ADVANCED QUANTUM TECHNOLOGIES
www.advquantumtech.com

Hybrid Encoder for Discrete and Continuous Variable QKD

*Mattia Sabatini, Tommaso Bertapelle, Paolo Villoresi, Giuseppe Vallone, and Marco Avesani**

Quantum key distribution (QKD) is emerging as a cutting-edge application of quantum technology, gradually integrating into the industrial landscape. Many protocols employing discrete or continuous variables have been developed over time. Whereas the firsts usually excel in covering longer distances, the seconds are typically superior in producing higher secret key rates at short distances. Present efforts aim to create systems that can exploit both these strengths, foreseeing the future challenge regarding the realization of a quantum network consisting of multiple and heterogeneous interconnected nodes. Within such a context, a possible solution is systems able to efficiently toggle between discrete and continuous variable working modes with hybrid quantum state encoders. Therefore, this study presents a new hybrid encoder based on an iPOGNAC modulator, ensuring compatibility with Discrete-Variable (DV) and Continuous-Variable (CV) QKD systems that can be assembled entirely with commercial-off-the-shelf components. The proposed scheme is the first supporting DV polarization protocols, thus making it an appealing candidate for space nodes of a future quantum network, given that polarization-based protocols are well suited for space links.

1. Introduction

One of the main goals of cryptography is to enable confidential and secure communication between two parties over an untrusted channel. To accomplish this, most existing protocols depend on computational security, meaning that they rely on mathematical problems believed to be unfeasible to solve by computers. However, this belief remains unproven, and it is conceivable that an efficient algorithm, whether classical or quantum, may exist to tackle the latter. Quantum Key Distribution (QKD)[1–3] offers a way to overcome the latter limitation by harnessing the principles of quantum mechanics. The approach enables the development of unconditionally secure protocols that can withstand adversaries possessing limitless classical or quantum computational power.

According to the degrees of freedom of the quantum phenomenon used, QKD can be categorized as Discrete Variables (DV) or Continuous Variables (CV).[4–7] The former usually exploits single photons, such as polarization and time-bin, whereas CV uses the quadratures of the quantized electromagnetic field. The BB84 protocol pioneered DV-QKD.[8] It relies on single photon sources and non-orthogonal states for information encoding. Over time, it was refined and underwent several improvements, such as decoy states to counter photon number-splitting attacks[9] and adopting fewer states to ease practical implementation.[10] For CV-QKD, GG02 is the protocol of reference.[11] It employs Gaussian states to encode the secret key and coherent detection to measure them. However, significant practical limitations hinder its adoption, such as requiring a continuous Gaussian modulator, low reconciliation efficiency, and computationally demanding error correction procedures.[12] These challenges can be mitigated using coherent state discrete constellation modulation protocols.[13,14] However, this comes at the price of limiting the number of secret bits that can be encoded per symbol, affecting thus the Secret Key generation Rate (SKR) when compared to the original GG02.

Discrete and continuous protocols offer different advantages over the other. DV-QKD is known for its more mature security proofs and ability to cover longer distances, reaching a record of 421 km for a fiber-based BB84 system[15] and 1002 km using the twin-field approach.[16] Conversely, CV-QKD offers higher SKR for short lengths.[17,18] Yet, due to loss sensitivity, the current record distance for fiber systems is limited to 203 km.[19] Nevertheless, compared with DV-QKD, CV systems can benefit from coherent detectors and widely accessible commercial integrated telecom components. The former can work at room temperature and do not suffer from the typical Single Photon Detectors (SPDs) limitations, such as dead-time, commonly used in DV-QKD;[20] a characteristic that positively contributes to the achievable SKR. The second allows the exploitation of a widely consolidated industry, potentially enhancing the accessibility and economic viability of CV-QKD for broad adoption.

M. Sabatini, T. Bertapelle, P. Villoresi, G. Vallone, M. Avesani
Dipartimento di Ingegneria dell'Informazione
Università degli Studi di Padova
via Gradenigo 6B, Padova 35131, Italy
E-mail: marco.avesani@unipd.it

P. Villoresi, G. Vallone, M. Avesani
Padua Quantum Technologies Research Center
Universitá degli Studi di Padova
via Gradenigo 6A, Padova 35131, Italy

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/qute.202400522

DOI: 10.1002/qute.202400522

QKD initially emerged as a technology facilitating safe point-to-point communications. However, progress in the field has now reached the stage where we are beginning to witness efforts to establish QKD networks involving multiple entities.[21–23] Such a quantum network implies the presence of multiple paths, including intermediary relay nodes, linking one end user to another. Consequently, depending on the available routes and the channel's parameter connecting each node, hops may better use DV or CV protocols to maximize the overall SKR. Rather than choosing between two dedicated transmitters, a more efficient strategy is to rely on a hybrid encoder design capable of switching between DV and CV.[24]

This approach offers the possibility of actively reconfiguring the network characteristics in a software-defined manner, thus increasing flexibility and improving the management and integration of QKD into the existing telecom infrastructure. Although dynamically re-configurable and SDN-controlled quantum networks are a relatively recent development, their adoption has accelerated significantly in recent years[25–27] due to initiatives like the EuroQCI program. A prime example of this trend is the MadQCI (Madrid EuroQCI network),[27] which successfully demonstrated dynamic reconfigurability and SDN orchestration in a large-scale, deployed metropolitan network. Thus, we believe the aforementioned factors represent key advantages in designing and implementing scalable QKD networks, particularly in dynamic environments.

