUB, for example,

$$\mathcal{B}_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ i & i & -i & -i \\ -1 & 1 & 1 & -1 \\ -i & i & -i & i \end{pmatrix}, \tag{35}$$

the 1-ququart can be also detected by projective measurements. In this case we obtain a second projector by introducing new initial phases in the above projector, that is, $\epsilon_1^2 = 0$, $\epsilon_2^2 = \epsilon_3^2 = -\pi/2$, $\epsilon_4^2 = \pi$, shown in Fig. 4; therefore, the above matrix is implemented on channels $j = 5, \ldots, 8$. For example, if we have the 1-ququart $(1/2)(|1_5\rangle + |1_6\rangle + |1_7\rangle + |1_8\rangle)$ the second projector gives the state $|1_5\rangle$, which makes a click in detector $D_{00}^{(2)}$ (bit 00), and so on.

On the other hand, as commented, FMFs and free-space optical communications can be considered problems of $2N$ collinear modes. Therefore, generation and measurement of quantum states have to be made by a spatial MUX-DEMUX process, although as commented above photonic lanterns can also multiplex from SMFs to FMFs and vice versa. Moreover, in free space a detailed study should incorporate mode diffraction; however, in most cases it can be reduced thanks to the high directionality of lasers, or it can simply be ignored since DFWM also compensates for diffraction (note that a diverging wave incident on a DFWM undergoes an optical phase conjugation and becomes a converging wave). In short, in both cases, once the spatial demultiplexing is done we can use most of the results obtained for MCFs. Finally, we must stress that this autocompensating method can also be applied to other protocols based on 1-qudits and also to the remarkable measurement-device-independent (MDI) QKD protocol [34–36], which uses biphoton states, such as will be shown in a next work, although preliminary results have already been obtained [37].

C. Security analysis

First of all, we study the phase-remapping (PR) attack [38], which is a specific attack for this loop configuration of a QKD system. We show that the efficiency of the attack is reduced with the dimension N. Afterwards, a secret key rate R is calculated for the case where bit information is carried by a train of weak coherent pulses propagating in links (optical fibers) with perturbations, and in particular, we consider the decoy-state approach [18,39], which overcomes the photon-number-splitting attack [40,41]. By introducing a proper modification in the key rate formula for ideal links (that is, without any perturbation), we show that perturbations along the link reduce in a significant way the key rate R, which in turn justifies the need for autocompensating methods.

In the PR attack, Eve takes advantage of the first trip of the light states from Bob to Alice in order to modify them before Alice encodes the information in them. The attack consists of Eve delaying (or advancing) the states sent by Bob with the purpose of making them arrive at the Alice EPS when it is not operating at its maximum output, but during its response time between the activation and the mentioned maximum output. In this way, if for example Alice tries to apply a phase shift $\pi/2$, as light is reaching the EPS before this one applies such a phase, Alice will be applying a phase δ $(0 < \delta < \pi/2)$ instead. Therefore, Eve can modify the phases φ_j of the state given by Eq. (32) from $\{0, \pi/2, \pi, 3\pi/2\}$ to $\{0, \delta, 2\delta, 3\delta\}$. Thus, Alice is unknowingly sending Bob the altered state

$$|L\rangle = \frac{1}{\sqrt{N}}\{e^{ip_1\delta}|1_1\rangle + \cdots + e^{ip_N\delta}|1_N\rangle\}, \tag{36}$$

where $p_j = 0, 1, 2, 3$. Next, Eve intercepts these altered states and measures them with a general positive operator-valued measurement, gaining more additional information than in the case when she measured the unaltered states. According with her measure, she sends Bob the corresponding unaltered state (32) to being measured in Bob's QPM. Thus, like in a regular intercept-and-resend attack in one-way QKD systems, Eve's presence can only be manifested by the errors she introduces when she makes a wrong measure and sends Bob a wrong state. However, the PR attack has the advantage that, by altering states and measuring them, she can reduce the QBER induced in the system. In a recent work [16], a security analysis was made for MCFs considering such an attack for a few modes due to the limitations of the cryptographical system. However, the present DFWM autocompensation allows us to use a large number of modes and therefore it is worth analyzing the corresponding QBER.

