Polarization Diverse True Heterodyne Receiver Architecture for Continuous Variable Quantum Key Distribution

Daniel Pereira, Armando N. Pinto, *Senior Member, IEEE*, and Nuno A. Silva

***Abstract*—We present a polarization diverse receiver architecture for continuous variables quantum key distribution. We demonstrate experimentally that our system is capable of reliably achieving theoretical security against collective attacks, even under very adverse random polarization drift scenarios, and is capable of functioning indefinitely without any user input. We show that, in a similar scenario, a standard CV-QKD system without polarization diversity cannot distribute keys securely. Our receiver architecture forgoes the need for any polarization matching calibrations or feedback loops and is usable in any locally generated local oscillator key distribution system. A theoretical study on the security impact of polarization drift is presented, based on which we show that, when using our polarization diverse receiver, it is possible to achieve the performance of a channel with zero polarization drift.**

***Index Terms*—Continuous variables, quantum key distribution, polarization diverse receiver, true heterodyne.**

I. Introduction

CONTINUOUS Variables Quantum Key Distribution (CV-QKD) tackles the problem of the generation and distribution of symmetric cryptographic keys, without assuming any computational limitations, while employing telecom compatible equipment [1]. However, the amount of information available to an eavesdropper is highly dependent on the excess noise observed in the channel, which demands a careful and precise estimation of noise sources [2]. When implemented over standard optical fibres, one major noise source is random polarization drift in the communication channel, which will degrade the efficiency of the coherent detection scheme [3]. Therefore a polarization drift compensation scheme is strictly necessary for the implementation of efficient and secure CV-QKD systems [2], [4], [5], [6].

Coherent-state CV-QKD typically encodes the information in the phase and amplitude of weak coherent states, thus allowing for implementation with current modulation methods and telecom-based equipment [1], [7]. The first implementations of CV-QKD protocols were carried out by using a transmitted local oscillator (LO) setup [8]. Nevertheless, that was found to be a security loophole, because an eavesdropper could manipulate the LO, thus hiding their tampering on the quantum signal itself [9], [10]. In that scenario, locally generated LO (LLO) techniques, usually employing a relatively high power pilot tone aided by digital signal processing (DSP), are today the most common implementations of CV-QKD systems [9], [10], [11]. In the CV-QKD community, any system that allows for simultaneous measurement of both quadratures is usually dubbed heterodyne, while for the telecommunications community at large heterodyne detection refers to detection systems where the frequencies of the signal and LO are different [12]. In order to distinguish between these two, we refer in this work to telecommunication community's definition of heterodyne detection as *true* heterodyne. Lately, LLO CV-QKD implementations using single-sideband modulation with true heterodyne detection have been proposed, avoiding low-frequency noise [9], [10]. In order to further maximize noise rejection, CV-QKD implementations using root-raised-cosine (RRC) signal modulation have been explored [9]. Nevertheless, those implementations do not consider the impact of polarization mismatch between the quantum signal and the LO. Random polarization drift occurs naturally in fibres subjected to vibrations, temperature fluctuations, among others [13]. Misalignments between the polarizations of the two laser fields interfering in the coherent detection scheme will severely reduce the efficiency of the detection scheme employed [3], [9]. In CV-QKD communication systems, polarization drift is typically avoided, during a limited time window, by manually aligning the polarization of the signal with that of the LO [9], [10]. This may be appropriate in a laboratory environment, where the system may be assembled in an air-conditioned environment and on devices such as optical tables, and thus stability times are typically in the range of hours [3]. However, in field deployed fibres, especially aerially deployed ones, this stability will be on the order of minutes [13]. A CV-QKD system using an electronic polarization controller coupled

Manuscript received 11 May 2022; revised 26 July 2022 and 6 October 2022; accepted 20 October 2022. Date of publication 25 October 2022; date of current version 15 January 2023. This work was supported in part by Fundação para a Ciência e a Tecnologia (FCT) through national funds, in part by the European Regional Development Fund (FEDER) through Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework, under Ph.D. Grant SFRH/BD/139867/2018, in part by QuantumPrime Project under Grant PTDC/EEI-TEL/8017/2020, in part by action QuRUNNER and QUESTS Project under Grant UIDB/50008/2020-UIDP/50008/2020, and in part by QuantaGenomics Project under Grant QuantERA/0001/2021. *(Corresponding author: Daniel Pereira.)*

Daniel Pereira and Armando N. Pinto are with the Instituto de Telecomunicações, 3810-193 Aveiro, Portugal, and also with the Department of Electronics, Telecommunications and Informatics, University of Aveiro, 3810-193 Aveiro, Portugal (e-mail: danielfpereira@ua.pt; anp@ua.pt).

Nuno A. Silva is with the Instituto de Telecomunicações, 3810-193 Aveiro, Portugal (e-mail: nasilva@ua.pt).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JLT.2022.3216754.

