Journal of the European Optical Society-Rapid Publications

RESEARCH Open Access

Autocompensating measurement-device-independent quantum cryptography in space division multiplexing optical fibers

J. Liñares*, G. M. Carral, X. Prieto-Blanco and D. Balado

Abstract

Single photon or biphoton states propagating in optical fibers or in free space are affected by random perturbations and imperfections that disturb the information encoded in such states and accordingly quantum key distribution is prevented. We propose three different systems for autocompensating such random perturbations and imperfections when a measurement-device-independent protocol is used. These systems correspond to different optical fibers intended for space division multiplexing and supporting collinear modes, polarization modes or codirectional modes such as few-mode optical fibers and multicore optical fibers. Accordingly, we propose different Bell-states measurement devices located at Charlie system and present simulations that confirm the importance of autocompensation. Moreover, these types of optical fibers allow the use of several transmission channels, which compensates the reduction of the bit rate due to losses.

Keywords: Quantum cryptography, Measurement-device-independent, Space division multiplexing, Autocompensation, Integrated quantum optics

Introduction

Over the last few years, space division multiplexing has been proposed to further increase the data bandwidth in optical communications; thus, high interest has arisen about new optical fibers such as few-mode fibers (FMFs) [1] and multicore fibers (MCFs) [2]. Consequently, the interest in the implementation of quantum cryptography in these new optical fibers has remarkably increased in the last few years [3–6]. Quantum cryptography states that the laws of quantum mechanics, if correct, guarantee unconditional security of communications under quantum key distribution protocols [7, 8]. At least, this is what theory teaches us. When it comes to real-life implementations, however, a number of problems arise that put such assertion in jeopardy. This is due to the fact that devices used in Quantum Key Distribution (QKD) protocols are imperfect in reality. Such imperfections open a backdoor for an eavesdropper (Eve) to obtain information that ideally would be perfectly concealed.

One of the most important problems corresponds to the detector side channel attacks. They are related to the fact that the detector apparatuses Alice and/or Bob use may be flawed, and that might give Eve an opportunity to extract secret information about the key without Alice and Bob knowing [9–11].

Fortunately for the security of communications, a quite good solution has been developed, that is, Measurement-Device-Independent quantum key distribution (MDI-QKD) [12]. This idea consists in making use of entanglement in such a way that the whole measurement process is treated like a black box. Traditionally, in QKD, the measurement is done by the partner sitting at the end of the line (normally Bob). In this case, a third party, called Charlie, makes the measurement. He performs a Bell measurement on the two-qubit state Alice and Bob

*Correspondence: suso.linares.beiras@usc.es
Quantum Materials and Photonics Research Group, Optics Area, Applied Physics Department, Universidade de Santiago de Compostela, Campus Vida s/n, E-15782 Santiago de Compostela, Galicia, Spain

send him. The key is that Charlie may be untrusted. He can be an eavesdropper himself. Charlie is only asked to report whether he obtained a successful or an unsuccessful result from his measurement, and he can of course lie. May the detectors he uses be flawed and/or may he be Eve in disguise: it does not matter. The detection process is a black box, what happens inside has no relevance, only what Charlie reports in relation to what quantum state Alice and Bob sent. To this last part, usual defence methods need to be applied (i.e. decoy states [13], etc). Thus, Alice and Bob can establish a secret key without the need to take into account detector side channel attacks. The main downside of this solution is that the key rate is small [14] compared to standard protocols. Also, sources need to be trusted and state preparation has to be almost perfect. There also other practical problems to overcome [15]. But, in all, among the proposals that inherently protect against side-channel attacks, MDI-QKD is the one of greater feasibility [8, 12].

Another class of practical problems in quantum (and classical) communications are the perturbations that photons suffer when they propagate along optical fibers. Certain perturbations and also imperfections in practical optical fibers randomly scramble the information encoded in photons, impairing QKD. When the link is very short this posses no real problem, but in real-life quantum communications links are required to be about a few hundreds of kilometres, and the aim is precisely to increase this limit. An example of such pertubations is the undesired birefringence most real-life fibers have, unless they are polarization-maintaining fibers [16], which have a high but tailored built-in birefringence, so as to preserve two particular linear polarization states of the travelling photons although the relative phase remains random. Information may be encoded in the photons polarization, and undesired birefringence alters the state of polarization unpredictably. In other words, such birefringence cannot be completely characterized, causing a random perturbation. Then, if polarization changes randomly when the photons are on the fly, no key can be established. On the other hand, in optical fibers intended for space division multiplexing, spatial perturbations, due to mechanical causes, thermal causes and so on, can also give rise to undesired and unpredictable couplings between spatial modes (modal crosstalk) with the same effect of precluding QKD. This last case is acute when one deals with many spatial modes and multicore optical fibers (MCFs) and even few-mode fibers (FMFs). Moreover, these spatial perturbations can also change with time although slowly with respect to transmission speed. Likewise, imperfections in optical fibers can also give rise to mode coupling. Solutions to such problems have been proposed in QKD protocols by the so-called autocompensating cryptography, thus, autocompensating QKD methods have been proposed for single photon states excited in polarization and/or spatial modes [17, 18]. Autocompensating cryptography consists in taking the travelling light and make it go through some determinate optical elements that alter its state in such a way that the perturbations become harmless. The price to pay is that light has to travel back-and-forth between the two ends of the line, that is, it has to travel at least two times the same distance. This enhances distance-related drawbacks like fiber losses. This won't be a problem, nonetheless, when we compute the key rate, since if we use coherent states they are only attenuated at Alice and Bob's sites, that is, the weak coherent states do not cover two times the distance between Alice/Bob and Charlie. Note that autocompensation does not eliminate or make any attempt to eliminate such perturbations, but their effects, restoring the photonic quantum state that was originally launched. At this point we must stress that in optical fibers for space division multiplexing several channels could be used, thus reducing the effects associated to fiber losses. Another solution exists, consisting in continuously monitoring the properties of the communication links like optical fibers, correcting in real time the undesired modifications the propagating state can undergo as for example relative phases, although coupling effects would be much more difficult to correct [19] and moreover, a complememtary light signal is required in order to measure the perturbations together with a complex electronic processing device.

In this work, we propose an Autocompensating MDI-QKD (A-MDI-QKD) protocol, which is based on biphoton states. We will do it in three ways, each one corresponding to a different photonic encoding: collinear modes, polarization modes and codirectional modes. By collinear modes we refer to modes propagating along the same direction, travelling in the same core of a fiber, such as Hermite-Gauss (HG) modes. Few mode optical fibers are the transmission lines for collinear modes, although optical communication in free space can make use of this kind of spatial modes. We will distinguish between polarization-maintaining few mode fibers (PM-FMFs) [16], where two particular linear polarizations are maintained for long distances, and space-maintaining few-mode fibers (SM-FMFs), where spatial modes are maintained decoupled for long distances [20]. By codirectional modes, we refer to modes travelling along different fibers or different cores of the same fiber. This kind of modes are directly compatible with integrated optics by using photonic lanterns or proper optical connectors. As commented, nowadays, research in MCFs is an active field, since MCFs can be used to increase to a large extent the communication capacities of fiber links. Moreover, this makes the adaptability to current (and future) systems a lot easier, with the possibility of using the available infrastructure to set up A-MDI-QKD protocols following a plug-and-play philosophy [21]. On the other hand, scalability, compactness, robustness an so on, are well-known attributes of optical integrated technologies [22]. Importantly, integrated devices, together with MCFs [3, 23, 24], open the possibility, in a very clear way, to extend the protocol to N dimensions, which increases security. At this point, we must also stress that the use of mode converters based on photonic lanterns [25] or multi-plane interfaces [26] between FMFs and channel waveguide modes also allows to use integrated optical components because collinear modes can be converted into codirectional modes, although in this work, for the sake of completeness, bulk components will also be used. The same interface procedure can be applied to polarization modes. Consequently, we will use four modes where two photons are excited, that is, two-qubits. Besides, as the algebraic mechanism to obtain autocompensation is different for each encoding, then we will deal with each case separately. Therefore, the plan of this paper is as follows. We start by proposing a full A-MDI-QKD optical system for collinear modes coming from PM-FMFs, which can provide several spatial channels for QKD because polarization is maintained across a long distance. Next, a A-MDI-QKD optical system for polarization modes of SM-FMFs is presented. Moreover, as in the spatial case it can also provide several polarization QKD channels because spatial modes are maintained decoupled for a long distance. Finally, we propose an A-MDI-QKD optical system for codirectional modes coming from MCFs by using integrated optics to measure the Bell states. The main conclusions are summarized at the end.

A-MDI-QKD system with collinear modes

As commented, for this case, we encode information in two collinear spatial modes of two PM-FMFs linking Alice-Charlie and Bob-Charlie as shown in Fig. 1. This kind of fibers have a birrefringence which is high enough to separate polarization modes, however, spatial modes can undergo coupling. For instance in this kind of fibers, there will be mode coupling between $\mathrm{LP}_{11H}^{(e)}$ and $\mathrm{LP}_{11H}^{(o)}$ modes, and $\mathrm{LP}_{11V}^{(e)}$ and $\mathrm{LP}_{11V}^{(o)}$ modes [16], with (e) indicating even mode ($\cos\varphi$) and (o) odd mode ($\sin\varphi$). However, polarization mode coupling is negligible. Obviously, each polarization can be considered as a potentially useful channel for QKD, therefore, we could use several independent channels to perform QKD, which would increase the bit rate and therefore would reduce the loss effects and larger distances would be achieved. For example, let us consider without loss of generality that the quantum states are excited in the particular modes $\mathrm{LP}_{11H}^{(e)} \equiv X$ and $\mathrm{LP}_{11H}^{(o)} \equiv Y$, that is, in horizontal (X) and vertical (Y) Hermite-Gaussian (HG) modes polarized, for instance, along the horizontal direction. Single photon states are denoted as $|1_X\rangle$ and $|1_Y\rangle$. The vertical polarization direc-