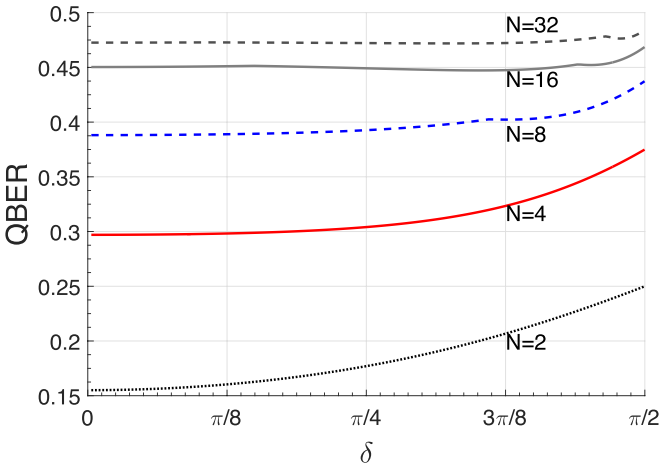

FIG. 5. QBERs obtained under the PR attack as a function of δ for dimensions $N = 2^m$, $m = 1, \ldots, 5$, employing two bases only.

In Fig. 5 we show the results of QBERs obtained as a function of the applied phase δ for dimensions $N = 2^m$, with m an integer, and making use of two bases. The figure is made by generalizing the method given in Ref. [38] using the MUB construction of Ref. [42]. We can see how the QBER is reduced with δ from its standard value of $\mathrm{QBER}_{\delta=\pi/2} = \frac{N-1}{2N}$, going from 25% to around 15% for the case $N = 2$ (two spatial modes or one spatial modes and two polarizations). However, we can also observe how the relative reduction between the minimum and maximum QBERs decreases at higher dimensions, going from around 47% to 45% for dimension $N = 32$ (32 spatial modes, or 16 spatial modes and two polarizations), for example. Just like with $\mathrm{QBER}_{\delta=\pi/2}$, $\mathrm{QBER}_{\mathrm{min}}$ also appears to tend to 50% when the dimension grows. Thus, the higher the dimension, the less useful the PR attack is. Moreover, in Ref. [16] we have shown, as well, that the PR attack cannot reduce the QBER enough in order to enter the range of values that generates a secret key rate under a cloning attack in a normal one-way system. Consequently, protocols based on autocompensating round trips between Alice and Bob do not actually make the system more vulnerable.

Next, we present the impact on the secret key rate R when perturbations in the link (optical fibers or free space) are considered and a comparison with the compensated case is shown. In order to calculate R we follow the procedure introduced in Ref. [43] and followed in Refs. [6,12,13], that is, a high-dimensional decoy-state method with two weak decoy states with average photon flux $\nu < \mu < 1$ and a vacuum state. However, we have to perform a modification in the error rates for dealing with the perturbations introduced by the link, which has not been taken into account in previous works. As commented above, the use of weak coherent states requires the use of decoy states to overcome the photon-number-splitting attack [18,39], which can be generated with the present system by using the EOA or the DFWM itself as analyzed previously. In other words, only the distance L between Alice and Bob affects the key rate R; the previous propagation distance L between Bob and Alice only prepares the state in order to be compensated.

By using decoy-state QKD and in the case of collective attacks, it is possible to obtain the secret key rate for an N-dimensional problem as a function of the link length and without perturbations, that is, the following asymptotic key rate formula [6,12,13]

$$R \geqslant \frac{1}{M}\{Q_0 \log_2(N) + Q_1[\log_2(N) - H(e_1, N)] - Q_\mu H(E_\mu, N) f(E_\mu)\}, \tag{37}$$

with M the number of bases used, in this case $M = 2$, and N the dimension of the bases. The function $H(x, N) = -x \log_2(x/(N-1)) - (1-x)\log_2(1-x)$ is the N-dimensional Shannon entropy. The overall gain is given by $Q_\mu = \sum_n Q_n = \sum_n Y_n P_n$, where a summation over all possible states is made, with Q_n the n-photon gain, $P_n = e^{-\mu}\mu^n/n!$ the photon Poisson distribution, and $Y_n = Y_0 + \eta_n$ the yield of the state $|n\rangle$, with Y_0 the yield of the vacuum state (dark counts). Therefore, Q_μ provides the probability of obtaining a detection when the signal state is sent. The parameter $\eta_n = 1 - (1-\eta)^n$ of the yield Y_n is related to the overall efficiency given by $\eta = \eta_d \eta_B \eta_{AB}$, with η_d the detector efficiency, η_B the internal transmittance of Bob's system, and $\eta_{AB} = 10^{-\alpha_{\mathrm{att}} L/10}$ the link transmittance due to the optical fiber losses, where α_{att} is the attenuation coefficient measured in dB/km and L the length of the optical fiber. On the other hand, we have the value $E_\mu = \sum_n e_n Y_n P_n / Q_\mu$, that is, the overall error rate, with $e_n = (e_0 Y_0 + e_{\mathrm{opt}}\eta_n)/Y_n$ the error associated to the states $|n\rangle$, where e_{opt} is the error due to the optical misalignment of the detection system. Importantly, it is the error to be modified when perturbations are considered along the optical fiber. Finally, $e_0 = (N-1)/N$ is the detection error (random dark count in a detector which is not expected to fire).