Digital Object Identifier 10.1109/JLT.2022.3216754

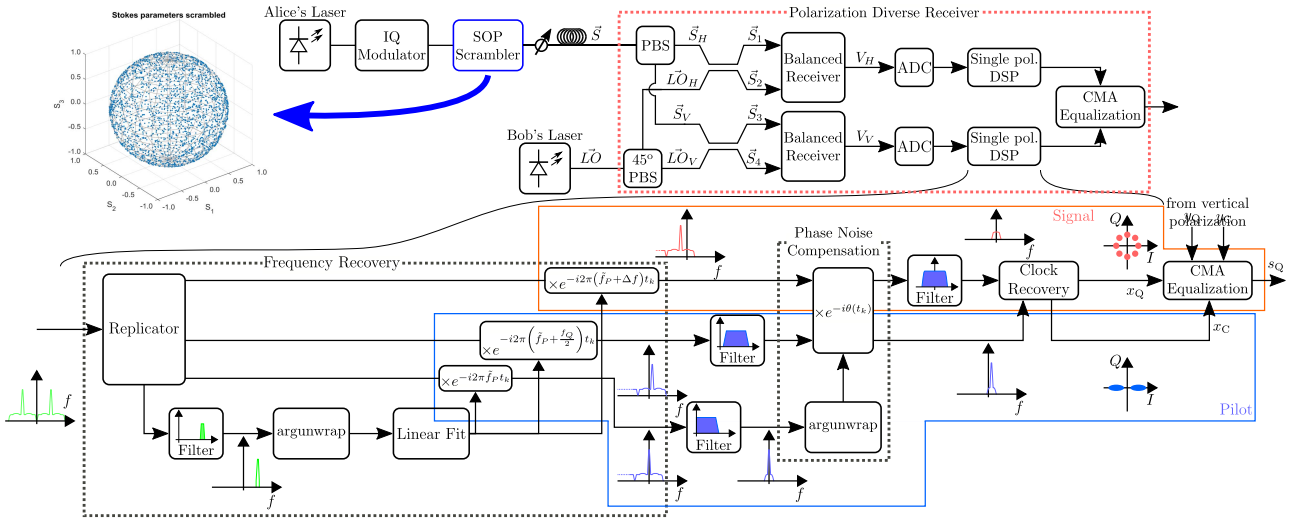

Fig. 1. Block diagram of the experimental system, the polarization diverse receiver system is highlighted.

with a dynamic feedback system was proposed in [3], using a transmitted LO design. However, this solution increases cost and introduces experimental complexity. Conversely, in classical communications, random polarization drift is compensated for by detecting both polarizations of the incoming light field and then compensating for the time-evolving drift in DSP [14]. A system employing DSP aided polarization mismatch recovery was presented in [4], using two optical hybrids coupled with four balanced coherent receivers.

A polarization diverse receiver setup employing true heterodyne detection, for use in CV-QKD applications, is presented, requiring only two balanced receivers. The use of heterodyne detection allows us to use half the number of balanced coherent receivers than the system presented in [4], effectively halving the power requirements of the receiver. This is, to the best of our knowledge, the first demonstration of a true heterodyne polarization diverse receiver for CV-QKD systems. The presented system is able to achieve secure transmissions even in very adverse random polarization drift scenarios.

This work is organized as follows. We begin by fully describing our experimental system and the corresponding digital signal processing (DSP) utilized. Secondly, we study the impact of our receiver setup on the system's security. We then present and discuss experimental results extracted from the previously described system, showing the evolution of its estimated channel transmission, excess noise and secure key-rate. We finalize this work with a summary of the major conclusions.

II. System Description

A block diagram of our system is presented in Fig. 1. Alice starts by modulating the optical signal that she extracts from her local coherent source, which consists of a Yenista OSICS Band C/AG TLS laser, tuned to 1550.006 nm. RRC modulation is chosen because of the possibility of using matched filtering at the receiver without inter-symbolic interference [14], thus allowing for optimum Gaussian white-noise minimization. The symbol rate was set at 38.4 MBd, with an 8-phase-shift keying (8-PSK) constellation, the security of which, in the asymptotic regime, was established in [15] and has since been updated in [16]. In order to avoid the high levels of noise present in the low frequency part of the electromagnetic spectrum [17], the RRC signal is up-converted in the transmitter to an intermediate frequency, $f_Q = 38.4$ MHz. Furthermore, this signal is frequency multiplexed with a DC pilot tone, i.e. $f_P = 0$ Hz, which will be used for frequency and phase recovery at the receiver. This signal is fed into a Texas Instruments DAC39J84EVM digital to analog converter (DAC), which in turn drives a u2t Photonics 32 GHz single polarization IQ modulator coupled with a SHF807 RF amplifier and a YYLabs software bias controller. The single polarization modulated signal is first passed through a Thorlabs PL100S State Of Polarization (SOP) Locker/Scrambler, which allows us to scramble the polarization state of the signal. The action of the SOP Locker/Scrambler in scrambled mode is visible in the Poincaré sphere included as an inset. The results for this sphere were taken during 2 minute period. Note that the SOP Locker/Scrambler is used in order to emulate the polarization drift that would be observed in the field, thus it is not an integral part of the system and during normal operation it would not be included. After scrambling, the signal is then attenuated using a Thorlabs EVOA1550F variable optical attenuator until the signal has, on average 0.33 photons, per symbol. This value is calibrated by connecting the system in a back-to-back configuration and estimating the channel transmission. As in a back-to-back configuration the channel transmission is 1, any deviation from that value is actually a deviation from the desired output channel power. In a field implementation, this could be accomplished by having a copy of the receiver architecture at Alice's side or by using an optical spectral analyser. The signal is then sent through a single-mode fibre spool with a length of 40 km before arriving at the receiver. At the receiver side, the signal is first passed through a PBS, splitting its polarizations and sending each to different 50/50 beam-splitters, where they are mixed with the LO. The LO consists of a Yenista OSICS

Band C/AG TLS laser tuned to 1549.999 nm, in this situation the signals have a frequency shift of $f_S \approx 1$ GHz, a value chosen to coincide with the flattest region of the balanced detectors' frequency response. The LO is also passed through a PBS, this one with its fast-axis shifted 45° in relation to the polarization alignment of the laser, effectively sending half the power to each individual 50/50 beam-splitter. Both 50/50 beam-splitters are polarization maintaining, ensuring that the polarization of both the signal and LO mixed in each match. The outputs of each 50/50 beam-splitter are fed into a pair of Thorlabs PDB480C-AC balanced optical receivers, connected to the inputs of a Texas Instruments ADC32RF45EVM ADC board, which is running at a sample rate of 2.4576 GS/s. The digitized signal is then fed into the DSP stage, which is also presented in Fig. 1. The bulk of the DSP is performed independently for each polarization, before the recovered constellations from each polarization are combined in a constant modulus algorithm (CMA) step.