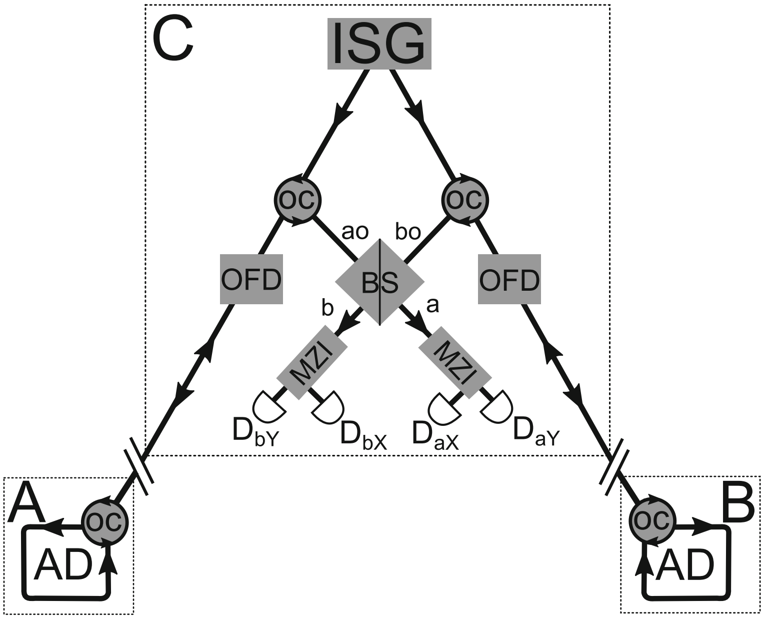

Fig. 1 A-MDI-QKD system for collinear modes. Light comes from Charlie along PM-FMF optical fibers. States are delayed by OFDs. They arrive at Alice's and Bob's laboratories, where they travel along local loops equipped with autocompensating devices (AD) and phase modulators. Local loop structure is symbolized by a loop with AD inside. Light returns to Charlie, and optical circulators (OC) direct the photons towards a Bell-state measurement apparatus composed by a BS and two MZIs working as mode sorters, together with the corresponding detectors

tion could be used as a second channel. More channels could be considered if other modes are used as, for example, $\mathrm{LP}_{21H}^{(e)}$ and $\mathrm{LP}_{21H}^{(o)}$ modes, and $\mathrm{LP}_{21V}^{(e)}$ and $\mathrm{LP}_{21V}^{(o)}$ modes [16].

The A-MDI-QKD system is shown in Fig. 1. As autocompensation requires light to go back-and-forth, then the light source must be located at Charlie. Such source can be a SPDC or two independent lasers emitting WCPs (weak coherent pulses) and ensuring photon indistinguishability. Accordingly, Charlie prepares the following state

$$\left(\frac{|1_X\rangle+|1_Y\rangle}{\sqrt{2}}\right)_a\otimes\left(\frac{|1_X\rangle+|1_Y\rangle}{\sqrt{2}}\right)_b \tag{1}$$

and sends each part of it to Alice and Bob. Indexes a and b stand for Alice's and Bob's paths, respectively. If WCPs are used then decoy states are also required in order to prevent photon number splitting (PNS) attacks. We group whatever source Charlie uses to generate those states under the name Initial States Generator (ISG). Next, light reaches Charlie's optical circulators (OC), which direct the light towards Alice's and Bob's sites. After the circulators optical fiber delay (OFD) devices are placed to delay states excited in mode Y a time τ with respect to states excited in mode X, meaning that we will have $|1_X\rangle$ and $|1_{Y\tau}\rangle$. The OFDs (see Fig. 2) consist on a Mach-Zehnder interferometer (MZI) with a Dove prism (DP) in one of its arms. They work in the following way. When the quantum state reaches the first beam splitter (BS), one part of it goes into the horizontal (h) path and another on the vertical (v) path. Then, the Dove prism in the vertical path introduces the following transformation on the modes

$$D_\vartheta=\begin{pmatrix}\cos 2\vartheta & \sin 2\vartheta\\ \sin 2\vartheta & -\cos 2\vartheta\end{pmatrix}, \tag{2}$$

where ϑ is the angle in which the normal of the prism is rotated. This means that if we have states $|1_X\rangle$ and $|1_Y\rangle$ as input, the output will be a $|1_{X'}\rangle$ mode given by the linear combination $|1_{X'}\rangle = \cos 2\vartheta|1_X\rangle + \sin 2\vartheta|1_Y\rangle$, and analogously for $|1_Y\rangle$. Setting $\vartheta = 0$ we obtain the transformations $|1_{X'}\rangle = |1_X\rangle$ and $|1_{Y'}\rangle = -|1_Y\rangle$. So, for an input $\frac{1}{\sqrt{2}}(|1_{hX}\rangle + |1_{hY}\rangle)$ at the horizontal input of the first BS, the emergent state after the second BS is $\frac{1}{\sqrt{2}}(|1_{vX}\rangle - |1_{hY}\rangle)$. This means that the X mode exits the vertical port of the second BS and is directed towards Alice (and Bob), while the Y mode exits the horizontal port, and is directed towards an external optical path that feeds the vertical port of the first BS. The result is that the Y mode gets delayed with respect to the X mode, by a quantity we call τ. This delay will allow Alice and Bob to introduce relative phases between X and Y modes. Thus, the state after the OFDs is

$$|L_e\rangle=\left(\frac{|1_X\rangle+|1_{Y\tau}\rangle}{\sqrt{2}}\right)_a\otimes\left(\frac{|1_X\rangle+|1_{Y\tau}\rangle}{\sqrt{2}}\right)_b. \tag{3}$$

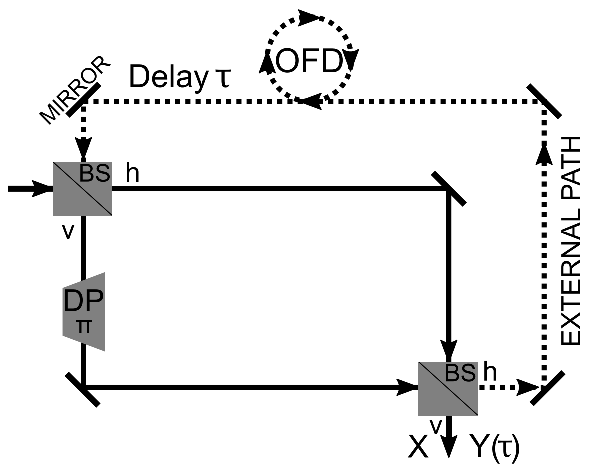

Fig. 2 Scheme of a MZI operating with HG modes. A Mach-Zehnder Interferometer together with a Dove prism in one of its arms operates as a HG mode sorter. At the output of the last BS, the X mode emerges on the v path and the Y mode on the h path. This modes can be either redirected to detectors, as in Figure 1, to project onto Bell states, or the Y mode can be redirected into a external path (dashed line), introducing a delay τ between modes, that is, $|1_X\rangle$ and $|1_{Y\tau}\rangle$. Thus, such MZIs can be used as 'polarizing' beam splitters (thinking of X and Y as polarizations) for Bell-state detection as well as OFD devices

Now, photons enter (and then exit) optical fiber circuits at Alice and Bob's sites trough optical circulators. Note that Alice and Bob's laboratories need to be well shielded from eavesdroppers. No information should leak out. In these circuits, autocompensating devices are located, together with phase modulators by which Alice and Bob encode their bits. Electro-optical phase shifters implement this task. Alice and Bob introduce a relative phase $e^{i\theta}$ between $|1_X\rangle$ and $|1_Y\rangle$, randomly chosen from the set $\theta = \{-\pi/2, 0, \pi/2, \pi\}$, in order to encode information in one of the two following mutually unbiased bases (MUBs), that is, diagonal and circular bases,

$$\mathcal{B}_D:\left\{|1_D\rangle=\frac{|1_X\rangle+|1_Y\rangle}{\sqrt{2}},|1_A\rangle=\frac{|1_X\rangle-|1_Y\rangle}{\sqrt{2}}\right\}, \tag{4}$$

$$\mathcal{B}_C:\left\{|1_L\rangle=\frac{|1_X\rangle+i|1_Y\rangle}{\sqrt{2}},|1_R\rangle=\frac{|1_X\rangle-i|1_Y\rangle}{\sqrt{2}}\right\}. \tag{5}$$

It is worth writing the transformation between absorption operators $\hat{a}$ in both bases, that is

$$\hat{a}_{\binom{D}{A}}=\frac{1}{\sqrt{2}}\left(\hat{a}_X\pm\hat{a}_Y\right);\quad \hat{a}_{\binom{L}{R}}=\frac{1}{\sqrt{2}}\left(\hat{a}_X\mp i\hat{a}_Y\right). \tag{6}$$

Note again that autocompensation requires light to follow a closed path. As in MDI-QKD the photons end at Charlie's site, if we add autocompensation, light needs to start its way at Charlie's site too. Charlie provides the input light and Alice and Bob modulate its phase in order to generate quantum states on which encode their bits. It is clear why we can not use the usual basis $\{|1_X\rangle, |1_Y\rangle\}$

(socalled the Z or rectilinear basis and used normally in MDI-QKD protocol [12]) because it can not be converted in any other basis by phase modulation. Obviously, rotations can be used to change basis, but, in that case, the autocompensating transformation we will describe afterwards would become useless, hence autocompensation would not work. We will ignore the perturbations for a while to explain the measurement process, then we will deal with the autocompensation method.

