Research Article

ADVANCED PHOTONICS

High-performance heterodyne receiver for quantum information processing in a laser-written integrated photonic platform

Andrea Peri,[a,†] Giulio Gualandi,[b,c,†] Tommaso Bertapelle,[a] Mattia Sabatini,[a] Giacomo Corrielli,[c] Yoann Piétri,[a] Davide Giacomo Marangon,[a,d] Giuseppe Vallone,[a,d] Paolo Villoresi,[a,d] Roberto Osellame,[c] and Marco Avesani[a,d,*]

[a]Università degli Studi di Padova, Dipartimento di Ingegneria dell'Informazione, Padua, Italy
[b]Politecnico di Milano, Dipartimento di Fisica, Milan, Italy
[c]Consiglio Nazionale delle Ricerche (CNR), Istituto di Fotonica e Nanotecnologie, Milan, Italy
[d]Università degli Studi di Padova, Padua Quantum Technologies Research Center, Padua, Italy

Abstract. Continuous variable quantum key distribution (CV-QKD) and continuous variable quantum random number generation (CV-QRNG) are critical technologies for secure communication and high-speed randomness generation, exploiting shot-noise-limited coherent detection for their operation. Integrated photonic solutions are key to advancing these protocols, as they enable compact, scalable, and efficient system implementations. We introduce femtosecond laser micromachining (FLM) on borosilicate glass as a platform for producing photonic integrated circuits (PICs) realizing coherent detection suitable for quantum information processing. Employing off-chip detectors, we exploit the specific features of FLM to produce a PIC designed for CV-QKD and CV-QRNG applications. The PIC features fully adjustable optical components that achieve precise calibration and reliable operation under protocol-defined conditions. The device exhibits low insertion losses (≤ 1.28 dB), polarization-insensitive operation, and a common-mode rejection ratio exceeding 73 dB. These characteristics allowed the experimental realization of a source-device-independent CV-QRNG with a secure generation rate of 42.74 Gbit/s and a quadrature phase-shift-keying-based CV-QKD system achieving a secret key rate of 3.2 Mbit/s. Our results highlight the potential of FLM technology as an integrated photonic platform, paving the way for scalable and high-performing quantum communication systems.

Keywords: continuous variable quantum key distribution; quantum random number generation; femtosecond laser writing; photonic integrated circuit; coherent detection; continuous variable.

Received Jun. 23, 2025; revised manuscript received Oct. 18, 2025; accepted for publication Oct. 29, 2025; published online Feb. 4, 2026.

[DOI: 10.1117/1.AP.8.1.016009]

1 Introduction

In recent years, quantum information processing has witnessed exponential advancements, especially in the fields of quantum random number generators (QRNGs) and quantum key distribution (QKD). The former aims to provide true randomness, whereas the latter enables information-theoretic secure communications among parties over an untrusted channel. QRNG and QKD protocols can be classified as either discrete variables (DVs) or continuous variables (CVs), based on the degrees of freedom of the underlying quantum systems. The latter approach, based on coherent detection, is particularly attractive in terms of performance and compatibility with the telecommunication industry. In fact, continuous variable quantum random number generators (CV-QRNGs) can achieve generation rates of several Gbit/s,[1–3] and continuous variable quantum key distribution (CV-QKD) can reach higher key rates compared with DV systems, although for shorter distances.[4–6]

Along with the progress made in the aforementioned areas, there have also been significant improvements in the methods and materials used for their implementation. Coherent detection

*Address all correspondence to Marco Avesani, marco.avesani@unipd.it
†These authors contributed equally to this work.

systems consist of an optical front end connected to an electrical back end, which together enable the realization of either balanced homodyne or heterodyne detection. Research has focused on miniaturizing these systems by leveraging integrated photonics to develop high-performance, scalable, and mass-manufacturable photonic integrated circuits (PICs).[7–10] The level of integration that PICs can achieve depends on the substrate used. For example, planar lightwave circuits realized in silica cannot monolithically incorporate either active components or pin photodiodes, which must be externally coupled.[11] Silicon photonics instead relies on silicon-on-insulator (SOI) wafers as its semiconductor substrate, making SOI technology compliant with complementary metal-oxide-semiconductor (CMOS) fabrication techniques. SOI chips can include complex waveguide structures and active control elements, such as Mach–Zehnder, multimode interferometers, and phase shifters. Light sources can only be externally coupled, but pin photodiodes can be hybridly (InGaAs)[12,13] or monolithically (Ge) integrated.[14–18] Moreover, the compatibility of SOI PICs with standard CMOS processes enables the coexistence of silicon electronics and photonics on the same substrate. In fact, custom transimpedance amplifiers were recently integrated into a silicon chip,[19] a solution that may enhance the capabilities of already existing high-performance CV-QKD receivers operating at tens of GHz[6,20] and CV-QRNGs achieving rates of hundreds of Gbit/s.[21,22] Another platform recently developed is indium phosphide (InP), which supports the monolithic integration of lasers and photodiodes alongside all the active and passive optical elements common to SOI technology. This makes InP capable of reaching the highest degree of integration of optical components.[23,24] However, both SOI and InP platforms typically exhibit significant polarization dependence, requiring careful polarization control and limiting their applicability in scenarios where polarization is not fixed or cannot be easily managed. In addition, miniaturization is not the only figure of merit when developing integrated photonics for quantum technologies. Indeed, one of the key challenges in quantum communication protocols is the minimization of optical losses, especially at the receiver side for QKD, because they result in irreversible information loss.

In this work, we introduce femtosecond laser micromachining (FLM) on borosilicate glass as a powerful platform to manufacture PICs designed for high-performance quantum coherent detection. With FLM, waveguides can be directly written within transparent materials with three-dimensional features and essentially at any wavelength across the VIS–NIR range by focusing short and intense laser pulses for direct core writing.[25] Although offering lower miniaturization capabilities compared with other photonic platforms, due to the relatively low refractive index contrast achievable (up to 10^{-2}), FLM provides enhanced modularity, low losses, and cost-effective fabrication. The close match between waveguide modes (a few μm^2) and standard optical fibers ensures efficient edge coupling, with interface losses as small as 0.2 dB and propagation losses around 0.1 dB/cm at 1550 nm. These features make glass-based devices highly suitable for quantum photonic experiments, where minimizing attenuation is essential.

Furthermore, the technology enables the realization of polarization-insensitive devices: any polarization state injected in the chip undergoes the same unitary transformation because directional couplers implement the same splitting ratio for any polarization state, and the weak residual birefringence (10^{-6} to 10^{-5}, mainly due to core-shape anisotropy) induces the same rotation across all paths. This intrinsic polarization insensitivity allows modular interconnection of multiple devices without the need for precise polarization control, in contrast to other integrated platforms. These features, which have already been exploited in various quantum information processing tasks,[26–33] not only simplify system design but also unlock new possibilities beyond the reach of conventional photolithographic techniques. Here, we demonstrate the suitability and versatility of glass FLM for the implementation of quantum coherent detection for state-of-the-art CV-QRNG and CV-QKD protocols. Specifically, we developed a PIC that serves as a low-loss polarization-insensitive optical front-end of a heterodyne receiver. Such properties allow for efficient coupling of the chip with commercial-off-the-shelf (COTS) fiber-based lasers and balanced detectors. Moreover, the PIC was designed with tunable capabilities: the relative phase of the heterodyne measurements, as well as their balancing, can be fully adjusted. This not only enhances the performance of its electronic back-end but also allows the system to operate under conditions that best align with the theoretical requirements of CV protocols, thereby ensuring maximum reliability and assurance in their implementation.

We will detail the design of the PIC and its characterization in Sec. 2, the implementation of a source-device-independent random number generation protocol in Sec. 3, the implementation of the quadrature phase-shift-keying (QPSK) CV-QKD protocol in Sec. 4, and in Sec. 5 we will discuss our findings.

2 PIC Fabrication, Design, and Characterization

2.1 PIC Fabrication and Design

The glass-based optical circuit was manufactured using the FLM microfabrication technique.[25] This process tightly focuses ultra-short laser pulses inside a glass substrate, triggering nonlinear absorption that induces a permanent and localized increase in its refractive index, primarily driven by ion migration during the transient melting and rapid resolidification caused by the laser irradiation.[34] Such a process is confined to the pulse focal volume, allowing for the direct writing of waveguides upon translation of the substrate relative to the laser focus. Moreover, the possibility to move the sample in three dimensions enables the realization of out-of-plane photonic circuits. This versatile technique is suitable for fast prototyping and grants full control over multiple parameters during fabrication. Indeed, by changing the irradiation parameters, it is possible to optimize the properties of a waveguide, such as losses and birefringence, for any desired wavelength. Furthermore, as the waveguide geometry is controlled with an accuracy of tens of nanometers, directional couplers can be fabricated with splitting ratio tolerances $<1\%$. This enables the realization of high-quality balanced directional couplers and, consequently, Mach–Zehnder interferometers (MZIs) with high extinction ratios. The latter is a crucial factor that directly impacts the device's performance, as will be discussed in Secs. 3 and 4.

The device presented in this work was fabricated using femtosecond laser pulses with a wavelength of 1030 nm, a repetition rate of 1 MHz, and a pulse duration of 180 fs. Laser light was focused into the volume of an Eagle XG borosilicate glass substrate through a water immersion objective with a numerical aperture of 0.5, at a depth of 50 μm from the surface. For the

fabrication of single-mode waveguides, we adopted an energy of 500 nJ/pulse and repeated four overlapping writing scans per waveguide, each at a translation speed of 7 mm/s. To enhance the optical quality of the waveguides, we performed a thermal annealing step to relax any stresses formed during the fabrication process. This treatment improves the optical mode confinement, allowing bending radii of 10 mm.[35]

As illustrated in Fig. 1(a), the PIC implements a tunable optical hybrid composed of two 50:50 beam splitters (BSs), a variable phase shifter $\Delta\theta_{LO}$, and two variable beam splitters (vBSs) implemented as Mach–Zehnder interferometers. When $\Delta\theta_{LO} = \pi/2$ and the vBSs are balanced, the device corresponds to a 90-deg optical hybrid, a key component in quantum and classical coherent detection. An image illustrating the PIC's layout is reported in Fig. 1(b). The chip has a footprint of 1.5 cm × 3.7 cm with its main specifications listed in Table 1. The insertion losses of the fiber-pigtailed device relative to IN1 and IN2 were measured to be 1.05 and 1.28 dB, with negligible difference (<1%) with respect to input polarization. These values account for propagation and bending loss of the waveguides, coupling losses due to mode mismatch between fiber and waveguide fundamental modes, and fiber-to-fiber mating at the connector. The geometry of all directional couplers (DCs) was optimized to achieve a splitting ratio close to 50:50. For each DC, we also reported in Table 1 the measurement of their reflectivity for both horizontal (H) and vertical (V) polarizations. From such values, we can infer that they are almost polarization insensitive, deviating from ideality by <1%. To realize the tunable optical hybrid, we exploited the three-dimensional capabilities of FLM. As shown in Fig. 1(b), the two central waveguides cross each other at different depths, with 15-μm vertical spacing, resulting in no crosstalk among them.