The DSP is applied offline in a computer, starting by performing frequency recovery, where four copies of the signal obtained from the ADC are taken and a tight digital pass-band filter, centered at $\tilde{f}_P = f_P + f_S$, is applied to one of them. Extracting the phase from this filtered signal and fitting it against a time-vector will yield an estimation for $\tilde{f}_P$. One of the other copies from the original signal is then downconverted by multiplying it by the complex oscillator $e^{-i2\pi\tilde{f}_P t_k}$, where t_k is a time-vector, thus placing the pilot signal close to base band. This signal will later be used for phase noise compensation. The third copy of the original signal is downconverted by another complex oscillator of the form $e^{-i2\pi(\tilde{f}_P+\frac{f_Q}{2})t_k}$, which will cause the pilot to be located at roughly $\frac{f_Q}{2}$. This signal will later be used for clock recovery and aid in the CMA step. The fourth and final copy of the original signal is downconverted by a third complex oscillator of the form $e^{-i2\pi(\tilde{f}_P+\Delta f)t_k}$, where $\Delta f = f_Q - f_P$, resulting in the oscillator taking the explicit form $e^{-i2\pi(f_Q+f_S)t_k}$, this places the quantum signal at close to base band. Note that the estimation of $\tilde{f}_P$ is assumed to contain errors.

The frequency compensated pilot and clock signals are then passed through a low-pass and a band-pass filter, respectively. This filtering step will both reduce the noise present in the signals and isolate them from each other. The phase of the filtered pilot signal, which is equal to the phase mismatch between the two lasers apart from a constant value, which in turn is obtained during an initial calibration stage, is then extracted and used to compensate for the phase noise in both the quantum signal and the clock. Since the pilot and signal are sampled at the same instant, the phase mismatch estimated from the former will equal that of the latter, thus residual phase noise will arise mainly from amplitude noise degrading the accuracy of the estimation [9]. The phase compensated quantum signal is then passed through its own matched filter. The filtering stage on the quantum signal is postponed until after the phase compensation step, this is done because small errors in the frequency estimate can be corrected by the phase noise compensation and application of the matched filter on the signal while it is not at base band may cause distortion in the final obtained constellation.

Finally, the filtered clock is used to re-sample both itself and the filtered quantum signal to one sample per symbol, with one sample being taken of each for every 0 of the imaginary component of the clock signal. At the end of this clock recovery step we are in the possession of four constellations, two corresponding to the clock constellations of the clock signal, x_{C} and y_{C}, and two to the quantum signal ones, x_{Q} and y_{Q}.

These four constellations are then fed into the CMA algorithm, which follows a modified version of the method presented in [14]. Sliding blocks of N samples of each of the four constellations are isolated, taking the form of the column vectors

$$\vec{x}_{\mathrm{Ci}}(n) = [x_{\mathrm{C}}(n)\, x_{\mathrm{C}}(n-1) \ldots x_{\mathrm{C}}(n-N)]^T, \tag{1}$$

$$\vec{y}_{\mathrm{Ci}}(n) = [y_{\mathrm{C}}(n)\, y_{\mathrm{C}}(n-1) \ldots y_{\mathrm{C}}(n-N)]^T, \tag{2}$$

$$\vec{x}_{\mathrm{Qi}}(n) = [x_{\mathrm{Q}}(n)\, x_{\mathrm{Q}}(n-1) \ldots x_{\mathrm{Q}}(n-N)]^T, \tag{3}$$

$$\vec{y}_{\mathrm{Qi}}(n) = [y_{\mathrm{Q}}(n)\, y_{\mathrm{Q}}(n-1) \ldots y_{\mathrm{Q}}(n-N)]^T. \tag{4}$$

At the start of the algorithm, i.e. blocks $\vec{x}_{\mathrm{Ci,Qi}}(0)/\vec{y}_{\mathrm{Ci,Qi}}(0)$, are composed of all zeros except for the first element, which will consist of the first element of the corresponding constellation. The other elements of the sliding blocks are then progressively filled up. The blocks for each signal are concatenated, resulting in the input column vectors [14]

$$\vec{u}_{\mathrm{Ci}}(n) = [\vec{x}_{\mathrm{Ci}}(n);\, \vec{y}_{\mathrm{Ci}}(n)], \tag{5}$$

$$\vec{u}_{\mathrm{Qi}}(n) = [\vec{x}_{\mathrm{Qi}}(n);\, \vec{y}_{\mathrm{Qi}}(n)]. \tag{6}$$

Two N-tap filters are created, $\vec{h}_{\mathrm{x}}$ and $\vec{h}_{\mathrm{y}}$, consisting also of column vectors. At the start of the algorithm the first element of $\vec{h}_{\mathrm{x}}$ and $\vec{h}_{\mathrm{y}}$ is set to $\frac{1}{\sqrt{2}}$, with all the others being 0. These two filters are concatenated,

$$\vec{h} = [\vec{h}_{\mathrm{x}};\, \vec{h}_{\mathrm{y}}], \tag{7}$$

with the resulting filter being applied to the input column vectors following

$$s_{\mathrm{C}}(n) = \vec{h}^{\dagger} \cdot \vec{u}_{\mathrm{Ci}}(n), \tag{8}$$

$$s_{\mathrm{Q}}(n) = \vec{h}^{\dagger} \cdot \vec{u}_{\mathrm{Qi}}(n), \tag{9}$$

which correspond to the clock and quantum output constellations, respectively. Note that both $\vec{h}$ and $\vec{u}_{\mathrm{Ci,Qi}}(n)$ are $2N \times 1$ column vectors, so for each of the inner products in (8) and (9), one output constellation point will be generated. After each step n, the "error," ε, of the algorithm is computed through [14]

$$\varepsilon = \mathrm{E}[|\vec{x}_{\mathrm{C}}|] + \mathrm{E}[|\vec{y}_{\mathrm{C}}|] - s_{\mathrm{C}}(n), \tag{10}$$

which measures the distance of the amplitude of the latest output point of the clock constellation to the expected clock constellation amplitude. This "error" is then used to update the filter $\vec{h}$ through [14]

$$\vec{h} = \vec{h} + \mu\varepsilon s_{\mathrm{C}}^{*}(n)\vec{u}_{\mathrm{C}}(n) \tag{11}$$

