Multichannel Hybrid Quantum Cryptography for Submarine Optical Communications

JESÚS LIÑARES,[1] XESÚS PRIETO-BLANCO,[1,*], ALEXANDRE VÁZQUEZ-MARTÍNEZ,[1] AND EDUARDO F. MATEO,[2]

[1] *Optics Area. Applied Physics Department. QMatterPhotonics Research Group and iMATUS Institute. Campus Vida. Universidade de Santiago de Compostela, E-15782 Santiago de Compostela, Galicia, Spain*
[2] *Nippon Electric Company (NEC). Minato-ku. Tokyo. Japan*
[*] *xesus.prieto.blanco@usc.es*

Abstract: We present a multichannel hybrid quantum cryptography approach intended for submarine quantum optical communications between Alice and Bob separated a distance beyond the current QKD possibilities, each located on a coastline. It is based on the difficult of a simultaneous access to M optical submarine channels. The optical lines from the coastline and ideally to the end of the continental platform are governed by the quantum properties of the light under an autocompensating high-dimensional discrete-modulation continuous variable QKD protocol. The hybrid approach consists of combining several secret keys of the M channels and introducing extra layers of security, passive and/or active, on the non quantum optical lines located beyond the continental platform.

1. Introduction

The development of quantum optical communications is a major challenge before the inminence of quantum supremacy. Indeed, the security and confidentiality of communications is nowadays implemented by encryption methods that rely on mathematical problems that are computationally prohibitive to decrypt. However, these problems (such as factorization or large primes) can be easily solved by quantum computers. This threat to security can be solved by utilizing Quantum Key Distribution (QKD) [1]. QKD lines uses unique statistical features of quantum states which reveal, unconditionally, the presence of an eavesdropper. Usually these lines are terrestrial ones with optical fibres or free space lines which have a determined level of security and a secret key rates which decrease abruptly from a determined transmission distance. Secure distances about a few hundred of kilometres can be obtained. Practical optical networks require many access points to monitor the performance and integrity of the transmission links. QKD provides the means to stablish secure communications in such fibre plants, where an eavesdropper can easily access the data. One of the limitations of QKD is the incompatibility with optical amplifiers, which limits the transmission length of the key [2]. For that, complex topologies of secure-nodes are proposed to regenerate the cryptographic keys [3]. Although such secure-nodes do not provide unconditional security and require access ports for maintenance and monitoring, they are an acceptable approach for long-distance QKD in practical optical networks while new technologies such the quantum repeaters are not available.

On the other hand, submarine networks deliver 98% of transcontinental traffic and they are, in nature, very well protected against eavesdropping with respect to terrestrial or satellite communications. First, both fibre and amplifiers are inaccessible from the outside as they are tightly encapsulated in cables and housings supporting water depths up to 8000m. Additionally, submarine networks are heavily electrified since they are powered from the landing stations, often withstanding voltages up to 18kV. In deep waters, submarine systems are protected by kilometres of water pressure whereas in shallow waters, submarine cables and repeaters are typically armored with thick steel sections and buried 3-10m deep in the seafloor in paths where the water-depth is below 1000m. Inside the cable, fibre-independence is guaranteed by the submarine system supplier. On top of this natural protection, sensing techniques such as DAS are being proposed to detect vibrations and potential damages or attacks to the cable [4], and other types physical layer security methods could be used to maximize protection [5].

In this work we propose a hybrid approach that enables the distribution of cryptographic keys between distant nodes that are connected via submarine networks. It consists of several quantum optical lines on the submarine continental platform followed by several optical classical lines which will receive combined secret keys from the quantum lines providing an extra physical layer of security. As commented, such optical lines are protected in a natural way (water pressure, buried lines, tight encapsulation. . .) and we also propose a protection with additional physical layers of security over a certain distance before reaching deep waters (e.g., before a depth of 1000 m). Therefore, such approach requires that Eve implements simultaneous and complex attacks to several optical lines in deep waters and separated a certain distance. Moreover, for the quantum lines we propose a discrete-modulation continuous variable QKD (DM-CV-QKD) protocol with product weak coherent states (multimode states) measured by homodyne detection, which is usual in optical communications. The protocol is based on the seminal work by Namiki and Hirano for a single-mode weak coherent state [6], therefore it will correspond to a high dimensional protocol which also provides a larger quantum security [7]. Moreover, the QKD protocol will be a plug and play one, that is, an autocompensating protocol [8], and therefore we get the advantage to locate both the quantum sources and detectors at terrestrial points.

The plan of the paper is as follows. In section 2 we present, by taking into account the general topology of a submarine optical communication line, an autocompensating DM-CV-QKD protocol for two modes on the continental platform; two modes is enough to show the security properties of the high-dimensional protocol and its generalization to N modes (multimode case) is straightforward. Moreover, we show that the protocol can also be used between points located at both sides of the sea if the part of the line located in deep waters uses classical signals (hybrid protocol). Next, in section 3, we present a hybrid approach for QKD with M submarine channels (multichannel approach), that is, quantum channels connected to submarine non quantum channels located at deep waters with extra physical layers of security based on combining secret keys. In section 4 some examples of additional physical layers of security (APLS) will be presented for the submarine non-quantum channels before reaching deep waters. In section 5 conclusions are presented.

2. Autocompensating HD-DM-CV-QKD protocol on the continental platform

We show in Fig.1 a sketch of a submarine optical communication line. There are two terrestrial points A and B to share a key. We assume that A (B) can be connected by means of quantum lines to any subsystem A_i (B_i) located at the continental platform. Next, a non quantum optical line starts, which has a buried segment of the optical fibre line, and next the optical line is on surface lay. As it will be depicted, although the non quantum buried segment will be protected with the hybrid approach, it can be also protected with additional physical layers of security. For this proposal, additional points A'_i and B'_i are also shown in Fig.1. Finally, the lines $A'_i - B'_i$ will be protected, in principle, only with the hybrid approach.

2.1. High-Dimensional DM-CV-QKD protocol on the continental platform

The first practical aspect is worth discussing about our method, and is common to any QKD method, corresponds to maximizing the transmission distance and key-rate product, what we will made with a High-Dimensional (HD) DM-CV-QKD protocol which is fully compatible with the current optical communication technology. It is important to stress that HD QKD protocols increase the secure key rate, and usually they are based on quantum superposition states in discrete variable [9], however in this case we will use product states which are much more compatible with continuous variable. We will explain the fundamentals of this HD-DM-CV-QKD protocol between two general points $\mathcal{A}$ and $\mathcal{B}$, as for example A and A$_i$, or B and B$_i$, and for sake of

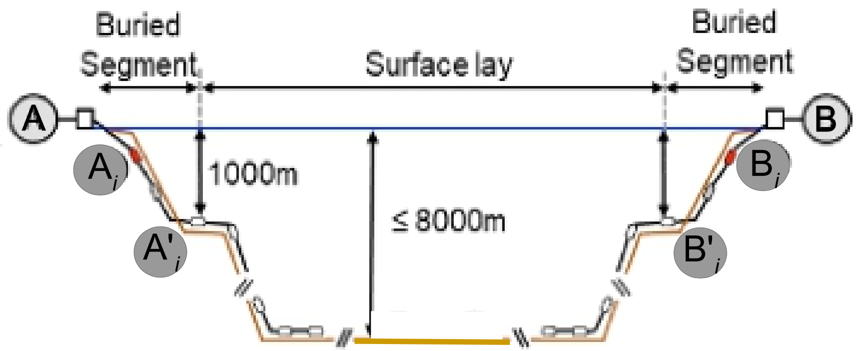


Fig. 1. Sketch of a submarine optical communication line. It is shown A and B, and arbitrary points with quantum lines A-A_i and B_i-B. Moreover, points A'_i and B'_i are considered to implement possible additional physical layers of security in optical lines A_i-A'_i and/or B'_i-A_i.

expository convenience, we only consider two spatial modes, although it can easily be generalized to N modes (HD). The protocol is based in sending from $\mathcal{A}$ product states of coherent states $|\alpha_{L1}\alpha_{S1}\alpha_{L2}\alpha_{S2}\rangle$ where $|\alpha_{Li}\rangle, i = 1, 2$ are local oscillators (to perform homodyne detection in $\mathcal{B}$) excited in a linear polarization mode, and $|\alpha_{Si}\rangle$ are signal weak coherent states excited in the orthogonal polarization mode. All of them are in the same quadrature (*basis*) and are propagated, for example, in two single mode optical fibres (SMF) or a two-core optical fibre.