On the other hand, we must indicate that $f(E_\mu)$ is the efficiency of the error correction code with a value $f(E_\mu) = 1.05$; Q_1 has a lower bound, and e_1 has an upper bound given by [6,12]

$$Q_1 \geqslant \frac{e^\mu}{\mu\nu - \nu^2}\{\mu^2 Q_\nu e^\nu - \nu^2 Q_\mu e^\mu - (\mu^2 - \nu^2) Y_0\}, \tag{38}$$

$$e_1 \leqslant \frac{1}{\nu Q_1 e^\mu}(E_\nu Q_\nu \mu e^\nu - \mu e_0 Y_0). \tag{39}$$

With all these definitions we can calculate the system parameters; thus, Q_0 can be directly estimated as $Q_0 = e^{-\mu} Y_0$, where Y_0 is the vacuum yield and, therefore, related to the dark count probability P_{dark} of a single detector. For N-dimensional QKD the yield of the vacuum is approximately given by $Y_0 \approx N P_{\mathrm{dark}}$ [12]. Moreover, it is easy to check that the following exact expressions are obtained for Q_μ, E_μ:

$$Q_\mu = Y_0 + 1 - e^{-\mu\eta}, \quad E_\mu = \frac{e_0 Y_0 + e_{\mathrm{opt}}(1 - e^{-\mu\eta})}{Q_\mu}. \tag{40}$$

Likewise, the upper bound of e_1 can be exactly calculated,

$$e_1 = \frac{e_0 Y_0 + e_{\mathrm{opt}}\eta}{Y_0 + \eta}, \tag{41}$$

and finally we have estimated the lower bound for Q_1 by assuming $P_n \ll 1$ for $n > 3$,

$$Q_1 \approx [(Y_0 + \eta) - \frac{\mu\nu}{6}(Y_0 + 1 - (1-\eta)^3)]\, \mu\, e^{-\mu}. \tag{42}$$

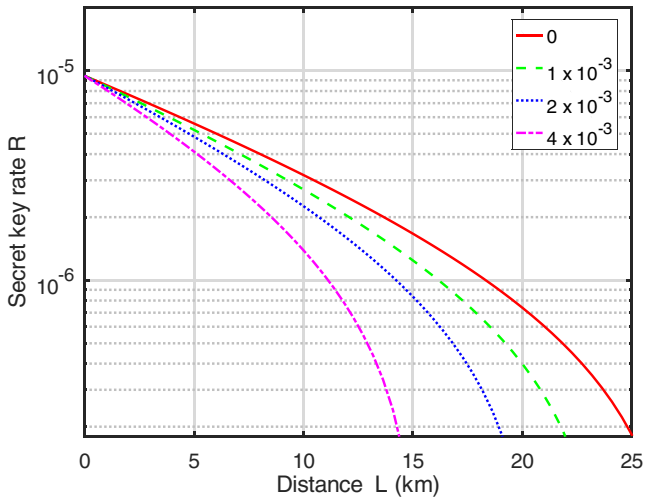

FIG. 6. Key rates in optical fibers without autocompensation and with different perturbation coefficients $\alpha_{\text{opt}} \neq 0$ (dashed lines). The case with autocompensation ($\alpha_{\text{opt}} = 0$) is shown in a solid line.