The output clock constellation can then be discarded, while the quantum output constellation is carried forward. Due to our CMA algorithm working based on the pilot tone, more precisely the clock constellation, it is expected to be agnostic,

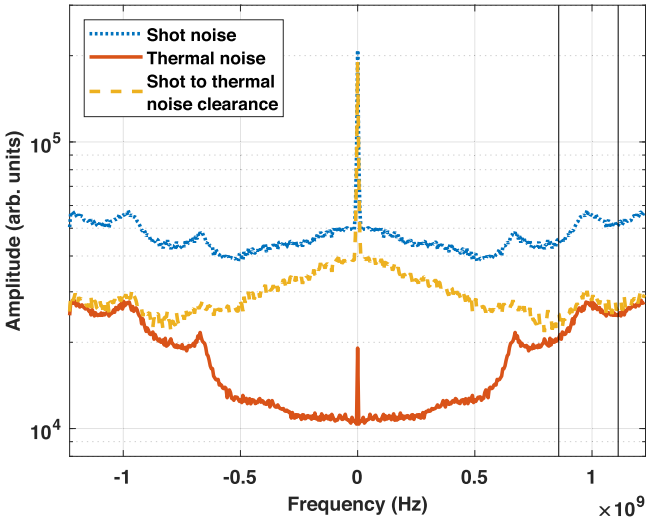

Fig. 2. Spectra of the thermal and shot noise snapshots taken from the experimental system. The spectral region occupied by the data snapshots in this work are delimited by the vertical black lines.

i.e. applicable to any constellation that may be chosen for the quantum signal. The performance of this system in high power was presented previously in [18].

The next step is to estimate Bob's receiver noise. The shot and thermal noise estimations were made with recourse to a capture of the receiver output with the transmitter laser turned off and with both lasers turned off, respectively. To obtain precise shot and thermal noise figures, the same DSP that was applied to the quantum signal was applied to the shot and thermal noise captures obtained previously, with the noise captures being down converted, phase compensated and filtered before their variance was computed. This was necessary because both are highly dependent on their spectral position, as can be seen in their spectra, shown here in Fig. 2, corresponding to the absolute value of the Fourier transform of the noise outputs. To better illustrate the dominance of the shot noise over the thermal noise in our receiver, we also show in Fig. 2 the spectrum of the shot to thermal noise clearance, which is obtained by subtracting the thermal noise spectrum from the shot noise one. Furthermore, we indicate the bandwidth utilized for data transmission in this experiment with two vertical lines. Since we cannot measure the shot noise without also including the thermal noise, the latter was obtained first and its value was subtracted from the variance of the former, yielding an estimate for the true shot noise. The variance of the shot and thermal noise signals, named here σ^2_{shot} and $\sigma^2_{\text{thermal}}$ respectively, are both expressed in ADC counts. Thermal noise is converted to shot noise units (SNU) by dividing it by the shot noise estimate σ^2_{shot}, explicitly

$$\epsilon_{\text{thermal}} = \frac{\sigma^2_{\text{thermal}}}{\sigma^2_{\text{shot}}}. \tag{12}$$

The signal output by Bob's DSP is also converted to SNU, this in turn is accomplished by dividing the ADC count output by $\sqrt{\sigma^2_{\text{shot}}}$. Bob's and Alice's states, b and a respectively, are related by the normal linear model [9]:

$$b = ta + z, \tag{13}$$

where a is assumed to be normalized such that $\mathrm{E}\{|a|^2\} = 1$, $t = \sqrt{\eta T 2 \langle n \rangle}$, where η is the quantum efficiency of Bob's detection system, T is the channel transmission and $\langle n \rangle$ is the average number of photons per symbol. z is the model's noise contribution, which follows a normal distribution with null mean and variance $\sigma^2 = 2 + 2\epsilon_{\text{thermal}} + \eta T \epsilon$, where ϵ is the excess channel noise. In (13), a is generated by Alice when she chooses the symbols to send, while b corresponds to Bob's output constellation after it has been converted to SNU. Moreover in (13), t and σ^2 can be estimated through [9]

$$\tilde{t} = \mathrm{Re}\left\{\frac{\sum_{i=1}^{N} a_i b_i^*}{N}\right\}, \qquad \tilde{\sigma^2} = \frac{\sum_{i=1}^{N} |b_i - \tilde{t} a_i|^2}{N}, \tag{14}$$

the transmission and excess noise are then estimated through

$$\tilde{T} = \frac{\tilde{t}^2}{\eta 2 \langle n \rangle}, \qquad \tilde{\epsilon} = \frac{\tilde{\sigma}^2 - 2 - 2\epsilon_{\text{thermal}}}{\eta \tilde{T}}. \tag{15}$$

In this work we have used $\eta = 0.72$, value taken from the device datasheet. Meanwhile, $\tilde{\epsilon}$ and $\epsilon_{\text{thermal}}$ were dynamically estimated for each measurement run. Note that, in removing the thermal noise from the noise variance estimate in (15), we are assuming the thermal noise to be trustworthy. The estimations of the channel parameters, thermal and shot noises have a finite precision, as a result they have an associated confidence interval. For security reasons, the confidence bound of each estimation that give the most advantage to Eve should be used, as these establish the most secure key [19]. However, considering the purpose of this work, the most likely values were used.