The protocol is as follows: for each single event, $\mathcal{A}$ randomly chooses the same quadrature (or *basis*) $\mathcal{E}$ or $\mathcal{P}$ for all modes. If she chooses the first quadrature $\mathcal{E}$, she applies a random phase $\phi_k = 0, \pi$ to each mode. On the contrary, she applies a random phase $\{\pi/2, 3\pi/2\}$ to select the second quadrature $\mathcal{P}$. Thus, for $N = 2$ the system $\mathcal{A}$ can send the following eight states in the $\mathcal{E}_1\mathcal{E}_2$ and $\mathcal{P}_1\mathcal{P}_2$ quadratures

$$|\alpha_1\ \alpha_2\rangle_{\mathcal{E}_1\mathcal{E}_2} = |\pm a \pm a\rangle, \tag{1}$$

$$|\alpha_1\ \alpha_2\rangle_{\mathcal{P}_1\mathcal{P}_2} = |\pm ia\ \pm ia\rangle, \tag{2}$$

with $a > 0$. If $N = 1$ then we would have only the two states $|\pm a\rangle$, in the $\mathcal{E}$-quadrature, and $|\pm ia\rangle$ in the $\mathcal{P}$-quadrature. These four states were used in the seminal work by Namiki and Hirano [6] for a single mode; however, for $N = 2$ we have eight states, that is, $2^{2(=N)+1}$=8 states. If we have $N = 3$ then a third weak coherent state is considered, and thus we will have the states $|\pm a \pm a \pm a\rangle$, in the $\mathcal{E}$-quadrature, and the states $|\pm ia \pm ia \pm ia\rangle$ in the $\mathcal{P}$-quadrature (16 states), and so on for N modes. Afterwards, Bob randomly chooses to measure the first or the second quadrature by a homodyne detection, that is, one of the conjugated basis $\mathcal{E}/\mathcal{P}$ is selected by applying the same phase $\phi_B = 0$ or $\phi_B = -\frac{\pi}{2}$ to the local oscillator for every mode. If Bob performs a homodyne measurement for all modes with phase $\phi_B = 0$ a product of weak coherent states in the optical field $\mathcal{E}$ basis for each mode will be measured, otherwise if $\phi_B = -\frac{\pi}{2}$ a measurement in the optical field momentum $\mathcal{P}$ basis is made.

At this point is interesting to note that in the $\mathcal{E}$-representation, and by using appropriate optical-quantum unities, the following equivalence is obtained $\mathcal{E} = \mathcal{R}e(\alpha)$ [10, 11]. In this representation $\mathcal{E}_1\mathcal{E}_2$ the probability of these states is given by the general expression

$$P(\mathcal{E}_1, \mathcal{E}_2) = |\langle\mathcal{E}_1\mathcal{E}_2|\alpha_1\ \alpha_2\rangle|^2 = \frac{2}{\pi}\ e^{-2(\mathcal{E}_1-\mathcal{R}e(\alpha_1))^2}\ e^{-2(\mathcal{E}_2-\mathcal{R}e(\alpha_2))^2}, \tag{3}$$

where $\mathcal{R}e(\alpha_1)$ and $\mathcal{R}e(\alpha_2)$ are mean optical fields, therefore we have the following probabilities for the eight states when are measured in the basis $\mathcal{E}_1\mathcal{E}_2$ when Bob applies a phase phase $\phi_B = 0$,

$$P(\mathcal{E}_1,\mathcal{E}_2) = |\langle\mathcal{E}_1\mathcal{E}_2|\alpha_1\,\alpha_2\rangle_{\mathcal{E}_1\mathcal{E}_2}|^2 = \frac{2}{\pi}\,e^{-2(\mathcal{E}_1\pm a)^2}\,e^{-2(\mathcal{E}_2\pm a)^2} \tag{4a}$$

$$P'(\mathcal{E}_1,\mathcal{E}_2) = |\langle\mathcal{E}_1\mathcal{E}_2|\alpha_1\,\alpha_2\rangle_{\mathcal{P}_1\mathcal{P}_2}|^2 = \frac{2}{\pi}\,e^{-2(\mathcal{E}_1^2+\mathcal{E}_2^2)}. \tag{4b}$$

where $\mathcal{R}e(\alpha_1) = \mathcal{R}e(\alpha_2) = \pm a$ are mean optical fields. In Fig.2 it is shown for N=2 a top view of these probabilities functions. Note that if Alice sends states given by Eq.(1) then Bob can determine with a high probability which state was sent by Alice, that is, he detects with probability given by Eq.(4a); however, if Alice sends states given by Eq.(2) then he can not determine with a high probability which state was sent by Alice because Bob detects with probabilities given by Eq.(4b). In this case if Bob would have changed the basis, that is, $\phi_B = -\frac{\pi}{2}$, then states would have again the probabilities given by Eq.(4a). In short, these are the main quantum properties to get a secure key in continuous variable.