Table 1 FLM-written PIC specifications. The table presents the insertion losses for inputs 1 and 2, as indicated in Fig. 1(b), along with the splitting ratio for the directional couplers relative to IN1 (DC1) and IN2 (DC2), for both horizontal and vertical polarizations. Finally, the power dissipation required to induce a 2π phase shift is reported.

Substrate	Borosilicate glass Eagle XG		
Insertion losses	IN1	1.05 dB	
	IN2	1.28 dB	
DC reflectivities	Polarization	DC1	DC2
	H	0.502	0.506
	V	0.502	0.502
Power dissipation	2π	70 mW	

Control over the optical phases, required for the proper operation of the PIC as a 90-deg hybrid and for tuning the splitting ratio of the vBSs, is achieved through integrated thermo-optical phase shifters (TOPSs). Each TOPS is fabricated by ablating with the femtosecond laser a 100-nm-thick Cr + Au layer, deposited on the substrate surface, to pattern its electrical pads and micro-heaters.[36] In addition, as shown in Fig. 1, insulating trenches were ablated alongside the waveguides to reduce thermal crosstalk and power consumption. In particular, these TOPSs introduce a 2π phase shift using 70 mW of dissipated electrical power. The TOPSs are addressed by electrically connecting the gold contact pads to a custom-made printed circuit board (PCB) using conductive epoxy and are driven via a voltage

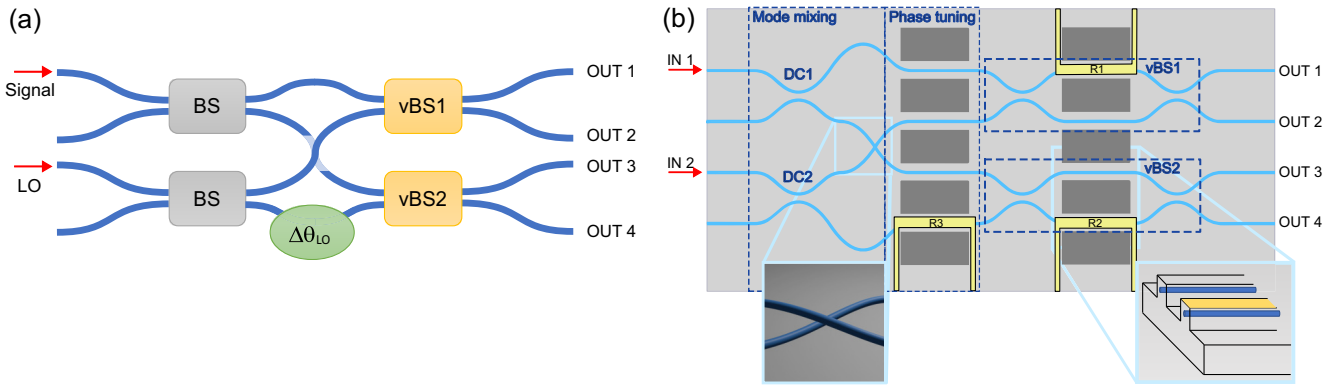

Fig. 1 FLM-written PIC layout. (a) Conceptual layout of the tunable optical hybrid, where we can independently control the phase shift $\Delta\theta_{LO}$ and the splitting ratio of the variable beam splitters (vBSs). The two red arrows indicate the inputs for the signal and local oscillator, which are then processed in balanced BSs, waveguide crossing, and variable beam splitters (vBSs). When the phase $\Delta\theta_{LO}$ is $\pi/2$ and the vBSs are perfectly balanced, the device acts as a 90-deg optical hybrid. (b) Schematic layout of the FLM-written photonic device. The dashed rectangle on the left highlights the mode mixing, where the two central modes swap by crossing one over the other (see left inset) thanks to the three-dimensional capabilities of FLM. The central dashed rectangle evidences the area where the thermal shifter tunes the $\Delta\theta_{LO}$ phase shift. The two dashed rectangles on the right mark the locations of the vBSs, implemented through reconfigurable Mach–Zehnder interferometers, used to balance the device's outputs. The thermo-optic phase shifters (associated with resistances R1, R2, and R3) are depicted in yellow, and the dark gray rectangles represent the trenches fabricated by FLM alongside the waveguides to provide increased thermal insulation (see right inset), thereby reducing power dissipation per micro-heater and minimizing thermal cross-talk.

source connected to the PCB. More details on the fabrication can be found in Refs. 37 and 38.

The FLM-written PIC is designed to implement a phase-diverse heterodyne coherent detection. Therefore, it must be ensured that the quantum signal properly interferes with a strong coherent beam (strong enough that its quantum behavior can be neglected and thus described classically), commonly referred to as the local oscillator (LO). This is accomplished through the chip's optical routing and correct tuning of its TOPS voltages. In our case, the quantum signal and LO, entering the PIC through IN1 and IN2, respectively, are split by two 50:50 DCs. Next, each quantum signal path interferes with one LO branch via the vBSs, tuned as balanced beam splitters. The latter is obtained by inducing the correct phase shift with TOPS R1 (vBS1) and R2 (vBS2). The optical signals from each vBS are connected off-chip to a pair of balanced photo-detectors (BPDs) for the simultaneous detection of two quadratures of the input quantum state. Moreover, to ensure orthogonality of the detected quadratures, one of the aforementioned LO branches is phase-shifted on-chip by $\pi/2$ with TOPS R3. This design ensures flexibility and accurate control over the PIC operation, boosting the heterodyne receiver's performance.

2.2 Measurement Setup

In Fig. 2, we reported the schematic of the experimental setup used to operate the heterodyne optical receiver. The latter was designed to allow the characterization of the PIC and the implementation of both the QRNG and QKD experiments, avoiding unnecessary hardware reconfigurations. A 1550-nm external cavity laser (ECL) (Thorlabs SFL1550S) with a linewidth of ~50 kHz was used to generate the optical signal and the local oscillator. We cascaded the laser with an optical isolator (ISO) and a polarizing beam splitter (PBS), whose optical axes do not require to be aligned with respect to the PIC given its polarization transparency. The former component prevents back-scattered light from causing stability issues with the ECL, whereas the latter avoids possible polarization drifts. To ensure all light is coupled to the PBS branch leading to the optical heterodyning, we used a polarization controller (PC) before the PBS and monitored the optical power of its other arm with a power meter (PM-1). The PC is adjusted to minimize the power reading on PM-1. Following the PBS, a 99:1 beam splitter (BS-1) directs 1% and 99% of the laser light to the PIC's signal and LO port, respectively. The light traveling through the 1% arm (signal line) is modulated using a polarization-insensitive phase encoder[39] incorporating a lithium niobate phase modulator (iXblue MPZ-LN-10), driven by a field-programmable gate array (FPGA) (AMD Xilinx RFSoC 4×2) working as an arbitrary waveform generator. The encoder has two different purposes throughout this work. On one hand, it is used to generate the classical signals required to configure the chip as a 90-deg optical hybrid. On the other hand, in the CV-QKD experiment, it will serve as part of the optical transmitter. After the phase encoder, a polarization controller (PC-2) maximizes the interference between the modulated signals and the receiver LO at the PIC input. A 99:1 beam splitter (BS-2) then splits the optical power: the 1% branch is routed to the heterodyne signal port through a short fiber and a 1.7-dB optical attenuator, whereas the 99% branch is directed to the power meter (PM-2) used to monitor the signal power. The LO line (BS-1 99% arm) includes an optical delay line (ΔL) to match its overall length to that of the signal line, thereby minimizing phase instabilities at the receiver end. It also features an electrically controlled variable optical attenuator (VOA-1) to adjust the LO power entering the PIC. To estimate the latter quantity, a 99:1 beam splitter (BS-3) redirects 1% of the LO light to the power-meter (PM-3).

The phase-modulated signal and LO constitute the PIC's inputs, where they interfere according to the TOPSs configuration. The latter is set by a multi-channel voltage generator with sub-mV resolution. In the context of QRNG and CV-QKD operation, the TOPSs are tuned to introduce the correct phases required for the heterodyne architecture, which samples two orthogonal quadratures of the quantum signal. Thermal control of the PIC, achieved via a Peltier element, ensures robust operation of the heterodyne configuration. Finally, the optical signals at the PIC's outputs are processed into electrical signals by a pair of BPDs with a 2.5-GHz bandwidth (Thorlabs PDB780CAC), filtered by an analog 1-MHz high-pass filter (HPF) to reject low-frequency noise, digitized by a 25-GSa/s oscilloscope (Tektronix DPO70404C) with 8-bit resolution per channel and transferred to a computer for digital processing.

2.3 PIC Characterization

Throughout this work, the PIC was employed as a heterodyne receiver to detect quantum signals at the shot-noise limit using BPDs. This requires to appropriately configure the chip's TOPSs. In particular, the LO's phase entering vBS2 is set (through R3) to be $\pi/2$ out-of-phase, and the vBSs are finely balanced using R1 and R2. This fine control of the optical components within the vBSs allows us not only to suppress the common-mode classical noise introduced by the laser but also to increase the LO power at the heterodyne input, ultimately boosting the performance of the quantum devices. These performance enhancements are possible by configuring each output of the system, composed of the integrated vBS and the off-chip BPD, to maintain a 50:50 splitting ratio. This is accomplished by maximizing the system's common-mode rejection ratio (CMRR), which is estimated by directly modulating the ECL laser with a 500-kHz sine-wave electrical signal while blocking the signal line. As detailed in Appendix A, the CMRR is computed by evaluating the ratio of the BPD's electrical power at 500 kHz when completely unbalancing and balancing the vBSs. Figure 3(a) shows the relationship between vBS2 CMRR and the driving voltage of the associated TOPS. As can be seen, it closely follows the trend

$$\mathrm{CMRR} = -20\log(|\sin\phi_{\mathrm{R2}}| + \delta). \tag{1}$$

This equation corresponds to the standard sinusoidal response of an MZI as a function of the interferometric phase ϕ_{R2}, with the latter being polynomially dependent on the TOPS voltage V_{R2}.[40] The parameter δ quantifies the maximum CMRR achievable by the system, and it is estimated based on the system noise floor, as detailed in Appendix A.