III. Security Impact of Polarization Drift

Protocol security is evaluated following the methodology presented in [15] and updated in [16]. As part of this proof the prepare and measure scheme is first converted to an equivalent entanglement based one. In the following development we assume an ideal scenario, where the polarization beam-splitters split the polarizations with perfect 90° of separation and both employed receivers exhibit the same quantum efficiency and gain. The achievable secret key rate is given by

$$K = \beta I_{\text{BA}} - \chi_{\text{BE}}, \tag{16}$$

where β is the reconciliation efficiency, I_{BA} is the mutual information between Bob and Alice, given by [15]

$$I_{\text{BA}} = \log_2\left(1 + \frac{2T\eta \langle n \rangle}{2 + T\eta\epsilon + 2\epsilon_{\text{thermal}}}\right). \tag{17}$$

The mutual information between Alice and Bob for each polarization channel can be obtained by taking (17) and scaling the transmission by the angle projection

$$I_{\text{BA,H}} = \log_2\left(1 + \frac{2T\cos^2(\theta)\eta \langle n \rangle}{2 + T\cos^2(\theta)\eta\epsilon + 2\epsilon_{\text{thermal}}}\right), \tag{18}$$

$$I_{\text{BA,V}} = \log_2\left(1 + \frac{2T\sin^2(\theta)\eta \langle n \rangle}{2 + T\sin^2(\theta)\eta\epsilon + 2\epsilon_{\text{thermal}}}\right), \tag{19}$$

where θ is the angle between the polarization of the quantum signal at the output of the fibre and that of the LO. In (16), χ_{BE} describes the Holevo bound that majors the amount of information that Eve can gain on Bob's recovered states, being obtained through [15].

$$\chi_{\text{BE}} = \sum_{i=1}^{2} G\left(\frac{\mu_i - 1}{2}\right) - \sum_{i=3}^{4} G\left(\frac{\mu_i - 1}{2}\right), \tag{20}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$. In (20), $\mu_{1,2}$ are the symplectic eigenvalues of the covariance matrix describing the states shared by Alice and Bob while $\mu_{3,4}$ are the non-unitary symplectic eigenvalues of the covariance matrix that describes Bob's projective measurement.

For this development, we assume that Alice modulates only the horizontal polarization. The covariance matrix of the two-mode system at the output of Alice's system is given by [15]

$$\gamma_{\text{A}} = \begin{bmatrix} V\mathbb{I}_2 & Z\sigma_Z \\ Z\sigma_Z & V\mathbb{I}_2 \end{bmatrix}, \tag{21}$$

where V is the variance of the signal at the output of the transmitter, Z is a measure of the covariance between the mode Alice keeps and the one she sends to the fibre, $\mathbb{I}_2$ is the 2×2 identity matrix and $\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. In order to study the effects of polarization drift, we expand γ_A by adding another mode, corresponding to the channel's vertical polarization

$$\gamma_{\text{A,MP}} = \begin{bmatrix} V\mathbb{I}_2 & Z\sigma_Z & 0 \\ Z\sigma_Z & V\mathbb{I}_2 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \tag{22}$$

Note that, in these matrices of matrices, the 0 represent a 2×2 matrix of zeros. The matrix that describes the channel's polarization rotation by θ degrees is defined as [20]

$$J_{\text{Ch}} = \begin{bmatrix} \cos(\theta)\mathbb{I}_2 & \sin(\theta)\mathbb{I}_2 \\ -\sin(\theta)\mathbb{I}_2 & \cos(\theta)\mathbb{I}_2 \end{bmatrix}, \tag{23}$$

where we have included the identity matrices, $\mathbb{I}_2$, to separate the effect along the real and imaginary parts of the signal, we assume that the polarization rotation does not cause cross-talk between the two. Combining this matrix with that of a beam-splitter with transmission coefficient T, yields the matrix that describes the full channel's action, both transmission and a polarization rotation, given by

$$\Lambda_{\text{Ch}} = \begin{bmatrix} \sqrt{T}J_{\text{Ch}} & \sqrt{1-T}J_{\text{Ch}} \\ \sqrt{1-T}J_{\text{Ch}} & \sqrt{T}J_{\text{Ch}} \end{bmatrix}. \tag{24}$$

The full system with the unmixed noise mode is represented by the following covariance matrix

$$\gamma_N = \gamma_A \oplus \begin{bmatrix} (1 + \frac{T}{1-T}\epsilon)\mathbb{I}_2 & 0 \\ 0 & 0 \end{bmatrix}. \tag{25}$$

We assume here that the excess noise at the input of the channel is contained only in the horizontal polarization and that this noise will be distributed by the channel, alongside the signal. This corresponds to assuming that Eve has access to the signal at Alice's system output, before any polarization drift has occurred, and that she then causes the polarization rotation. Applying the channel transmission matrix to (25) as

$$\gamma'_N = (\mathbb{I}_2 + \Lambda_{\text{Ch}})^T \gamma_N (\mathbb{I}_2 + \Lambda_{\text{Ch}}), \tag{26}$$

where $\cdot^T$ indicates the transpose matrix. Equation (26) returns the modes at the output of the transmission channel, and selecting Alice's and Bob's modes returns

$$\gamma_{\text{AB,MP}} = \begin{bmatrix} V\mathbb{I}_2 & \sqrt{T}\cos(\theta)Z\sigma_Z & \sqrt{T}\sin(\theta)Z\sigma_Z \\ \sqrt{T}\cos(\theta)Z\sigma_Z & \cos^2(\theta)V_B\mathbb{I}_2 & \cos(\theta)\sin(\theta)V_B\mathbb{I}_2 \\ \sqrt{T}\sin(\theta)Z\sigma_Z & \cos(\theta)\sin(\theta)V_B\mathbb{I}_2 & \sin^2(\theta)V_B\mathbb{I}_2 \end{bmatrix}, \tag{27}$$

where

$$V_B = TV + 1 - T + T\epsilon. \tag{28}$$

By choosing either Bob's horizontal or vertical polarization, we obtain the covariance matrix for each channel individually

$$\gamma_{\text{AB,H}} = \begin{bmatrix} (V_{\text{A}} + 1)\mathbb{I}_2 & \sqrt{T}\cos(\theta)Z\sigma_Z \\ \sqrt{T}\cos(\theta)Z\sigma_Z & \cos^2(\theta)V_B\mathbb{I}_2 \end{bmatrix}, \tag{29}$$

$$\gamma_{\text{AB,V}} = \begin{bmatrix} (V_{\text{A}} + 1)\mathbb{I}_2 & \sqrt{T}\sin(\theta)Z\sigma_Z \\ \sqrt{T}\sin(\theta)Z\sigma_Z & \sin^2(\theta)V_B\mathbb{I}_2 \end{bmatrix}. \tag{30}$$

