



HAL
open science

Experimental demonstration of Continuous-Variable Quantum Key Distribution with a silicon photonics integrated receiver

Yoann Piétri, Luis Trigo Vidarte, Matteo Schiavon, Laurent Vivien, Philippe Grangier, Amine Rhouni, Eleni Diamanti

► To cite this version:

Yoann Piétri, Luis Trigo Vidarte, Matteo Schiavon, Laurent Vivien, Philippe Grangier, et al.. Experimental demonstration of Continuous-Variable Quantum Key Distribution with a silicon photonics integrated receiver. 2023. hal-04307734

HAL Id: hal-04307734

<https://hal.science/hal-04307734>

Preprint submitted on 26 Nov 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Experimental demonstration of Continuous-Variable Quantum Key Distribution with a silicon photonics integrated receiver

Yoann Piétri,¹ Luis Trigo Vidarte,² Matteo Schiavon,¹ Laurent Vivien,³ Philippe Grangier,⁴ Amine Rhouni,¹ and Eleni Diamanti¹

¹*Sorbonne Université, CNRS, LIP6, 75005 Paris, France*

²*ICFO-Institut de Ciències Fòniques, The Barcelona Institute of Science and Technology, Castelldefels (Barcelona) 08860, Spain*

³*Université Paris-Saclay, CNRS, Centre de Nanosciences et de Nanotechnologies (C2N), 91120 Palaiseau, France*

⁴*Université Paris-Saclay, Institut d'Optique Graduate School, CNRS, Laboratoire Charles Fabry, 91127 Palaiseau, France*

(Dated: November 14, 2023)

Quantum Key Distribution (QKD) is a prominent application in the field of quantum cryptography providing information-theoretic security for secret key exchange. The implementation of QKD systems on photonic integrated circuits (PICs) can reduce the size and cost of such systems and facilitate their deployment in practical infrastructures. To this end, continuous-variable (CV) QKD systems are particularly well-suited as they do not require single-photon detectors, whose integration is presently challenging. Here we present a CV-QKD receiver based on a silicon PIC capable of performing balanced detection. We characterize its performance in a laboratory QKD setup using a frequency multiplexed pilot scheme with specifically designed data processing allowing for high modulation and secret key rates. The obtained excess noise values are compatible with asymptotic secret key rates of 2.4 Mbit/s and 220 kbit/s at an emulated distance of 10 km and 23 km, respectively. These results demonstrate the potential of this technology towards fully integrated devices suitable for high-speed, metropolitan-distance secure communication.

I. INTRODUCTION

Quantum Key Distribution (QKD) is a cryptographic task enabling two trusted users, usually referred to as Alice and Bob, who have access to an insecure quantum channel and a public but authenticated classical channel, to exchange a random string of bits whose security is ensured by the laws of physics. This means that a potential eavesdropper has a negligible amount of information on the final string of bits, the secret key [1]. This task combined with the use of encryption schemes such as the One-Time Pad (OTP) [2] allows for information-theoretic, long-term security for secret message exchange.

The two main families of QKD protocols rely on encoding the information on discrete degrees of freedom of single photons, such a polarization [3], in so-called discrete-variable (DV) QKD, or on continuous degrees of freedom of light, such as the quadrature components of coherent states [4], in CV-QKD. Driven by the need to protect the transmission of sensitive data against attacks enabled by rapid technological advancements, significant progress has been achieved in QKD systems from both families in the last years [1, 5]. This includes proposals of important variants, such as measurement device independent and twin-field QKD [6, 7], records in secret key generation distance and rate [8–11], and demonstrations or feasibility studies over satellite links [12, 13].

Several challenges towards improving the performance and practical deployment of QKD systems in terms of key rate, distance, practical security, cost, size, stability or satellite communication may be effectively

addressed with photonic integration. For this reason, significant efforts have been put in this direction, for both the transmitter and receiver devices. For DV-QKD systems, which enjoy maturity and good loss tolerance, the integration of transmitters continues to progress with very promising results [14, 15], but there is an important gap with the development of integrated receivers [16]. This is mainly due to the difficulty in integrating avalanche photodiodes and Superconducting Nanowire Single-Photon Detectors (SNSPD) with other photonic circuits. Even with the development of technologies such as waveguide-integrated SNSPD [17], the cooling requirement is an issue since those detectors only achieve their targeted sensitivity at (sub)Kelvin temperatures. CV-QKD systems on the other hand benefit from an operation that only requires coherent detectors with standard room-temperature photodiodes, which opens the way to a high overall level of integration. Although this still remains challenging, some promising demonstrations of integrated circuits capable of performing homodyne detection [18, 19] and applications to CV-QKD [20, 21] have already been shown. In [20], silicon (Si) photonic integrated devices are used for both the transmitter and the receiver. The implemented scheme is based on a pulsed configuration, with a transmitted phase reference (or local oscillator) and homodyne detection. More recent works tend to implement CV-QKD protocols with heterodyne detection and advanced pulse shaping to maximise the bandwidth usage, such as in the work in [21] where the authors used a Si photonic integrated receiver that performs phase-diverse heterodyne detection, with two balanced detectors. While our frequency scheme is similar to the one in this work, our receiver is based on a single balanced