The experimental data exhibit a sharp peak located in the region where the vBS splitting ratio is close to the ideal 50:50, with a full width at half-maximum (FWHM) of 2.0 mV and a maximum measured CMRR of ~73.8 dB. The vBS1 shows an analogous behavior. This indicates that a resolution of fractions of mV is required to drive the integrated TOPS to ensure the vBSs are highly balanced. However, external factors such as

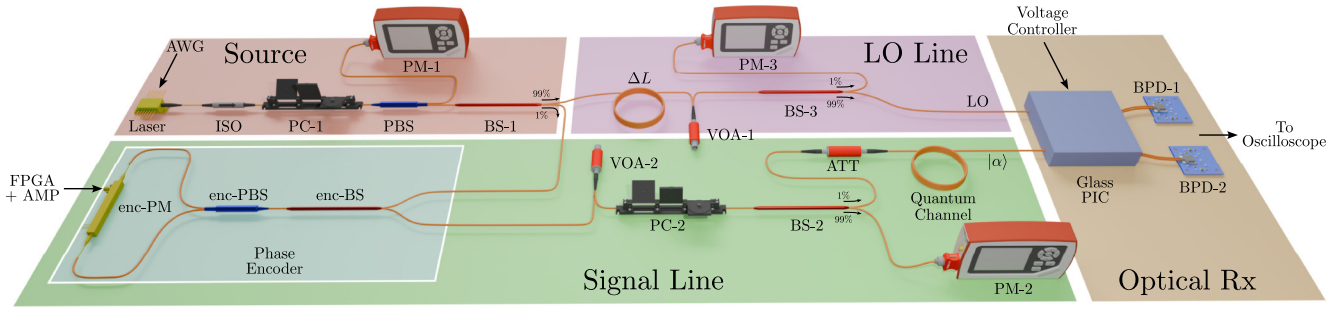

Fig. 2 Experimental setup. The figure details the optical components used for both the PIC characterization and the implementation of the CV quantum protocols. The optical source provides a coherent beam with fixed power and polarization. Such optical power is split and undergoes different paths, generating the LO and the phase-modulated quantum signal $|\alpha\rangle$. These modes are coupled at the PIC's inputs and then converted into electrical signals by two balanced photo-detectors to measure the quadratures of the quantum signal. The configuration of the PIC as an optical heterodyne receiver consists of balancing the chip's outputs and setting the tunable optical hybrid as a 90-deg one. Although the balancing procedure is performed just with the LO optical beam, setting the hybrid required a phase-modulated classical signal along with the LO. Once configured, the device is exploited as the optical receiver for CV-QRNG and CV-QKD protocols. AWG, arbitrary waveform generator; ISO, optical isolator; PC, polarization controller; PBS, polarizing beam splitter; BS, beam splitter; PM, power meter; FPGA, field-programmable gate array; AMP, RF amplifier; VOA, variable optical attenuator; ATT, optical attenuator; BPD, balanced photo-detector.

small temperature and polarization drifts may affect the high CMRR values reached while configuring the device, leading to a degradation of such a quantity over time. As shown in Table 1, the couplers in the PIC have an excellent polarization insensitivity; however, even a dependence on the third decimal place of the splitting ratio limits the CMRR to ∼30 dB. Therefore, to enhance the stability of the CMRR in the 70 dB range, it is crucial to suppress polarization drifts. For the aforementioned reasons, we thermally stabilized the PIC and placed a PBS at the laser output to stabilize the polarization of the optical source.

To ensure that the heterodyne receiver measures two orthogonal quadratures, we acted on R3 to provide a phase shift $\Delta\theta_{\mathrm{LO}}$ of $\pi/2$ to the LO entering vBS2. To reach such a condition, by referring to Fig. 2, the light in the signal line was modulated with a triangular waveform covering the whole 2π range of the state's encoder. In Fig. 3(b), we show the relation between $\Delta\theta_{\mathrm{LO}}$ and V_{R3} driving voltage. Despite the polynomial dependence among the latter quantities mentioned above, a first-order approximation is sufficient to describe the behavior of the device in the 90-deg neighborhood, demonstrating a phase voltage sensitivity of 0.14 deg /mV.

Finally, we evaluated the device's temporal stability over two 8-h tests, monitoring the vBSs' CMRR and $\Delta\theta_{\mathrm{LO}}$. The results are shown in Fig. 4. Fluctuations in the measured quantities are

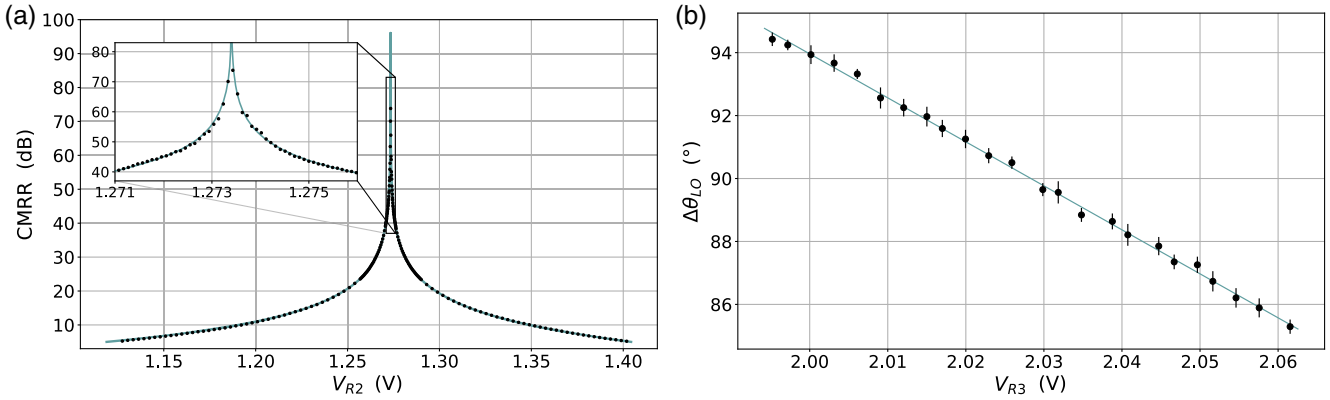

Fig. 3 Characterization of the PIC optical configuration. (a) CMRR response of the variable beamsplitter vBS2 with respect to the voltage applied to TOPS R2. The experimental data closely match the theoretical model described in Eq. (1). By fine-tuning V_{R2}, the device achieved a CMRR as high as ∼73.8 dB. The vBS1 tunable BS displays a similar trend and performance. (b) Phase shift applied to the LO by TOPS R3 as a function of the driving voltage V_{R3}. In the region of $\Delta\theta_{\mathrm{LO}} \approx 90$ deg, we estimate from the fitted linear coefficient a phase voltage sensitivity of 0.14 deg /mV, quantifying the TOPS response to the applied voltage.

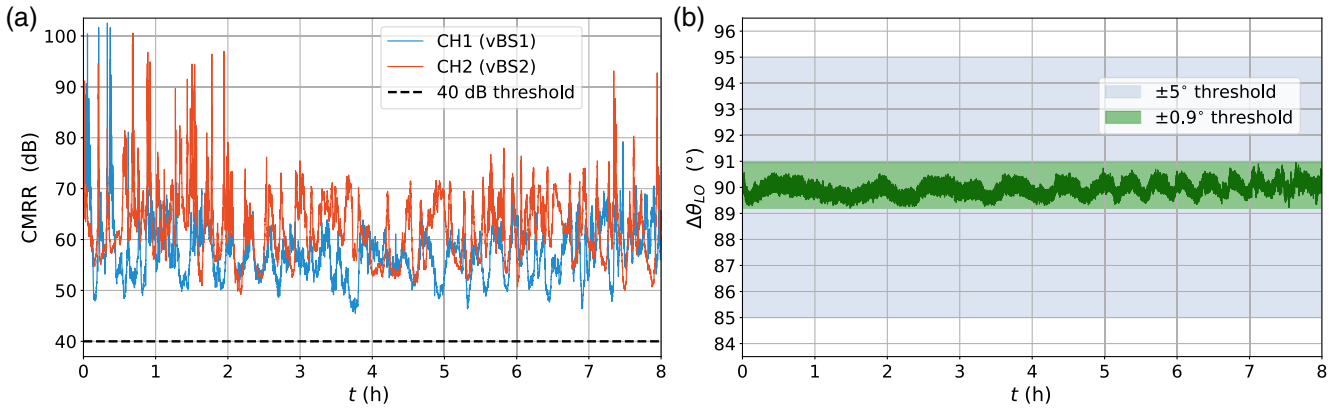

Fig. 4 Temporal stability of the PIC heterodyne configuration. (a) CMRR stability is shown for both the vBSs. For quantum protocols implementations, a CMRR lower threshold is set to 40 dB because higher values do not lead to a significant improvement in receiver performance, as we will discuss in Sec. 3 and shown in Fig. 5. Higher CMRR values are consistently measured throughout the test duration. (b) Stability of the LO 90-deg phase shift. The plot compares the PIC phase stability (in green) with the ±5- deg phase error commonly reported for commercial 90-deg optical hybrid devices (in blue). Apart from temperature stabilization, no active mechanism was employed to maintain the device configuration.

attributed to limitations of the PID control loop regulating the PIC temperature. Nevertheless, despite these fluctuations, the CMRR reads well above the 40-dB threshold throughout the duration of the test. As it will be discussed in Sec. 3, this level is more than sufficient to ensure reliable operation for both QRNG and CV-QKD applications. Figure 4(b) shows a highly stable 90-deg optical hybrid operation, with a maximum phase fluctuation of ±0.9 deg around a mean value of 90.0 deg. The stability of the LO phase is compared with the phase error generally reported for bulk, commercially available 90-deg optical hybrid devices, which is in the order of ±5 deg (Table 2). These tests, along with the characterization reported above, guarantee an accurate and stable control over the PIC operation, showcasing the capabilities of our device.

Table 2 compares the performance of our PIC with commercially available devices and implementations reported in the literature based on 90- and 180-deg hybrids, mainly focusing on those used in QRNG and CV-QKD experiments. This showcases the high input-to-output efficiency of our PIC compared with other platforms that suffer from higher coupling losses. The phase deviation is also shown for 90-deg hybrids when the information was available. Note that this value is usually given

Table 2 Comparison of commercially available and PIC-based hybrids. The two first entries correspond to commercially available hybrids. IL, insertion losses, including propagation losses. When the separation between insertion losses and coupling losses is not known, the overall hybrid losses are indicated. The symbol "N/A" denotes that the parameter is not applicable to the device, while "NR" indicates that the value was not reported in the reference.

Technology	Hybrid type (deg)	Hybrid losses		Detector efficiency (%)	Overall efficiency (%)	Phase deviation (deg)	Ref.
		On-chip (dB)	Coupling (dB)				
Micro-optics	90	1 (typ.)		N/A	N/A	±5	Exail COH90
Silicon	90	3.19		80 (typ. Ge)[b]	38.4	±7.5	Finisar CPRV
Silicon	180	5.1		64[b]	20	N/A	14
Silicon	180	5		73 (inferred)[b]	49.8	N/A	15
Silicon	90	2.5		88[b]	44	NR	20
Silicon	180	4		64[b]	22.7	N/A	41
GaInAsP/InP[a]	90	0.5	6.9	N/A	N/A	±5	42
Si_3N_4[a]	90	<1	NR	N/A	N/A	<8	43
Silicon	180	2.1	3	80[b]	26	N/A	17
FLM	90	0.65	0.4	75 (avg.)	59.3	±0.9	This work

[a]The device was not used for quantum communication applications.
[b]The photo-detectors are integrated on the chip.

over the entire bandwidth, whereas in our case it corresponds to the value achieved at 1550 nm. However, the reconfigurability of our PIC allows us to reach such precision also for different wavelengths. In addition, our PIC could be combined with even higher-efficiency detectors. For example, commercially available solutions with 1.2 A/W of responsivity at 1550 nm would enable our implementation of a coherent receiver to reach an overall efficiency of 77%. As can be seen in Table 2, our FLM chip performs better than existing implementations in terms of optical losses and phase deviation.