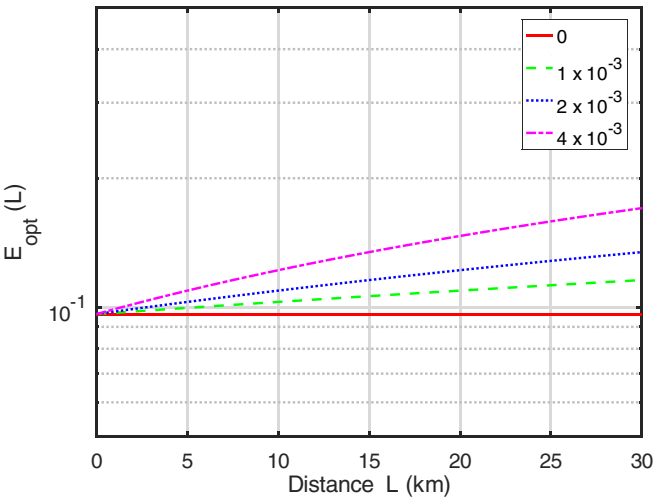

FIG. 7. Function $E_{\text{opt}}(L)$ for several perturbation coefficients $\alpha_{\text{opt}} \neq 0$ (dashed lines). The value $\alpha_{\text{opt}} = 0$ (solid line) corresponds to the autocompensation case.

Next, all these values are inserted into Eq. (37) to obtain R; however, as commented above, the error e_{opt} has to be modified in order to take into account the perturbations along the optical fiber. For that, we use the following trial function $E_{\text{opt}}(L)$ monotonically increasing with L, as for example $E_{\text{opt}}(L) = A - Be^{-\alpha_{\text{opt}}L}$, where α_{opt} is the perturbation coefficient (which has nothing to do with the attenuation coefficient α_{att}), A and B are constants, and the following physical limiting values are imposed: $E_{\text{opt}}(0) = e_{\text{opt}}$ and $E_{\text{opt}}(\infty) = (N-1)/N$; that is, at large distances the accumulated perturbations make sure that all states have the same probability $1/N$ to be detected and therefore the optical error will be $(N-1)/N$ as it also occurs for e_0. Therefore, we obtain the values $A = (N-1)/N$ and $B = A - e_{\text{opt}}$, and consequently

$$E_{\text{opt}}(L) = e_{\text{opt}} + \left(\frac{N-1}{N} - e_{\text{opt}}\right)(1 - e^{-\alpha_{\text{opt}}L}). \tag{43}$$

Note that for $e_{\text{opt}} = 0$ we only have the error due to perturbations; that is, $E_{\text{per}} = [N-1)/N][1 - e^{-\alpha_{\text{opt}}L}]$. Now, we substitute e_{opt} for $E_{\text{opt}}(L)$ into the expression for E_μ given in Eq. (40) and the expression for e_1 given by Eq. (41). Values of α_{opt} in the interval $(1\times10^{-3}, 4\times10^{-3})$ are compatible with those found in the literature about modal cross-talking due to perturbations. For instance, for $\alpha_{\text{opt}} = 2\times10^{-3}$ km^{-1} we obtain an error of 1.5×10^{-3}, which is approximately -28 dB. This value is a realistic one because spatial and polarization mode cross-talking in optical fibers can take values around -30 dB or even larger [44,45]. In short, cross-talking provides an estimation of errors due to the loss of information (bits) carried by an optical mode.

In Fig. 6 the key rates for different perturbation coefficients and with $N = 4$ are shown, that is, the ideal or autocompensated case characterized by $\alpha_{\text{opt}} = 0$ (solid line), and three realistic cases $(1, 2, 4)\times10^{-3}$ km^{-1} with $e_{\text{opt}} = 0.0964$. The following values have been used: $\mu = 0.2$, $\nu = 0.1$, $P_{\text{dark}} = 2.06\times10^{-7}$, $\alpha_{\text{att}} = 0.4$ dB/km, $\eta_d = 6.09/100$, and $\eta_B = 10^{-2.45}$ [12]. Note that for $\alpha_{\text{opt}} = 2\times10^{-3}$ km^{-1} the key rate is reduced along the optical fiber in a significant way.

In Fig. 7 the error $E_{\text{opt}}(L)$ is plotted with the distance. Note that at $L = 25$ km we have $E_{\text{opt}}(25\text{ km}) = 0.121$; that is, the error due to perturbations is only 0.025 but with a great impact in the key rate as shown in Fig. 6. Furthermore, we must stress that larger key rates are obtained for $N > 4$. All these results justify the use of high-dimensional autocompensation methods as those proposed in this work.