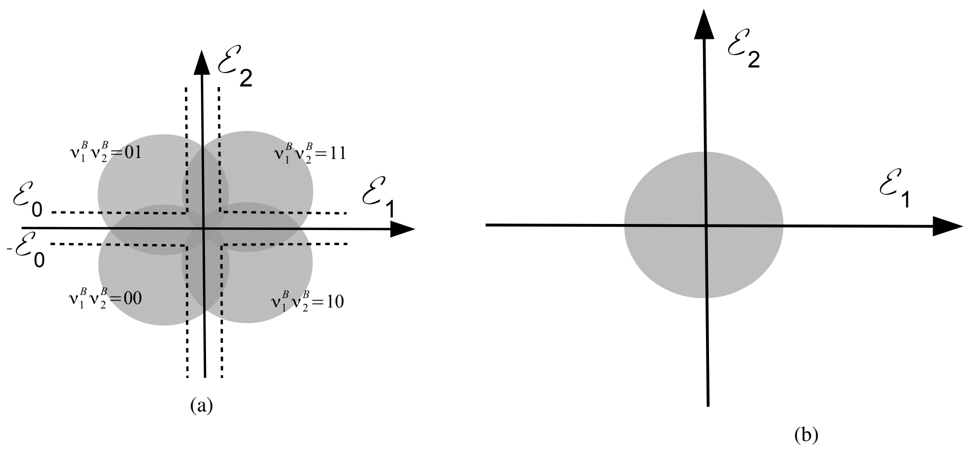


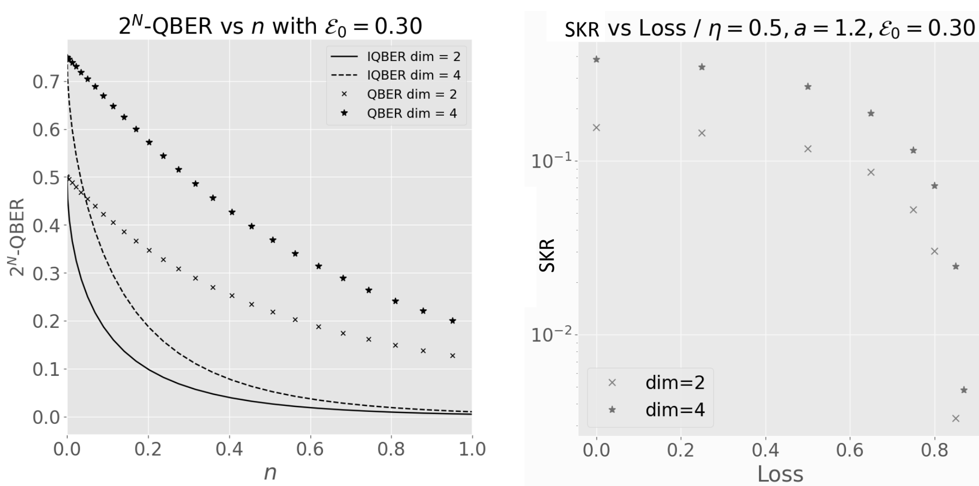
Fig. 2. (a) The four weak coherent states for N=2 modes represented in the two-dimensional first quadrature space $\mathcal{E}_1\mathcal{E}_2$. The states are centred on $(\mathcal{E}_1\mathcal{E}_2) = (\pm a \pm a\rangle$. The values $\nu_1^B\nu_2^B$ for N=2 are indicated within the threshold regions with squared frontiers in the two-dimensional first quadrature space $\mathcal{E}_1\mathcal{E}_2$; the same thresholds $\pm\mathcal{E}_o$ has been chosen for each dimension. (b) The states in the basis $\mathcal{P}$, that is, the vacuum state $|00\rangle$ is shown.

Next, Alice and Bob, by public announce of bases, retain the pulses with coincident basis obtaining a sifted key. Due to overlapping among these states, a threshold $\mathcal{E}_o$ for the optical field detected has to be chosen by Bob to discriminate between states (postselection) and therefore a bit assignment criteria is constructed. Thus, for $N = 2$ we have

$$\nu_1^B\nu_2^B = \begin{cases} 11 & \text{if } \mathcal{E}_1 \geq \mathcal{E}_o \text{ and } \mathcal{E}_2 \geq \mathcal{E}_o \\ 10 & \text{if } \mathcal{E}_1 \geq \mathcal{E}_o \text{ and } \mathcal{E}_2 \leq -\mathcal{E}_o \\ 01 & \text{if } \mathcal{E}_1 \leq -\mathcal{E}_o \text{ and } \mathcal{E}_2 \geq \mathcal{E}_o \\ 00 & \text{if } \mathcal{E}_1 \leq -\mathcal{E}_o \text{ and } \mathcal{E}_2 \leq -\mathcal{E}_o \\ \text{none} & \text{if } |\mathcal{E}_1| < \mathcal{E}_o \text{ or } |\mathcal{E}_2| < \mathcal{E}_o, \end{cases} \tag{5}$$

where $\mathcal{E}_{1,2}$ are the results of Bob's measurements. If some optical field value does not fulfil the criteria then no bits are distilled. These thresholds could have been selected arbitrarily, but for a practical case rectilinear frontiers have been selected, as shown in Fig.2, and accordingly square thresholds regions are defined. Therefore, when Alice announces the basis, that is, the quadrature used, then the Bob's task will be to distinguish as best as possible between the four states of the first ($\mathcal{E}$) or the second ($\mathcal{P}$) quadrature. The criteria given by Eq.(5) is used to perform the mentioned task by using a balanced homodyne detection and thus a secret key can be sifted.

On the other hand, the homodyne detection produces an intrinsic quantum bits error (IQBER) which can be eliminated by error corrections. The intrinsic error consist of measuring, for example, $(\mathcal{E}_1 > \mathcal{E}_o, \mathcal{E}_2 < -\mathcal{E}_o)$ or $(\mathcal{E}_1 < -\mathcal{E}_o, \mathcal{E}_2 > \mathcal{E}_o)$, or $(\mathcal{E}_1 < -\mathcal{E}_o, \mathcal{E}_2 > \mathcal{E}_o)$, and nevertheless Alice sent the state $|aa\rangle$ and therefore Bob should have measured $\mathcal{E}_1 > \mathcal{E}_o, \mathcal{E}_2 > \mathcal{E}_o$. On the other hand, we will have QBER due to Eve's attacks, for example, an intercept-resend attack by performing simultaneous measures in the two quadratures, therefore, Eve only can use the half of mean photons of each weak coherent state to identify the bits. Recently, it has been calculated both the total QBER as the Secure Key Rate (SKR) for HD-DM-CV-QKD for this attack, and it has been shown that both QBER and SKR increase with dimension [12], that is, the security is clearly increased. In Fig.3 and for an illustrative purpose we present results for $N = 1, 2$ of the IQBER and QBER as a function of the mean number of photons and for a fixed threshold $\mathcal{E}_o = 0.75$. Likewise, for $N = 1, 2$ modes and a Eve's partial attack of 50%, that is, a fraction of attacks $\eta = 0.5$, SKR is plotted as a function of the losses as shown in Fig.3 for a mean optical field $a = 1.2$ and threshold $\mathcal{E}_o = 0.3$. Note that losses are related to the propagation distance depending on the optical fibre attenuation. The most important conclusion is that the SKR increases with dimension, and therefore we can use a greater QKD distance. It is also interesting to indicate that the rate R_2 for $N = 2$ is greater than the corresponding to two independent single channels with rate R_1, that is, $R_2 > 2R_1$. In these calculations we have assumed that errors due to optical perturbations are negligible because an active or passive compensation technique has been applied to the perturbed quantum states, as shown in next subsection.



(a) (b)

Fig. 3. (a) QBER for 1 and 2 modes (cross and star dots) as a function of mean photon number; intrinsic QBER is shown for completeness (solid and dashed lines). (b) Secret Key Rate (SKR) as a function of losses for 1 and 2 modes (cross and star dots) for a mean optical field $a = 1.2$ and threshold $\mathcal{E}_o = 0.3$.

2.2. Efficient QKD and reduction of technological complexity by autcompensating

It is well-known that quantum states are perturbed under propagation in optical fibres due to intrinsic imperfections, mechanical and thermal perturbations and so on. Accordingly, errors appear and QKD efficiency is reduced in the quantum lines, and therefore it is important to restore the quantum states. For that, active compensators of the perturbations can be used although present a certain technological difficulties. Alternatively, passive compensation techniques (autocompensation) can also be used [8, 13–16]. We must note that these passive techniques have been proposed to achieve a plug and play system and thus to increase the key-rate and transmission distance, that is, the efficiency of the QKD protocols. They use a round-trip propagation that compensates, by inserting a proper modal unitary transformation, the perturbations undergone by the quantum states. In our case, A and B will play the role of $\mathcal{B}$ and A_i and B_i the role of $\mathcal{A}$, and the autocompensating technique will be applied to polarization modes and implemented by locating the sources and homodyne detectors at terrestrial points A and B, which has a certain advantage as to reduce the technological complexity. On the other hand, quantum random number generators (QRNG) and phase modulators will be located at the submarine subsystems A_i and B_i. As commented, an active compensating device could be used, but a passive compensation (autocompensation) of QKD supposes a very practical solution. Thus, optical elements like Faraday Mirrors can be used to implement autocompensation in polarization modes, but in our case we will use a Half Wave Plate (HWP) which, as we will show, is a most versatile solution to implement an autocompensating HD-DM-CV-QKD protocol. First of all, we present the fundamentals to understand how a HWP implements autocompensation in the polarization modes by using a closed cycle located, for example, in subsystem B_i belonging to the arbitrary quantum line B_i-B. In Fig.4 a sketch of the autocompesation system is shown (optical fibre lines are indicated with thick lines and electrical lines with thin lines). At the top right, an optical fibre closed cycle is shown (enclosed in a dotted circle) whre the input to the cycle and output from the cycle is implemented by an Optical Circulator (OC). The cycle contains Modulators and Attenuators controlled by AC optics, and a HWP.