3 QRNG Configuration

In the context of QRNGs for cryptographic applications, our PIC enables the implementation of heterodyne-based protocols by providing a stable coherent receiver with high CMRR and precise control of the $\pi/2$ phase difference among the measured quadratures. In this work, we implement the source-device independent protocol described in Ref. 2, which provides secure randomness regardless of the quantum state used, even if it is fully controlled by an attacker. Indeed, even in the case of general attacks, the positive operator-valued measurement (POVM) structure of the optical heterodyne receiver lower-bounds the quantum conditional min-entropy

$$H_{\min}(X|E) \geq -\log_2\left(\frac{\delta_x\delta_p}{\pi}\right)^n, \tag{2}$$

where n is the number of rounds of the protocol, and $\delta_{x,p}$ denote the device's phase space resolution. The quantity $H_{\min}(X|E)$, in turn, upper bounds the number of secure true random bits that can be extracted from a sequence of heterodyne measurement outcomes. In addition, compared with implementations belonging to the broader class of semi-device independent generators,[44] our protocol of choice is considerably simpler to implement, it does not require external sources of randomness or real-time min-entropy analysis[45] and can deliver significantly higher performances.[46]

Before running the QRNG, the receiver must be characterized; specifically the device's phase-space resolution $\delta_{x,p}$ must be determined. This characterization is essential to ensure the security of the generated numbers. To this end, we followed the procedure outlined in the Supplementary Materials of Ref. 2. As the device's photo-detectors must operate within the linear regime, the quadrature measurement outcomes scale proportionally with the local oscillator's power P_{LO}. Therefore, the phase-space resolutions $\delta_{x,p}$ of the receiver, expressed in shot-noise units, are given by

$$\delta_{x,p} = \frac{\delta_{\mathrm{VU}}}{\sqrt{2m_{x,p}P_{\mathrm{LO}} + 2q_{x,p}}} \leq \frac{\delta_{\mathrm{VU}}}{\sqrt{2m_{x,p}P_{\mathrm{LO}}}}, \tag{3}$$

where δ_{VU} is the resolution in volt units, $q_{x,p}$ account for the classical noise due to the receiver electronics, and $m_{x,p}$ are the proportionality coefficient relating the variance of the heterodyne signals to P_{LO}. Notice that the latter upper bound is obtained by untrusting the classical electronic noise. This effectively reduces the generator's rate but enhances the device security against the potential manipulation of such noise by an attacker. Moreover, as the attacker's guessing probability decreases with increasing LO power, it is desirable to maximize P_{LO} while avoiding the non-linear effects of the BPDs. As we demonstrate below, higher CMRR values enable the use of stronger LO, thus enhancing the generation rate. After calibration, the QRNG performance was evaluated as a function of the CMRR, and data were collected for randomness extraction and analysis with the standard NIST test suite.[47]

3.1 Experimental Setup

A schematic representation of the experimental setup used to implement the QRNG protocol is shown in Fig. 2. The laser light is divided between the signal and local oscillator lines, where VOA-1 is only required for calibrating the receiver by estimating the $m_{x,p}$ coefficients. Meanwhile, the signal line is detached from the PIC input to guarantee the injection of the vacuum state into the QRNG. Although it is crucial to know which state we are using during calibration, its nature is not essential when running the protocol because it operates in the source-device independent framework. Therefore, we opted for the vacuum state as the device input for randomness generation, given the simplicity with which it can be realized.

At the receiver end, the optical signals extracted by the PIC are converted into electrical ones by a pair of BPDs. These signals are then further filtered by additional 50-MHz RF high-pass filters to improve low-frequency noise rejection. Finally, the resulting heterodyne measurements are digitized by an 8-bit oscilloscope with a frame duration of 400 μs, and subsequently transferred to a computer for off-line digital processing, accounting for digital signal processing (DSP) and randomness extraction. The former is based on Ref. 13 and is used to prepare the data for either QRNG performance estimation or randomness distillation. The DSP extracts and isolates via digital resampling a portion of the measurement spectrum, which must be sufficiently flat to avoid temporal correlations in the random string. According to such, we selected a spectral window range of 0.5 to 2.3 GHz. This choice also rejects the technical noise present at lower frequencies, is sufficiently far from the BPDs' upper cutoff frequency of 2.5 GHz, and ensures that the signals possess a clearance of at least 12 dB (see Sec. 7.2 in Appendix B). To extract secure true randomness, the raw data, pre-processed with the methods outlined above, are hashed with a two-universal hashing function.[48] The latter is implemented as a binary matrix-vector multiplication, and the final data are analyzed with the standard NIST test suite.

3.2 Results

After the PIC was configured as a heterodyne receiver and characterized, we determined the performance that can be achieved by the QRNG and reported it in Fig. 5(a). We show the quantum conditional min-entropy $H_{\min}(X|E)$, which quantifies the extractable truly random bits from a 16-bit heterodyne measurement (8-bit per channel), as a function of the receiver's CMRR. Notice that as the CMRR increases, the value of $H_{\min}(X|E)$ also increases. However, for higher values, the improvements become progressively smaller, and a CMRR greater than 40 dB yields no significant gain in $H_{\min}(X|E)$. Therefore, if we consider a CMRR of at least 40 dB, the QRNG presented here lower bounds $H_{\min}(X|E)$ to $\sim$11.98 bits (corresponding to a phase-space resolution of $\delta_x \sim 2.94 \times 10^{-2}$ and $\delta_p \sim 2.65 \times 10^{-2}$), thus achieving a secure generation rate of

$$R_{\mathrm{sc}} = R_{\mathrm{raw}} H_{\min}(X|E) \approx 43.13 \text{ Gbit/s}, \tag{4}$$

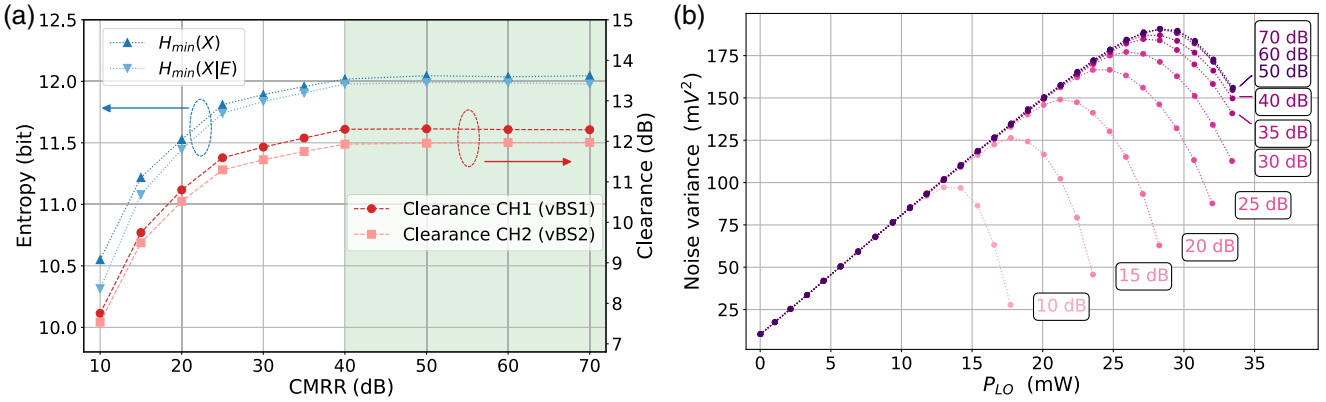

Fig. 5 QRNG performance and receiver characterization as a function of the receiver's CMRR. (a) Blue curves represent the classical min-entropy $H_{\min}(X)$ and the lower-bound on the quantum conditional min-entropy $H_{\min}(X|E)$ for different CMRR values. In red, the clearance of the two output channels of the heterodyne receiver is shown. Data were collected at the highest LO power compatible with detector linearity. The green region highlights CMRR values ≥40 dB, which we identified as the operational range suitable for randomness generation. (b) Receiver characterization obtained for different CMRR values. The plot shows the characterization of output channel CH2, related to vBS2. Higher CMRR values expand the exploitable linear region for randomness generation, allowing for higher clearance and rate. For CMRR values above 40 dB, no further expansion of the BPD linear region is observed. The noise variance data are extracted from heterodyne detections filtered in the 0.5 to 2.3 GHz frequency range, satisfying the flat-spectra requirement for secure randomness generation.

with $R_{\text{raw}} = 3.6$ GSa/s the equivalent ADC sampling rate after digital re-sampling, which is performed offline. It is worth mentioning that the gain in terms of the quantum conditional min-entropy is due to the expansion of the BPD linear region thanks to the higher CMRR. This allows for the exploitation of a greater local oscillator power while the coefficient $m_{x,p}$ remains unchanged. Figure 5(b) shows the behavior just outlined for one output channel, whereas the other acts similarly. From the acquired data, we estimated a coefficient of $m_x = (5.68 \pm 0.01) \times 10^{-3}$ V^2/W for the photodetector attached to vBS1 and $m_p = (6.95 \pm 0.02) \times 10^{-3}$ V^2/W for the photodetector attached to vBS2, reported in Fig. 5(b). In Fig. 5(a), we also reported the device's classical min-entropy $H_{\min}(X)$, a quantity that upper bounds $H_{\min}(X|E)$ and represents the number of truly random bits that can be extracted by considering a fully trusted randomness generator. As can be seen, the gap among the latter quantities becomes smaller with increasing CMRR values because the device's clearance improves. This reduces the impact of classical noise, leading to better phase-space quadrature resolution and higher generation rate. Notice that even at low CMRRs, the gap is small, highlighting the capabilities of our heterodyne receiver.

Following the characterization of the QRNG receiver, we collected ∼500 GB of data for random number extraction. For this purpose, we set P_{LO} to 22.5 mW which corresponds to the maximum value allowing for linear operation of the BPDs, given a CMRR of at least 40 dB. After the acquisition and preprocessing, which accounts for spectral isolation through digital resampling, we distilled random numbers with a two-universal hashing function implemented as a Toeplitz bit-wise matrix-vector multiplication. The latter used $n = 28{,}532$ rows and $m = 38{,}208$ columns resulting in an individual-run epsilon-security parameter of the order of $\varepsilon \sim 10^{-40}$ and an actual generation rate

$$R_{\text{sc}} = \left(\frac{n}{m}\right) n_{\text{bit}} R_{\text{raw}} \approx 43.01 \text{ Gbit/s}, \tag{5}$$

where $n_{\text{bit}} = 16$ is the number of bits acquired for each heterodyne outcome. Hence, with such choices concerning preprocessing and the matrix dimensions, we obtained ∼48 GB of hashed data from the original ∼500 GB of raw heterodyne measurements with an overall security parameter $\varepsilon' \sim 10^{-33}$. Subsequently, the processed random numbers were analyzed using NIST standard random test battery suits, with the results reported in Appendix C. The results did not reveal any significant non-ideality in the randomness of the generated numbers.