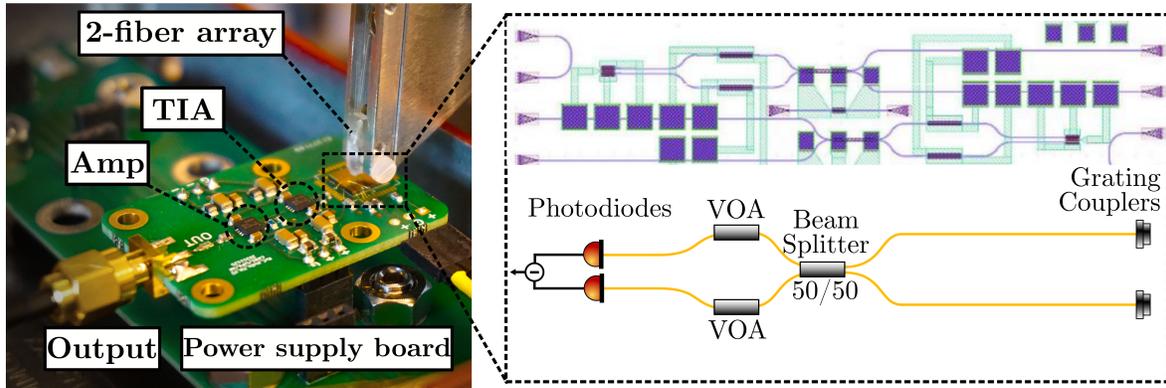


Figure 1. **The CV-QKD Si PIC receiver platform.** On the left, a picture of the platform. The photonic integrated chip (PIC) is wirebonded to the printed circuit board (PCB), which is itself on its power supply board. Optical coupling is done through a fiber array with two fibers on a 5-axis mechanical stage. The transimpedance and voltage amplifiers and the output of the device are also shown. On the right, the layout of the area of interest in the PIC and the associated schematic view, showing two grating couplers, one 50/50 beam splitter, two variable optical attenuators and two photodiodes. The chip hosts other photonic functions that are beyond the scope of this paper.

detector in an RF-heterodyne configuration.

More specifically, in this work we present and characterize a receiver platform based on a Si PIC and we report on its use in a CV-QKD setup with Gaussian modulated states and Optical Single Sideband modulation. We apply a scheme that optimizes bandwidth utilisation similar to the work in [22], featuring specifically designed data processing algorithms, with shaped and frequency displaced quantum symbols, and frequency multiplexed pilots, allowing for high baud rates for the quantum symbols, and hence higher key rates. In section II, we describe the receiver platform and in particular the PIC (subsection II A) and its amplification circuit (subsection II B). Measured performances of the receiver as a standalone device for CV-QKD are provided in section III, while in section IV, we demonstrate the achieved performance when it is used into a full CV-QKD setup. We conclude in section V with further challenges and perspectives.

II. PRESENTATION OF THE RECEIVER PLATFORM

The receiver platform is composed of two main parts, as shown in Fig. 1: the Si photonic integrated circuit and the amplification chain circuit. The PIC was fabricated at CEA/Leti and includes several functions: grating couplers, splitters, Variable Optical Attenuators (VOA) and germanium photodiode detectors. The layout is zoomed on the area of interest showing the photonic components discussed in this paper. The receiver is mounted on a power supply board capable of hosting up to four boards.

A. Photonic Integrated Circuit

The PIC hosts four Balanced Homodyne Detectors (BHD) accessible through input grating couplers. In this application, we use a single BHD.

The signal carrying the quantum information and the local oscillator (LO) are injected using a fiber array through a pair of grating couplers, with a pitch of $127\ \mu\text{m}$. Both travel through waveguides until they are mixed in a 50/50 beam splitter acting as a 180° hybrid mixer. Two germanium photodiodes connected in series receive the mixed outputs through the VOAs. These allow to balance the optical power in both arms, which is critical to avoid saturation and non-linearity. They are driven by applying an external voltage making use of the free carrier plasma dispersion effects to change the waveguide absorption and reflection coefficients [23].

We performed on-chip static current voltage (I-V) measurements using an electrical probe station for voltage biasing and a single mode fiber for optical coupling under dark and illumination conditions (at a wavelength $\lambda = 1550\ \text{nm}$). Fig. 2 shows the results for each photodiode of the BHD. The dark current increases as a function of the reverse voltage while the photocurrent remains almost constant up to 1.5 V. The difference in the dark current contribution for each photodiode is due to dislocation. To guarantee a high photo-to-dark current ratio and for a better common mode rejection, we set the reverse voltage at 0.5 V for all measurements in this work.