Bell-state measurement device

After exiting the fiber circuits, light goes back to Charlie. At Charlie's circulators light is directed towards a Bell-state measurement device. This device is composed by a beam splitter (BS) plus two MZI identical to the MZIs present above in Fig. 2 (except that they lack the external optical path for OFD). The BS acts the usual way, entangling photons and producing Bell states, which will be postselected afterwards. As analyzed, the MZIs act as a polarizing beam splitter would do in the polarization case, that is, they sort X and Y modes, each one in one different port, as we have seen. Then, photons are directed towards detectors $D_{aX}, D_{aY}, D_{bX}, D_{bY}$ and Bell states will be measured. In detail, the working principle of this Bell-state measurement apparatus is the following. Let's call the input ports of the BS after the OCs in Fig. 1 as *ao* and *bo*, and the output ports as *a* and *b*. Now, assume that such BS is of the type that induces the following transformation between the input and output modes, with corresponding photon emission operators $\hat{a}^\dagger_{ao}, \hat{a}^\dagger_{bo}, \hat{a}^\dagger_{a}, \hat{a}^\dagger_{b}$:

$$\hat{a}^\dagger_{ao} = \frac{\hat{a}^\dagger_a + i\hat{a}^\dagger_b}{\sqrt{2}}; \quad \hat{a}^\dagger_{bo} = \frac{i\hat{a}^\dagger_a + \hat{a}^\dagger_b}{\sqrt{2}}. \tag{7}$$

Now, when Alice and Bob choose the same basis (else the data is discarded), there are two classes of input states. The first one is when Alice and Bob prepare the same state and the second one is when they prepare different states. Consider the first case of a diagonal basis. Let us consider, for instance, that the state that reaches the BS is

$$|L_{nf}\rangle = |1_{aoD}\rangle|1_{boD}\rangle. \tag{8}$$

This state corresponds to the case so-called not bit-flip case. This state can be rewritten, by taking into account the transformation given by Eq. (7), as follows

$$|L_{nf}\rangle = \frac{i}{2}\left(\hat{a}^{\dagger 2}_{aD} + \hat{a}^{\dagger 2}_{bD}\right)|00\rangle. \tag{9}$$

Next, by using the measurement modes X and Y we obtain

$$|L_{nf}\rangle = \frac{i}{4}\left\{\left(\hat{a}^\dagger_{aX} + \hat{a}^\dagger_{aY}\right)^2 + \left(\hat{a}^\dagger_{bX} + \hat{a}^\dagger_{bY}\right)^2\right\}|00\rangle. \tag{10}$$

Note that by one hand we obtain the following state

$$|L_{nc}\rangle = \frac{\sqrt{2}}{4}(|2_{aX}\rangle + |2_{aY}\rangle + |2_{bX}\rangle + |2_{bY}\rangle), \tag{11}$$

that is, we detect the two photons in only one detector, that is, there are no coincidences with a probability equal to 1/2. On the other hand, we also obtain with a probability equal to 1/2, the following Bell state $|\Phi^+\rangle$ (with respect to the detectors *a* and *b*),

$$|L_c\rangle = \frac{\sqrt{2}}{2}|\Phi^+\rangle = \frac{\sqrt{2}}{2}\frac{(|1_{aX}1_{aY}\rangle + |1_{bX}1_{bY}\rangle)}{\sqrt{2}}, \tag{12}$$

meaning that there are coincidences in the same output, *a* or *b*, that is, there will be a simultaneous click between the same pair of detectors, either D_{aX} together with D_{aY} or D_{bX} together with D_{bY}. However, if the input state is, for instance,

$$|L_f\rangle = |1_{aoD}\rangle|1_{boA}\rangle, \tag{13}$$

which corresponds to a bit-flip, then by taking into account the transformation given by Eq. (7), the state can be rewritten as

$$|L\rangle = \frac{i}{2}\left(\hat{a}^\dagger_{aD} + i\hat{a}^\dagger_{bD}\right)\left(i\hat{a}^\dagger_{aA} + \hat{a}^\dagger_{bA}\right)|00\rangle. \tag{14}$$

By following the same procedure as in the above case, we obtain both states corresponding to non coincidences and the following Bell state, with a probability equal to 1/2,

$$|L_c\rangle = \frac{\sqrt{2}}{2}|\Psi^-\rangle = \frac{\sqrt{2}}{2}\frac{(|1_{aX}1_{bY}\rangle - |1_{bX}1_{aY}\rangle)}{\sqrt{2}}, \tag{15}$$

that is, coincident clicks between D_{aX} and D_{bY} or D_{aY} and D_{bX}, are obtained, which is precisely the $|\Psi^-\rangle$ Bell state. Now, each photon emerges in a different port. We must stress that the non coincidences can be used to calibrate the system, that is, we must detect the same amount of coincidences and non coincidences to make sure that the system is aligned and adjusted and therefore the protocol can be implemented. However, we still need to eliminate the effect of possible perturbations by an autocompensating method.

Autocompensation method

As commented, we encode information in two collinear spatial modes propagating in a PM-FMF along the z-direction, in particular, $\mathrm{LP}^{(e)}_{11H} \equiv X$ and $\mathrm{LP}^{(o)}_{11H} \equiv Y$. We will describe in detail the autocompensation mechanism that enables to get rid of perturbations that arise when such modes propagate along optical fibers. The aim of autocompensation is that the photonic state emerges restored after it has travelled the path, back and forth, between the starting point and the endpoint of the fiber link. Intrinsic imperfections of dielectric permitivitty or perturbations $P(x,y)$ produced by mechanical and/or thermal causes give rise to modal coupling between optical modes. The two-mode coupling coefficient is given by

$$\kappa_s = \int e_1(x,y)P(x,y)e_2(x,y)dxdy, \tag{16}$$

where $e_1(x,y)$ and $e_2(x,y)$ are the mode amplitudes. $P(x,y)$ is a random perturbation, which can regarded as z-invariant in a short propagation distance z. Therefore the total perturbation is a sequence of q perturbations with different coupling coefficients. Each perturbation $k = 1,...q$ can be described by an asynchronous modal coupling, that is, the formal solution for the absorption operators is given by

$$\begin{pmatrix} \hat{a}_{k1} \\ \hat{a}_{k2} \end{pmatrix} = S_k \begin{pmatrix} \hat{a}_{k01} \\ \hat{a}_{k02} \end{pmatrix} = \begin{pmatrix} A_k & iB_k \\ iB_k & A_k^* \end{pmatrix} \begin{pmatrix} \hat{a}_{k01} \\ \hat{a}_{k02} \end{pmatrix}. \qquad (17)$$

Now, we can model the perturbations along the fiber as a discrete number q of perturbations, acting on the absorption operators. Moreover, since we are dealing with single-photon states in each link, it can be shown that the solutions to the Heisenberg equations for spatial propagation apply directly to photonic states [27]. Thus, if $|\psi\rangle$ is a photonic state, then $|\psi(z)\rangle = S|\psi(0)\rangle$, where S is the total matrix $S = S_q, S_{q-1}...S_2S_1$.

On the other hand, the coupling coefficients remain invariant under backpropagation, that is, by defining a new reference system given, for instance, by $(-X)Y(-Z)$, the original one being given by XYZ, it is easy to check that κ_s does not change under backpropagation, therefore, the matrices S_k do not change under backpropagation. We write down explicitly the transformation the photonic states would experience when going back-and-forth along the optical fiber. When going from Charlie to Alice (and Bob), we have $T_{\rightarrow} = S_q...S_1$, and, when going back from Alice (Bob) to Charlie, we have again $T_{\leftarrow} = S_1...S_q$. Between these two operations, we have to put the right transformation, implemented by the adequate autocompensating devices, so that we restore the original photonic state. The full transformation the light experiences on a roundtrip is

$$T_{\leftarrow}MT_{\rightarrow} = S_1...S_qMS_q...S_1, \qquad (18)$$

where M represents the operation of the autocompensating devices. It is easy to check that $M = i\sigma_y$, with σ_y the second Pauli matrix, restore the state, that is

$$S_kMS_k = \begin{pmatrix} A_k & iB_k \\ iB_k & A_k^* \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} A_k & iB_k \\ iB_k & A_k^* \end{pmatrix}, \qquad (19)$$

then $S_kMS_k = M$. This means that the state of the emergent light, back at Charlie's circulators, has been properly restored, albeit a deterministic swapping transformation $M = i\sigma_y$, which we can account for.

Next, we must answer the question of how to implement the operation $M = i\sigma_y$ with HG modes. This can be done by using two cylindrical lens converters (CLCs) [28] and a Dove prism with $\vartheta = \pi/4$, plus a phase shifter (PS) introducing a global phase $\phi = -\pi/2$, as shown in Fig. 3. The Dove prism is sandwiched between the CLCs [29]. The CLCs rotate the X and Y modes by phases $\pm\pi/2$, respectively. They convert Hermite-Gauss modes into Laguerre-Gauss ones. In matrix form, this can be written as

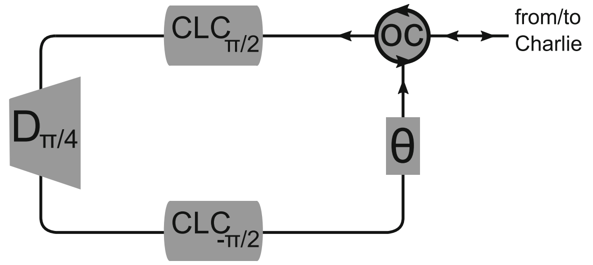

Fig. 3 Autocompensating devices for collinear modes and state generation by phase modulation. At Alice's and Bob's sites local loops equipped with autocompensating devices and phase modulators are located. The combination of two CLCs and a Dove prism, each one with a determinate orientation, implements the matrix $-\sigma_y$, which suffices to autocompensate for perturbations due to modal coupling. The phase modulator introduces a phase θ by which to send photons back to Charlie in one of the two MUBs $\boldsymbol{\mathcal{B}}_1$ and $\boldsymbol{\mathcal{B}}_2$ described above

$$CLC_{\pm\pi/2} = \begin{pmatrix} 1 & 0 \\ 0 & \pm i \end{pmatrix}. \qquad (20)$$

Now, the Dove prism is rotated $\pi/4$, therefore, from (2), it implements the operation $D_{\pi/4} = \sigma_x$. Therefore, we obtain the desired transformation,

$$M = e^{-i\pi/2}CLC_{-\pi/2}D_{\pi/4}CLC_{\pi/2} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \qquad (21)$$

We left some more nuances along the road that deserve however more attention. First of all, when we wrote (18), it may seem that we forgot about the phase gate Alice and Bob apply in order to obtain the different quantum states in which encode their bits. However, we must recall that at Alice and Bob systems the states are excited in retarded modes as given by Eq. (3). In other words, autocompensation is for the retarded states $|1_X\rangle$ and $|1_{Y\tau}\rangle$ in an individualized fashion. The transformation $U(\theta) = \text{diag}\left(1, e^{i\theta}\right)$ implementing the phase modulation acts on the above states, in particular on $|1_{Y\tau}\rangle$. Another subtlety is that the fiber circuits, where the autocompensation devices and phase modulators are located, have a very small length. Note that this path is never autocompensated but is however so small that is contribution to a perturbation of the photonic states is negligible. They are local fiber loops. We remark that this will be common to all three encodings described in this paper. Moreover, we must note that the delay introduced in OFD when the photons come back cancels the delay introduced at the beginning. This is because the Dove-$\pi/4$ prism formally swaps modes X and Y but does not swap their identity. This implies that, if when the photons first went through the OFD, the X mode went ahead of Y, then after the

Dove-$\pi/4$ prism, it is the Y mode who goes ahead. Then, again at the OFD device, the Y gets retarded and waits for the X mode so that they reach Charlie's Bell state apparatus exactly at the same time. This can be calibrated by using the HOM states that are produced at the BS.