In this work, we present the first hybrid encoder designed to be compatible with polarization-based DV and CV QKD protocols. In fact, all the other schemes previously proposed are limited to phase-encoded and time-bin DV systems.[24] The system is realized only with fiber Commercial-Off-The-Shelf (COTS) telecom components and tested using two different setups for DV and CV, each paired with the respective receiver. The paper is structured as follows: Section 2 briefly outlines the working principles of the proposed hybrid encoder, Section 3 describe the experimental setup adopted for CV and DV operations, while in Section 4 the results obtained.

2. Hybrid QKD

2.1. Applications of Hybrid QKD Encoders in Quantum Networks

Today's telecommunication systems rely on cryptographic procedures vulnerable to adversaries holding quantum computing capabilities. This spurred research and industry to develop countermeasures like QKD, a solution devised to ensure Information Theoretic Security (ITS). However, the latter was mostly developed as a point-to-point connection requiring additional specialized infrastructure, which presents some challenges when integrating it into the current telecom grid. Moreover, such an approach encounters scaling issues for deploying QKD networks, as it is costly and increases the complexity of its management. Mitigating such issues is possible by relying on the Software Defined Network (SDN) model that is progressively embraced by telecom providers, given its ability to facilitate the integration of new services within a network infrastructure. Since the success of QKD technology, either CV or DV, will depend on the ability to integrate it within the existing infrastructures, adopting the SDN method becomes appealing due to the aforementioned benefits. Indeed, it should not impose the modification of each network device to establish a quantum link. Additionally, being SDNs centrally supervised, the routes connecting two endpoints can be easily reconfigured by deciding, due to security concerns, upon discrete or continuous mode before starting the secret key exchange and maintaining it until it successfully ends or aborts. When paired with SDNs' inherited ability for real-time network monitoring, which includes quantum metrics for the case, it enables the optimization of the SKR between parties. For instance, Hugues-Salas et al.[28] demonstrated the ability to switch channels amid an attack, while Alia et al.[26] showed link reorganization if the QBER exceeds a certain threshold. The aforementioned flexibility and performance can improve by letting the controller adopt DV or CV QKD protocols for a given intermediate link based on the values of the observed quantum parameters. For example, the controller can utilize CV-QKD for shorter connections as it typically offers higher transmission rates compared to DV-QKD, while preferring the latter for longer distances due to its ability to extend much further with current technology. The method can also better adapt to the already deployed telecommunication infrastructure, which commonly employs multiple wavelengths for communication. Indeed, in such an integrated scenario, quantum and classical channels will likely share the same propagating media. A hybrid strategy can provide the SDN controller with a broader range of options to enhance node-to-node communication and organize the communication considering the particular status of the link.

Within this context, a transmitter equipped with an encoder that can generate both CV and DV quantum states and easily switch between the latter well suits the task. Moreover, such hybrid encoders may be a significantly cheaper alternative to two dedicated units while having a less complex yet compact and more adaptable design that can contribute to better system integration without compromising functionality.

2.2. Hybrid CV-DV Encoder

The hybrid encoder design we introduce relies on the iPOGNAC,[29] a polarization modulator that showed remarkable temporal stability due to a self-compensating Sagnac loop. Such a technique gained attention in the QKD field[30–33] due to its ability to counteract any drifts leading to enhanced stability and simplicity. The iPOGNAC's operational principle can be understood from **Figure 1**. As can be seen, diagonally polarized light pulses are injected into the modulator. The input Beam Splitter (BS) acts like a circulator guiding the transmitted photons to a Polarization Beam Splitter (PBS) through a Polarization Maintaining Fiber (PMF). Then, the PBS outputs are connected to form an asymmetric Sagnac loop comprising a delay line and a phase modulator. The former enables the phase modulator to apply a different phase shift to the horizontal and vertical polarization propagating through the Sagnac loop. Indeed, the light entering the latter from the PBS vertical output travels clockwise. Upon exiting the loop, it emerges horizontally polarized with an additional "early" phase shift ϕ_e induced by the phase modulator. On the other hand, the light entering through the PBS horizontal output moves counterclockwise, gains a "late" phase shift ϕ_l, and exits vertically polarized. The "early" and "late" light pulses