B. Amplification chain circuit

The main function of the BHD is to provide a current proportional to the difference between the two incident light powers, leading to common mode suppression. In-

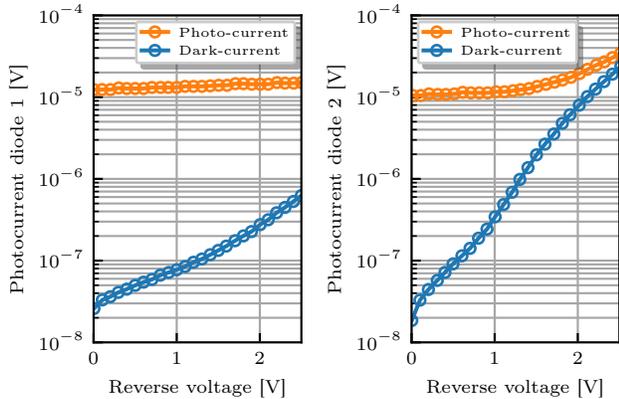


Figure 2. **I-V characteristics of the balanced photodetector.** The curves correspond to the two photodiodes shown in Fig. 1 under dark and illumination conditions. To keep a low dark current and hence a low electronic noise, we choose a reverse bias of 0.5 V.

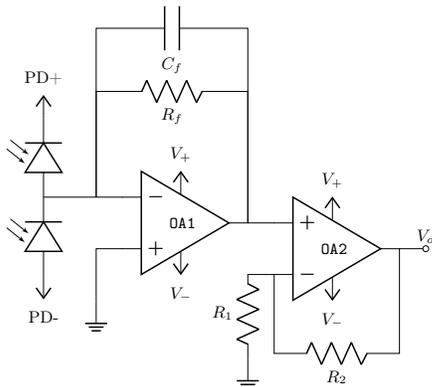


Figure 3. **Principle scheme of the amplification chain.** The circuit is composed of a transimpedance amplifier followed by a non-inverting voltage amplifier. PD+ and PD- are the reverse bias voltages of the photodiodes. The power supply voltage filters and the 50 Ohms output DC filter are not shown.

deed, since the signal and the local oscillator are mixed on the 50/50 beamsplitter and the BHD is balanced thanks to the VOAs, the resulting output current is very weak. Thus, analog signal conditioning (amplification and filtering) before sampling is necessary through first a Transimpedance Amplifier (TIA) and then a voltage amplifier. The methodology for the design of the TIA for our PIC was driven by the optimization of the principal parameters: signal-to-noise ratio (SNR), bandwidth and stability (all related and sensitive to parasitic components). We also emphasize the importance of the output impedance matching and the supply voltage filter in obtaining the best noise performance.

We studied several TIA architectures based on RF amplifiers; see appendix A for more details. The tests of the electronics were performed both alone, using electronic test inputs, and with a bulk BHD made of

photodiodes (Hamamatsu) before a final test with the PIC. After a series of comparative tests, we selected the OPA818 (Texas Instruments) for its best trade-off between gain-bandwidth product and SNR. We set the TIA minimum acceptable specifications for our system to be a closed-loop Fc_{-3dB} bandwidth = 100 MHz, with a clearance (shot noise to electronic noise ratio) of at least 10 dB.

The scheme of the BHD is given in Fig. 3. The first stage is the TIA, whose gain is defined by R_f , and the minimum phase margin for stability is ensured by the compensation capacitor C_f . The second stage is the non-inverting voltage amplifier whose gain is set by R_1 and R_2 . The I-V characteristics discussed previously have shown that PD+= 0.5 V and PD-= -0.5 V, while reducing the junction capacitance, guarantee the optimum bias point for an identical responsivity at low dark currents for both photodiodes of the BHD. Following a thorough iterative procedure between simulations and fine tuning tests, we optimized the gain and capacitance values of the amplification chain circuit; see appendix A for more details.

Fig. 4 shows the BHD noise performance for the two designed receivers, namely the bulk detector with the Hamamatsu photodiodes ($C_f = 250$ fF) and the PIC receiver platform ($C_f = 200$ fF). The significant improvement of the frequency bandwidth and the SNR that we observe for the PIC receiver was achieved due to the choice of a wire bonding solution of the PIC instead of a package and to a meticulous routing on PCB, which suppress almost all parasitic components. We estimate the resulting total equivalent input capacitance to be in the range of 1.8 pF – 2 pF.

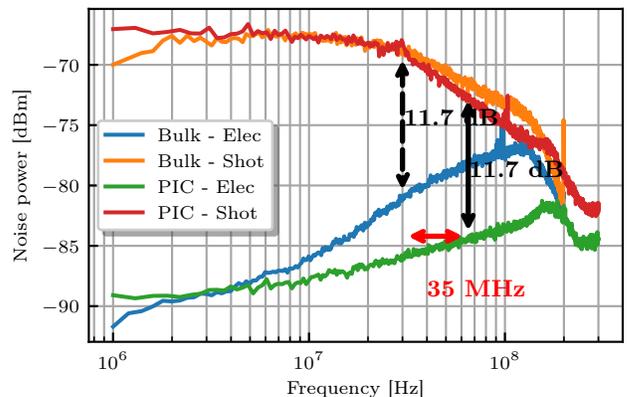


Figure 4. **Noise performance comparison between PIC and bulk BHDs.** The curves show a significant increase in the frequency bandwidth for an identical TIA between a solution with bulk photodiodes from Hamamatsu and a second with integrated photodiodes. In the second case, the parasitic capacitance at the input of the TIA is considerably reduced with respect to the test with bulk photodiodes due to wire bonding. In the working frequency range, the clearance has therefore been improved.