Let us consider an anisotropic perturbation P before the closed cycle, that is, a perturbation of the polarization of the quantum states. An anisotropic perturbation is represented by an unitary matrix M for progressive modes and M' for regressive modes, that is,

$$M = \begin{pmatrix} a & ib \\ ib & a^* \end{pmatrix}, \quad M' = \begin{pmatrix} a & -ib \\ -ib & a^* \end{pmatrix}, \tag{6}$$

where parameter b is a real number, then, by using a HWP rotated $\pi/4$ an antidiagonal matrix D' is implemented and then we obtain

$$M'D'M = \begin{pmatrix} a & -ib \\ -ib & a^* \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & ib \\ ib & a^* \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{7}$$

that is, an autocompensation is obtained although polarizations have been permuted what has not any relevant effect. Obviously if there is more perturbations the same autocompensation is obtained. In short, if we start with a coherent state $|\alpha_H \alpha_V\rangle$, the state after a round trip, where it has undergone perturbations, becomes the state $|\alpha_V \alpha_H\rangle$. This will be the result that we will use to get autocompensation (technical details can be found in [8, 16]).

Now we explicit a little more the physical process in any subsystem B-B_i (or A-A_i) to achieve an autocompensating QKD protocol. The laser (coherent) sources and detectors (homodyne detection connected to a processing unity) will be located at a terrestrial point B as shown in Fig.4, which offers a certain advantage, as commented. We have to remember that the protocol

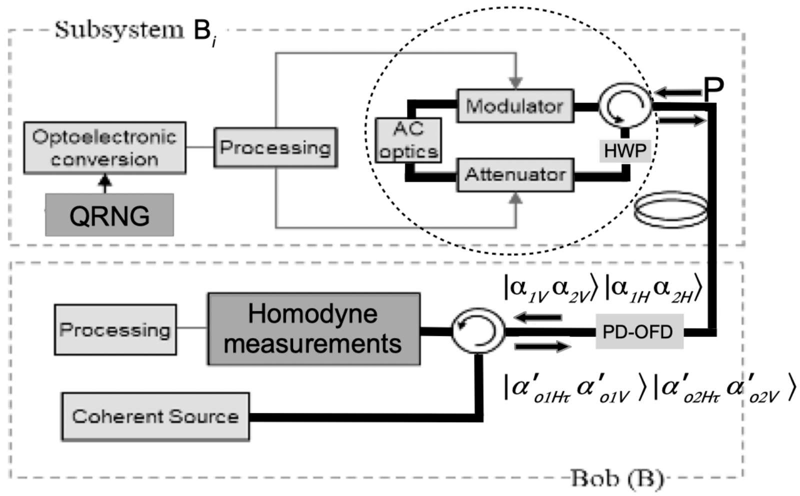


Fig. 4. Sketch of the autocompensation system. It is shown a product coherent state with two polarizations one for the local oscillator and the other one for the signal. An arbitrary perturbation P is indicated. Note the location of the HWP (Half Wave Plate) in the closed cycle (enclosed in a dotted circle) and the location of the PD-OFD (Polarization Dependent Optical fibre Delay) at the start of the quantum line.

described above is implemented by a scheme assisted by polarization, that is, quantum states (signal) and LO will be excited in different polarization modes, and moreover several types of fibres can be used such as few mode fibres (FMF), multicore fibres (MCF) and even a bundle of single-mode fibres (SMF). In all these cases it can be assumed that there is no spatial coupling, particularly if we use SMF, however, polarization modal coupling limits their applicability for long distance links. Such coupling is due to slow external random perturbations (mechanical, thermal...) or to waveguide birefringence (imperfections) of the optical fibres, and thus an autocompensation of these perturbations is required.

Autocompensation is obtained as follows: Bob emits a spatial two-mode coherent pulse with the same mean number of photons in each mode (we must indicate that now the role of Alice $\mathcal{A}$ is played by B_i and the role of Bob $\mathcal{B}$ is played by the own B). The above two-mode coherent pulse can be obtained by using a coherent source (a laser), as shown in Fig.4, which can be divided by a beam splitter and coupled to two SMF optical fibres. The output state from Bob can be written as follows

$$|\Psi_o\rangle = |\alpha'_{o1H\tau}\alpha'_{o1V}\rangle\,|\alpha'_{o2H\tau}\alpha'_{o2V}\rangle, \tag{8}$$

where τ is a delay produced by a Polarization Dependent Optical fibre Delay (PD-OFD [8] and it has been assumed that $\alpha'_{oiH} = A'e^{i\phi_{oi}}, \alpha'_{oiV} = A'e^{i\phi_{oi}}$ $(i = 1, 2)$, that is, the coherent states in each polarization space have the same phase ϕ_{oi}.

Next, under propagation each coherent state is perturbed, for example, $|\alpha'_{o1H}\rangle \rightarrow |\tilde{\alpha}_{o1H}\tilde{\alpha}_{o1V}\rangle$. When the signal arrives to Alice, that is, to the mentioned closed cycle at B_i, each perturbed polarization coherent state of the product state passes through a HWP with angle $\pi/4$ ($\mathrm{HWP}_{\pi/4}$) and therefore compensation of polarization perturbations is achieved when the pulses return to Bob, as analysed above, although polarization modes will arrive permuted (H→V, V→H) (that is, a logic X gate is applied). Moreover, in such a closed cycle a modulation (determined by a QRNG and an optoelectronic conversion and the corresponding processing) and an attenuation of the signal product coherent state is realized. In short, an autocompensation is successfully performed and the state reaching the detection system at Bob is given by

$$|\Psi\rangle = |\alpha_{1V}\alpha_{2V}\rangle\,|\alpha_{1H}\alpha_{2H}\rangle, \tag{9}$$

which, depending on the (random) modulation and the attenuation applied in the closed cycle, are given by the following expressions

$$|\Psi\rangle = |\pm ae^{i\phi_1} \pm ae^{i\phi_2}\rangle\,|Ae^{i\phi_1}Ae^{i\phi_2}\rangle \quad \mathcal{E}\text{ basis} \tag{10}$$

or

$$|\Psi\rangle = |\pm iae^{i\phi_1} \pm iae^{i\phi_2}\rangle\,|Ae^{i\phi_1}Ae^{i\phi_2}\rangle \quad \mathcal{P}\text{ basis}, \tag{11}$$

where $a \ll A < A'$, that is, $|\alpha_{1V}\alpha_{2V}\rangle$ is a weak coherent state, and ϕ_1 and ϕ_2 are global phases acquired by the optical modes without any relevance in the homodyne detection. The final measuring step (homodyne measurements) begins with a PBS at 45^o which splits again the light into signal and LO [6, 17], both polarized at the contrary as Bob's output, due to the permutation of the HWP. For each spatial mode an Electro-Optical Phase-Modulators is used, which applies a random phase ϕ_B to the LO (horizontal polarization) and the same for the LO of each mode. Finally, a homodyne detection is made at each spatial mode by using a pair of photodetectors capable of measuring the homodyne current. In short, the HD-DM-CV-QHD protocol is implemented and a high rate of secure key can be distilled.