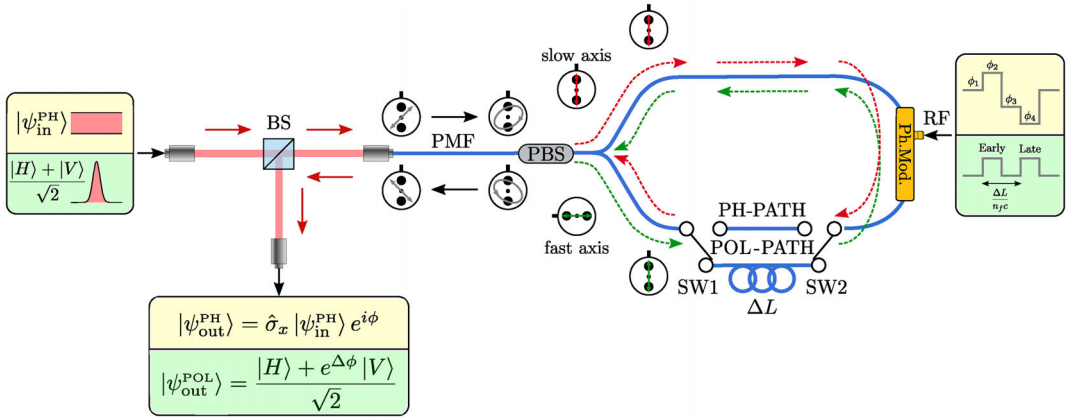

Figure 1. A schematic representation of our proposed hybrid encoder design. The device is set in DV or CV mode according to the optical path selected: POL-PATH for the former and PH-PATH for the second. In the DV configuration, the encoder is the standard iPOGNAC in which the source is a pulsed laser aligned in such a way that the light enters the system diagonally polarized. The latter vertical and horizontal components are spatially and temporally separated by a PBS and an optical delay line ΔL and undergo an early and late phase shift through the phase modulator. The electrical signals required to obtain such phase shifts are square pulses separated by $n_f \Delta L/c$, where n_f is the PMF fiber slow-axis refractive index and c is the speed of light in vacuum. In CV mode, instead, the laser source operates in CW (Continuous Wave), the ΔL is bypassed, and by properly setting the amplitude of the electrical pulses, M-PSK modulation constellations can be obtained.

are recombined at the PBS and travel backward toward the BS. The transmitted component exits the iPOGNAC, up to a global phase, with a polarization state:

$$|\psi_{\text{out}}^{\text{POL}}\rangle = \frac{|H\rangle + e^{i(\phi_l - \phi_e)}|V\rangle}{\sqrt{2}} \tag{1}$$

Notice that by adjusting the phases ϕ_e and ϕ_l, it is possible to generate any balanced superposition of horizontal and vertical polarization states.

By removing the iPOGNAC's delay-line ΔL, the Sagnac loop is now symmetric. In this configuration, the same phase shift is applied simultaneously to both polarizations propagating through such a loop. In a left-handed reference frame whose z-axis is directed toward the photon propagation direction, the PBS and Sagnac loop map $|H\rangle \rightarrow -|V\rangle$ and $|V\rangle \rightarrow |H\rangle$, which is described by the $i\hat{\sigma}_y$ operator. If also the action of the BS is considered, then the device implements a $\hat{\sigma}_x$ operation up to a deterministic global phase. As a result, regardless of the injected polarization state, the output is a fixed transformation of the input with an additional phase shift ϕ set by the phase modulator:

$$|\psi_{\text{out}}^{\text{PH}}\rangle = \hat{\sigma}_x |\psi_{\text{in}}\rangle\, e^{i\phi} \tag{2}$$

allowing thus the implementation of M-PSK (Phase Shift Keying) modulation schemes, where M is the discrete set of ϕ values used. The geometry of the Sagnac loop ensures that, from the phase modulator perspective, both clockwise and counterclockwise components are always aligned with only one of its axis. This prevents the phase of the input's $|H\rangle$ and $|V\rangle$ components from being unevenly modulated due to the modulator's polarization-dependent characteristics. The aforementioned property is also a welcome feature since CV-QKD systems usually employ phase modulators that exhibit unwanted polarization dependency that must be controlled and stabilized with additional equipment.

Since the iPOGNAC and the CV phase encoder differ only by the optical delay line from a hardware perspective, the two can be integrated into a single system. The operational mode of this unified device can be set through two optical switches, SW1 and SW2, as illustrated in Figure 1. Indeed, the latter enables ΔL to be bypassed. Switches SW1 and SW2 can be implemented in different ways. However, since the operating mode is established before starting the QKD protocol and maintained until it is completed successfully or aborted, we do not foresee the need for high performance in terms of speed and latency. Hence, we believe MEMS optical switches will suffice for this particular case. They are straightforward to use, relatively inexpensive, reliable, and have low insertion loss. Furthermore, the latter can also be electrically controllable, which implies that transitioning from DV to CV, or the reverse, can be achieved remotely with ease, in real-time, and without significant effort.

3. Experimental Section

The capabilities of the proposed hybrid scheme were demonstrated using a DV and CV setup, each of which had its corresponding receiver. Given the nature of these experiments and the fact that detectors capable of working for both DV and CV protocols are missing, besides early proposals that may hint to such a direction,[34,35] testing of the switching mechanism was avoided. However, future work will focus on implementing such a mechanism with MEMS technology and assessing it with appropriate experiments.

3.1. CV Setup

A schematic representation of the experimental setup used to test our hybrid encoder in CV mode is represented in **Figure 2**. As can be seen, a 99:1 Beam Splitter (BS-1) divided the light of a single-mode continuous-wave 1550 nm laser with a line-width of $\approx$ 100 kHz. An optical isolator (ISO) was positioned before BS-1 to prevent back-reflected light from causing laser instabilities.