III. PERFORMANCE OF THE CV-QKD RECEIVER PLATFORM

The performance of the receiver platform was first evaluated as a standalone device checking that it is linear and shot noise limited. We also measured the clearance and efficiency, which are necessary for calculating the secret key rate (SKR) of the CV-QKD exchange. Finally, we measured the frequency bandwidth of the system, which is required to bound the symbol rate and the parameters of the Digital Signal Processing (DSP), which is, as we will see later, crucial for the optimisation of the system performance.

A laser at a wavelength of 1550 nm was used to characterize the receiver. The injected power to the chip was manually controlled with an external VOA and a 1-to-2 50/50 beam splitter, with one output to the chip and the other to an optical power meter. A two channel voltage power was used to reverse bias and to monitor the photocurrent of each photodiode. The reverse bias voltage was set to 0.5 V. A second low noise power supply source was used to power the amplification circuit through adapted on-board filters with +5 V and -5 V. The two on-chip VOAs were driven with individual variable voltages that can be tuned between 0 V and +5 V. The output of the receiver was connected to a spectrum analyser (Rohde&Schwarz FPL1003).

We first determined the receiver's efficiency by measuring its responsivity as follows:

$$\eta = \frac{1}{1.25} \frac{I_+ + I_-}{P_{LO}}, \quad (1)$$

where P_{LO} is the LO power and 1.25 A/W is the maximal responsivity at 1550 nm. The VOAs were not polarized, in order to get the maximal reachable efficiency, and the responsivity was measured with a linear regression over an acquisition of several input powers, for both inputs. For the best receiver among the devices that we tested, the efficiency from the input of the fiber array to the detection was around 26%.

We then measured the linearity, bandwidth and the electronic-to-shot-noise ratio which are the three more important characteristics along with the efficiency for a CV-QKD receiver. For the latter parameter, the clearance was actually measured, which differs from the electronic-to-shot-noise ratio in the following sense:

$$\begin{aligned} \text{electronic-to-shot-noise ratio} &= V_{el} = \frac{\sigma_{el}^2}{\sigma_0^2} \\ \text{clearance} &= \frac{\sigma_0^2 + \sigma_{el}^2}{\sigma_{el}^2} \simeq \frac{1}{V_{el}}, \end{aligned} \quad (2)$$

where σ_{el}^2 and σ_0^2 are the noise variance of the electronic noise and shot noise, respectively, and the approximation is true in the regime where $\sigma_{el}^2 \ll \sigma_0^2$. The clearance is typically given in dB and can be found by subtracting the noise power under illumination by the noise power with no illumination. However the electronic and shot noise are actually frequency-dependent;

this is why we will present part of these results as Power Spectral Densities (PSDs), and these equations are then true when we integrate over the frequency spectrum. For the CV-QKD protocol, the considered spectrum is the bandwidth where the signal lies.

To estimate the three characteristics, the on-chip VOAs were tuned to reach the best common mode suppression (and prevent saturation of the receiver) and the noise power density was acquired for different input powers (including no input power for electronic noise). Those noise densities are plotted in Fig. 5.

As expected, the noise power increases with respect to the input optical power and should increase linearly. The linearity can be checked by plotting the integration of this noise as a function of the input power, as shown in Fig. 6. Here we see that the noise varies linearly until we reach an input power of about 8 mW. Knowing the global efficiency, we can estimate that the saturation happens at approximately 1.1 mW of received power per photodiode.

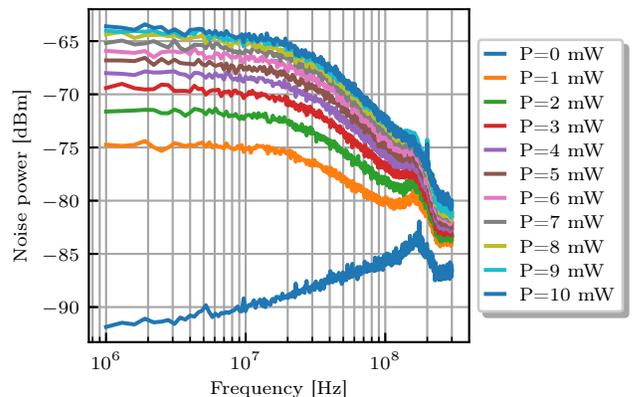


Figure 5. **Noise Power Spectral Densities (PSDs) for several input LO power levels.** The power is given at the input of the receiver. The result for $P = 0$ mW corresponds to the electronic noise.

Knowing the linearity range, we can take the last PSD for which the linearity is ensured, and compute the clearance by calculating the ratio (or difference if in log-scale) with the electronic noise PSD. The clearance depends on the frequency as shown in Fig. 7. We reach a high clearance at low frequencies, around 26 dB at 1 MHz, and then it decreases with the frequency. The frequency bandwidth of the receiver is defined relatively to this clearance. As a clearance greater than 10 dB allows in general for CV-QKD operation, we choose this threshold to define the bandwidth, which is thus around 150 MHz for our PIC receiver. However, the spectrum up to 250 MHz can be used also to place the classical signals for recovering the clock, the frequency and the phase (the pilot tones), since they can withstand more electronic noise (relative to the shot noise) than the quantum signal.