2.3. Hybrid HD-DM-CV-QKD protocol on the submarine line A-B

In the subsection 2.1 the role of $\mathcal{A}$-$\mathcal{B}$ were played by A_i-A, and B_i-B, however it is also possible to use A-B, where A_i and B_i are intermediate points where modulation is performed, and the lines A_i-B_i are non quantum ones once more, that is, we would have a hybrid protocol. We briefly describe this hybrid protocol [18], for that, let us consider that at A_i there is a QRNG device which determines in a random way what states must be sent to A and to B from A_i, obviously the information will reach B_i by a non quantum channel but in deep waters. The QRNG determines the phase modulation $(0, \pi, \pi/2; 3\pi/2)$, according to the DM-CV-QKD protocol explained in subsection 2.1, that must be applied at each mode of a strong multimode product coherent state coming from A and B. Note that we are considering the autocompensating system explained in the above section. After modulation the states are attenuated and sent from A_i to A, and from B_i to B. At A and B homodyne detection is used to measure the quantum states (weak coherent states). For that, A and B have to choose which basis use, that is, first or second quadrature, to measure the quantum state. Next, by public channel, A and B announce the bases used, and moreover A_i also communicate the basis of each of the states sent. Note that in this case there are bases coincidences in 25%, unlike the case non hybrid of section 2.1 where the bases coincidences was 50%. With this information a key can be shared between A and B. Note that the Eve's attack has also to be made in the non quantum lines A_i-B_i, but now the QRNG systems are reduced by half, which, once more allows a reduction of the technological complexity.

3. Hybrid approach with M combined submarine channels

Submarine optical communications are usually established between points A and B separated a long distance. The standard hybrid solution would be the use of several submarine trusted nodes which means a high technological difficulty since the current submarine lines have not these nodes for quantum communications. Obviously, the region between, for instance, A_1-B_1 (see Fig.1), could be considered a node but not fully trusted, because although an optical attack, such as optical fibre tapping, would have an extremely high technological difficulty, it would be possible. Therefore, the solution would be to add one or several physical layers of security. We must stress that a similar situation is found in QKD with satellites where the region A_1-B_1 would

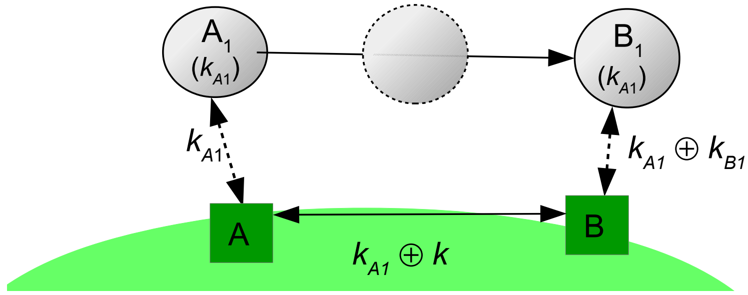


Fig. 5. Sketch of extra physical layer of security between A and B connected with one satellite as trusted node travelling from a point above A to a point above B.

correspond to the satellite (see Fig.5) which contains a classical signal that can be copied, that is, there is no quantum security within the satellite. As suggested by Huttner *et.al.* [19] an extra physical layer security can be included by introducing a second channel, in this case a terrestrial one, apart from the first channel (satellite channel), and then two secret keys are combined and transmitted over two channels.

We will adapt this suggestion to submarine optical communications. We briefly remember this hybrid approach for earth-satellite QKD. In Fig.5 a satellite shares a key k_{A1} at the quantum line A-A$_1$ and another key k_{B1} at the quantum line B$_1$-B. The satellite transport the key k_{A1} from a point over A to a point over B and the it sends the key under the XOR operation $k_{A1} \oplus k_{B1}$. Obviously, the satellite is a classical channel, therefore has not a fundamental protection, it only has a certain physical protection corresponding to the difficulty for accessing to it, and then the best option is to include an extra physical layer of security. Such as suggested in [19] a classical terrestrial channel can be used where a new key k is transmitted as $k_{A1} \oplus k$ from A to B, and thus Eve has to break security in two channels; we must note that the attack can be made in any point of the terrestrial optical line.

3.1. Double radial multichannel topology

The above hybrid approach will be adapted to the submarine case, that is, the extra optical line (or lines) should be located as far into the sea as possible to increase the difficulty of an optical attack. Let us consider the additional points A$_i$ and B$_i$, $i = 1, ..., M$, therefore there are M channels (multichannel scheme) between A and B (double radial multichannel topology), that is, A is connected to M subsystems A$_i$ and B is connected to M subsystems B$_i$ with quantum lines, such as shown in Fig.6, that is, in each quantum line a key is shared, that is, k_{Ai} and k_{Bi}. With this topology we can generalize the above approach to M channels, and moreover we will be able to introduce different combinations of keys. We start with the first key $k_{A1} \equiv k_1$ generated in the quantum line A-A$_1$; this key is sent along the non quantum channel 1 from A$_1$ to B$_1$ (this is analogous to the path A-A$_1$ in the satellite case). At B$_1$ a key k_{B1} is used to forward to B the XOR of key k_1. Likewise, the key k_{A2} is used in A to forward to A$_2$ the XOR of this key with a composed key $k_2 + k_1$ (the key k_2 is generated at A), which is sent along channel 2 to B$_2$; the composed key is transmitted to B by making a XOR operation with the key k_{B2}. At this stage the key shared between A and B is k_2, therefore with the additional channel A$_2$-B$_2$ we have an important layer of security, analogous to the satellite-earth case presented above, however we emphasize that the classical lines are as far into the sea as the quantum lines allow.

The security can be increased by introducing an arbitrary number M of these hybrid channels according to both the existing fibre optic network and the technological possibilities. Thus the key k_{A3} is used in A to forward to A$_3$ the XOR of this key with a new composed key $k_3 + k_2$ (the

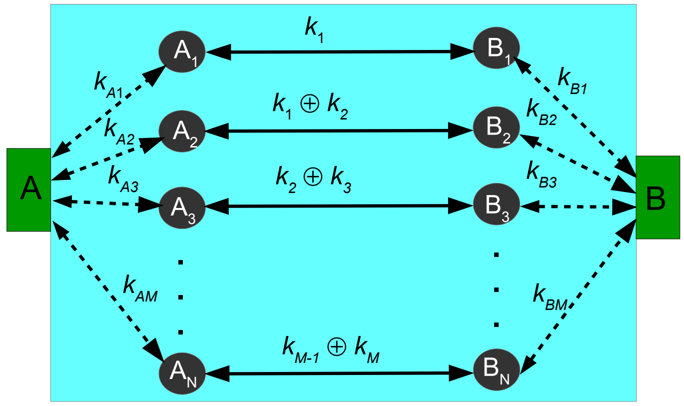


Fig. 6. Sketch of the double radial topology of M submarine (hybrid) channels between two nodes A and B.

key k_3 is generated at A), which is sent along channel 3 to B_3. This composed key is transmitted to B by making a XOR operation with the key k_{B3}. At this stage the key shared between A and B is k_3, therefore with this additional channel A_3-B_3 an additional layer of security is introduced in deep waters. In short, by this concatenated local processing, that is, a XOR in each channel, the key shared between A and B will be k_M, therefore Eve must attack M classic lines located under the sea and separated from each other by a distance of several kilometres.

Alternatively, a simpler approach can be implemented if a key is constructed by combining the quantum keys k_{Ai}, that is, by choosing a common logic operation in A and B the new key is obtained. We can use a XOR logic operation, a XNOR logic operation or combinations of them (or other operations), therefore we could obtain

$$k = k_{A1} \oplus k_{A2} \oplus \ldots \oplus k_{AM-1} \oplus k_{AM}, \tag{12a}$$

$$k' = k_{A1} \odot k_{A2} \odot \ldots \odot k_{AM-1} \odot k_{AM}, \tag{12b}$$

$$k'' = k_{A1} \odot k_{A2} \oplus \ldots \odot k_{AM-1} \oplus k_{AM}. \tag{12c}$$

The keys k_{Ai} are sent along the non quantum lines to subsystems B_i where the operations XOR $k_{Ai} \oplus k_{Bi}$ are made and sent to B. Since A and B will made the same logic operations with the keys received a new key will be shared between them. The main advantage of this approach is that it does not require to generate keys at A and do logic operations in nodes A_i.