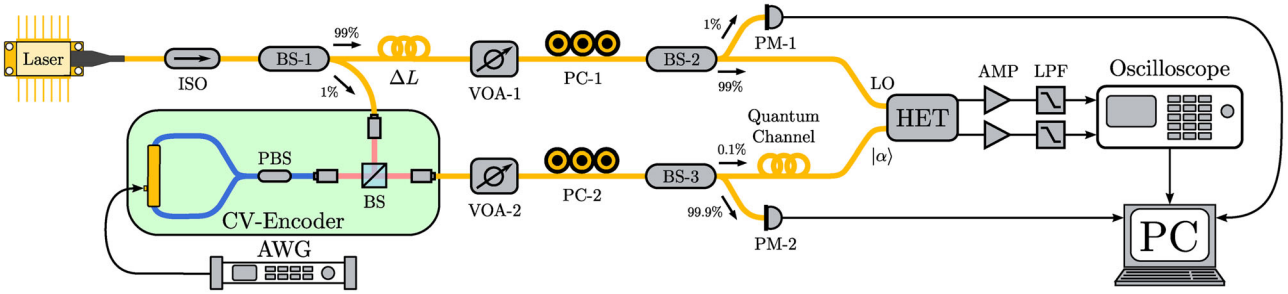

Figure 2. Schematic representation of the CV experimental setup used. The latter consists of a 1550 nm Continuous Wave (CW) laser, the output of which is divided by a 99:1 beam-splitter (BS-1). The majority of such (99%) is directed towards a heterodyne receiver (HET) acting, thus, as a Local Oscillator (LO). The rest (1%) is sent to the CV encoder for CV quantum state phase modulation and then routed, through a fiber quantum channel, to the heterodyne's signal input port. Subsequently, the heterodyne measurements are digitized by an oscilloscope and delivered to a PC for data processing. Notice that additional optical components are present between the 99% BS-1 arm and the HET, as well as between the CV encoder and the HET. The former are required to characterize the heterodyne receiver (such as photodiode linearity and clearance), while the latter attenuate the modulated coherent state generated by the encoder to the quantum level. Finally, the image provides a color-coded representation of the fibers used: blue for single-mode polarization-maintaining and yellow for single-mode non-polarization-maintaining.

Then, 99% of the light from BS-1 was directed to an integrated COTS heterodyne receiver with ≈ 13 10^{B} of clearance, serving as a Local Oscillator (LO). Before entering the receiver, the light passed through a Variable Optical Attenuator (VOA-1), a Polarization Controller (PC-1), and a 99:1 Beam-Splitter (BS-2). This splitter sent 1% of the light to a monitoring Power Meter (PM-1) while the remaining 99% to the photonic chip. The power meter PM-1 and the VOA-1 were required only for calibrating the heterodyne receiver, a procedure in which the linearity of its photodiodes was tested and the parameters to convert the measured heterodyne signals from volt units into shot-noise units were estimated. The polarization controller, instead, is necessary to maximize the amount of optical power coupled into the chip due to the LO inlet being polarization-sensitive. Conversely, the BS-1 1% branch sent the light to the hybrid encoder configured to work in CV. The light from this encoder then traveled through VOA-2, the polarization controller PC-2, and the 99.9:0.1 BS-3. Given the dual-polarization feature of the heterodyne receiver, PC-2 aligned the light polarization state to ensure that only one of the two polarization-dependent heterodyne was used. Moreover, with this cascade the incoming light could attenuate to the required quantum level and monitor such with the PM-2 power meter at the 99.9% branch of BS-3. The BS-3 0.1% branch was subsequently connected to the heterodyne's signal input port through a quantum channel. Notice that the signal and LO paths shared the same 1550 nm laser and maintained identical lengths, with additional ΔL fiber at the LO branch, to minimize phase noise and instabilities at the receiver. Since the objective was to evaluate the CV encoding scheme, this approach eased the experimental implementation compared to the more secure Local-Local oscillator technique.[36,37] After detection, the electrical signals from the integrated chip were amplified using two RF amplifiers and subsequently filtered by two RF low-pass filters. Each RF component had a bandwidth of 500 MHz. Then, these signals were digitized by a 4 GHz oscilloscope with a resolution of 8-bit and a sampling rate of 25 GSs^{-1}. Finally, the digitized data was streamed to a computer for further offline analysis. The latter procedure accounted for constellation reconstruction and estimation of the main encoder parameters for CV-QKD, i.e., electronic noise, excess noise, and transmittance. To test the performance of the CV encoder, the ϕ-phase shifts $\pi/2$, $3\pi/2$, $-3\pi/2$, and $-\pi/2$ were used. The electrical control signals were generated by a 16-bit Arbitrary Waveform Generator (AWG) operating at a symbol rate of 50 MBaud. To simplify post-processing, the oscilloscope's data acquisition was synced with the AWG via a reference clock.