Finally, note that we are saying that modes coming from Alice's and modes coming from Bob's reach the Bell-state projector at the same time, but separately, in the sense that the X mode of Alice (Bob) and the Y mode of Alice (Bob) become synchronous again once they have travelled the OFD twice, but there is still needed that Alice's modes and Bob's modes reach the measurement apparatus at the same time. For that, their paths need to be adjusted to avoid mismatch [15]. Alternatively, if WCPs are used, the pulses generated at the ISG could be delayed such that they return simultaneously. This calibration task is simpler than in a standard configuration as Charlie can perform it without the involvement of Alice or Bob.

A-MDI-QKD system with polarization modes

For the sake of completeness, we describe the polarization encoding scheme. Polarization is perhaps the best known and most used of all possible photonic encodings, and A-MDI schemes involving it have already been proposed [30]. Still, we describe it here for two reasons in addition to the mentioned completeness. The first one is because we do it using a different autocompensating device (a closed cycle with a HWP) to the one used in reference [30] where Faraday mirrors are used. The second, and most important, is because in SM-FMF for space division multiplexing, as for example an elliptical FMFs, spatial modes are separated but polarization modes are close [20]. Therefore in these optical fibers we can use these separated space modes as different channels with two polarization modes to perform QKD. Then, as in the above case, we could use several independent channels to carry out QKD, which would increase the bit rate and thus would reduce the loss effects and larger distances would be achieved in QKD.

The basic scheme of the AD subystem is shown in Fig. 4. A biphoton source or two independent lasers producing WCP is required at Charlie's site, together with decoy states. While the working principle is the same, there will be a number of changes on the optical devices used. Charlie sends the state

$$\left(\frac{|1_H\rangle + |1_V\rangle}{\sqrt{2}}\right)_a \otimes \left(\frac{|1_H\rangle + |1_V\rangle}{\sqrt{2}}\right)_b, \tag{22}$$

where again a stands for Alice's path and b for Bob's path. Note that the formal study is identical to the case of spatial modes X and Y but with the formal changes $X \rightarrow H$ and $Y \rightarrow V$. Therefore, the implementation of the MDI protocol is made in the same way and consequently the results found above can be easily used for polarization. However, the autocompensation process will be different. As in the spatial mode case optical fiber delays are again required.

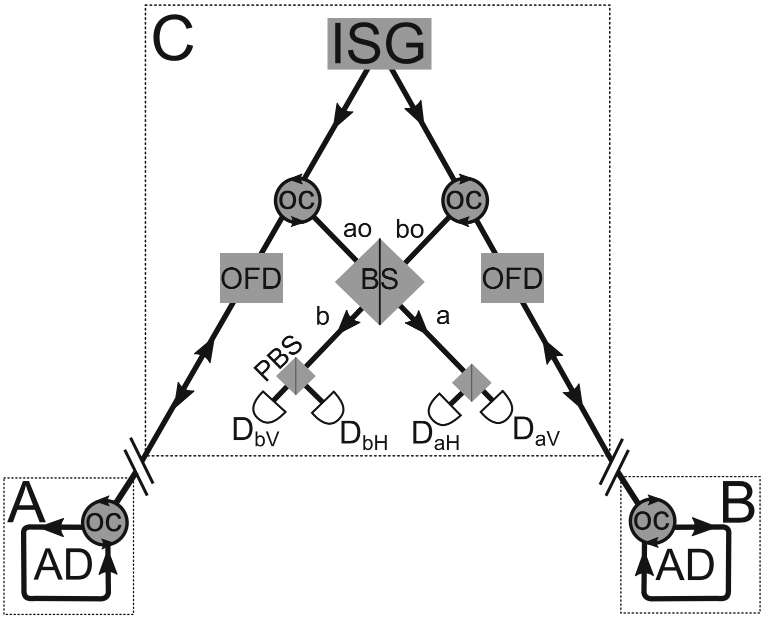

Fig. 4 A-MDI-QKD system for polarization encoding. Charlies generates suitable polarization states and launches them towards Alice and Bob. They autocompensate and modulate the relative phase between the horizontal and vertical components so as to encode their information. Light comes back to Charlie. Circulators redirect it to a polarization Bell-state analyser (Innsbruck scheme)

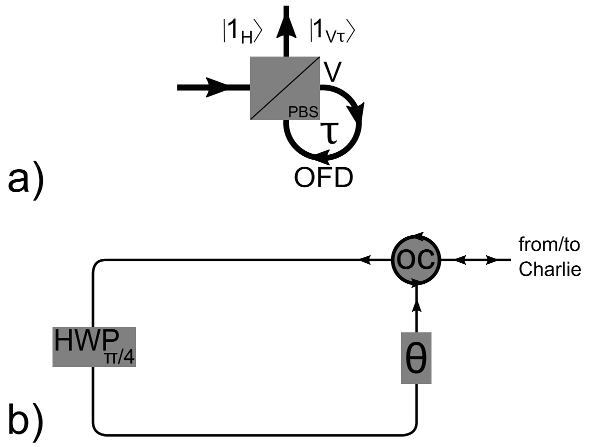

Fig. 5 a Optical Fiber Delay (OFD) by using a PBS. **b** Autocompensating device and phase modulator for polarization encoding: photons coming from Charlie enter the local loops at Alice's and Bob's sites. There, a HWP rotated 45° degrees implement the appropriate autocompensating transformation. Next relative phases are introduced for state generation

This can be implemented for this case with the aid of a PBS [29], as shown in Fig. 5a. As we will see, the autocompensating device again implements a swapping operation required to cancel such delay so that states reach Charlie's Bell-state analyzer at the same time. Light goes towards Alice's and Bob's sites, each one equipped with autocompensating devices. Photons enter optical fiber circuits at Alice and Bob's sites trough optical circulators. By means of electro-optical phase shifters, Alice and Bob encode their bits. As before, Alice and Bob introduce a relative phase θ between $|1_H\rangle$ and $|1_V\rangle$, randomly picked from the set $\theta = \{-\pi/2, 0, \pi/2, \pi\}$, in order to encode information in one of the two MUBs (diagonal or σ_x and circular or σ_y) .

After exiting the optical fiber circuits at Alice and Bob's sites, light returns to Charlie. At Charlie's circulators light is directed towards a linear optics system which implements a Bell-state measurement (Innsbruck scheme). At the beam-splitter BS Bell states are produced. Afterwards, two polarizing beam-splitters (PBS) with their corresponding detectors D$_{aH}$, D$_{aV}$ and D$_{bH}$, D$_{bV}$ project into the individual polarizations. In particular, we obtain the following Bell state for the not bit-flip case

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|1_{aH}1_{aV}\rangle + |1_{bH}1_{bV}\rangle), \tag{23}$$

meaning that there are coincidences in the same output, a or b, that is,there will be a a simultaneous click between the same pair of detectors, either D_{aH} together with D_{aV} or D_{bH} together with D_{bV}. However, for bit-flip cases we obtain

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|1_{aH}1_{bV}\rangle - |1_{bH}1_{aV}\rangle), \tag{24}$$

that is, coincident clicks between D_{aH} and D_{bV} or D_{bH} and D_{aV}, are obtained.

Autocompensation method

We assume that the optical fiber has birefringency perturbations acting on polarization states. Moreover, as commented this perturbation can vary in time, but slowly. Such perturbation can be also represented by the matrix S_k given by Eq. (17). In fact, it is also an asynchronous coupling but with polarization modes coupled by birefringence. However in this case the coupling coefficient between polarization modes is given by

$$\kappa_p = \int e_H(x,y)P(x,y)e_V(x,y)dxdy. \tag{25}$$

Then under backpropagation, that is, by defining a new reference system given, for instance, by $(-X)Y(-Z)$, the original one being given by XYZ, polarization modes must be changed, that is, $H \rightarrow -H$, that is, $e_H(x,y) \rightarrow -e_H(x,y)$, and accordingly the coupling coefficient κ_p changes its sign. The main consequence is that matrices S'_k for backpropagation also change, that is,

$$S'_k = \begin{pmatrix} A_k & -iB_k \\ -iB_k & A^*_k \end{pmatrix}. \tag{26}$$

These results can easily checked by analysing the matrix of particular wave-plate for backpropagation, for instance, a HWP forming an angle γ with respect to the axis X, that is,

$$HWP_\gamma = \begin{pmatrix} -i\cos 2\gamma & -i\sin 2\gamma \\ -i\sin 2\gamma & i\cos 2\gamma \end{pmatrix}, \tag{27}$$

where under backpropagation the angle γ becomes $-\gamma$, therefore $\sin 2\gamma \rightarrow -\sin 2\gamma$ as established by Eq. (26). On the other hand, it is easy to check that autocompensation is achieved by a matrix σ_x, which can be implemented by a HWP rotated $\pi/4$ degrees together with a global phase $e^{i\pi/2}$, that is,

$$M' = e^{i\pi/2}\, HWP_{\pi/4} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{28}$$

therefore, by taking into account the last birefringent perturbation q we have

$$\begin{pmatrix} A_q & -iB_q \\ -iB_q & A^*_q \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A_q & iB_q \\ iB_q & A^*_q \end{pmatrix} = M', \tag{29}$$

and so on, then $S_1 ... S'_q M' S_q ... S_1 = M'$. This means that the state of the emergent light, back at Charlie's circulators, has been properly restored, albeit a deterministic swapping transformation $M' = \sigma_x$, which we can account for. In Fig. 5b the implementation of the autocompensation is shown. It is made by using a HWP$_{\pi/4}$ and an optical circulator to get a closed circuit. The phase shifter θ used to generate quantum states is also shown. In short, if we take a input polarization state $|L\rangle$, after it has traveled back and forth between Charlie and Alice (Charlie and Bob), it emerges as $\sigma_x|L\rangle$, that is, unaltered. The unpredictable changes it would have experienced if it were not for the autocompensating device have been removed. We must note that the usual rectilinear (Z) basis for MDI protocol could not be used for autocompensating purposes because we would have to rotate the state in order to generate different bits, for instance $|1_H\rangle \rightarrow |1_V\rangle$, however, rotations are not autocompensated.