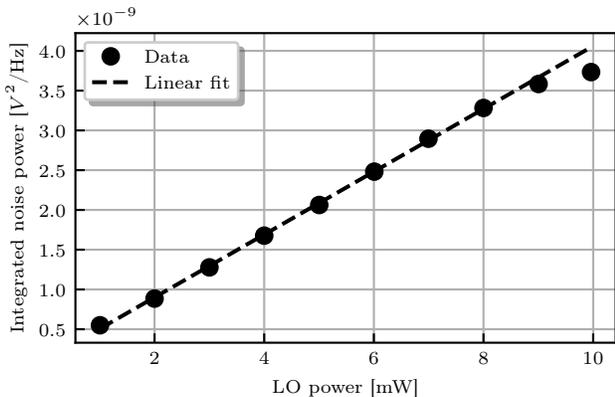


Figure 6. **Noise integration vs. input LO power.** The integration bandwidth is the bandwidth of the spectrum acquisition, *i.e.* 300 MHz. The linearity is ensured up to 8 mW of optical input power for this detector. The linear fit in the figure corresponds to the experimental values until 8 mW. In this range the dimensional non-linearity was $0.02 \times 10^{-9} \text{V}^2/\text{Hz}$, and relative non-linearity was 0.80%.

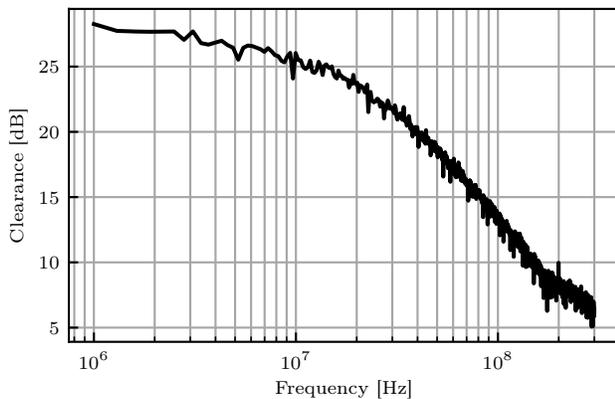


Figure 7. **Clearance vs. frequency.** The clearance decreases with the frequency as the electronic noise increases. It is around 26 dB at 10 MHz, 14 dB at 100 MHz, 9 dB at 200 MHz and 6 dB at 300 MHz.

IV. CV-QKD SYSTEM PERFORMANCE

A. Description of our CV-QKD scheme

We implement a variant of the GG02 protocol [4] using coherent states with Optical Single Sideband (OSSB) modulation. The general steps of the protocol are summarized in Fig. 8. At step 1, Alice draws random symbols according to a predefined probability distribution (Gaussian, Phase-Shift Keying (PSK), Quadrature-Amplitude Modulation (QAM), Probabilistic Constellation Shaping (PCS)-QAM) and prepares the signal for the transmission by applying her Digital Signal Processing (DSP). At step 2, Alice generates the coherent states for the protocol by applying the signal to an IQ modu-

lator and sends them to Bob through a quantum channel defined by its transmittance T and excess noise ξ . At step 3, Bob detects the states using coherent detection, which has efficiency η and electronic noise σ_{el}^2 . At step 4, Bob applies his DSP to the received signal to recover the symbols sent by Alice. More information on the DSP can be found in subsection IV B and Fig. 9. At step 5, Alice and Bob use the classical channel and estimate the parameters needed to calculate the secret key rate, namely the modulation variance V_A , T and ξ . At step 6, they use the classical channel to perform reverse reconciliation, whereby Alice corrects her data to match Bob's data. Finally, at step 7, they perform privacy amplification. At the end of this step, Alice and Bob share a secret common bitstring.

In this work, we implemented steps 1 to 5. While steps 6 and 7 are crucial for a real CV-QKD exchange since they allow the extraction of a secret key, their implementation is beyond the scope of this paper. More information on the related techniques can be found in [24, 25].

The general schematic view of the optical setup is shown in Fig. 8. Alice is composed of a continuous wave laser (NKT Koheron Basik) that is used for the generation of the signal, which goes into an IQ modulator (Exail) controlled by its Modulator Bias Controller (MBC). The role of the MBC is to act as a feedback loop to apply the required bias voltages to the modulator. After the MBC, the path goes into an electronic VOA (Thorlabs VP1150A) and a 95/5 beam splitter, where 95% of the light is measured on a photodiode to estimate Alice's modulation variance V_A , related to the mean number of photons emitted per symbol by $\langle n \rangle = \frac{V_A}{2}$. Finally, a fixed 10 dB attenuator allows reaching the quantum levels required for CV-QKD ($\langle n \rangle \sim 1 - 3$ photons per symbol). Alice's DAC has 1 GHz bandwidth and maximal sample rate 2 GSa/s (Teledyne SDR14Tx).

Fiber loss in the quantum channel is then emulated by an electronic and polarization maintaining VOA (Thorlabs V1550PA) that can attenuate the signal in a range from 0 to 31 dB, allowing for emulation of up to 155 km of distance considering an attenuation of 0.2 dB/km for the optical fiber.