Following the methodology described in [15] to obtain $\mu_{1,2,3,4}$, we can obtain the mutual information between Eve and Bob for each polarization channel. From these mutual informations obtained from both (18)–(19) and (29)–(30), we can define the key rates that would be obtained if Bob were to monitor only one of the polarization channels

$$K_{\text{H}} = \beta I_{\text{BA,H}} - \chi_{\text{BE,H}}, \tag{31}$$

$$K_{\text{V}} = \beta I_{\text{BA,V}} - \chi_{\text{BE,V}}. \tag{32}$$

We can now trace both key rates in function of the polarization angle, results shown here in Fig. 3, alongside the key rate expected from a channel without polarization drift. From the results in Fig. 3, we can see the key rate's dependence on the polarization drift angle, with the key rate of each individual polarization channel exhibiting a maximum when the signal's polarization is aligned to it (polarization angles of $n\pi$ for the horizontal channel and of $(2n+1)\pi$ for the vertical channel, $n \in \mathbb{N}$), and decreasing until it reaches a negative value as it misaligns. The maximum value corresponds to the key rate of the ideal, non-rotating channel. Note that these key rates should not be understood as independent from each other, but rather as the key rates that would be observed if Bob were to monitor only one of the polarization channels.

The application of a CMA-like algorithm to achieve full random drift polarization compensation can be described by the rotator matrix

$$\Lambda_{\text{CMA}} = \begin{bmatrix} h_{xx}\mathbb{I}_2 & h_{xy}\mathbb{I}_2 \\ h_{yx}\mathbb{I}_2 & h_{yy}\mathbb{I}_2 \end{bmatrix}, \tag{33}$$

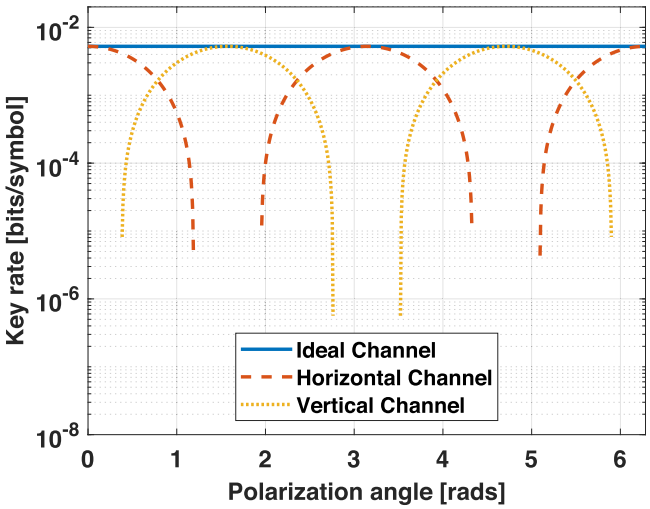

Fig. 3. Key rate in function of the polarization angle for the vertical and horizontal polarization "channels". These key rates are not independent from each other, rather they are the key rates that would be observed if Bob were to monitor only one of the polarization channels. Parameters assumed were $\beta = 0.95$, $T = 0.1585$, $\epsilon = 0.03$ SNU, $\epsilon_{\text{th}} = 0.35$ SNU, $\langle n \rangle = 0.33$.

to the multi-polarization covariance matrix (27). Parameters h_{xx} and h_{xy} are analogous to the vectors $\vec{h}_{\text{x}}$ and $\vec{h}_{\text{y}}$ from (7). Since we wish to recover the signal onto one of the polarizations, we can simplify (33) to

$$\Lambda_{\text{CMA}} = \begin{bmatrix} h_{xx}\mathbb{I}_2 & h_{xy}\mathbb{I}_2 \\ 0 & 0 \end{bmatrix}. \tag{34}$$

Since Bob controls this process, he can force h_{yx} and h_{yy} to be 0. Applying this rotator to (27) we get

$$\begin{aligned} \gamma'_{\text{AB,MP}} &= (\mathbb{I}_2 \oplus \Lambda_{\text{CMA}})^T \gamma_{\text{AB,MP}} (\mathbb{I}_2 \oplus \Lambda_{\text{CMA}}) \\ &= \begin{bmatrix} (V_{\text{A}}+1)\mathbb{I}_2 & & \\ \sqrt{T}(h_{xx}\cos(\theta) + h_{yx}\sin(\theta))Z\sigma_Z & & \\ 0 & & \end{bmatrix} \\ &\quad \begin{bmatrix} \sqrt{T}(h_{xx}\cos(\theta) + h_{yx}\sin(\theta))Z\sigma_Z & 0 \\ (h_{xx}\cos(\theta) + h_{yx}\sin(\theta))^2 V_{\text{B}}\mathbb{I}_2 & 0 \\ 0 & 0 \end{bmatrix}. \end{aligned} \tag{35}$$

Note that the noise present in the two input polarization modes now appears in the recovered polarization mode. By discarding the empty polarization modes from (35), and setting $h_{xx} = \cos(\theta)$ and $h_{yx} = \sin(\theta)$, we obtain the final covariance matrix

$$\gamma_{\text{AB}} = \begin{bmatrix} (V_{\text{A}}+1)\mathbb{I}_2 & \sqrt{T}Z\sigma_Z\sqrt{T}Z\sigma_Z & V_{\text{B}}\mathbb{I}_2 \end{bmatrix}, \tag{36}$$

which corresponds directly to the covariance matrix in [16], apart from $\sqrt{T}$ having been put in evidence. From this development we see that, assuming an ideal performance of the DSP stage, our CMA implementation is transparent to the covariance matrix, thus having no effect on security. A non-ideal performance of the CMA DSP step would result in the h_{xx} and h_{yx} parameters not equalling $\cos(\theta)$ and $\sin(\theta)$, respectively, but rather to follow some other angle ϕ. This would result in a degradation of the observed channel transmission, described here by the parameter