3.2. Non-radial multichannel topology

A most flexible topology can be used as shown in Fig.7, that is, we consider M trusted nodes A_{oi} outside the sea and connected between them by quantum lines, where any of them can be Alice, and, on the other side of the sea, we will also have M trusted nodes B_{oi} outside the sea and also connected by quantum lines, where any of them can be Bob. Therefore this non radial topology would require to place trusted nodes in A_{oi} and B_{oi} or to use the existent standard terrestrial nodes; besides the quantum lines would go straightforwardly into the sea to the nodes A_i and B_i without following oblique paths as in the above radial topology, and accordingly the distance to the subsystems located further away from A (or B) would be reduced. Likewise, as commented, with this topology the systems A and B could be any terrestrial trusted node A_{0i} and B_{0i} providing a greater flexibility to the system, although all the keys k_{Ai} have to be sent to the trusted node playing the role A, and all keys k_{Bi} have to be sent to the trusted node playing the

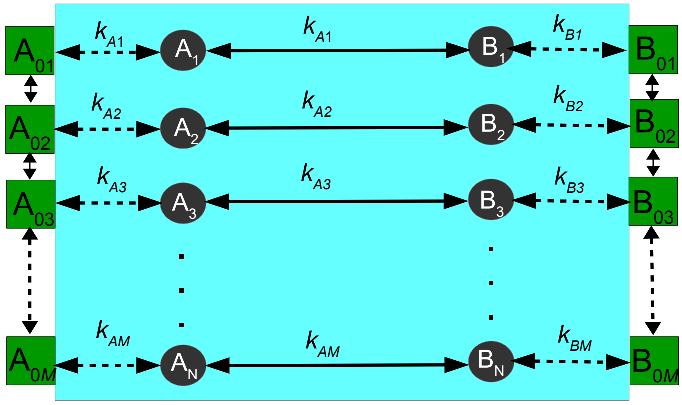


Fig. 7. Sketch of the non radial topology of M submarine (hybrid) channels between nodes A_{0i} and B_{0i}.

role B. Obviously this is a small disadvantage compared to the double radial topology where all signals is going out from A and going into B.

On the other hand, we take advantage of this topology to indicate how to apply the hybrid protocol described in section 2.3. Such a protocol would be implemented in each channel A_{0i}-B_{0i}, therefore we have the keys $k_{Ai} = k_{Bi} \equiv k_i$ which are protected in a quantum way in the paths A_{0i}-A_i and B_i-B_{0i}, and by the multichannel hybrid scheme approach in deep waters. As commented, with the hybrid protocol we reduce the number of QRNG devices, and moreover the keys k_{Bi} are not necessary, therefore the multichannel hybrid approach is simplified. Obviously the double radial topology could also be used with this hybrid protocol.

In short, M extra physical layers of security have been introduced. We must stress that M submarine optical fibre channels would have to be hacked and besides to establish an efficient communication system between hacked points On the other hand, we could even introduce Additional Physical Layers of Security (APLS) in a part of the non quantum lines. In the next section some APLS will be presented, many of them are related to the type optical fibres used in the channels.

4. Hybrid approach with additional physical layers of security

We present in this section several APLS in an increasing order of technological complexity. These layers can be implemented along an optical line between A_i (or B_i) and some point A'_i (or B'_i) beyond continental platform, if possible, that is, along the buried segment of the submarine optical communications lines as shown in Fig.1. We have to indicate that the arbitrary point A'_i could reach the point B_i if it were technologically feasible. Therefore, optical lines would be protected by additional layers of security in submarine depths less than 1000m, which would require Eve to perform optical tapping in much deeper waters. We will present these APLS into two categories: passive APLS and active APLS, if moreover an additional optoelectronic processing is required.

4.1. Hybrid protocol with passive APLS

APLS can be introduced by taking into account both the properties of the optical fibres used in the lines A_i-A'_i (or B'_i-B_i) and the protocol QKD used in the quantum lines. In section 2 we have presented a protocol with N modes in each quantum line. This multimode solution is highly compatible with both single mode fibres and multicore optical fibres. Therefore, we present some passive physical layers of security implemented with such optical fibres.

4.1.1. APLS with N single mode optical fibres

Let us consider the general case of N modes at the generic submarine quantum lines A-A_i, then N bits can be distributed in N modes in each quantum line. Next, these bits are coupled to N single mode fibres at each node A_i. Therefore, Eve will have to tap a number N of SMFs (optical lines) at A_i-A'_i of each submarine channel and therefore a total number MN of SMFs. This represents a straightforward physical layer of security by using optical fibres which could already be installed in the classical channels.

4.1.2. APLS with multicore optical fibres

On the other hand, if we have multicore optical fibres then new physical layers of security can be incorporated. Let us consider, for the convenience of exposition, $N = 2$ (two bits) at the submarine quantum line A-A_1, then each bit can be transmitted in a different spatial mode. Next, these bits are coupled to a two-core optical fibre located at the classical channel segment A_1-A'_1. A tapping on this optical fibre can be made, however Eve has to distinguish from which core comes each bit. Obviously for several cores the difficulty is increased. Therefore, tapping has to be completed with some optical device that can determine from which core the light goes out. Obviously, if these two-core optical fibres are already installed in all submarine optical lines (or some of them) this passive APLS could already be introduced.

4.1.3. APLS with spatial and/or polarization modal coupling

We can use the spatial or polarization modal coupling to protect the bits information. Thus, we can transmit each bit in a different polarization mode, then modal coupling appears and therefore Eve has to implement some optical device to restore information (MIMO, ...) [2]. The disadvantage in this case is that the optical devices to restore information have to be also installed at one or several submarine channels A_i-B_i.

4.2. Hybrid protocol with active APLS

The above physical layers are based on the technological difficulty to make tapping and extract information, however we can also use the own optical fibres to detect attacks by optical tapping, that is, by processing the optical signals. We present two active physical layers with a certain detail, the first one is based in a simple detection of energy in a dark mode, and the second one is based in the use of a secret key obtained by classical perturbations (therefore it has not a fundamental protection). Besides, these active APLS can be mixed with the above passive ones.