On Bob's side, another continuous wave laser of the same type as the one at Alice's setup is used to generate the powerful LO, in a so-called true local oscillator configuration. The LO is mixed with the signal on chip in a 50/50 beam splitter and detected by the coherent detector. Bob's ADC works at up to 1.25 GHz and at a maximal sample rate of 2.5 GSa/s (Teledyne ADQ32).

We recall here that in CV-QKD one usually works in Shot Noise Units (SNU) [26], where the quantum noise has unit variance, which corresponds to choosing $\hbar = 2$. This means that we normalize all measurements at Bob's side by the shot noise, and every noise variance will thus be given in SNU. At Alice's side, the normalisation is done through the average number of photons $\langle n \rangle$, as explained above, so that Alice and Bob evaluate their quantities in the same units.

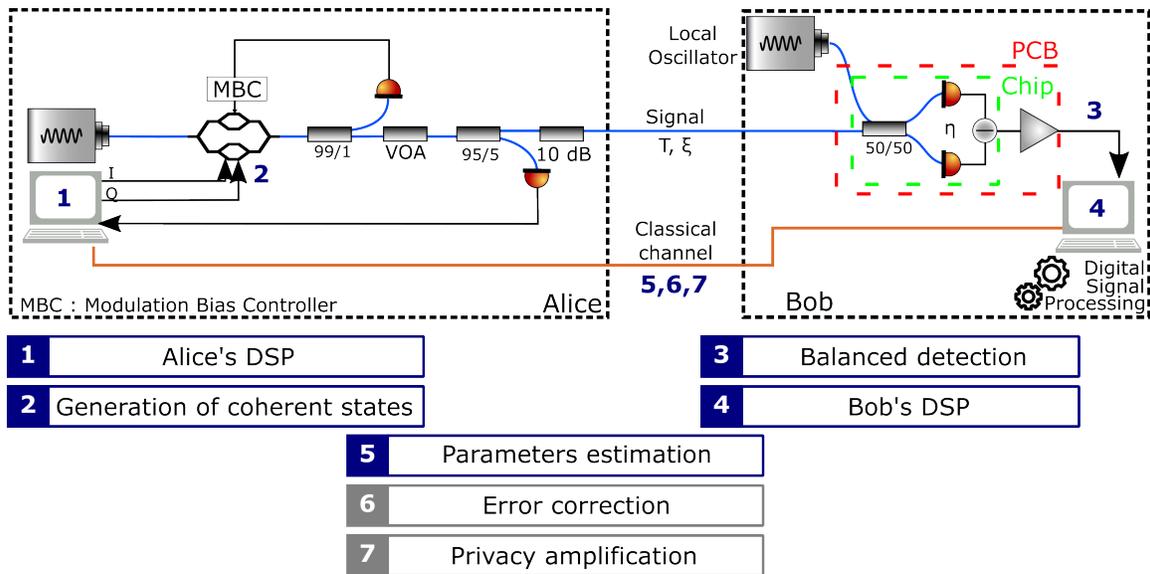


Figure 8. **Experimental scheme of our CV-QKD system.** In our experiment, the classical channel is a local ethernet link. The quantum channel is emulated by an electronic VOA. ADC and DAC are PCIe cards. An electronic VOA is used to tune the output power at Alice's site. In our experiment, steps 1 to 5 of the CV-QKD protocol are implemented.

Calibration is an important part of the CV-QKD protocol implementation since parameters typically vary. A first category of calibrations are made only once (or each time the optical setup is changed). This is the case for the calibration of the power ratio between the monitoring photodiode and the output of Alice (this will later allow us to estimate $\langle n \rangle$), the efficiency of the detector η and the value of the electronic noise, which is assumed to be constant. A second category of calibrations are made between each CV-QKD frame. This concerns the estimation of the shot noise, which allows us to take possible power fluctuations of Bob's laser into account. The average number of photons $\langle n \rangle$ is also computed for each frame. Both the electronic noise and shot noise acquisitions are then processed using the same DSP as for the quantum signal before being used to compute σ_0^2 and σ_{el}^2 (whose value can then slightly change at each round).

B. Digital Signal Processing

Digital Signal Processing is the ensemble of the actions of generating the symbols and preparing them for physical transmission at Alice's side and receiving and recovering the symbols at Bob's side making use of digital filters and operations. We implemented a specifically designed DSP for CV-QKD including the steps shown in Fig. 9.

On Alice's side, the symbols are generated using a modulation pattern and a source of entropy. Here a standard pseudo-random number generator was used as source of entropy but in a full implementation a Quantum Random Number Generator (QRNG) would

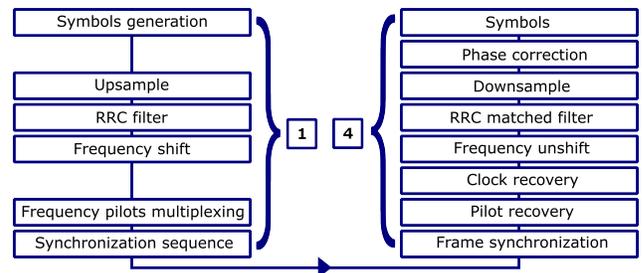


Figure 9. **Digital Signal Processing scheme.** Step 1 corresponds to the DSP on Alice's side, and should be read from top to bottom. Step 4 corresponds to the DSP on Bob's side and should be read from bottom to top.