TABLE I
CHANNEL TRANSMISSIONS FOR SINGLE POLARIZATION AND RECOVERED CHANNELS

Channel	$\text{E}\left[\tilde{T}\right]$	$\text{Var}\left[\tilde{T}\right]$
Horizontal	0.088	0.0064
Vertical	0.068	0.0047
Recovered Channel	0.113	0.0014
Actual Transmission	**0.116**	

$\eta_{\text{DSP}} = \cos(\phi)\cos(\theta) + \sin(\phi)\sin(\theta)$, from which definition it can be shown that $|\eta_{\text{DSP}}| \leq 1$. Since the same CMA DSP that is applied to the signal is then applied to the shot and thermal noise figures, the effect of the non-ideal application of the DSP will also be present in the shot noise estimate, thus its contribution in (28) will still be read as 1 and (36) becomes

$$\gamma_{\text{AB, non ideal}} = \begin{bmatrix} (V_{\text{A}}+1)\mathbb{I}_2 & \sqrt{\eta_{\text{DSP}}T}Z\sigma_Z \\ \sqrt{\eta_{\text{DSP}}T}Z\sigma_Z & (\eta_{\text{DSP}}TV + 1 - \eta_{\text{DSP}}T + \eta_{\text{DSP}}T\epsilon)\mathbb{I}_2 \end{bmatrix}, \tag{37}$$

from which we see that a non-ideal application of the CMA step will result in a degradation of the observed channel transmission. This degradation does not give any advantage to Eve, but rather reduces the system's performance.

IV. EXPERIMENTAL RESULTS

The system was run freely for a half hour in scrambled mode and, for comparison purposes, fifteen minutes in unscrambled mode, with 2 ms snapshots taken every 10 seconds. The usage of the SOP Locker/Scrambler in the scrambled mode allows us to emulate the polarization drift that would be observed during an hours or days long experiment in minutes. This effect can also be observed in the Poincaré sphere included as an inset in Fig. 1, for which we monitored the SOP of the signal prior to the attenuation for only 2 minutes. In this work 200 snapshots were taken in the scrambled scenario and 100 in the unscrambled one, each snapshot containing 65536 symbols. The reduced number of symbols utilized, coupled with the fact that post-processing is done offline, means that our system remains a proof of concept one. Snapshots of the thermal and excess noises were obtained immediately before the data snapshots. The behaviour for the channel transmissions of both the single polarization and the recovered channels, in the scrambled scenario, are presented here in Table I. From the results in Table I we can see that the single polarization channels exhibit a much lower average transmission and much higher variance of the transmission estimates, when compared to the values observed for the recovered channel. The average estimated transmission obtained from the constellations is also very close to the transmission that was measured a-priori, which took into account both the losses of the 40 km spool and in the receiver, which were measured as 8.32 dB and 1.03 dB, respectively, corresponding to a transmission of 0.116. In Fig. 4 we present the values of the estimated excess noise in the recovered channel observed for each of the 200 results taken

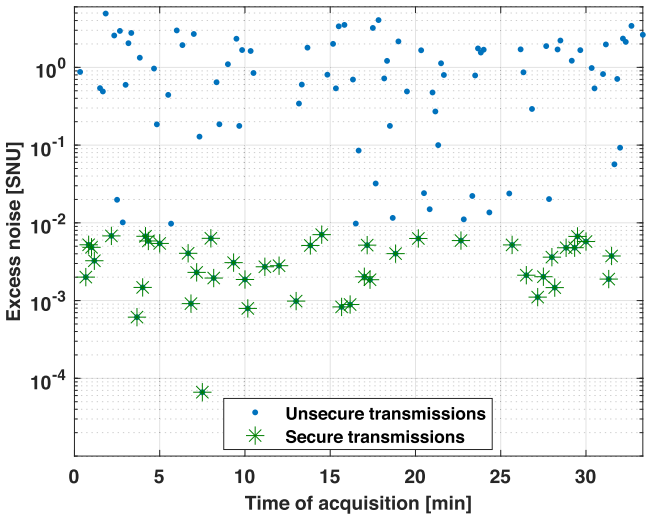

Fig. 4. Evolution of the estimated excess noise for the 200 results taken. Situations where the a secure key was able to be transmitted are highlighted with green asterisks. Note that these results were taken considering the use of a state of polarization scrambler, which allows us to emulate the polarization drift that would be observed during days-long field experiment in a matter of minutes.

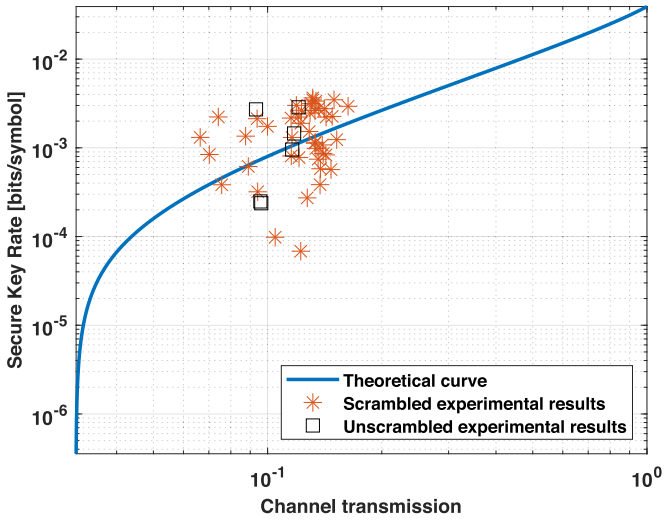

Fig. 5. Achievable key rate, given by (16), for our polarization diverse receiver, with $\beta = 0.95$.