4.2.1. Active APLS based on modal power transference

Let us consider, for example, optical fibres with three cores, two of them are single-mode cores and one of them is a few-modes core. Tapping can be considered as an optical perturbation and therefore it can induce modal coupling, therefore if in the few-modes core the fundamental mode is excited then by tapping a fraction of optical power is transferred to the first excited mode and then the presence of Eve can be detected at the end of the fibre if energy is measured in the first excited mode. A perturbative theory of modal coupling can be used to calculate the energy transferred from the fundamental mode [20] to other modes. Next, we present a possible modelling of the perturbation by optical tapping by fibre bending and the modal coupling efficiency from fundamental mode to the first excited mode in a Few Modes optical fibre (FMF) (in our case a few-modes core). For illustrative purposes we assume that the parabolic approximation for the first modes of a graded-index optical fibre can be made, that is, the refractive index profile is given by

$$n^2(x, y) \approx n_o^2[1 - g_o^2(x^2 + y^2)], \tag{13}$$

where n_o is the axial index and g_o the graded-index parameter, therefore, separable Hermite-Gaussian modes will be used for numerical calculations. First of all we write the expression of the coupling coefficients between modes of order m and n under a perturbation $\Delta n^2(x, y, z)$,

$$K_{nm} = \omega\epsilon_o \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \mathrm{d}x\mathrm{d}y \Delta n^2(x, y, z) e_n(x, y) e_m^\star(x, y), \tag{14}$$

where ω is the angular frequency, ϵ_o s the vacuum permittivity, and $e_n(x, y)$, $e_m(x, y)$ are the normalized optical modes [21] of order n and m, respectively, with propagation constants $\beta_{n,m} = k_o N_{n,m}$, where $N_{m,n}$ are the effective indices. Next, by taking into account the above coupling constants and the propagation constants, the well-known asynchronous modal coupling equations system $-i\mathrm{d}a_n/\mathrm{d}z = a_n + K_{nm}a_m$, with repeated indices indicating sum, has to be solved for the mode amplitudes $a_n = A_n e^{i\beta_n z}$. Then under the perturbative approximation we have the following formal solution for the modal amplitudes $A_n(z)$ at the end of the fibre (z-direction)

$$A_n(z) \approx \sum_n \int_{-\infty}^{+\infty} \mathrm{d}z\, A_m(0) K_{nm}(z) e^{i(\beta_m - \beta_n)z}. \tag{15}$$

We have also assumed that the initial amplitudes $A_n(0)$ can be considered as constants in the perturbative approximation.

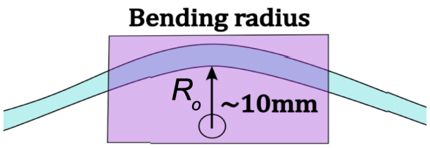
Let us consider a macro-bending of the optical fibre, then the refractive index profile is perturbed and the following perturbation Δn^2 can be used [22],

$$\Delta n^2(x, y, z) = \frac{2(1+\kappa)x}{R(z)} n^2(x, y) \tag{16}$$

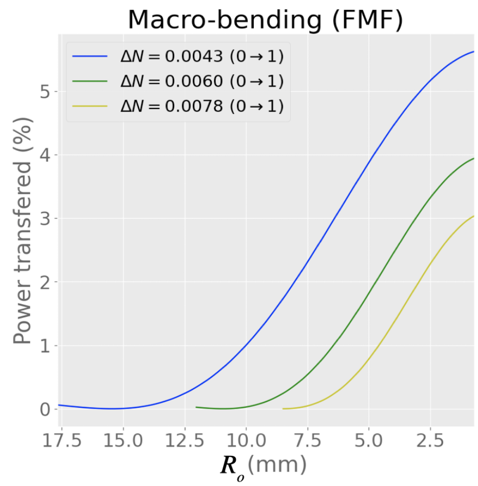
where κ is a coefficient dependent of the elasto-optic properties of the optical fibre [5] and $R(z)$ characterize the local curvature radius in the perturbed region by tapping as shown in Fig.8a. We assume the following trial function describing the z-dependence of the local radius $R(z) = R_o e^{z^4/d^4}$, where the parameter R_o is the bending radio at $z = 0$ and d is related to the reaching of the perturbation. Besides, a linear dependence between these parameters is assumed, that is, $R_o = a_o d$, where a_o is a constant related to the bending angle of the optical fibre. Finally, the symmetry of the perturbation allows only even-odd coupling, for example, between the fundamental and first excited modes with effective indices N_0 and N_1, and therefore a difference $\Delta N = N_1 - N_0$. Next, by using the perturbative solution given by Eq.15 for modal coupling [20], then transferred power curves to the first mode, that is, $P_1 = |a_1|^2$, as a function of bending radius R_o can be obtained. In Fig.8b we present some of these curves for different ΔN. Note that a compromise between ΔN and transferred power is required, that is, ΔN must be large enough to avoid spurious modal coupling but small enough to obtain modal coupling by tapping. Anyway, curves show that a significant and measurable amount of energy can be transferred to the first mode with usual values of the bending radius to achieve tapping. In short, in lines A_i-A'$_i$ or B'$_i$-B_i we can detect the presence of an eavesdropper by monitoring the transferred power P_1.

4.2.2. Active APLS based on multicore modal reciprocity

Finally we present a more complex active APLS. Let us consider a MCF with N cores coupled, that is, N spatial modes and polarization modes H and V (2N-dimensional space), which connects points A_1 and A'$_1$ shown in Fig.1. As commented, the submarine optical line A_1-A'$_1$ can reach points beyond continental platform. The MCF provides 2N modes H1, V1, H2, V2,. . . , HN, VN and then we can define input and output vectors at A_1 and A'$_1$, that is, $\boldsymbol{V}_{A_1}$, $\boldsymbol{V}_{A'_1}$ and $\boldsymbol{U}_{A_1}1$, $\boldsymbol{U}_{A'_1}$ with 2N components corresponding to complex amplitudes of the optical field in each mode. On the other hand, it can be proven that the channel from A_1 to A'$_1$ can be characterized by a matrix $H_{A_1 A'_1}$ of dimension $2N\mathrm{x}2N$, including polarization. Such a matrix fulfils the following



(a)



(b)

Fig. 8. (a) Image of a macro-bending for tapping a multimode optical fibre. (b) Power transfered between modes $m = 0$ and $m = 1$ by macro-bending tapping as a function of curvature radius R_o.

reciprocity property (analogue to wireless communications [23, 24] but including polarization modal coupling) with the matrix propagation $H_{A'_1 A_1}$ from A'$_1$ to A$_1$ [16]

$$H_{A'_1 A_1} = D(H^t_{A_1 1 A'_1 1})D, \tag{17}$$

with t indicating transpose and $D = I_N \otimes Z$, where $\otimes$ is the tensor product, Z is the third Pauli's matrix and I_N the matrix identity. In the simpler case A$_1$ and A'$_1$ transmit to each other the i-th and j-th element of the input vectors $\boldsymbol{V}_{A1}, \boldsymbol{V}_{A'1}$ and detect the same i-th and j-th element of the output vector $\boldsymbol{U}_{A1}, \boldsymbol{U}_{A'1}$. Importantly, the reciprocity property shows that A$_1$ and A'$_1$ measure the same intensity. Since these coefficients change randomly we can generate a random sequence of signals S. At each point A$_1$ and A'$_1$ has to be a transmitter and a detector of a classical signal and some processing electronic devices for classical low speed fibre communications. We can codify the intensity of signals S with two levels corresponding to bits $\{0, 1\}$ and therefore a classical key can be shared. Obviously, the use of this APLS in the other lines A$_i$-A'$_i$ will provide a larger security.