V. CONCLUSIONS

In conclusion, we have proved that a fully autocompensating high-dimensional quantum cryptography in optical fibers and free space can be achieved by degenerate four-wave mixing. A single round trip allows to autocompensate the undesired modal coupling and random phase shifts among spatial and polarization modes, due to a myriad of (mechanical, thermal, geometrical, etc.) perturbations and imperfections and thus high-dimensional QKD protocols such as the BB84 can be physically implemented in a plug-and-play way. We have presented a fiber-optic setup for the case of multicore optical fibers which in turn can be connected to integrated devices to perform generation and projective measurements of states for both weak coherent states and single-photon states. Special attention has been paid to an integrated passive device for quantum random choice of the measurement basis which aids increases of the security of the system as dimension increases. Likewise, a brief security analysis for a phase-remapping attack has been made and it is concluded that QBER tends to 50% as dimensionality increases, and moreover the round trips for getting autocompensation do not make the system more vulnerable. Likewise, variation of the security key rates with the distance have been analyzed when optical fibers undergo perturbations which have not been compensated. Significant increase in the secret key rate and therefore in the security distance of decoy-state QKD is obtained when autocompensation is used, which justifies the usefulness of the proposed autocompensating optical method to cancel such perturbations.

ACKNOWLEDGMENTS

The authors wish to acknowledge the financial support of this work by Xunta de Galicia, Consellería de Educación, Universidades e FP, with a Consolidation-GRC Grant No. ED431C2018/11, a Strategic Grouping of Materials (AeMAT) Grant No. ED431E 2018/08, and two predoctoral grants (D.B., 2017, and G.M.C., 2020), co-financed with the European Social Fund: Galicia ERDF 2014-20 OP.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[2] N. Bai, E. Ip, Y. Huang, E. Mateo, F. Yaman, M. Li, S. Bickham, S. Ten, J. Liñares, C. Montero, V. Moreno, X. Prieto, V. Tse, K. M. Chung, A. P. T. Lau, H. Tam, C. Lu, Y. Luo, G. Peng, G. Li, and T. Wang, Mode-division multiplexed transmission with inline few-mode fiber amplifier, Opt. Express **20**, 2668 (2012).

[3] G. Li, N. Bai, N. Zhao, and C. Xia, Space-division multiplexing: The next frontier in optical communication, Adv. Opt. Photon. **6**, 413 (2014).

[4] L. Zou, X. Gu, and L. Wang, High-dimensional free-space optical communications based on orbital angular momentum coding, Opt. Commun. **410**, 333 (2018).

[5] N. J. Cerf, M. Bourennade, A. Karlsson, and G. Gisin, Security of Quantum Key Distribution Using *d*-Level Systems, Phys. Rev. Lett. **88**, 127902 (2002).

[6] 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).

[7] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Plug and play systems for quantum cryptography, Appl. Phys. Lett. **70**, 793 (1997).

[8] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, Quantum cryptography, Appl. Phys. B **67**, 743 (1998).

[9] R. Bedington, J. M. Arrazole, and A. Ling, Progress in satellite quantum key distribution, npj Quantum Inf. **3**, 30 (2017).

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

[11] D. Jin, Y. Guo, Y. Wang, and D. Huang, Parameter estimation of orbital angular momentum based continuous-variable quantum key distribution, J. Appl. Phys. **127**, 213102 (2020).

[12] G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. Ferreira 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).

[13] D. Bacco, Y. Ding, K. Dalgaard, K. Rottwitt, and L. K. Oxenløwe, Space division multiplexing chip-to-chip quantum key distribution, Sci. Rep. **6**, 12459 (2017).

[14] J. F. Dynes, S. J. Kindness, S. W.-B. Tam, A. Plews, A. W. Sharpe, M. Lucamarini, B. Fröhlich, Z. L. Yuan, R. V. Penty, and A. J. Shields, Quantum key distribution over multicore fiber, Opt. Express **24**, 8081 (2016).

[15] D. S. Bethune and W. P. Risk, Autocompensating quantum cryptography, New J. Phys. **4**, 42 (2002).

[16] D. Balado, J. Liñares, X. Prieto-Blanco, and D. Barral, Phase and polarization autocompensating N-dimensional quantum cryptography in multicore optical fibers, J. Opt. Soc. Am. B **36**, 2793 (2019).

[17] D. Balado, J. Liñares, and X. Prieto-Blanco, Phase autocompensating high-dimensional quantum cryptography in elliptical-core few-mode fibers, J. Mod. Opt. **66**, 947 (2019).