in the scrambled mode. Situations where a secure key was able to be transmitted are highlighted with green asterisks. We can see that our system was able to recover secure keys for the duration of the experiment, with the excess noise being close to 0, apart from some deviations caused by failures in signal recovery. Some situations exhibit negative excess noise, these are not present in Fig. 4 due to the use of a logarithmic scale, these can be attributed to the low number of samples used in this estimation. The average width of the 99% confidence interval for the excess noise estimates is roughly 3.5 SNU, while the average excess noise observed in our system is approximately 0.5 SNU. Nevertheless, negative excess noise estimations are not unheard off, having been reported in [9], and a contributing factor may be time-evolving imbalances of the optical components [6]. Further optimization of the noise calibration step could improve the overall efficiency of the system. Finally, we show the experimentally observed secure key rates in function of channel transmission in Fig. 5, alongside with the corresponding theoretical curve, for which the average values of the observed excess noise and thermal noise were used. Data from both scrambled and unscrambled polarization scenarios is included. We can see that our experimental results closely adhere to the theoretical curve and that the system performs equally in both situations. We see that, in both scenarios, we were able to achieve secure key rates of roughly 0.004 bits/symbol, slightly below that reported in [9], albeit using more accessible components. As mentioned before, the reduced number of symbols utilized, coupled with the fact that post-processing is done offline, means that the security of our system remains a proof of concept one. No secure transmissions were observed for the individual polarization channels.

V. Conclusion

In summary, we present a polarization diverse receiver architecture that avoids the need for manual calibration or complex feedback loops to recover from random polarization drift. We also study the impact of polarization drift on security and show that our system, under an ideal scenario, is capable of fully mitigating it. Our system works by passively monitoring both polarizations continuously and recovering the full channel from the single polarization ones. Our system was capable of working for an indefinite period of time at a transmission distance compatible with metro network connections. Furthermore, this stability is achieved with a relatively simple and inexpensive receiver design. We were able to generate 50 secure keys, in the asymptotic regime, from our 300 snapshots.

References

[1] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, 2002, Art. no. 057902.

[2] F. Laudenbach et al., "Continuous-variable quantum key distribution with Gaussian modulation–the theory of practical implementations," *Adv. Quantum Technol.*, vol. 1, no. 1, 2018, Art. no. 1800011.

[3] W. Liu, Y. Cao, X. Wang, and Y. Li, "Continuous-variable quantum key distribution under strong channel polarization disturbance," *Phys. Rev. A*, vol. 102, no. 3, 2020, Art. no. 032625.

[4] T. Wang, P. Huang, S. Wang, and G. Zeng, "Polarization-state tracking based on Kalman filter in continuous-variable quantum key distribution," *Opt. Exp.*, vol. 27, no. 19, pp. 26689–26700, Sep. 2019. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-27-19-26689

[5] Y. Zhao, Y. Zhang, Y. Huang, B. Xu, S. Yu, and H. Guo, "Polarization attack on continuous-variable quantum key distribution," *J. Phys. B: Atom., Mol. Opt. Phys.*, vol. 52, no. 1, 2018, Art. no. 015501.

[6] D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and N. A. Silva, "Impact of receiver imbalances on the security of continuous variables quantum key distribution," *EPJ Quantum Technol.*, vol. 8, no. 1, pp. 1–12, 2021.

[7] M. Almeida, D. Pereira, N. Muga, M. Facão, A. N. Pinto, and N. A. Silva, "Secret key rate of multi-ring M-APSK continuous variable quantum key distribution," *Opt. Exp.*, vol. 29, no. 23, pp. 38669–38682, 2021. [Online]. Available: https://doi.org/10.1364/oe.439992

[8] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, Dec. 1999, Art. no. 010303. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.61.010303

[9] S. Kleis, M. Rueckmann, and C. G. Schaeffer, "Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals," *Opt. Lett.*, vol. 42, no. 8, pp. 1588–1591, 2017.
[10] F. Laudenbach et al., "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," *Quantum*, vol. 3, p. 193, 2019.
[11] D. B. Soh et al., "Self-referenced continuous-variable quantum key distribution protocol," *Phys. Rev. X*, vol. 5, no. 4, 2015, Art. no. 041010.
[12] H. H. Brunner et al., "A low-complexity heterodyne CV-QKD architecture," in *Proc. 19th Int. Conf. Transp. Opt. Netw.*, 2017, pp. 1–4.
[13] R. Liu et al., "Analysis of polarization fluctuation in long-distance aerial fiber for QKD system design," *Opt. Fiber Technol.*, vol. 48, pp. 28–33, 2019.
[14] M. S. Faruk and S. J. Savory, "Digital signal processing for coherent transceivers employing multilevel formats," *J. Lightw. Technol.*, vol. 35, no. 5, pp. 1125–1141, Mar. 2017.
[15] A. Becir, F. El-Orany, and M. Wahiddin, "Continuous-variable quantum key distribution protocols with eight-state discrete modulation," *Int. J. Quantum Inf.*, vol. 10, no. 01, 2012, Art. no. 1250004.
[16] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum*, vol. 5, p. 540, 2021.
[17] R. B. Tomer, *Getting the Most out of Vacuum Tubes: Electron Tubes Valves*, vol. 2, Indianapolis, IN, USA: Howard W. Sams & Co., 1960.
[18] D. Pereira, N. A. Silva, and A. N. Pinto, "A polarization diversity CV-QKD detection scheme for channels with strong polarization drift," in *Proc. IEEE Int. Conf. Quantum Comput. Eng.*, 2021, pp. 469–470.
[19] A. Leverrier, "Theoretical study of continuous-variable quantum key distribution," Ph.D. dissertation, Télécom ParisTech, Palaiseau, France, 2009.
[20] D. H. Goldstein, *Polarized Light*. Boca Raton, FL, USA: CRC Press, 2017.