A-MDI-QKD system with codirectional modes

Space division multiplexing can be also implemented by using multicore fibers (MCFs), that is, by using codirectional modes, therefore, we must also consider these optical fibers for QKD. We must stress that there are many configurations of MCFs [31], that is, different groupings of the cores as for example at the vertices of triangle, a square, or even grouping in pairs [32]. These groupings are enough separated to consider that non modal coupling is produced, however, groups of cores can undergo modal coupling and then are processed by MIMO (Multiple-input Multiple-output) technique. The goal of the groups of cores is to enlarge the transmission capacity by increasing the density of cores. In this work we consider grouping in pairs of single-mode cores, and propose a method for autocompensating the modal coupling between the corresponding modes of two cores [32]. Moreover, an integrated device to measure the Bell states is also proposed. We must stress that sometimes the mentioned cores also are far enough apart and therefore only relative phases are compensated, however, the proposed method can also compensate some possible residual coupling, in fact, mechanical and thermal perturbations can induce mode coupling. The matrix describing an arbitrary perturbation $k(=1,...,q)$ is also given by the matrix S_k shown in Eq. (17) where now the modes e_1 and e_2 correspond to the fundamental modes of the single-mode cores. Finally, we must stress that polarization is ignored because it is assumed that due to the proximity between cores the polarization changes are common to both cores, that is, a single photon state can be represented as follows

$$|L\rangle = c_1|1_1\rangle + c_2|1_2\rangle, \quad |1_j\rangle = c_H|1_{jH}\rangle + c_V|1_{jV}\rangle, \tag{30}$$

with $j = 1, 2$. This indicates that the polarization state is the same for both cores. From a classical point of view it means that the total optical field can be factorized as $\boldsymbol{e} = (c_1e_1 + c_2e_2)\boldsymbol{u}$, with $\boldsymbol{u} = (c_H\boldsymbol{u}_H + c_V\boldsymbol{u}_V)$ an unpredectible polarization unitary vector but non relevant to spatial coupling. In short, the autocompensating method consists of implementing once more the matrix $M = i\sigma_y$ used in collinear modes. However, we must stress that unlike of a single-photon QKD we have two photons coming from Alice and Bob, therefore a polarization autocompensating is also required. Such autocompensation will be obtained as indicated in the case of polarization modes, that is, by a HWP rotated $\pi/4$.

On the other hand, the way to encode information obeys the following spatial scheme: if the photon travels path 1 (core 1) that corresponds to bit 0 and if it travels path 2 (core 2) that would correspond to bit 1. The result is that a photon can propagate in a superposition of path 1 and path 2. Note that this corresponds to the usual dual-rail logic. Formally, $|1_1\rangle \rightarrow$ *path* 1 and $|1_2\rangle \rightarrow$ *path* 2. The experimental implementation parallels that of the previous collinear case, as seen in Fig. 6. There are however a number of changes, especially regarding both the autocompensating process and the Bell-state measurement device (BMD), which in this case is implemented by a optical integrated circuit. Now, each state travels its own path, there being two paths for Alice and two paths for Bob. Each path corresponds by the above encoding to a quantum state. If we label Alice's paths by a and Bob's paths by b, we have, for Alice, paths a_1, a_2 and b_1, b_2 for Bob.

In an analogous fashion with respect to the collinear case, Charlie sends a pair of qubits from his ISG, using either a single-photon source or WCPs (decoy states are also required, as usual, for protection against PNS attacks, if WCPs are used). We need to introduce an OFD device in order to introduce a delay between the fundamental states $|1_1\rangle$ and $|1_2\rangle$, for the same reason as before. An example of such a device is shown in Fig. 7. It consists on a pair of photonic lanterns (PL) that extract the modes from the MCF into two parallel SMFs. In one of them, a fiber loop producing a delay τ is located, as in the MZI. Another photonic lantern takes the photons and puts them into the two cores of the MCF again. Therefore, after the OFDs we have the biphoton state

$$\left(\frac{|1_1\rangle + |1_{2\tau}\rangle}{\sqrt{2}}\right)_a \otimes \left(\frac{|1_1\rangle + |1_{2\tau}\rangle}{\sqrt{2}}\right)_b. \tag{31}$$

Light travels along two cores of an MCF to meet Alice's and Bob's laboratories. There, local loops contain autocompensating devices and phase modulators. Optical circulators are also required for the local loops of Alice and Bob and to redirect photons to the Bell-state measurement apparatus. Note that circulators do not mix the paths 1 and 2. Although we draw only one circulator, a pair of circulators each one operating in one path is to be understood.

Bell-state measurement device

Finally, the light that returns to Charlie is directed to a Bell-state measurement device. In this case, such device will be an integrated optical circuit. It is shown in Fig. 8. It is a four-port device; its input fed with the emerging light that comes back to Charlie from Alice's and Bob's sites. Synchronous directional couplers (DC) and phase shifters (PS) implement the required transformations. Finally, at

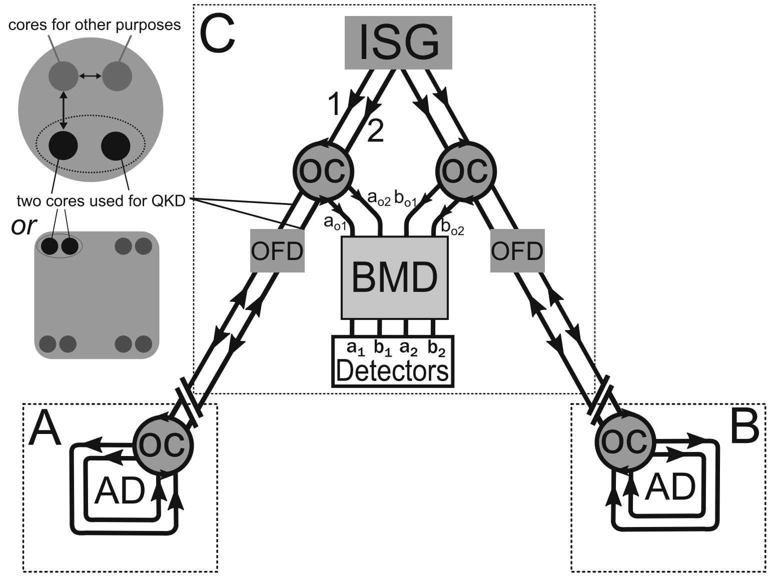

Fig. 6 A-MDI-QKD system for codirectional modes. Charlie uses his quantum state generator to send a pair of qubits to each Alice and Bob. After the delays, photons reach the local loops; in them, autocompensating devices and phase modulators are located. Afterwards, light returns to Charlie's six-port OCs, which direct the light towards a optical integrated circuit working as a Bell-state measurement apparatus. We made apparent the fact that we are using codirectional modes by explicitly showing the two paths of the photons, to be understood as two cores of a MCF as shown, although the representation of the system is somewhat schematic

the end of each port, a detector is located. The result is a integrated device that is totally analogous to an Innsbruck scheme but on a spatial encoding. Recall that a general synchronous directional coupler implements the following transformation

$$D(\alpha) = \begin{pmatrix} \cos\alpha & i\sin\alpha \\ i\sin\alpha & \cos\alpha \end{pmatrix}. \tag{32}$$

The value of $\alpha = \kappa L$ can be tailored to our choice according to the value of the coupling coefficient κ and the coupling length L. In this case, the integrated device requires the use of $D(\pi/4)$ and $D(\pi/2)$ couplers, along with a pair of $\phi = -\pi/2$ phase shifters.

A first $D(\pi/2)$ coupler is required; it couples inputs $\hat{a}_{o2}$ and $\hat{b}_{o1}$. Next, two $D(\pi/4)$ couplers are needed. They couple, respectively, inputs a_{o1} and b_{o2} to intermediate outputs a'_2 and b'_1, respectively. In terms of the photonic absorption operators, the implemented transformations are

$$a_{a'2} = \hat{a}_{ao1}; \quad a_{a'1} = \hat{a}_{ao2},$$

$$a^{\dagger}_{ao1} = \frac{\hat{a}^{\dagger}_{a1} + i\hat{a}^{\dagger}_{b1}}{\sqrt{2}}; \quad \hat{a}^{\dagger}_{a'2} = \frac{i\hat{a}^{\dagger}_{a1} + \hat{a}^{\dagger}_{b1}}{\sqrt{2}}, \tag{33}$$

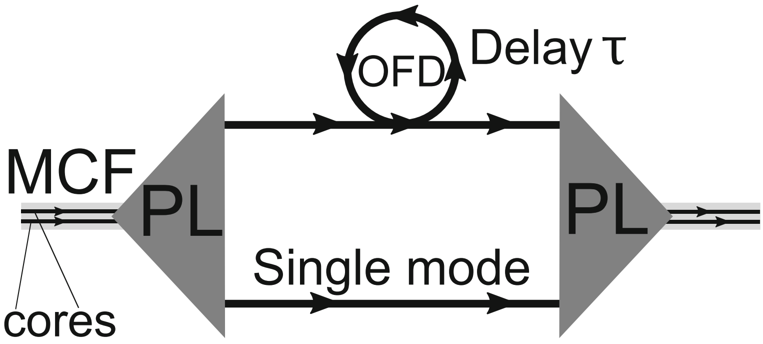

Fig. 7 OFD device for codirectional modes. Light comes from the two cores of a MCF and is directed, via, for example, photonic lanterns, to a pair of parallel single-mode fibers. In one of them, an optic fiber delay is placed, introducing a delay τ in one of the modes. Photons exit the SMFs through another PL and they are introduced back into the cores of an MCF

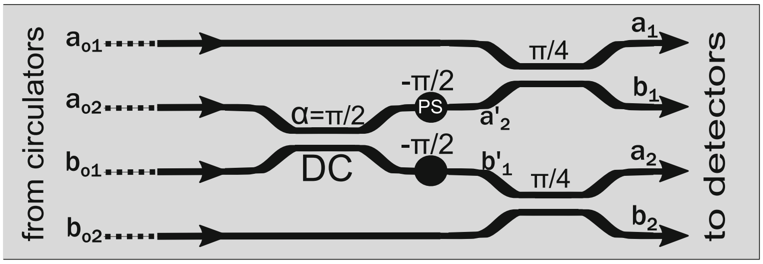

Fig. 8 Bell-state measurement device for codirectional modes. A four port optical integrated circuit serves as a Bell-state measurement device for codirectional modes. Photons coming from Charlie's OC enter the device, where three DCs and two phase shifters implement the suitable operations. When light reaches the detectors the Bell states $|\Psi^-\rangle$ and $|\Phi^+\rangle$ are unambiguously identified, as required by MDI-QKD

$$\hat{a}^\dagger_{b'1} = \frac{\hat{a}^\dagger_{a2} + i\hat{a}^\dagger_{b2}}{\sqrt{2}}; \quad \hat{a}^\dagger_{bo2} = \frac{i\hat{a}^\dagger_{a2} + \hat{a}^\dagger_{b2}}{\sqrt{2}}.$$