be used instead. The modulation can be chosen between Gaussian, PSK, QAM and PCS-QAM. Note that although the use of discrete modulations presents significant practical advantages, with a potential of excellent performance [10], the security analysis of such protocols has only recently progressed with security proofs in the asymptotic case [27, 28]. After symbol generation, the sequence is upsampled and pulse shaped using a Root Raised Cosine (RRC) filter. This is done to minimize Intersymbol Interference (ISI) and to optimize the transmission in the physical domain. The quantum symbols are then shifted in frequency, in order to reduce the excess noise coming from low frequencies and to be able to perform an RF-heterodyne, which allows to measure both quadratures with only one balanced detector; see appendix B for more details. Two pilot tones, which are complex exponentials, are then added to the signal at different frequencies. These tones are used to correct the clock difference, as a frequency reference and

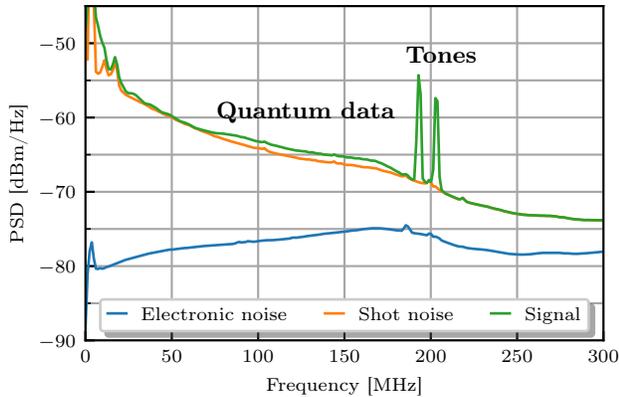


Figure 10. **Power Spectral Density of a representative received sequence.** The DSP parameters are similar to those used in the CV-QKD experiment (see table I). The signal has a bandwidth of 130 MHz and is centered at 125 MHz. The two pilots are at 190 MHz and 200 MHz. The 2 MHz frequency shift corresponds to the beat difference between the two lasers. Some noise can be seen at low frequencies and is filtered out during Bob’s DSP. For display purposes only, Alice’s variance was set at around 62 SNU in this plot. The frequency axis is shown here in linear scale for clarity.

as a phase reference to correct phase noise coming from the transmission. Finally a Zadoff-Chu synchronization sequence is added at the beginning of the sequence.

On Bob’s side, the signal is first detected; the Power Spectral Density of one received signal is shown as an example in Fig. 10. The DSP at Bob’s side goes as follows: the synchronization sequence is recovered by cross-correlating the received signal with the perfect Zadoff-Chu sequence. The frequencies of the two pilot tones are then recovered and the frequency difference allows to correct for a clock mismatch. Then the frequency of one of the pilots gives a frequency reference that is used for carrier frequency recovery. The quantum symbols are unshifted and filtered again using the same RRC filter, which in total gives a Raised Cosine (RC) filter, that is known to minimize ISI. The sequence is then downsampled by finding the optimal sampling point where the variance of the received signal is maximal. The phase is corrected using the phase reference tones and the global phase is corrected by maximising the covariance between Alice’s and Bob’s data.

This DSP scheme requires to set many parameters such as the symbol rate, the roll-off of the RRC filter, the frequency of the reference pilot, and the frequency shift of the quantum symbols (among others). We specifically optimized the values of those parameters to reach the best performance for the integrated receiver platform. The parameters are summarized in Table I.

The DSP was tested to check that it was able to recover frames of symbols sent by Alice, before moving to parameter estimation.

Parameter	Value
Modulation	Gaussian
Rate (R)	100 MBaud
Roll-off (β)	0.3
Bandwidth (B)	130 MHz
Freq. shift (f_{shift})	125 MHz
Pilot tone 1 ($f_{\text{pilot},1}$)	190 MHz
Pilot tone 2 ($f_{\text{pilot},2}$)	200 MHz
Num. of symbols (N)	10^6

Table I. **Summary of the chosen DSP parameters for the PIC-based receiver.** The power ratio between the pilot tones and the quantum signal is around 12 dB.

C. Excess noise estimation

As we discussed previously, in CV-QKD, parameter estimation is an important step where three parameters are typically estimated: Alice’s modulation strength V_A , the channel attenuation T and the excess noise at Alice’s output ξ . These parameters, along with the efficiency and the electronic noise of the receiver and the error correction efficiency, allow computing the secret key rate using the Devetak-Winter formula [29]:

$$k = \beta_{EC} I_{AB} - \chi_{BE}, \quad (3)$$

where β_{EC} is the error correction efficiency, whose standard value in the literature is 95%, $I_{AB} = \log_2(1 + \text{SNR})$ is the maximal mutual information between Alice and Bob, and χ_{BE} is the Holevo bound on the information shared between Bob and Eve, where this formula is true in the reverse reconciliation setting where Bob’s bit string is used to correct Alice’s string to match it with his. The usual technique to estimate those parameters is to use covariance matrices [26]. The mean number of photons measured at Alice’s monitoring photodiode allows finding the conversion factor and scaling Alice’s sequence accordingly. This sequence is then sent to Bob, who computes the covariance matrix and finds:

$$T = 2 \cdot \frac{\langle XY \rangle^2}{\eta V_A^2} \quad (4)$$

$$\xi = 2 \cdot \frac{\langle Y^2 \rangle - 1 - V_{el} - \frac{\eta T}{2} V_A}{\eta T},$$

where X and Y respectively correspond to a subset of Alice and Bob symbols that are announced on the public channel and discarded.