We present as an example and in an explicit the case of two spatial modes 1 and 2, along with polarization modes H and V, that is, four modes: $H1, V1, H2, V2$. By taking into account the reciprocity property the propagation matrices $M = H_{A_1 A'_1}$ and $M' = H_{A'_1 A_1}$ are given by the following expressions:

$$M = \begin{pmatrix} a_{H1H1} & a_{H1V1} & a_{H1H2} & a_{H1V2} \\ a_{V1H1} & a_{V1V1} & a_{V1H2} & a_{V1V2} \\ a_{H2H1} & a_{H2V1} & a_{H2H2} & a_{H2V2} \\ a_{V2H1} & a_{V2V1} & a_{V2H2} & a_{V2V2} \end{pmatrix}, \tag{18}$$

$$M' = \begin{pmatrix} a_{H1H1} & -a_{V1H1} & a_{H2H1} & -a_{V2H1} \\ -a_{H1V1} & a_{V1V1} & -a_{H2V1} & a_{V2V1} \\ a_{H1H2} & -a_{V1H2} & a_{H2H2} & -a_{V2H2} \\ -a_{H1V2} & a_{V1V2} & -a_{H2V2} & a_{V2V2} \end{pmatrix}. \quad (19)$$

Now, let us consider that A_1, for example, emits the vector $\boldsymbol{V}_{A_1} = (0,1,0,0)^t$ and detects in position two, that is, projects on the same vector (0,1,0,0), and A'$_1$, for example, emits the vector $\boldsymbol{V}_{A'_1} = (0,0,1,0)^t$ and detects in position three, that is, projects on the same vector $\boldsymbol{V}_{A'_1}$, then the following results are obtained: the state sent by A_1 is transformed under propagation, that is, $\boldsymbol{U}_{A_1} = M\boldsymbol{V}_{A_1}$, and therefore at A'$_1$ the state becomes $\boldsymbol{U}_{A_1} = (a_{H1V1}, a_{V1V1}, a_{H2V1}, a_{V2V1})^t$, and therefore A'$_1$ detects $\boldsymbol{U}_{A_1} \cdot \boldsymbol{V}_{A'_1} = a_{H2V1}$; on the other hand, the state sent by A'$_1$ is transformed under propagation, that is, $\boldsymbol{U}_{A'_1} = M'\boldsymbol{V}_{A'_1}$ and then at A_1 the state becomes $\boldsymbol{U}_{A'_1} = (a_{H2H1}, -a_{H2V1}, a_{H2H2}, -a_{H2V2})^t$, and therefore A_1 detects $\boldsymbol{U}_{A'_1} \cdot \boldsymbol{V}_{A_1} = -a_{H2V1}$. In short, the same power $|a_{H2V1}|^2$ is detected at A_1 and A'$_1$, and accordingly a classical key can be obtained. This key can be used to transmit the keys sent from A_1. Obviously, the same APLS can be used in some others lines A_1-A'$_1$ and/or B_1-B'$_1$.

4.2.3. Mixture of different APLS and other APLSs

It is interesting to comment that mixtures of different APLS can be used. For example, we can combine modal power transference and SMF fibres. For example, let us consider a SMF and a two-core optical fibre, with a single-mode core and a few-mode core. For the case $N = 2$ one bit can be sent through the SMF and the second bit can be sent through the single mode core, therefore Eve has to tap two optical fibres and moreover the few-mode core can undergo modal coupling and therefore the tapping can be detected. Finally, there are more complex APLS, as for example sensing techniques such as DAS which are being proposed to potential damages or attacks to the optical lines [4], however these sensing techniques require more studies and probes.

5. Summary

We have presented a hybrid QKD approach based on multichannel topologies for submarine optical communications. Several quantum lines on the continental platforms of Alice and Bob are installed where an autocompensating high-dimensional DM-CV-QKD protocol based on product states has been proposed. High dimensionality provides a high secret key rate, and the autocompensating technique reduces part of the hardware required to implement submarine QKD, such as coherent sources, photodetectors, and so on. Next, a local and/or global combination of secret keys in non quantum optical channels, as far away from shore as possible, provide layers of security that require Eve to perform simultaneous attacks on these channels in depth waters to break the security. Some possible topologies and keys processing methods have been presented according to the required level of security or the technological possibilities of the existing submarine optical lines. Finally, additional physical layers of security, both passive and active ones, have been proposed for the buried segment of submarine optical communications lines, which would require Eve to perform optical tapping in very deep waters. In short, while the distances between Alice (A) and Bob (B) for submarine optical communications are beyond the current QKD possibilities, these hybrid QKD approach can be very practical and useful solution.

Funding. This work was supported in part by the MICIN, European Union NextGenerationEU under Grant PRTR-C17.I1, and in part by the Galician Regional Government through Planes Complementarios de I+D+I con las Comunidades Autónomas in quantum communication. It was also funded in part by MCIU/ AEI / 10.13039/501100011033 / FEDER, UE under project PID2023-152607NB-I00.

Disclosures. EFM: NEC Corporation (E). The remaining authors declare no conflicts of interest.

References

1. S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).
2. N. Bai, E. Ip, Y.-K. Huang, *et al.*, "Mode-division multiplexed transmission with inline few-mode fiber amplifier," Opt. Express **20**, 2668–2680 (2012).
3. L. Salvail, M. Peev, E. Diamanti, *et al.*, "Security of trusted repeater quantum key distribution networks," J. Comput. Secur. **18**, 61–87 (2010).
4. X. Chen, N. Zou, Y. Wan, *et al.*, "On-line status monitoring and surrounding environment perception of an underwater cable based on the phase-locked Φ-OTDR sensing system," Opt Express **30**, 30312–30330 (2022).
5. N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," IEEE Trans. on Inf. Forensics Secur. **15**, 2692–2705 (2020).
6. R. Namiki and T. Hirano, "Security of quantum cryptography using balanced homodyne detection," Phys. Rev. A **67**, 022308–1–7) (2003).
7. J. F. Dynes, S. J. Kindness, S. W.-B. Tam, *et al.*, "Quantum key distribution over multicore fiber," Opt. Express **24**, 8081–8087 (2016).
8. 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**, 2793–2803 (2019).
9. L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," Phys. Rev. A **82**, 030301 (2010).
10. W. P. Schleich, *Quantum Optics in Phase Space* (Wiley-VCH, Berlin, 2001).
11. R. Loudon, *The Quantum Theory of Light* (Clarendon Press, Oxford, 1983), 2nd ed.
12. A. Vázquez, X. Prieto-Blanco, E. Mateo, and J. Liñares, "2^N-dimensional autocompensating discrete modulation CV-QKD protocol in optical fibers," arXiv: 6707418 [quant-ph] (2025).
13. A. Muller, T. Herzog, B. Huttner, *et al.*, "Plug and play systems for quantum cryptography," Appl. Phys. Lett. **70**, 793–795 (1997).
14. D. S. Bethune and W. P. Risk, "Autocompensating quantum cryptography," New J. Phys. **4**, 42 (2002).
15. Y. Kawamoto, T. Hirano, R. Namiki, *et al.*, "Plug and play systems for quantum cryptography with continuous variables," in *International Quantum Electronics Conference, 2005.*, (2005), pp. 1612–1614.
16. J. Liñares, X. Prieto-Blanco, D. Balado, and G. M. Carral, "Fully autocompensating high-dimensional quantum cryptography by quantum degenerate four-wave mixing," Phys. Rev. A **103**, 043710 (2021).
17. A. Vázquez, X. Prieto-Blanco, E. Mateo, and J. Liñares, "2^N-dimensional autocompensating discrete modulation CV-QKD protocol in optical fibers," Optik (Submitted) (2025).
18. E. Mateo, J. Liñares, X. Prieto-Blanco, and Y. Inada, "A hybrid quantum cryptography method for submarine optical communications," in *Suboptic 2023, Conference Proceedings,* (2023), pp. WE3A:1–5.
19. B. Huttner, R. Alléaume, E. Diamanti, *et al.*, "Long-range qkd without trusted nodes is not possible with current technology," npj Quantum Inf. **8**, 108 (2022).
20. A. Vázquez, X. Prieto-Blanco, J. Liñares, *et al.*, "Comparison between few-mode and multi-core fibers for protection against tapping," in *Suboptic 2025, Conference Proceedings,* (2025), pp. NG01:1–5.
21. D. Lee, *Electromagnetic Principles of Integrated Optics* (Wiley, New York, 1986).
22. R. T. Schermer and J. H. Cole, "Improved bend loss formula verified for optical fiber by simulation and experiment," IEEE J. Quantum Electron. **43**, 899–909 (2007).
23. K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," IEEE Wirel. Commun. **18**, 6–12 (2011).
24. N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," IEEE Trans. on Inf. Forensics Secur. **15**, 2692–2705 (2020).