As in the previous cases, we will need suitable bases for autocompensation purposes. Therefore, we shall use the following two MUBs

$$\mathcal{B}_D : \left\{ |1_D\rangle = \frac{|1_1\rangle + |1_2\rangle}{\sqrt{2}}, |1_A\rangle = \frac{|1_1\rangle - |1_2\rangle}{\sqrt{2}} \right\}, \quad (34)$$

$$\mathcal{B}_C : \left\{ |1_L\rangle = \frac{|1_1\rangle + i|1_2\rangle}{\sqrt{2}}, |1_R\rangle = \frac{|1_1\rangle - i|1_2\rangle}{\sqrt{2}} \right\}. \quad (35)$$

Moreover, the transformation between absorption operators $\hat{a}$ in both bases is given by

$$\hat{a}_{\binom{D}{A}} = \frac{1}{\sqrt{2}} \left(\hat{a}_1 \pm \hat{a}_2\right); \quad \hat{a}_{\binom{L}{R}} = \frac{1}{\sqrt{2}} \left(\hat{a}_1 \mp i\hat{a}_2\right). \quad (36)$$

Let us assume, for instance, that Alice and Bob prepare the input state $|L_{nf}\rangle = |1_{aoD}1_{boD}\rangle = a^\dagger_{aoD}a^\dagger_{voD}|00\rangle$, then by taking into account Eq. (36) we obtain the state

$$\frac{1}{2}\{|1_{ao1}1_{bo1}\rangle + |1_{ao1}1_{bo2}\rangle + |1_{ao2}1_{bo1}\rangle + |1_{ao2}1_{bo2}\rangle\}. \quad (37)$$

With this in hand, together with the transformations in Eq. (33), we can make a Bell-state analysis of the device in Fig. 8. Thus, after a long but straightforward calculation, we will find that the output state is a superposition of states which do not produce coincidences and states producing coincidences, that is, $|L\rangle = |L_{nc}\rangle + |L_c\rangle$, with

$$|L_{nc}\rangle = i\frac{\sqrt{2}}{4}(|2_{a1}\rangle + |2_{b1}\rangle + |2_{a2}\rangle + |2_{b1}\rangle), \quad (38)$$

$$|L_c\rangle = \frac{i}{2}(|1_{a1}1_{a2}\rangle + |1_{b1}1_{b2}\rangle) \equiv i\frac{\sqrt{2}}{2}|\Phi^+\rangle. \quad (39)$$

Now, let us assume that Alice and Bob send back to Charlie orthogonal states but in the same (diagonal basis), i.e the input state is

$$|L_f\rangle = a^\dagger_{aoD}a^\dagger_{boA}|00\rangle. \quad (40)$$

In this case, by identical procedure, we will obtain number states $|2\rangle$ and the following Bell state $|\Psi^-\rangle$, with probability 1/2:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|1_{b1}1_{a2}\rangle - |1_{a1}1_{b2}\rangle). \quad (41)$$

Thus, the optical integrated circuit we propose works as a Bell-state analyser, as it should, and therefore the MDI protocol can be implemented. Next, we present the autocompensating method.

Autocompensating method

As in the collinear case, unpredictable coupling between modes of adjacent cores of an MCF results in a series of perturbations S_k, each which can be characterized again as a SU(2) matrix with the same form as Eq. (17). It represents, again, the perturbation associated to a short length, in the z-direction, of the core the photons travel along. The total matrix is again given by $S = S_qS_{q-1}...S_2S_1$. Importantly, these matrices have the same symmetries as the ones of collinear modes. Consequently, we need to find a way to implement the transformation $M = i\sigma_y$ on codirectional modes, so that we obtain $S_kMS_k = M$ for each perturbation k. There are a number of ways to implement such transformation. Here, we choose a simple one, consisting of a directional coupler together with phase shifter introducing a phase π, placed in a closed circuit, as shown in Fig. 9. Specifically, for the DC, we set $\alpha = \pi/2$, so from Eq. (32) we obtain

$$D(\kappa) = i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (42)$$

Next, place a π phase shifter on the path 2 and thus we obtain the transformation

$$U(\pi)D(\pi/2) = i\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad (43)$$

which is just what we wanted, up to a harmless global phase $\pi/2$. Note that the DC implements a swapping operation. This means that it exchanges the physical modes (not their identity), in the sense that the retarded mode will now follow the path which has no delay, and the

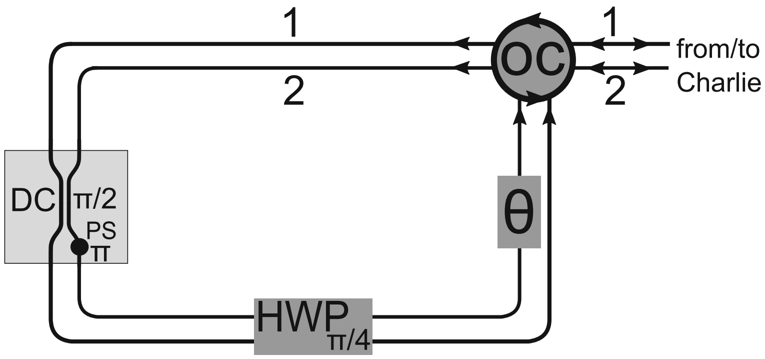

Fig. 9 Autocompensating devices for codirectional modes and phase modulators. Light enters local loops through OCs. In the local loops, a DC with $\kappa L = \pi/2$ plus a phase shifter introducing a phase π, for instance, in path 2. A HWP rotated $\pi/4$ is placed for polarization autocompensation. Afterwards, a phase modulator is placed, so as to introduce the phase θ and generate quantum states in order for Alice and Bob to encode their bits

advanced mode will be delayed. Thus, modes reach Charlie's Bell-state measurement apparatus at the same time and autocompensation is achieved. This is analogous to what happened in the collinear case.

Finally, a HWP is also included to autocompensate polarization because the perturbations in the optical fiber linking Alice & Charlie and the optical fiber linking Bob & Charlie will be different. Obviously, we can take advantage of this autocompensating polarization technique to use two different QKD channels, that is, collinear modes in H and V polarizations (channels), and therefore doubling the bit rate. We only need to separate the polarization channels (by using, for instance, PBSs) and to place two BMDs in the A-MDI-QKD system.

Secret key rate analysis

We shall now perform a secret key rate analysis by presenting a simulation of the impact on the key rate R when perturbations (cross-talk and phase shifting) are considered in the optical link and a comparison with the autocompensated case is shown. We consider cross-talk between modes of multicore optical fibers. This is a very interesting case [3–6] because, among other reasons, the use of this optical link avoids the requirement of alignment between the Alice and Bob bases, which is needed with both collinear modes and polarization modes, in order to avoid misalignment errors that reduce the secure key rates. Moreover, simulation will be made with optical perturbations modelized by a generalized optical error function $E_{opt}(L)$, where L is the propagation distance. We start by recalling that the expression of the lower bound of the key rate R of a MDI-QKD protocol, in the case of an infinitely long key and involving the use of decoy states, is given by [12, 33]

$$R \geq Q_{11}^{R}\left[1 - H\left(e_{11}^{D}\right)\right] - Q_{\mu_a\mu_b}^{R} f H\left(E_{\mu_a\mu_b}^{R}\right). \qquad (44)$$

Here, Q_{11}^{R} is the single-photon gain in the rectilinear (R) or Z basis, $\mathcal{B}_R = \{|1_1\rangle, |1_2\rangle\}$; e_{11}^{D} is the single-photon bit error in the diagonal or X basis $\mathcal{B}_D$; $Q_{\mu_a\mu_b}^{R}$ and $E_{\mu_a\mu_b}^{R}$ are, respectively, the total gain and total error rate in the rectilinear basis when signal WCP states of mean photon number μ_a and μ_b are sent by Alice and Bob, respectively; f is the error correction inefficiency and H is the binary Shannon entropy function, given by $H(a) = -a\log_2(a) - (1-a)\log_2(1-a)$. It is assumed that the WCPs are phase randomized.

Note that for our protocol, because it implements autocompensation, we need to encode the states in the diagonal and circular bases $\mathcal{B}_D$ and $\mathcal{B}_C$, respectively. However, the above key rate formula involves terms in the rectilinear and diagonal bases. We can use this equation, nonetheless, if we change the basis just before detection. This is, we encode in the diagonal and circular bases but we detect in the rectilinear and diagonal bases, thus Eq. (44) is still valid in our setting. The final expression of the key rate is general, and can be used in our case without modification. In fact, our experimental setting is similar to that of [33]. To change from the $\mathcal{B}_D$ and $\mathcal{B}_C$ bases to $\mathcal{B}_D$ and $\mathcal{B}_R$ we can use a simple 3dB synchronous directional coupler, putting $\alpha = \pi/4$ in Eq. (32), so that we obtain, up to global phases, the following map: $D(\pi/4)|1_L\rangle \rightarrow |1_1\rangle$; $D(\pi/4)|1_R\rangle \rightarrow |1_2\rangle$; $D(\pi/4)|1_D\rangle \rightarrow |1_D\rangle$; $D(\pi/4)|1_A\rangle \rightarrow |1_A\rangle$. We must stress that the detection devices already presented remain unchanged.

The multi-photon terms in the key rate formula are given by [33]

$$Q_{\mu_a\mu_b}^{R} = Q_C + Q_E, \qquad (45)$$

$$E_{\mu_a\mu_b}^{R} = \frac{e_{opt}Q_C + (1 - e_{opt})Q_E}{Q_{\mu_a\mu_b}^{R}}, \qquad (46)$$

where Q_C and Q_E are given by the following expressions

$$Q_C = 2(1-P_d)^2 e^{-\mu'/2}\left[1-(1-P_d)e^{-\eta_a\mu_a/2}\right] \times\left[1-(1-P_d)e^{-\eta_b\mu_b/2}\right], \quad (47)$$

$$Q_E = 2P_d(1-P_d)^2 e^{-\mu'/2}\left[I_0(2\xi)-(1-P_d)e^{-\mu'/2}\right], \quad (48)$$

with P_d the dark count rate of an individual detector ($Y_0/2$, Y_0 the background yield); $\mu' = \eta_a\mu_a + \eta_b\mu_b$, with η_a and η_b the transmission efficiency of Alice and Bob's channels, which we set equal $\eta_a = \eta_b$ (symmetric scenario). This is given, in turn, by, $\eta_{a,b} = 10^{-\alpha_{att}L/10}\eta_d\eta_C$, where α_{att} is the attenuation of the fiber link measured in dB/km, L the length of the fiber link (Alice/Bob to Charlie) and η_d and η_C are the detector's efficiency and internal transmittance of Charlie's devices, respectively. Moreover, ξ is given by $\xi = \sqrt{\mu_a\mu_b\eta_a\eta_b}/2$ and $I_0(\xi)$ is the modified Bessel function of the first kind. Finally, e_{opt} in Eq. (46) is the so-called optical misalignment-error probability [15, 33]. Importantly, it is the error to be modified when optical perturbations are considered along the optical fiber.