3.2. DV Setup

The experimental DV setup, shown in **Figure 3**, used was similar to the one described in ref. [38] for the transmitter, and to the one detailed in ref. [39] for the receiver. The source was a 1550 nm gain-switched laser emitting phase randomized pulses with a temporal width of 270 ps, measured at full-width-half-maximum, with a repetition rate of 50 MHz. The pulse amplitude was then modulated with a Sagnac interferometer,[31] which included a 70:30 BS, a phase modulator, and an optical delay line of 1 m. This Sagnac modulator was employed to generate the decoy states. Before entering the iPOGNAC, the polarization of the light pulse was rotated to guarantee that it enters diagonally polarized. It was obtained by rotating the iPOGNAC's input fiber collimator. Subsequently, the pulse polarization was adjusted using an iPOGNAC to produce the state $|D\rangle$ (diagonal), $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$ (circular right-handed), and $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$ (circular left-handed) by setting $\phi_l - \phi_e$ respectively equal to 0, $-\pi/2$, and $+\pi/2$. Before being sent to the receiver through a fiber quantum channel with ≈ 6.6 10^{B} of losses, these states were attenuated to the single-photon level by a calibrated VOA and filtered with a narrow-band optical filter centered at 1550.12 nm to reduce noise. The receiver then detected the incoming states by randomly alternating between the basis sets $\{|D\rangle, |A\rangle\}$ (check basis) and $\{|R\rangle, |L\rangle\}$ (key basis), each with an equal probability of selection. Such selection was passively realized using a 50:50 BS, and each projective measurement is implemented with an automatic polarization controller and a PBS. Moreover, a time and polarization multiplexing scheme performs the measurements using only one InGaAs/InP Single-Photon Avalanche Detector (SPAD). Finally, the photon's time-of-arrival is recorded by a Time-to-Digital-Converter (TDC), and the polarization and time reference frame synchronization

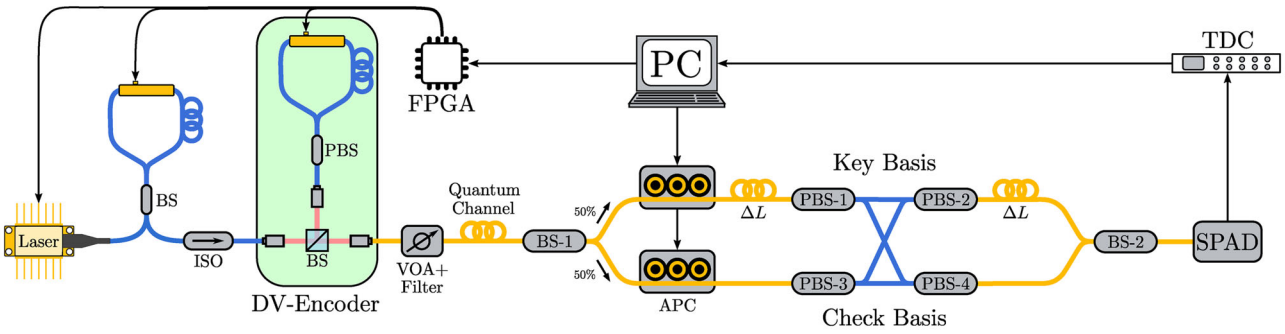

Figure 3. The system employs a 1550 nm pulsed laser, modulated by a Sagnac interferometer and iPOGNAC for decoy and quantum states $|D\rangle$, $|R\rangle$, $|L\rangle$ generation respectively. To guarantee that the iPOGNAC outputs $|D\rangle$, $|R\rangle$, $|L\rangle$, the input light must be $|D\rangle$, a condition achieved by carefully aligning such polarization modulator with the Sagnac, and the phase modulator must be operated with the appropriate electrical signals. The light is then attenuated to the single photon level by a Variable Optical Attenuator (VOA), filtered by a narrow-band optical filter centered at 1550.12 nm to reject noise, and directed, through a fiber quantum channel, to a time-multiplexed receiver with a Single Photon Avalanche Detector (SPAD) and two Automatic Polarization Controller (APDs) for QKD measurement. Finally, a time-tagger (TDC) records the SPAD signals for PC analysis. Notice that the signals controlling the Laser, Sagnac, and iPOGNAC are managed by an FPGA to ensure the correct timings. Moreover, the image provides a color-coded representation of the fibers used: blue for single-mode polarization-maintaining and yellow for single-mode non-polarization-maintaining fibers.

is performed continuously and automatically adjusted by the Qubit4Sync algorithm by using a few qubits from the quantum communication.[40]

4. Results

In the experiment with the CV phase encoder, we repeatedly transmitted four coherent states that formed a QPSK constellation. **Figure 4** depicts an example of the received constellation when Alice's modulation variance is approximately 12.4 SNU. Such a value is not suited for CV-QKD purposes. However, it allows us to resolve the constellation enough to showcase the encoder's modulation capabilities. For CV-QKD applications, the employed variance V_A is detailed in **Table 1**.

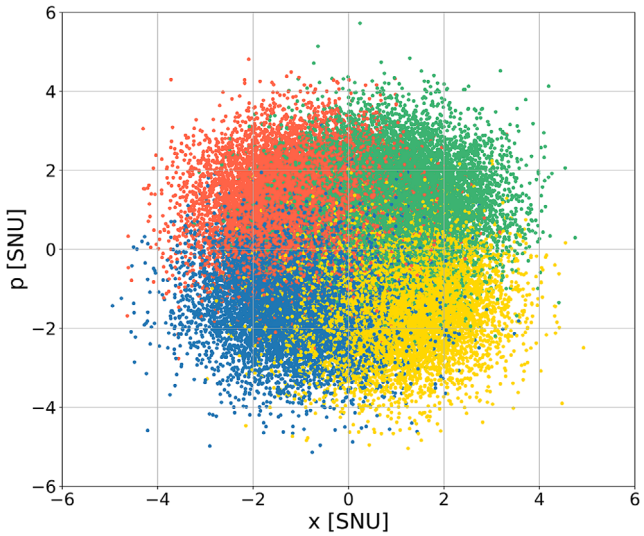

Figure 4. The picture showcases an example of QPSK constellation obtained with our CV-Encoder operating at a symbol rate of 50 MBaud and with Alice's variance V_A set to $\approx$ 12.4 SNU.