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

[19] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge, UK, 1995).

[20] A. Yariv and D. M. Pepper, Amplified reflection, phase conjugation, and oscillation in degenerate four-wave mixing, Opt. Lett. **1**, 16 (1977).

[21] D. M. Pepper, D. Fekete, and A. Yariv, Observation of amplified phase-conjugate reflection and optical parametric oscillation by degenerate four wave mixing in a transparent medium, Appl. Phys. Lett. **33**, 41 (1978).

[22] Y. Ben-Aryeh and S. Serulnik, The quantum treatment of propagation in non-linear optical media by the use of temporal modes, Phys. Lett. A **155**, 473 (1991).

[23] J. Liñares, M. C. Nistal, and D. Barral, Quantization of coupled 1D vector modes in integrated photonics waveguides, New J. Phys. **10**, 063023 (2008).

[24] S. Dong, X. Yao, W. Zhang, S. Chen, W. Zhang, L. You, Z. Wang, and Y. Huang, True single-photon stimulated four-wave mixing, ACS Photon. **4**, 746 (2017).

[25] F. D. Murnaghan, *The Unitary and Rotation Groups* (Spartan Books, Washington, DC, 1962).

[26] M. Reck, A. Zeilinger, H. Bernstein, and P. Bertani, Experimental Realization of any Discrete Unitary Operator, Phys. Rev. Lett. **73**, 58 (1994).

[27] H. de Guise, O. Di Matteo, and L. L. Sánchez-Soto, Simple factorization of unitary transformations, Phys. Rev. A **97**, 022328 (2018).

[28] M. V. Berry, Interpreting the anholonomy of coiled light, Nature **326**, 266 (1987).

[29] K. Kitayama, *Optical Code Division Multiple Access* (Cambridge University Press, Cambridge, UK, 2014).

[30] Y. Fujii, Compact high-isolation polarization-independent optical circulator, Opt. Lett. **18**, 250 (1993).

[31] S. G. Leon-Saval, A. Argyros, and J. Bland-Hawthorn, Photonic lanterns, Nanophotonics **2**, 429 (2013).

[32] J. Liñares, X. Prieto-Blanco, C. Montero-Orille, and V. Moreno, Spatial mode multiplexing/demultiplexing by Gouy phase interferometry, Opt. Lett. **42**, 93 (2017).

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

[34] H. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[35] F. Xu, M. Curty, B. Qi, and H. Lo, Measurement-device-independent quantum cryptography, IEEE J. Sel. Top. Quantum Electron. **21**, 6601111 (2015).

[36] F. Xu, M. Curty, B. Qi, and H.-K. Lo, Practical aspects of measurement-device-independent quantum key distribution, New J. Phys. **15**, 113007 (2013).

[37] J. Liñares-Beiras, X. Prieto-Blanco, D. Balado, and G. M. Carral, Autocompensating measurement-device-independent quantum cryptography in few-mode optical fibers, EPJ Web Conf. **238**, 09002 (2020).

[38] C. H. F. Fung, B. Qi, K. Tamaki, and H. K. Lo, Phase-remapping attack in practical quantum-key-distribution systems, Phys. Rev. A **75**, 032314 (2007).

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

[40] H. P. Yuen, Quantum amplifiers, quantum duplicators and quantum cryptography, Quantum Semiclass. Opt. **8**, 939 (1996).

[41] N. Lütkenhaus and M. Jahma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack, New J. Phys. **4**, 44 (2002).

[42] A. Klappenecker and M. Rötteler, Constructions of mutually unbiased bases, in *Finite Fields and Applications*, edited by G. L. Mullen, A. Poli, and H. Stichtenoth (Springer, Berlin, 2003), p. 137.

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

[44] Z. Wang, X. Hu, M. Lin, Q. Mo, H. Wen, and G. Li, Measurements of Polarization Crosstalk in a Polarization-Maintaining Few-Mode Optical Fiber, in *Conference on Lasers and Electro-Optics*, OSA Technical Digest (online) (Optical Society of America, 2017), paper JW2A.70.

[45] L. Zhu, J. Liu, Q. Mo, C. Du, and J. Wang, Encoding/decoding using superpositions of spatial modes for image transfer in km-scale few-mode fiber, Opt. Express **24**, 16934 (2016).