On the other hand, in a practical situation, with a finite number of decoy states, Q^R_{11} and e^D_{11} in Eq. (44) need to be estimated from the total gains and error rates. In that case, a good estimation is provided by a decoy setting employing a signal state, a weak decoy and a vacuum. For that, we use the bounds for $Q^R_{11} = \mu_a\mu_b e^{-\mu_a\mu_b}Y^R_{11}$ and e^D_{11} obtained by [34]. First of all, we need to reproduce the total gains and errors in the diagonal basis, from [33], that is,

$$Q^D_{\mu_a\mu_b} = 2\gamma^2\left[1+2\gamma^2-4\gamma I_0(\xi)+I_0(2\xi)\right], \quad (49)$$

$$Q^D_{\mu_a\mu_b}E^D_{\mu_a\mu_b} = e_0 Q^D_{\mu_a\mu_b} - 2(e_0-e_{opt})\gamma^2\left[I_0(2\xi)-1\right], \quad (50)$$

where $\gamma = (1-P_d)^{-\mu'/4}$ and $e_0 = 1/2$ is the dark count error, that is, the random dark count in a detector which is not expected to fire. Equations (45) to (50) can be particularized for any intensity setting by simply substituting the intensities' values. Now, say that Alice sends a signal state μ_a, a weak decoy ν_a and a vacuum. Bob sends μ_b, ν_b and a vacuum. Following [34], define $m = \min(a,b,c)$, where

$$\begin{aligned} a &= \frac{\mu_a\mu_b^2-\nu_a\nu_b^2}{\mu_a\nu_b^2+\nu_a\mu_b^2}, \\ b &= \frac{\mu_a^2\mu_b-\nu_a^2\nu_b}{\mu_a^2\nu_b+\nu_a^2\mu_b}, \\ c &= \frac{\mu_a^2\mu_b^2-\nu_a^2\nu_b^2}{\mu_a^2\nu_b^2+\nu_a^2\mu_b^2}. \end{aligned} \quad (51)$$

Furthermore, with $\beta = \{R,D\}$, the following parameters are defined

$$\begin{aligned} g_1^\beta &= e^{\mu_b}Q^\beta_{0\mu_b} + e^{\mu_a}Q^\beta_{\mu_a 0} - e^{\nu_b}Q^\beta_{0\nu_b} - e^{\nu_a}Q^\beta_{\nu_a 0}, \\ g_2^\beta &= m\left(e^{\mu_a+\nu_b}Q^\beta_{\mu_a\nu_b} - e^{\nu_b}Q^\beta_{0\nu_b} - e^{\mu_a}Q^\beta_{\mu_a 0} + Q^\beta_{00}\right), \\ g_3^\beta &= m\left(e^{\nu_a+\mu_b}Q^\beta_{\nu_a\mu_b} - e^{\mu_b}Q^\beta_{0\mu_b} - e^{\nu_a}Q^\beta_{\nu_a 0} + Q^\beta_{00}\right), \\ g_4^\beta &= e^{\nu_b}Q^\beta_{0\nu_b}E^\beta_{0\nu_b} + e^{\nu_a}Q^\beta_{\nu_a 0}E^\beta_{\nu_a 0} - Q^\beta_{00}E^\beta_{00}. \end{aligned} \quad (52)$$

With these in hand, the lower bound of Y^β_{11} and upper bound of e^β_{11} are given by [34]

$$Y^\beta_{11} \geq \frac{g_1^\beta + g_2^\beta + g_3^\beta - e^{\mu_a+\mu_b}Q^\beta_{\mu_a\mu_b} + e^{\nu_a+\nu_b}Q^\beta_{\nu_a\nu_b}}{\nu_a\nu_b - \mu_a\mu_b + m\mu_a\nu_b + m\nu_a\mu_b}, \quad (53)$$

$$e^\beta_{11} \leq \frac{e^{\nu_a+\nu_b}Q^\beta_{\nu_a\nu_b}E^\beta_{\nu_a\nu_b} - g_4^\beta}{\nu_a\nu_b Y^\beta_{11}}. \quad (54)$$

Next, by particularizing for $\beta = R$ in Y^β_{11} and for $\beta = D$ in e^β_{11} one can obtain the remaining parameters of Eq. (44).

As commented above, in order to take into account the perturbations on the fiber producing undesired coupling (cross-talk) we present the following model for the optical error, already introduced in [35] for a high-dimensional QKD analog of the BB84 protocol. The expression of the optical error is modelled as follows

$$e_{opt} \rightarrow E_{opt} = e_{opt} + \left(\frac{1}{2} - e_{opt}\right)\left(1 - e^{-\alpha_{opt}L}\right), \quad (55)$$

where α_{opt} is the perturbation coefficient along the fiber. Note that this error increases monotonically with L and it is reduced to e_{opt} when $\alpha_{opt} = 0$, and it goes to 1/2 for $\alpha_{opt} \gg 1$, that is, for large perturbations all states have the same probability 1/2 to be detected (two states in each base) and therefore the error will be also equal to 1/2 as it also occurs for e_0. In short, E_{opt} generalizes the misalignment error e_{opt} above.

To perform a numerical simulation of the key rate, given by Eq. (44), we use the equations above, substituting e_{opt} by E_{opt}, for a series of realistic values of α_{opt}, including $\alpha_{opt} = 0$, which is the case when the perturbations have been successfully autocompensated. Thus, we will use values of α_{opt} in the interval $(0.5 \cdot 10^{-3}, 2 \cdot 10^{-3})$ which are compatible with those ones found in the technical literature about modal cross-talking due to perturbations in optical fibers. For instance, for $\alpha_{opt} = 2 \cdot 10^{-3}\text{km}^{-1}$ we obtain an optical error about $1.0 \cdot 10^{-3}$ which corresponds approximately to -28 dB. This value is a realistic one because both spatial and polarization mode cross-talking in optical fibers can take values around -30 dB or even larger [36, 37]. In short, cross-talking provides an

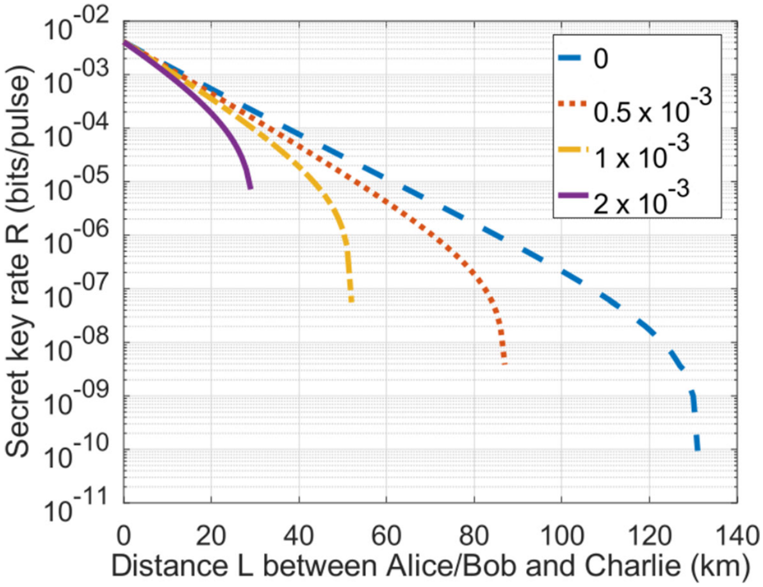

Fig. 10 Secure key rate vs fiber length for different values of α_{opt}. We set $\alpha_{opt} = \{0, 0.5, 1, 2\} \cdot 10^{-3} km^{-1}$. Regarding the other parameters, the following values have been used: $f = 1.16$, $P_d = 3.01 \cdot 10^{-6}$, $e_{opt} = 1.5\%$, $\eta_d = 93\%$, $\eta_C = 0.5$, $\alpha_{att} = 0.2$ dB/km, $\mu_a = \mu_b = 0.36$ and $\nu_a = \nu_b = 0.001$

estimation of errors due to the loss of information (bits) carried by an optical mode.

As one can see in Fig. 10, the range at which we can transmit secure information depends critically on the value of α_{opt}. The values for the parameters used in the simulation were taken across the relevant literature [15, 30, 33, 34] and are detailed in Fig. 10. Moreover, we have imposed the optimal conditions $\mu_a\eta_a = \mu_b\eta_b$ and $\nu_a = \nu_b$ [15, 33]. The results under full autocompensation gives a secure key rate up to a distance about 130 km between Alice (Bob) and Charlie, therefore 260 km between Alice and Bob. If we consider a perturbation coefficient of $\alpha_{opt} = 0.5 \cdot 10^{-3}$ a reduction of 38% in such a distance is obtained, that is, a secure key rate distance about 160 km between Alice and Bob. In the case $\alpha_{opt} = 2.0 \cdot 10^{-3}$ a dramatic reduction of the secure key rate distance is obtained. Therefore, these results show that the optical perturbations in the links for MDI protocol are an important source of errors what contributes to a remarkable reduction of the secure key rate distance, which is more important than in the case of protocols based on a single photon, like, for example, the BB84 one [35].

Conclusions

We have shown how to implement a A-MDI-QKD protocol in different settings according to the kind of optical fiber used for space division multiplexing, that is, few-mode optical fibers maintaining polarization modes (PM-FMF) or maintaining space modes (SM-FMF) and MCFs. In particular, we have proposed three systems for A-MDI-QKD by using collinear, polarizations and codirectional modes. Discrete and/or integrated components have been used for both measuring Bell states and achieving autocompensation. As such fibers are assumed to be the links of present and near-future optical networks, then implementation of QKD in them and in a plug-and-play fashion would offer clear practical benefits, as for example, to use several channels for MDI-QKD what would in turn compensate the losses and therefore increase the bit rate. Finally, simulations of secret key rates with perturbations in the link has been made what has shown that a remarkable reduction of secret key rate distances is obtained if an autocompensating method is not used. Simulations have been made for codirectional modes (MCFs) because they have the advantage that no alignment of quantum states bases is required, but the results can be easily extended to polarization and collinear modes (FMFs).