Table 1 reports the parameters estimated for our phase encoder.

Assuming a trusted detector scenario, the heterodyne receiver was calibrated estimating its electric noise V_{el} and losses η (the product of the efficiency of its photodetectors and transmittance) which resulted approximately 0.081 SNU and 0.27 respectively. The modulation variance V_A of the symbols transmitted by Alice was measured by the power meter PM-2 giving the value $\approx$ 0.45 SNU (we recall that such quantity is related to the mean photon number μ of the generated states as $V_A = 2\mu$). The excess noise parameter ξ_A and channel transmittance T were obtained by the following relations:

$$\langle X_A X_B \rangle = \sqrt{\frac{\eta T}{2}} V_A \tag{3}$$

$$V_B = 1 + V_{el} + \frac{\eta T}{2} V_A + \frac{\eta T}{2} \xi_A \tag{4}$$

with $\langle X_A X_B \rangle$ the covariance matrix elements and V_B Bob's variance estimated by analyzing a dataset of $1.5 \cdot 10^6$ symbols acquired with the oscilloscope.

Table 1. Values of the parameter estimation using the CV-Encoder with 50 MBaud QPSK modulation and setting the information reconciliation efficiency to 95%. The results are obtained by analyzing 30 samples, each with 50 000 symbols.

Parameter	Symbol	Value	Units
Electronic noise variance	V_{el}	0.081	SNU
Receiver losses	η	0.30	
Alice's variance	V_A	0.45	SNU
Channel transmittance	T	0.72	
Excess noise	ξ_A	0.012	SNU
SDP Asymptotic Secret Key Rate	SKR	0.021	bits/symbol
LC Asymptotic Secret Key Rate	SKR	0.026	bits/symbol

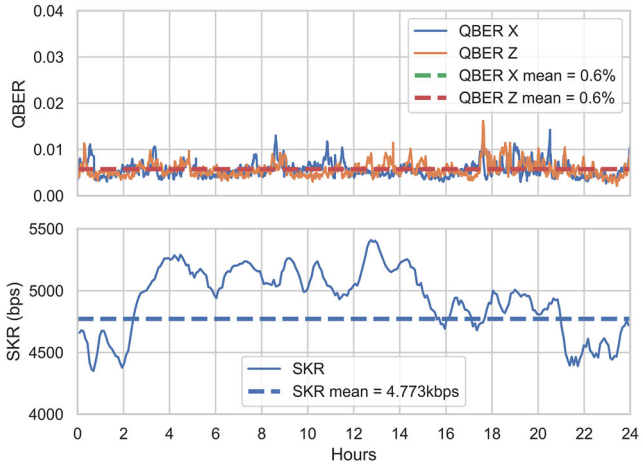

Figure 5. The picture illustrates the performance achieved during 24 h of continuous operation with our hybrid encoder in DV mode. The upper panel displays the QBER for both the key (Z) and check (X) basis, averaging 0.6% in each case. The lower panel shows the associated finite-size SKR, which averages 4.7 kbps.

The ideal asymptotic SKR obtained with our device is approximately 0.021 bits/symbol, which leads, given a symbol-rate of 50 MBaud, to a bit-rate of ≈ 1.1 Mbps. To compute the latter, we use the well-known Devetak-Winter bound[41] $SKR = \beta I_{AB} - \chi_E$, where β set at a value of 95% (typically employed in the literature[14,42]) is the error correction efficiency, I_{AB} is the mutual information between Alice and Bob, and χ_E the Holevo bound on the information between Bob and Eve in the reverse reconciliation scenario.

To compute the Holevo bound χ_E, we relied on a recent security proof based on a Semi-Definite Programming (SDP) method outlined in [14, 43] which directly considers discrete modulations schemes including QPSK. However, the approach does not consider hardware non-idealities like the electronic noise V_{el} and the detector's efficiency η. For completeness, we also report the performance obtained with the Linear Channel (LC) model, almost 0.026 bits/symbol and ≈ 1.3 Mbps given the 50 MBaud rate, which takes into account the aforementioned non-idealities, although it restricts the possible attacks that the eavesdropper can perform. In both cases, the tolerable excess noise for QPSK is very low, limiting the SKR and reachable distances. Improving the latter requires larger constellation schemes.[14,44]

For the DV encoder, we estimated the QBER and SKR when implementing the efficient three-states one-decoy protocol. The results are shown in **Figure 5**. As can be seen, the finite-size SKR shows very high stability during 24 h of data acquisition, with an average of 4.7 kbps. This is further demonstrated by the intrinsic QBER plot, which remains very low with an average of 0.6% for both bases. The results further confirm the excellent performance of the iPOGNC as a polarization encoder in terms of QBER and long term stability.