4 CV-QKD Configuration

In this section, we evaluate the capabilities of our PIC, configured as a heterodyne receiver, for CV-QKD applications. We opted for the discrete-modulated coherent states protocol,[49] specifically employing the quadrature phase-shift-keying constellation. Compared with the Gaussian modulation technique,[50] the constellation-based method mitigates some implementation limitations such as the need for a continuous Gaussian state encoder, low reconciliation efficiency, and computationally demanding error correction procedures,[51] albeit at the cost of a reduced performance in terms of secret key rate (SKR). The latter is computed using the Devetak–Winter bound,[52] expressed as $\text{SKR} = \beta I_{\text{AB}} - \chi_{\text{BE}}$, where β is the error correction efficiency, I_{AB} is the mutual information between Alice and Bob, and χ_{E} is the Holevo bound, which upper bounds the information accessible to Eve about Bob's data in the reverse reconciliation scenario. Notice that in our setup, Alice is represented by the source and signal line without ATT and the quantum channel, and Bob comprises the LO line and optical Rx. Although I_{AB} can be determined from Alice's and Bob's data, the Holevo bound is

computed as the worst-case scenario compatible with Bob's measurement. To this end, we used the theoretical framework of Ref. 49 and extended it to account for the trusted detector assumption, where the efficiency η and the electronic noise V_{el} of the receiver are characterized and considered inaccessible to an eavesdropper (this work will be detailed in a future publication). A detailed explanation of the receiver characterization procedure is given in Appendix B. At each round of the protocol, the covariance matrix of Alice's and Bob's data $\langle X_A X_B \rangle$ is computed and Alice's variance V_A is estimated from the optical power P_{tx} measured by PM-2 as twice the mean number of photon $\langle n \rangle$ per symbol,

$$V_A = 2 \cdot \langle n \rangle = 2 \frac{P_{\mathrm{tx}}}{E_{\mathrm{ph}} R}, \tag{6}$$

where E_{ph} is the photon's energy, and R is the system's repetition rate. Then, χ_{E} is bounded by estimating the channel's parameters, namely, the transmittance T and the excess noise ξ_A reported at Alice's side, and using the calibrated values V_A, η and V_{el}. The channel transmittance T and excess noise are obtained from the following relations:

$$\langle X_A X_B \rangle = \sqrt{\frac{\eta T}{2}} V_A, \tag{7}$$

$$V_B = 1 + V_{\mathrm{el}} + \frac{\eta T}{2} V_A + \frac{\eta T}{2} \xi_A, \tag{8}$$

whereas the receiver losses η are derived from detector efficiency (Appendix B) and PIC insertion losses.

4.1 Experimental Setup

The setup used to assess the PIC's performance for CV-QKD is shown in Fig. 2. The signal line phase encoder generates a 250-MBaud optical QPSK signal. The modulating signals provided by the FPGA are shaped with a root-raised-cosine (RRC) filter with a roll-off factor of 0.3 to ensure efficient use of the electronic bandwidth. Then, the variable optical attenuator VOA-2 is used to optimize the modulation variance V_A, considering the additional attenuation provided by the fixed optical attenuator ATT. Moreover, the polarization controller PC-2 ensures that the polarization state of both signal and LO is matched at the PIC's input. To estimate V_A, 99% of the optical power is tapped with BS-2 and measured by the power meter PM-2. As both the signal and the LO originate from the same laser, we used a fiber delay of length ΔL to match both optical paths, reducing phase instabilities. The choice to rely on a shared laser simplifies the experimental implementation of the setup. Although the local–local oscillator (LLO) technique is preferred for actual CV-QKD implementations due to security, performance, and practical reasons,[53] the shared approach is still adequate to evaluate the performance of CV-QKD systems. However, we note that our heterodyne receiver can, in principle, be integrated with a CV-QKD system exploiting the LLO technique, as the additional complexity arises mainly at the DSP stage and is independent of the specific receiver technology adopted.

Upon entering the heterodyne receiver through the input port, the quantum signal interferes with the LO, and its optical quadratures are extracted by a pair of BPDs. Such electrical signals are then digitized by the oscilloscope and streamed to a computer for offline DSP, data analysis, and parameter estimation. The former accounts for a 50-MHz high-pass filter and an RRC filter matching the one used at the transmitter side to reject technical noise and to minimize inter-symbol interferences, respectively.

4.2 Results

The main parameters of our CV-QKD system are summarized in Table 3. As we assumed a trusted detector scenario, the overall system losses η were 0.55, and the electronic noise was 0.029 shot noise units (SNUs), corresponding to a receiver clearance of ∼16 dB. The electronic noise variance was measured when the laser was turned off, and the shot noise variance was obtained by injecting light only into the LO port while the signal input was attenuated by VOA-2 by ∼80 dB. More details can be found in Appendix B. It is worth noting that one of the key advantages of FLM technology for CV-QKD is the low optical losses that such a platform can grant. The modulation variance V_A of the symbols transmitted by Alice was measured using the PM-2 power meter and taking into account the 30-dB optical attenuator ATT. The obtained value is 0.46 SNUs. Then, the excess noise parameter ξ_A and channel transmittance T were determined using Eqs. (7) and (8) with $\langle X_A X_B \rangle$ and V_B estimated by analyzing a dataset of 12.5×10^6 symbols acquired with the oscilloscope. The values obtained were respectively $\xi_A = 0.015$ SNUs and $T = 0.73$. Finally, the asymptotic SKR reached by the system is ∼0.013 bit/symbol, corresponding to ∼3.2 Mbit/s given the 250-MBaud symbol rate.

In our CV-QKD implementation, we adopted a QPSK modulation scheme, which is relatively straightforward to implement. However, this simplicity comes at the cost of a lower secret key rate compared with more sophisticated modulation schemes. As a matter of fact, the best results are obtained using Gaussian modulation, and the latter performance can be approached with high-density discrete constellations. Therefore, to better assess the potential of our system, we simulated the SKR that can be achieved as a function of transmittance, under the assumption that ξ_A, V_{el}, and η do not change and by adopting the optimal V_A for each attenuation. The results are shown in Fig. 6, where we considered QPSK, eight-phase-shift-keying (PSK), 16-PCS-QAM, 64-PCS-QAM, and Gaussian as alternative approaches.

Table 3 Summary of the parameters of the CV-QKD experiment. Results of parameter estimation employing a 250-MBaud QPSK modulation and with reconciliation efficiency set to 95%. The results are obtained by analyzing 50 acquisitions, each with an acquisition time of 1 ms and 25,000 recorded symbols.

Parameter	Symbol	Value	Units
Electronic noise variance	V_{el}	0.029	SNU
Receiver efficiency	η	0.55	
Channel transmittance	T	0.73	
Alice's variance	V_A	0.46	SNU
Excess noise	ξ_A	0.015	SNU
Asymptotic secret key rate	SKR	0.013	bit/symbol
Asymptotic secret key rate	SKR	3.2	Mbit/s

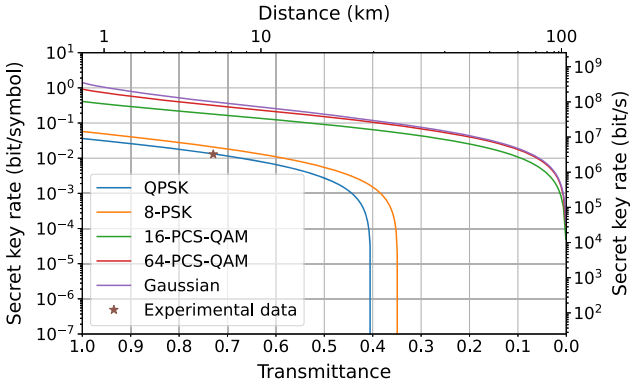

Fig. 6 Simulated CV-QKD performance with different modulation formats. Simulation of the asymptotic secret key rate for different CV-QKD protocols, using the experimental parameters obtained from the parameter estimation reported in Table 3. For each transmittance value, Alice's variance was optimized to maximize the secret key rate. In addition, for PCS-QAM protocols, the probability distribution parameter was optimized as well.

As can be seen, by increasing the constellation dimension of a PSK-based modulation format, performance can improve, although the gains are marginal compared with what can be obtained with the probabilistic constellation shaping (PCS) quadrature amplitude modulation (QAM) or the Gaussian modulation technique. Implementing these higher-performance schemes would require incorporating an intensity modulator, which we plan to investigate in future work to enhance our system's capabilities.

5 Conclusion

In this work, we demonstrated the successful implementation of a glass-based PIC specifically designed to serve as a versatile coherent receiver for CV quantum information protocols. Manufactured using the FLM technique, the PIC offers several advantages, including a compact footprint, low overall losses, and insensitivity to input polarization. These characteristics enable seamless integration with COTS components, such as lasers and wide-band detectors, making it a cost-effective solution for CV quantum information and communications, with promising strategies for integration of active elements, quantum light sources, and detectors already demonstrated.[54–56] The device's high tunability, enabled by the integrated TOPSs, ensures adaptability to different operational conditions. After proper calibration, it supports the implementation of a heterodyne receiver with precise $\pi/2$ quadrature phase shift and high CMRR (>73 dB). These performance metrics enabled the optimal operation of the coherent receiver in both CV-QRNG and CV-QKD applications. In particular, our QRNG device achieved a secure generation rate of 42.74 Gbit/s, which, to the best of our knowledge, represents a record-high result within the source-device-independent framework. On the other hand, our CV-QKD system, employing a QPSK modulation format, reached an SKR of 3.2 Mbit/s. In addition, the PIC exhibited excellent operational stability over extended use, further supporting its suitability for practical quantum communication deployments.

Through this work, we benchmarked and demonstrated the suitability of FLM-fabricated glass PICs for CV quantum communication, demonstrating their effectiveness for coherent heterodyne detection. Besides clear advantages in terms of compactness for integrated solutions, the use of glass offers an intrinsically inert material, highly resistant to environmental perturbations. Moreover, waveguides buried in 3D within the volume are naturally shielded, a feature that provides circuit resilience even under the harsh conditions of space missions,[57,58] further strengthening the real-world relevance of FLM-fabricated devices.

6 Appendix A: PIC Configuration Methods

In this appendix, we describe the procedures used to characterize the heterodyne configuration of the PIC, specifically the balancing of the two output channels and the phase shift applied to the local oscillator to ensure a 90-deg hybrid operation.