Abbreviations

QKD: Quantum Key Distribution; MDI-QKD: Measurement-Device-Independent Quantum Key Distribution; MCF: Multicore Optical Fiber; FMF: Few-Mode Fiber; A-MDI-QKD: Autocompensating Measurement-Device-Independent Quantum Key Distribution; HG: Hermite-Gauss; PM-FMF: Polarization-Maintaining Few Mode Fibers; SP-SMF: Space-Maintaining Single Mode Fiber; SPDC: Spontaneous Parametric Down-Conversion; WCP: Weak Coherent Pulses; PNS: Photon Number Splitting; ISG: Initial States Generation; OC: Optical Circulators; OFD: Optical Fiber Delay; MZI: Mach-Zehnder Interferometer; DP: Dove Prism; BS: Beam Splitter; PBS: Polarizing Beam Splitter; CLC: Cylindrical Lens Converter; DC: Directional Coupler; HWP: Half-Wave Plate; PS: Phase Shifter; BMD: Bell-state Measurement Device; MIMO: Multiple-input Multiple-output

Acknowledgements
We acknowledge the helpful supervision of Dr. E.F. Mateo (NEC Corporation, Tokyo) on the transmission properties of optical fibers in the numerical simulations.

Authors' contributions
JL and XP-B conceived the presented idea. All authors developed the methodology, discussed the results, wrote the paper, and read and approved the final manuscript.

Funding
Financial support by Xunta de Galicia, Consellería de Educación, Universidades e FP, through a grant Consolidation-GRC Ref.-ED431C2018/11, and two predoctoral grants (D. Balado, 2017 and G. Carral, 2020), both co-financed by the European Social Fund.

Availability of data and materials
Data is contained within the article.

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 2 January 2021 Accepted: 18 August 2021
Published online: 09 September 2021

References

1. Bai, N., Ip, E., Huang, Y.-K., Mateo, E., Yaman, F., Li, M.-J., Bickham, S., Ten, S., Liñares, J., Montero, C., Moreno, V., Prieto, X., Tse, V., Chung, K. M., Lau, A. P. T., Tam, H.-Y., Lu, C., Luo, Y., Peng, G.-D., Li, G., Wang, T.: Mode-division multiplexed transmission with inline few-mode fiber amplifier. Opt. Express. **20**(3), 2668–2680 (2012)
2. Saitoh, K., Matsuo, S.: Multicore fiber technology. J. Lightwave Tech. **34**, 55–66 (2016)
3. Cañas, G., Vera, N., Cariñe, J., González, P., Cardenas, J., Connolly, P. W. R., Przysiezna, A., Gómez, E. S., Figueroa, M., Vallone, G., Villoresi, P., da Silva, T. F., Xavier, G. B., Lima, G.: High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers. Phys. Rev. A. **96**, 022317 (2017). https://doi.org/10.1103/PhysRevA.96.022317
4. Ding, Y., Bacco, D., Dalgaard, K., Cai, X., Zhou, X., Rottwitt, K., Oxenløwe, L. K.: High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. NPJ Quantum Inf. **3**, 25 (2017)
5. Bacco, D., Da Lio, B., Cozzolino, D., Da Ros, F., Guo, X., Ding, Y., Sasaki, Y., Aikawa, K., Miki, S., Terai, H., Yamashita, T., Neergaard-Nielsen, J. S., Galili, M., Rottwitt, K., Andersen, U. L., Morioka, T., Oxenløwe, L. K.: Boosting the secret key rate in a shared quantum and classical fibre communication system. Commun. Phys. **2**, 140 (2019)
6. Xavier, G. B., Lima, G.: Quantum information processing with space-division multiplexing optical fibres. Commun. Phys. **3**, 140 (2020)
7. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145–195 (2002)
8. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., Wallden, P.: Advances in Quantum Cryptography (2019). http://arxiv.org/abs/1906.01645
9. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C., Lo, H.-K.: Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. Phys. Rev. A. **78**, 042333 (2008)
10. Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., Makarov, V.: Hacking commercial quantum cryptography systems by tailored bright illumination. Nat. Photonics. **4**(10), 686–689 (2010)
11. Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., Makarov, V.: Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nat. Commun. **2**, 349 (2011). https://doi.org/10.1038/ncomms1348
12. Lo, H.-K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)
13. Hwang, W.-Y.: Quantum key distribution with high loss: Toward global secure communication. Phys. Rev. Lett. **91**, 057901 (2003)
14. Dellantonio, L., Sørensen, A. S., Bacco, D.: High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces. Phys. Rev. A. **98**, 062301 (2018). https://doi.org/10.1103/PhysRevA.98.062301
15. Xu, F., Curty, M., Qi, B., Lo, H.-K.: Practical aspects of measurement-device-independent quantum key distribution. New J. Phys. **15**(11), 113007 (2013)
16. Yan, H., Li, S., Xie, Z., Zheng, X., Zhang, H., Zhou, B.: Design of panda ring-core fiber with 10 polarization-maintaining modes. Photon. Res. **5**, 1–5 (2017)
17. Bethune, D. S., Risk, W. P.: Autocompensating quantum cryptography. New J. Phys. **4**, 42–42 (2002)
18. Balado, D., Liñares, J., Prieto-Blanco, X., Barral, D.: Phase and polarization autocompensating ℵ-dimensional quantum cryptography in multicore optical fibers. JOSA B. **34**, 2793–2803 (2019)
19. Hu, X.-M., Xing, W.-B., Liu, B.-H., He, D.-Y., Cao, H., Guo, Y., Zhang, C., Zhang, H., Huang, Y.-F., Li, C.-F., Guo, G.-C.: Efficient distribution of high-dimensional entanglement through 11 km fiber. Optica. **7**, 738–743 (2020)
20. Ip, E., Milione, G., Li, M.-J., Cvijetic, N., Kanonakis, K., Stone, J., Peng, G., Prieto, X., Montero, C., Moreno, V., Liñares, J.: SDM transmission of real-time 10GbE traffic using commercial SFP + transceivers over 0.5km elliptical-core few-mode fiber. Opt. Express. **23**, 240421 (2015)
21. Muller, A., Herzog, T., Huttner, B., Tittel, W., Zbinden, H., Gisin, N.: "Plug and play" systems for quantum cryptography. Appl. Phys. Lett. **70**(7), 793–795 (1997)
22. Sibson, P., Kennard, J. E., Stanisic, S., Erven, C., O'Brien, J. L., Thompson, M. G.: Integrated silicon photonics for high-speed quantum key distribution. Optica. **4**(2), 172–177 (2017)
23. Dynes, J. F., Kindness, S. J., Tam, S. W.-B., Plews, A., Sharpe, A. W., Lucamarini, M., Fröhlich, B., Yuan, Z. L., Penty, R. V., Shields, A. J.: Quantum key distribution over multicore fiber. Opt. Express. **24**(8), 8081–8087 (2016)
24. Bacco, D., Ding, Y., Dalgaard, K., Rottwitt, K., Oxenløwe, L. K.: Space division multiplexing chip-to-chip quantum key distribution. Sci. Rep. **7**, 12459 (2017)
25. Riesen, N., Gross, S., Love, J. D., Sasaki, Y., Withford, M. J.: Monolithic mode-selective few-mode multicore fiber multiplexers. Sci. Rep. **7**, 69711 (2017)
26. Labroille, G., Barré, N., Pinel, O., Denolle, B., Lenglé, K., Garcia, L., Jaffrès, L., Jian, P., Morizur, J.-F.: Characterization and applications of spatial mode multiplexers based on multi-plane light conversion. Opt. Fiber Technol. **35**, 93–99 (2017)
27. Liñares, J., Nistal, M. C., Barral, D.: Quantization of coupled 1d vector modes in integrated photonic waveguides. New J. Phys. **10**(6), 063023 (2008). https://doi.org/10.1088/1367-2630/10/6/063023
28. Beijersbergen, M. W., Allen, L., van der Veen, H. E. L. O., Woerdman, J. P.: Astigmatic laser mode converters and transfer of orbital angular momentum. Opt. Commun. **96**, 123–132 (1993)
29. Balado-Souto, D., Liñares, J., Prieto-Blanco, X.: Phase auto-compensating high-dimensional quantum cryptography in elliptical-core few-mode fibres. J. Mod. Opt. **66**, 947–957 (2019)
30. Hu, M., Zhang, L., Guo, B., Li, J.: Polarization-based plug-and-play measurement-device-independent quantum key distribution. Opt. Quant. Electron. **51**(1), 22 (2019)
31. Hayashi, T., Nakanishi, T.: Multi-core optical fibers for the next-generation communications. SEI Tech. Rev. **86**, 23–28 (2018)
32. Sakamoto, T., Mori, T., Wada, M., Yamamoto, T., Yamamoto, F., Nakajima, K.: Strongly-coupled multi-core fiber and its optical characteristics for mimo transmission systems. Opt. Fiber Technol. **35**, 8–18 (2016)
33. Ma, X., Razavi, M.: Alternative schemes for measurement-device-independent quantum key distribution. Phys. Rev. A. **86**, 062319 (2012)
34. Sun, S.-H., Gao, M., Li, C.-Y., Liang, L.-M.: Practical decoy-state measurement-device-independent quantum key distribution. Phys. Rev. A. **87**, 052329 (2013)
35. Liñares, J., Prieto-Blanco, X., Balado, D., Carral, G. M.: Fully autocompensating high-dimensional quantum cryptography by quantum degenerate four-wave mixing. Phys. Rev. A. **103**, 043710 (2021)
36. Zhu, L., Liu, J., Mo, Q., Du, C., Wang, J.: Encoding/decoding using superpositions of spatial modes for image transfer in km-scale few-mode fiber. Opt. Express. **24**, 16934 (2016)

37. Wang, Z., Hu, X., Lin, M., Mo, Q., Wen, H., Li, G.: Measurements of polarization crosstalk in a polarization-maintaning few-mode optical fiber. Conf. Lasers Electro-Opt. **24**, 2–70 (2017)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.