5. Conclusions

Hybrid QKD systems are powerful tools for managing a complex quantum network. When paired with the functionalities provided by an SDN, these systems can enable a more flexible and optimized allocation of its resources. Such versatility is largely due to their ability to toggle between DV and CV protocols, which is fundamental for implementing these networks. In this work, we present a hybrid encoder to support both CV and polarization-based DV QKD protocols, which, to the best of our knowledge, is the first of its kind. Our approach leverages an iPOGNAC for DV, where the polarization encoder's Sagnac loop is asymmetric due to an optical delay line, and for CV applications, in which the loop is symmetric as the previously mentioned delay is bypassed.

We remark that since we are exploiting a Sagnac loop, all perturbations are canceled. For DV-QKD, this improves the system's QBER. Indeed, we obtained a low value of ≈ 0.6% for the latter over 24 h, which led to a finite size SKR of ≈ 4.7 kbps. For the CV scenario, alongside improved stability, the loop's structure also makes the encoder polarization-insensitive, and we were able to achieve an asymptotic SKR of almost 0.021 bits/symbol, which translates to a bit-rate of ≈ 1.1 Mbps with the symbol-rate of 50 MBaud used. Concerning the latter insensitivity, due to the light horizontal and vertical components always being aligned with only one of the phase modulator's principal axes, we would like to highlight that this is a welcome feature for CV-QKD. In fact, such systems typically adopt modulators that exhibit unwanted polarization dependency. To ensure proper functioning, they must be controlled and stabilized with extra equipment that adds system complexity. In light of such, our scheme also simplifies the realization of a CV state encoder by avoiding the need for the aforementioned additional equipment.

Furthermore, we believe that the aforementioned compatibility of our device with polarization-based DV-QKD makes our scheme an attractive solution for free-space links for which polarization is usually employed, given its enhanced robustness considering the properties of the free-space channel itself. It is worth noting that free-space channels include satellite-to-satellite and satellite-to-ground connections, which are of great interest both for research and industry. On top of this, there is a growing interest in developing CV-QKD systems for satellite applications. Within such a context, our scheme can provide additional benefits other than integrating a DV and CV state encoder due to its lower complexity compared to two dedicated modules, such as a reduction in size, power consumption, and cost over two dedicated encoder modules due to its lower complexity.

In conclusion, this work introduces a hybrid encoder compatible with CV and polarization-based DV QKD protocols built entirely from COTS components. Furthermore, it features high stability alongside polarization insensitivity, and by integrating supplementary external components, it can also support additional phase-based DV protocols. We believe that our design represents an advancement in the realization of flexible and re-configurable nodes for the quantum networks of the future in which simplicity and compactness also matter.

Acknowledgements

The authors would like to thank Dr. Matteo Schiavon and Dr. Yoann Piétri for the useful discussions. The authors also thank the CloudVeneto facility for computational resources. The authors would like to thank also the European Union's Horizon Europe research and innovation programme under the project QUANGO (grant agreement No 101004341) and the

project "Quantum Secure Networks Partnership" (QSNP, grant agreement No 101114043) for providing preliminary research basis for this work. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission-EU. Neither the European Union nor the granting authority can be held responsible for them.

Open access publishing facilitated by Universita degli Studi di Padova, as part of the Wiley - CRUI-CARE agreement.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Keywords