Concerning the first point, the architecture of the glass-based PIC provides the capability to tune the splitting ratio of the vBSs through its integrated TOPSs. Considering a single balanced detector connected to a vBS, let i_1 and i_2 denote the photocurrents generated by the BPD's photodiodes in the balanced configuration ($i_1 \sim i_2$). According to the standard definition of CMRR as the ratio between the differential and common-mode gain, such quantity is derived as

$$\begin{aligned}\mathrm{CMRR} &= 20\log_{10}\left(\frac{(i_1+i_2)/2}{|i_1-i_2|}\right)\\ &= -20\log_{10}\left(2\left|\frac{i_1}{i_1+i_2}-\frac{i_2}{i_1+i_2}\right|\right)\\ &= -20\log_{10}(2|2r-1|),\end{aligned} \tag{9}$$

where $r=\frac{i_1}{i_1+i_2}$ corresponds to the photocurrent splitting ratio. To achieve optimal performance, a balanced receiver requires the maximization of the CMRR, which occurs when $i_1 \sim i_2$ (i.e., $r \sim 0.5$), corresponding to a 50:50 BS under the condition of equal photodiode gains. However, in practical implementations, slight mismatches in photodiode responsivities and variations in PIC-to-BPD coupling efficiencies may lead to uneven photocurrents, even with a perfectly balanced vBS. To address this, the PIC allows for the compensation of such non-idealities by acting on the integrated TOPS.

In practice, the CMRR is measured based on the BPD electrical output, which is proportional to the photocurrent difference $i_1 - i_2$. The measurement is conducted in an AC setting by modulating the optical power of the laser with a $f_{\mathrm{mod}} = 500$-kHz sinusoidal waveform. The modulated light is coupled into the PIC, where each vBS splits the optical power among its output arms according to a controllable splitting ratio. The BPD's electrical signals exhibit a residual modulation whose amplitude depends on the photocurrent imbalance. To estimate the CMRR, we consider the two limiting cases of optimal balance and complete unbalance. The first condition is obtained by minimizing the f_{mod} component in the power spectral density (PSD) of the BPD signal. Its minimization, achieved by finely tuning the TOPS bias voltage with sub-millivolt resolution, yields a minimum spectral power P_{bal}. The unbalanced condition is obtained by directing the entire light to a single vBS output arm, resulting in a spectral power P_{un}. The latter power levels are related to the quantities in Eq. (9) as follows:

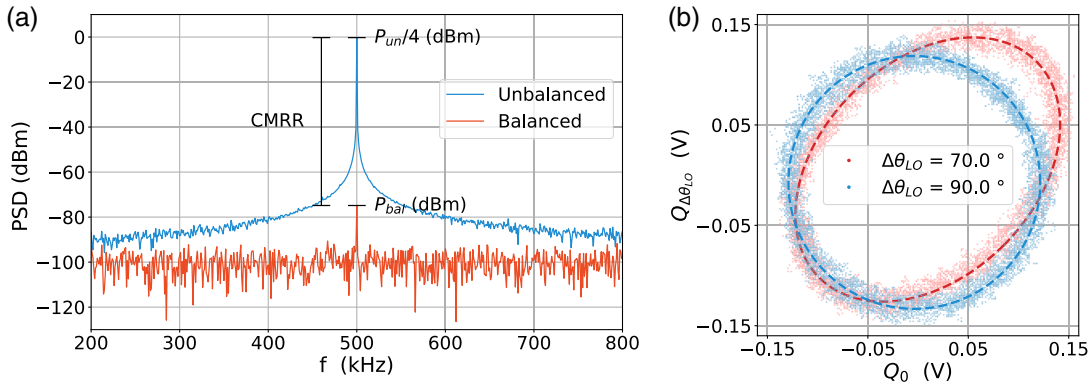

Fig. 7 Example of a PIC heterodyne configuration measurement. (a) Power spectral density (PSD) of CH2 BPD signals, connected to the output of vBS2, shown for the unbalanced (blue) and balanced (red) configuration. The CMRR is extracted from the difference in spectral power at the modulation frequency, yielding a CMRR of 74.6 dB. (b) Phase space representation of the heterodyne quadrature detections acquired with two different LO phase-shifts $\Delta\theta_{\mathrm{LO}}$. The measured quadrature samples are shown as scatter points, with the corresponding elliptical fit indicated by dashed lines. For optimal $\Delta\theta_{\mathrm{LO}} = 90$ deg, the ellipse approaches a circular shape, indicating the detection of two orthogonal quadratures.

$$\begin{cases} P_{\mathrm{bal}} = \frac{G^2}{R} \cdot |i_1 - i_2|^2 \\ P_{\mathrm{un}} = \frac{G^2}{R} \cdot i_1^2 = \frac{G^2}{R} \cdot (i_1 + i_2)^2|_{i_2=0} \end{cases}, \tag{10}$$

where G denotes the transimpedance gain and R the load impedance. The ratio between P_{un} and P_{bal} defines the system's CMRR as

$$\mathrm{CMRR} = 10\log_{10}\left(\frac{P_{\mathrm{un}}/4}{P_{\mathrm{bal}}}\right). \tag{11}$$

Figure 7(a) shows a representative PSD of signals corresponding to the balanced and unbalanced configurations, yielding power levels of $P_{\mathrm{un}}/4 = -0.3$ dBm and $P_{\mathrm{bal}} = -74.9$ dBm. From these values, we obtain a CMRR estimation of 74.6 dB. The system's maximum attainable CMRR is constrained by the noise floor σ_0 in the balanced configuration, measured at -97.7 dBm [Fig. 7(a)]. As P_{bal} cannot fall below this limit, the maximum CMRR and the corresponding parameter δ from Eq. (1) (discussed in the main text) are given by

$$\mathrm{CMRR}_{\max} = P_{\mathrm{un}}/4\ [\mathrm{dBm}] - \sigma_0 = 97.4\ \mathrm{dB}, \tag{12}$$

$$\delta = 10^{-\mathrm{CMRR}_{\max}/20} = 1.3 \times 10^{-5}. \tag{13}$$

The second characterization procedure involves estimating the LO phase shift introduced by TOPS R3, which is required to enable the detection of two orthogonal quadratures of the quantum state at the PIC input. To this end, we employed a classical signal with a triangular phase modulation ϕ_t imposed by the phase encoder. Assuming the LO to be in-phase with the modulated signal in vBS1, the two vBSs sample two different quadratures given by

$$\begin{cases} x \coloneqq Q_0 & = V_1\ \cos(\phi_t)\ \text{from CH1} \\ y \coloneqq Q_{\Delta\theta_{\mathrm{LO}}} & = V_2\ \cos(\phi_t + \Delta\theta_{\mathrm{LO}})\ \text{from CH2} \end{cases}. \tag{14}$$

As can be seen, in the desired case of $\Delta\theta_{\mathrm{LO}} = \pi/2$, the detected quadratures are orthogonal to each other. The pair (x, y) parametrizes an ellipse in the optical phase space, with the signal phase ϕ_t acting as the parametric variable. The resulting ellipse satisfies the implicit equation $Ax^2 + By^2 + Cxy + Dx + Ey = 1$, where the quadratic and cross terms are

$$\begin{cases} A & = (V_1\ \sin(\Delta\theta_{\mathrm{LO}}))^{-2} \\ B & = (V_2\ \sin(\Delta\theta_{\mathrm{LO}}))^{-2} \\ C & = -2(V_1 V_2\ \sin(\Delta\theta_{\mathrm{LO}})\tan(\Delta\theta_{\mathrm{LO}}))^{-1} \end{cases}. \tag{15}$$

From these coefficients, the LO phase shift is computed as

$$\Delta\theta_{\mathrm{LO}} = \arccos\left(-\frac{C}{2\sqrt{AB}}\right). \tag{16}$$

Experimentally, $\Delta\theta_{\mathrm{LO}}$ is estimated by acquiring the voltage traces from the two BPDs, which are then mapped in the phase space and fitted to an ellipse. The fitted curve parameters are then used in Eq. (16) to compute the phase shift. With this method, we perform 20 subsequent acquisitions to obtain an average estimation of $\Delta\theta_{\mathrm{LO}}$, resulting in a measurement uncertainty of $\sim$0.2 deg.

7 Appendix B: Calibration

In this appendix, we provide the details concerning the characterization of the heterodyne receiver used for both QRNG and CV-QKD applications. The analysis accounts for assessing the photodetector responsivity and both electronic noise and clearance estimation.

7.1 Photo-Detector Efficiency

The efficiency of the balanced photodetectors (Thorlabs PDB780CAC) was determined by a responsivity measurement. We injected light with known power P_{in} in each photodiode of the two BPDs separately, and the corresponding amplified

output voltage V_{out} was recorded. The responsivity was then estimated as

$$\mathcal{R} = \frac{I_{\text{out}}}{P_{\text{in}}} = \frac{V_{\text{out}}}{G_{\text{TIA}} \cdot P_{\text{in}}}, \tag{17}$$

where $I_{\text{out}} = \frac{V_{\text{out}}}{G_{\text{TIA}}}$ is the photocurrent generated by the photodiode, and G_{TIA} is the trans-impedance amplifier (TIA) gain. The quantum efficiency η_{PD} is then computed as

$$\eta_{\text{PD}} = \frac{h\nu}{e}\mathcal{R}, \tag{18}$$

where h is Planck's constant, ν is the optical frequency, and e is the elementary charge. The measured efficiencies were 85.12%, 71.68%, 78.12%, and 71.10% averaging at 76.505%, compatible with the typical efficiency of these detectors.

7.2 Electronic Noise and Clearance

The electronic noise of the receiver is estimated when no light is present at the device inputs (neither local oscillator nor signal).

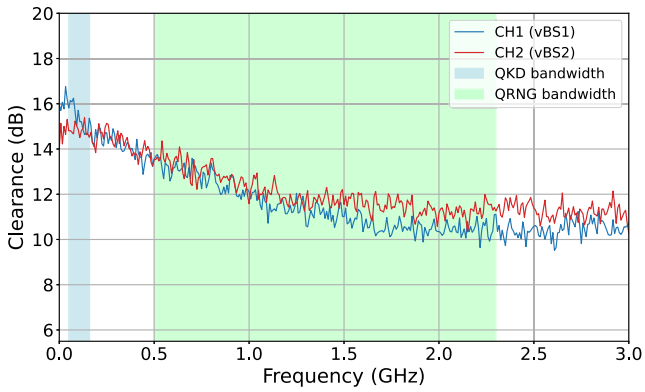

Fig. 8 Clearance of the receiver output channels. The traces are obtained by subtracting the PSD of signals acquired with maximum LO power (compatible with detector saturation) and no LO power. The integral over the spectrum used for QRNG (0.5 to 2.3 GHz) and CV-QKD (50 to 160 MHz) applications provides the system's overall clearance which is ∼12 dB for the former case and ∼15 dB for the second.

The receiver shot noise is acquired when only the local oscillator is present. By computing the difference in the power spectral density associated with shot (PSD_{LO}) and electronic (PSD_{el}) noise, we obtain the receiver clearance (Fig. 8),

$$\text{clearance} = 10\log_{10}\frac{\text{PSD}_{\text{LO}}}{\text{PSD}_{\text{el}}}. \tag{19}$$

As can be seen, this quantity varies across the bandwidth ranges chosen for QRNG (0.5 to 2.3 GHz) and CV-QKD (50 to 162.5 MHz) applications.

For CV-QKD, we ensured that the same DSP used for the signal is also used for both the electronic and shot noise sequences to ensure the selection of the same mode. The variance of the heterodyne measurements with and without LO, σ^2 and σ_{el}^2, is then computed, leading to an estimate of the shot noise variance $\sigma_0^2 = \sigma^2 - \sigma_{\text{el}}^2$. Finally, the electronic noise V_{el} is determined as $V_{\text{el}} = \sigma_{\text{el}}^2/\sigma_0^2$, and the recovered data are normalized in shot noise units by dividing the data by σ_0.

8 Appendix C: Randomness Statistical Tests

The random string generated by the presented QRNG and processed through a randomness extraction procedure was tested with the NIST SP 800-22 battery of statistical tests for randomness assessment. We generated 345 binary files with a length of 10^9 bits. The suite divides each file into 10^3 substrings with a length of 10^6 bits. A total of 188 tests are then applied to the set of substrings and each test outputs a p-value. For each test, two criteria are then used to assess whether a file has passed it. One checks that the proportion of substrings with a p-value larger than 10^{-2} is above a given threshold. The other is a second-order test checking whether the previous 10^3 p-values are uniformly distributed: a chi-square test is applied to their distribution, and the test is passed if the resulting p-value is larger than 10^{-4}. In Fig. 9, we report a heatmap of the passing ratios for the files tested. From the map, we excluded tests from 160 to 185 corresponding to the random excursion and random excursion variant test, because they feature passing thresholds that vary from file to file. In Fig. 10, we instead report the second-order uniformity p-values. The results of the analysis did not indicate any suspicious behavior, as no tests consistently failed.

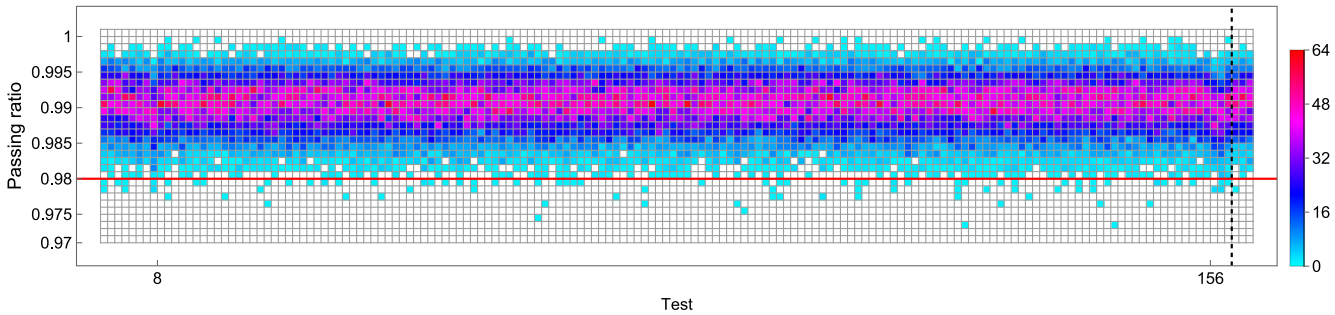

Fig. 9 Heatmap of the passing ratio for the NIST battery applied to 345 files with a size of 10^9 bits. Columns correspond to the tests from 1 to 159 and from 186 to 188 (after the dashed line). Columns from 9 to 156 correspond to the non-overlapping template test. The solid red line is the passing threshold. Tests from 160 to 185 are not reported because they feature a different threshold for each of the files.

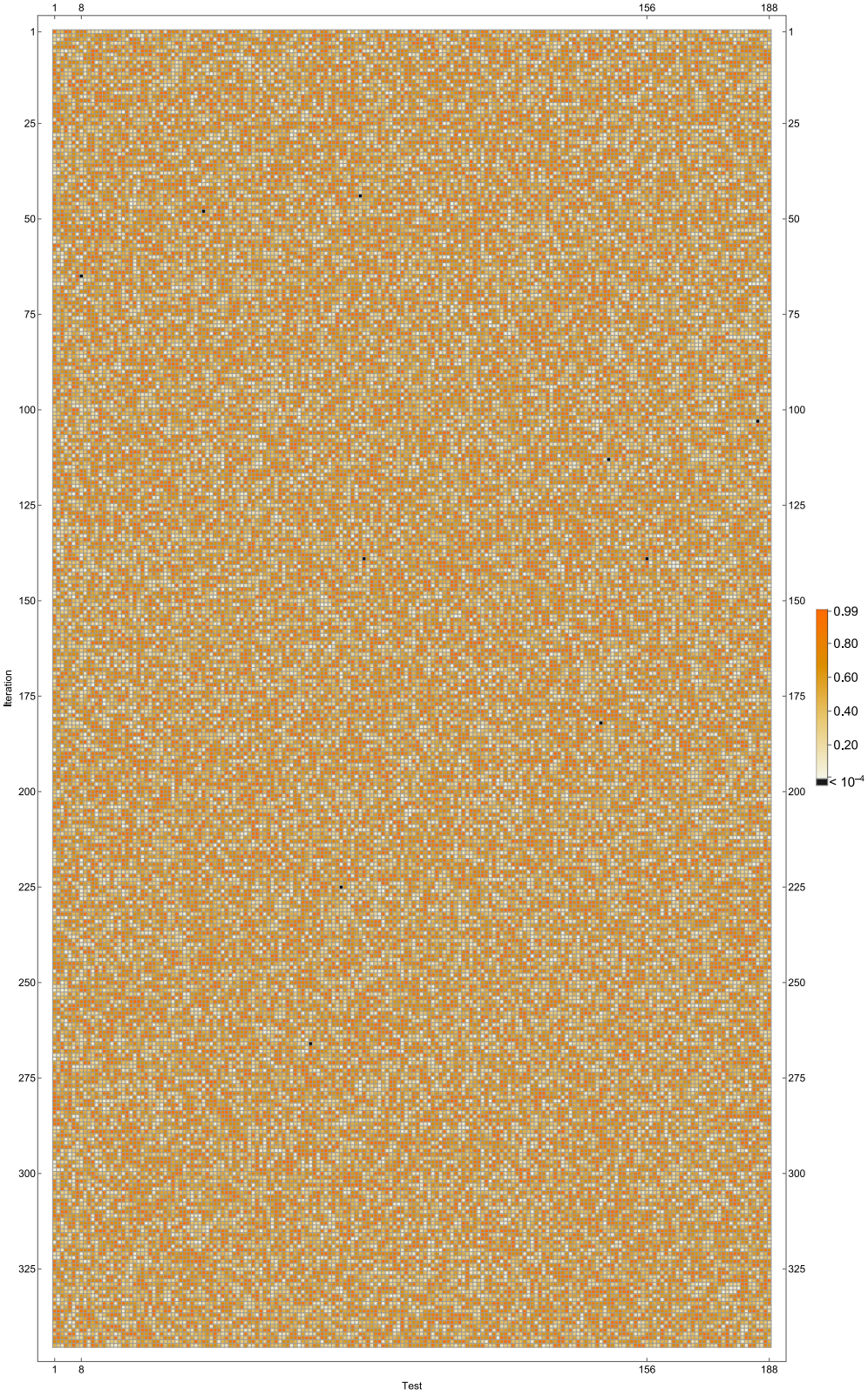

Fig. 10 *p*-values of the second-order test on the uniformity of the *p*-values. Each row corresponds to a file analyzed, whereas each column corresponds to a test. A *p*-value lower than 10^{-4} is considered critical and is flagged in black.

Disclosures

The authors declare that they have no competing interests.

Code and Data Availability

The data and code supporting this study are available from the corresponding author upon reasonable request.

Author Contributions

GG manufactured and calibrated the photonic device. AP performed the optical characterization. TB supervised the optical characterization. TB and AP performed the QRNG experiment. DM and TB performed the NIST tests. MS, AP, and YP performed the QKD experiment. YP compared the results with those of other state-of-the-art PICs. GC and RO supervised the chip design and fabrication process. DM, GV, PV, and MA supervised the quantum application experiments. MA, GV, PV, and RO conceived the initial concept and methodology. AP and TB wrote the initial draft of the paper. All authors discussed the methods and the results and contributed to the writing of the final paper.

Acknowledgments

This work was financially supported by European Union's Horizon Europe research and innovation program under the project Quantum Secure Networks Partnership (QSNP), Grant Agreement No. 101114043. Views and opinions expressed are however those of the authors 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. In addition, we acknowledge the scientific-technical contribution of the QUADRIC project, by the European Union – NextGenerationEU Italian National Resistance and Resilience Plan (PNRR) Mission 4, Component 2, Investment 1.3, CUP C63C22000830006.