CV/DV, hybrid, QKD, reconfigurable, SDN

Received: October 14, 2024
Revised: April 7, 2025
Published online: May 20, 2025

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, *Rev. Mod. Phys.* **2009**, *81*, 1301.
[2] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Rev. Mod. Phys.* **2002**, *74*, 145.
[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, *Rev. Mod. Phys.* **2020**, *92*, 025002.
[4] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, S. Lloyd, *Rev. Mod. Phys.* **2012**, *84*, 621.
[5] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, H. Hübel, *Adv. Quantum Technol.* **2018**, *1*, 1870011.
[6] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, P. Wallden, *Adv. Opt. Photonics* **2020**, *12*, 1012.
[7] Y. Zhang, Y. Bian, Z. Li, S. Yu, H. Guo, *Appl. Phys. Rev.* **2024**, *11*, 011318.
[8] C. H. Bennett, G. Brassard, *Theor. Comput. Sci.* **2014**, *560*, 7.
[9] G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, *Phys. Rev. Lett.* **2000**, *85*, 1330.
[10] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, H. Zbinden, *Appl. Phys. Lett.* **2018**, *112*, 051108.
[11] F. Grosshans, P. Grangier, *Phys. Rev. Lett.* **2002**, *88*, 057902.
[12] M. Almeida, D. Pereira, N. J. Muga, M. Facão, A. N. Pinto, N. A. Silva, *Opt. Express* **2021**, *29*, 38669.
[13] A. Leverrier, P. Grangier, *Phys. Rev. Lett.* **2009**, *102*, 180504.
[14] A. Denys, P. Brown, A. Leverrier, *Quantum* **2021**, *5*, 540.
[15] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, H. Zbinden, *Phys. Rev. Lett.* **2018**, *121*, 190502.
[16] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, J.-W. Pan, *Phys. Rev. Lett.* **2023**, *130*, 210801.
[17] R. Asif, W. J. Buchanan, in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. **2017**, pp. 910–916.
[18] T. Wang, P. Huang, L. Li, Y. Zhou, G. Zeng, *New J. Phys.* **2024**, *26*, 023002.
[19] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, H. Guo, *Phys. Rev. Lett.* **2020**, *125*, 010502.
[20] X.-J. Huang, F.-Y. Lu, S. Wang, Z.-Q. Yin, Z.-H. Wang, W. Chen, D.-Y. He, G.-J. Fan-Yuan, G.-C. Guo, Z.-F. Han, *Phys. Rev. A* **2022**, *106*, 062607.
[21] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, et al., *New J. Phys.* **2009**, *11*, 075001.
[22] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, et al., *Opt. Express* **2011**, *19*, 10387.
[23] A. Aguado, V. Lopez, D. Lopez, M. Peev, A. Poppe, A. Pastor, J. Folgueira, V. Martin, *IEEE Commun. Mag.* **2019**, *57*, 20.
[24] I. H. L. Grande, S. Etcheverry, J. Aldama, S. Ghasemi, D. Nolan, V. Pruneri, *Opt. Express* **2021**, *29*, 14815.
[25] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, H.-F. Zhang, K. Cui, H. Liang, X.-G. Li, Y. Mao, L.-J. Wang, S.-B. Feng, Q. Chen, Q. Zhang, L. Li, N.-L. Liu, C.-Z. Peng, X. Ma, Y. Zhao, J.-W. Pan, *npj Quantum Inf.* **2021**, *7*, 134.
[26] O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, D. Simeonidou, *J. Lightwave Technol.* **2022**, *40*, 5816.
[27] V. Martin, J. P. Brito, L. Ortíz, R. B. Méndez, J. S. Buruaga, R. J. Vicente, A. Sebastián-Lombraña, D. Rincón, F. Pérez, C. Sánchez, M. Peev, H. H. Brunner, F. Fung, A. Poppe, F. Fröwis, A. J. Shields, R. I. Woodward, H. Griesser, S. Roehrich, F. de la Iglesia, C. Abellán, M. Hentschel, J. M. Rivas-Moscoso, A. Pastor-Perales, J. Folgueira, D. López, *npj Quantum Inf.* **2024**, *10*, 80.
[28] E. Hugues-Salas, F. Ntavou, D. Gkounis, G. T. Kanellos, R. Nejabati, D. Simeonidou, *J. Opt. Commun. Networking* **2019**, *11*, A209
[29] M. Avesani, C. Agnesi, A. Stanco, G. Vallone, P. Villoresi, *Opt. Lett.* **2020**, *45*, 4706.
[30] B. Qi, L.-l. Huang, H.-k. Lo, L. Qian, In *2006 IEEE International Symposium on Information Theory*. **2006** 2090–2093, https://ieeexplore.ieee.org/document/4036337, ISSN: 2157-8117.
[31] G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, A. J. Shields, *Opt. Lett.* **2018**, *43*, 5110.
[32] H. Zhao, H. Li, Y. Xu, P. Huang, T. Wang, G. Zeng, *Opt. Lett.* **2022**, *47*, 2939.
[33] R. Mandil, L. Qian, H.-K. Lo, Long-fiber Sagnac interferometers for twin field quantum key distribution networks, **2024**, http://arxiv.org/abs/2407.08009, ArXiv:2407.08009 [quant-ph].
[34] B. Qi, *Phys. Rev. A* **2021**, *103*, 012606.
[35] J. S. Sidhu, R. Maggi, S. Pascazio, C. Lupo, Security of hybrid bb84 with heterodyne detection, **2024**, https://arxiv.org/abs/2402.16941.
[36] D. B. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, M. Sarovar, *Phys. Rev. X* **2015**, *5*, 041010.
[37] B. Qi, P. Lougovski, R. Pooser, W. Grice, M. Bobrek, *Phys. Rev. X* **2015**, *5*, 041009.
[38] M. Avesani, L. Calderaro, G. Foletto, C. Agnesi, F. Picciariello, F. B. L. Santagiustina, A. Scriminich, A. Stanco, F. Vedovato, M. Zahidy, G. Vallone, P. Villoresi, *Opt. Lett.* **2021**, *46*, 2848.

[39] M. Avesani, G. Foletto, M. Padovan, L. Calderaro, C. Agnesi, E. Bazzani, F. Berra, T. Bertapelle, F. Picciariello, F. B. L. Santagiustina, D. Scalcon, A. Scriminich, A. Stanco, F. Vedovato, G. Vallone, P. Villoresi, *J. Lightwave Technol.* **2022**, *40*, 1658.
[40] L. Calderaro, A. Stanco, C. Agnesi, M. Avesani, D. Dequal, P. Villoresi, G. Vallone, *Phys. Rev. Appl.* **2020**, *13*, 054041.
[41] I. Devetak, A. Winter, *Proc. R. Soc. A: Math., Phys. Eng. Sci.* **2005**, *461*, 207.
[42] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, W. Huang, B. Xu, *Commun. Phys.* **2022**, *5*, 1.
[43] S. Ghorai, P. Grangier, E. Diamanti, A. Leverrier, *Phys. Rev. X* **2019**, *9*, 021059.
[44] W. Zhao, R. Shi, Y. Feng, D. Huang, *Phys. Lett. A* **2020**, *384*, 126061.