References

1. D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent ultrafast quantum random number generation," *Phys. Rev. Lett.* **118**(6), 060503 (2017).
2. M. Avesani et al., "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps," *Nat. Commun.* **9**(1), 5365 (2018).
3. T. Gehring et al., "Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information," *Nat. Commun.* **12**(1), 605 (2021).
4. Y. Zhang et al., "Continuous-variable quantum key distribution system: past, present, and future," *Appl. Phys. Rev.* **11**(1), 011318 (2024).
5. T. Wang et al., "High key rate continuous-variable quantum key distribution using telecom optical components," *New J. Phys.* **26**(2), 023002 (2024).
6. A. A. E. Hajomer et al., "Chip-based 16 GBaud continuous-variable quantum key distribution," arXiv:2504.09308 (2025).
7. J. Wang et al., "Integrated photonic quantum technologies," *Nat. Photonics* **14**(5), 273–284 (2020).
8. G. Moody et al., "2022 roadmap on integrated quantum photonics," *J. Phys. Photonics* **4**(1), 012501 (2022).
9. J. Aldama et al., "Integrated QKD and QRNG photonic technologies," *J. Lightw. Technol.* **40**(23), 7498–7517 (2022).
10. W. Luo et al., "Recent progress in quantum photonic chips for quantum communication and internet," *Light Sci. Appl.* **12**(1), 175 (2023).
11. L. Huang and H. Zhou, "Integrated Gbps quantum random number generator with real-time extraction based on homodyne detection," *J. Opt. Soc. Am. B* **36**(3), B130–B136 (2019).
12. B. Bai et al., "18.8 Gbps real-time quantum random number generator with a photonic integrated chip," *Appl. Phys. Lett.* **118**(26), 264001 (2021).
13. T. Bertapelle et al., "High-speed source-device-independent quantum random number generator on a chip," *Optica Quantum* **3**(1), 111–118 (2025).
14. F. Raffaelli et al., "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," *Quantum Sci. Technol.* **3**(2), 025003 (2018).
15. G. Zhang et al., "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nat. Photonics* **13**(12), 839–842 (2019).
16. Y. Jia et al., "Silicon photonics-integrated time-domain balanced homodyne detector for quantum tomography and quantum key distribution," *New J. Phys.* **25**(10), 103030 (2023).
17. Y. Piétri et al., "Experimental demonstration of continuous-variable quantum key distribution with a silicon photonics integrated receiver," *Optica Quantum* **2**(6), 428–437 (2024).
18. L. Li et al., "On-chip source-device-independent quantum random number generator," *Photonics Res.* **12**(7), 1379–1394 (2024).
19. J. F. Tasker et al., "A Bi-CMOS electronic photonic integrated circuit quantum light detector," *Sci. Adv.* **10**(20), eadk6890 (2024).
20. A. A. Hajomer et al., "Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver," *Optica* **11**(9), 1197–1204 (2024).
21. C. Bruynsteen et al., "100-Gbit/s integrated quantum random number generator based on vacuum fluctuations," *PRX Quantum* **4**(1), 010330 (2023).
22. A. Bomhals, C. Bruynsteen, and X. Yin, "64.9 Gbit/s real-time quantum random number generator," in *ECOC 2023: 49th Eur. Conf. Opt. Commun.*, pp. 1174–1177 (2023).
23. P. Kincaid et al., "Source device independent quantum random number generator with integrated InP photonics," in *Int. Conf. Photonics Switch. Comput. (PSC)*, IEEE, pp. 1–3 (2023).
24. J. Aldama et al., "Integrated InP-based transmitter for continuous-variable quantum key distribution," *Opt. Express* **33**(4), 8139–8149 (2025).
25. G. Corrielli, A. Crespi, and R. Osellame, "Femtosecond laser micromachining for integrated quantum photonics," *Nanophotonics* **10**(15), 3789–3812 (2021).
26. G. D. Marshall et al., "Laser written waveguide photonic quantum circuits," *Opt. Express* **17**(15), 12546–12554 (2009).
27. A. Crespi et al., "Anderson localization of entangled photons in an integrated quantum walk," *Nat. Photonics* **7**(4), 322–328 (2013).
28. A. W. Schell et al., "Three-dimensional quantum photonic elements based on single nitrogen vacancy-centres in laser-written microstructures," *Sci. Rep.* **3**(1), 1577 (2013).
29. A. Crespi et al., "Particle statistics affects quantum decay and Fano interference," *Phys. Rev. Lett.* **114**(9), 090201 (2015).
30. A. Seri et al., "Laser-written integrated platform for quantum storage of heralded single photons," *Optica* **5**(8), 934–941 (2018).
31. Y.-C. Chen et al., "Laser writing of individual nitrogen-vacancy defects in diamond with near-unity yield," *Optica* **6**(5), 662–667 (2019).
32. F. Hoch et al., "Reconfigurable continuously-coupled 3D photonic circuit for boson sampling experiments," *npj Quantum Inf.* **8**(1), 55 (2022).
33. R. Sax et al., "High-speed integrated QKD system," *Photonics Res.* **11**(6), 1007–1014 (2023).
34. T. T. Fernandez et al., "Bespoke photonic devices using ultrafast laser driven ion migration in glasses," *Prog. Mater. Sci.* **94**, 68–113 (2018).

35. A. Arriola et al., "Low bend loss waveguides enable compact, efficient 3D photonic chips," *Opt. Express* **21**(3), 2978–2986 (2013).
36. M. Pont et al., "High-fidelity four-photon GHZ states on chip," *npj Quantum Inf.* **10**(1), 50 (2024).
37. R. Albiero et al., "Toward higher integration density in femtosecond-laser-written programmable photonic circuits," *Micromachines* **13**(7), 1145 (2022).
38. F. Ceccarelli et al., "Low power reconfigurability and reduced crosstalk in integrated photonic circuits fabricated by femtosecond laser micromachining," *Laser Photonics Rev.* **14**(10), 2000024 (2020).
39. M. Sabatini et al., "Hybrid encoder for discrete and continuous variable QKD," *Adv. Quantum Technol.* **8**(8), 2400522 (2025).
40. F. Ceccarelli et al., "Thermal phase shifters for femtosecond laser written photonic integrated circuits," *J. Lightwave Technol.* **37**(17), 4275–4281 (2019).
41. Y. Bian et al., "Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip," *Appl. Phys. Lett.* **124**(17), 174001 (2024).
42. S.-H. Jeong and K. Morito, "Novel optical 90° hybrid consisting of a paired interference based 2 × 4 MMI coupler, a phase shifter and a 2 × 2 MMI coupler," *J. Lightwave Technol.* **28**(9), 1323–1331 (2010).
43. J. Yu et al., "High-performance 90° hybrids based on MMI couplers in Si_3N_4 technology," *Opt. Commun.* **465**, 125620 (2020).
44. X. Ma et al., "Quantum random number generation," *npj Quantum Inf.* **2**(1), 16021 (2016).
45. H. Tebyanian et al., "Semi-device-independent randomness from-outcome continuous-variable detection," *Phys. Rev. A* **104**(6), 062424 (2021).
46. M. Avesani et al., "Unbounded randomness from uncharacterized sources," *Commun. Phys.* **5**(1), 273 (2022).
47. NIST, "Random bit generation project: documentation and software," https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software (2014).
48. M. Tomamichel et al., "Leftover hashing against quantum side information," *IEEE Trans. Inf. Theory* **57**(8), 5524–5535 (2011).
49. A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum* **5**, 540 (2021).
50. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.* **88**(5), 057902 (2002).
51. M. Almeida et al., "Secret key rate of multi-ring M-APSK continuous variable quantum key distribution," *Opt. Express* **29**(23), 38669–38682 (2021).
52. I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proc. R. Soc. A: Math. Phys. Eng. Sci.* **461**(2053), 207–235 (2005).
53. B. Qi et al., "Generating the local oscillator 'locally' in continuous-variable quantum key distribution based on coherent detection," *Phys. Rev. X* **5**, 041009 (2015).
54. J. B. Spring et al., "On-chip low loss heralded source of pure single photons," *Opt. Express* **21**(11), 13522–13532 (2013).
55. X. Hou et al., "Waveguide-coupled superconducting nanowire single-photon detectors based on femtosecond laser direct writing," *Opt. Express* **29**(5), 7746–7756 (2021).
56. G. Gualandi et al., "Laser-written reconfigurable photonic integrated circuit directly coupled to a single-photon avalanche diode array," *Light Sci. Appl.* **14**(1), 199 (2025).
57. S. Piacentini et al., "Space qualification of ultrafast laser-written integrated waveguide optics," *Laser Photonics Rev.* **15**(2), 2000167 (2021).
58. N. Ahmadi et al., "QUICK– design of a satellite–based quantum light source for quantum communication and extended physical theory tests in space," *Adv. Quantum Technol.* **7**(4), 2300343 (2024).

Andrea Peri received his master's degree in physics of data from the University of Padua in 2024. He is currently a PhD student in the QuantumFuture Research Group in Padua. His research focuses on quantum communication, with a focus on the intersection of integrated photonics, quantum key distribution and quantum random number generation.

Giulio Gualandi is a PhD candidate in integrated photonics at Politecnico di Milano, working in the FAST group led by Dr. Roberto Osellame (CNR). His research focuses on the design, fabrication, and testing of reconfigurable photonic integrated chips for quantum and classical applications using femtosecond laser micromachining. He earned his MSc degree in engineering physics from Politecnico di Milano in 2022, developing a wavelength division multiplexer via femtosecond laser writing.

Tommaso Bertapelle received his MSc (2020) and PhD (2024) degrees in information and communication technologies from the University of Padova, Italy, where he is now a postdoctoral researcher in information engineering. His work focuses on quantum photonics and quantum information, with applications in quantum random number generation and quantum communication.

Mattia Sabatini obtained his MSc degree in physics from the University of Padova, Italy, in 2022, where he is currently pursuing a PhD in quantum communication. His research focuses on quantum key distribution and quantum random number generation, with particular emphasis on continuous-variable protocols.

Giacomo Corrielli holds a senior researcher position at the Institute for Photonics and Nanotechnologies (IFN) of the National Research Council (CNR) in Milan (Italy). He earned his PhD in physics from Politecnico di Milano in 2015, and his research activity focuses on photonic integrated circuits for quantum technologies, authoring more than 40 papers on this topic. During his career, he completed visiting stays at leading institutions such as ICFO in Barcelona and LMU in Munich. In 2022, he co-founded Ephos, where he serves as CTO, driving the development of next-generation photonic technologies.

Yoann Piétri obtained his PhD in information science from Sorbonne Université in 2024, and pursued his research on quantum communication as a post-doctoral research at the University of Padova. He is currently an associate professor at Sorbonne Université where his research spans quantum communication, photonic integration, energetics and quantum communication-computing interface.

Davide Giacomo Marangon is a researcher in quantum key distribution and quantum random number generation. He is a former assistant professor of quantum technologies at the Department of Engineering of Information at the University of Padova, Italy, and is currently a senior research scientist in the Quantum Information Group at Toshiba Europe Ltd. in Cambridge, UK.

Giuseppe Vallone received his MS degree in physics and his PhD in theoretical physics from the University of Torino, Turin, Italy, in 2002 and 2006, respectively. Since 2024, he has been a full professor with the Department of Information Engineering, University of Padova, Padua, Italy. He has co-authored more than 120 articles in peer-reviewed journals and participated in more than 30 scientific research projects. His research interests include quantum information, experimental quantum optics, and quantum communications

Paolo Villoresi is currently a full professor of physics with the University of Padova, where he teaches quantum optics and related subjects. He has authored more than 170 publications in peer-refereed journals and editor of two books and co-authored more than 200 congress contributions in the areas of quantum communications, quantum optics, laser–matter interaction, and atomic and plasma physics.

Roberto Osellame is a research director at the Institute for Photonics and Nanotechnologies (IFN) of the National Research Council (CNR) in Milan (Italy). He received his PhD in physics from the Politecnico di Torino in 2000. His research interests focus on microfabrication of integrated photonic devices for quantum technologies, lab-on-a-chip, and optical communications. He is co-author of more than 300 publications and holds 15 patents. He is a Fellow of Optica and an ERC awardee.

Marco Avesani is an assistant professor at the University of Padova, where he also obtained his master's degree in physics in 2015 and his PhD in information engineering in 2020. His research is centered on quantum communication, both in fiber and free-space, utilizing bulk and integrated photonics. He focuses on developing high-performance and secure quantum random number generators and quantum key distribution systems. He is also a co-founder of ThinkQuantum, a university spinoff commercializing quantum cybersecurity solutions.