These steps were implemented after the DSP. We performed two experiments for excess noise measurement, each experiment consisting of the acquisition of 300 CV-QKD frames and roughly 15 h of acquisitions and DSP. The first experiment was conducted with the VOA voltage set at 2.5 V (theoretical attenuation of 2 dB corresponding to 10 km of equivalent distance) and the second one with a voltage of 2.9 V (theoretical attenuation of 3.8 dB corresponding to 19 km of equivalent distance). The actual attenuation in the second exper-

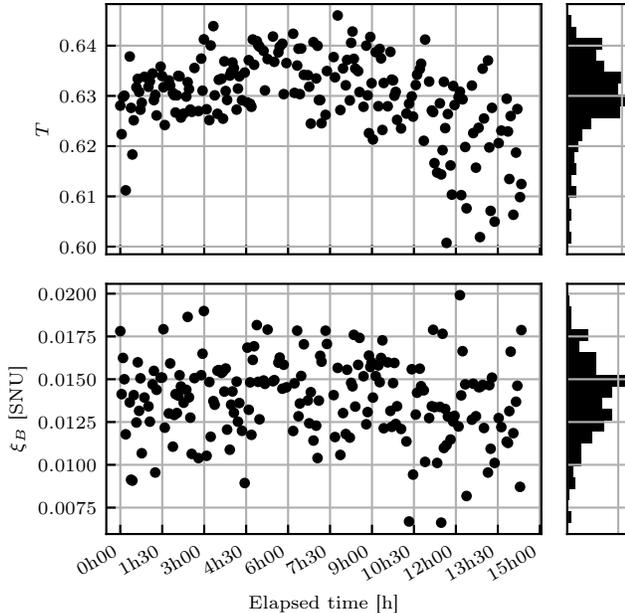


Figure 11. **Excess noise measurements for the successful frames over 15 hours on the receiver platform for the 10 km experiment.** The upper plot shows the evolution of T assuming constant $\eta = 0.175$, while the lower plot shows the evolution of the excess noise ξ_B (at Bob's side). On the right of each plot, the histogram of the data with 20 bins.

iment was measured to be slightly higher, at an equivalent distance of 23 km. The results of the two experiments are shown in Figs. 11 and 12, respectively. Out of the 300 CV-QKD frames the DSP failed 107 times for the first experiment and 82 times for the second experiment, respectively yielding 193 and 218 exploitable frames. These numbers are reflected in the Frame Error Rate (FER) values given in Table II.

The plots show the values of T and $\xi_B = \eta T \xi$ at Bob's side during the measurements. Some fluctuations are clearly seen and we attribute them to physical vibrations slowly moving the fiber array away from the optimal coupling position. Indeed, although our coupling remains stable in time, it is sensitive to mechanical vibrations on the optical table and more generally in the experimental laboratory. A similar analysis (using the same software) with the same setup for Alice and a setup with bulk components for Bob yielded better stability performance. These fluctuations are definitely a challenge for this integrated receiver and indicate that fiber attachment would greatly benefit its operation.

Regarding the coupling, we also remark that the 26% of efficiency obtained in the characterisation experiments was actually hard to reach in full system operation. The optical input that featured the best balance with the minimal attenuation on the VOAs was used for the local oscillator in the CV-QKD experiment to prevent saturation in the electronics and get the best

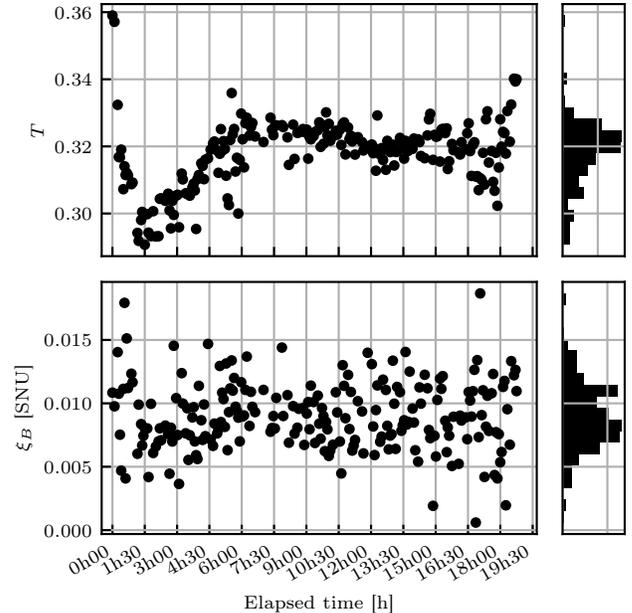


Figure 12. **Excess noise measurements for the successful frames over 18 hours on the receiver platform for the 23 km experiment.** The upper plot shows the evolution of T assuming constant $\eta = 0.161$, while the lower plot is the evolution of the excess noise ξ_B (at Bob's side). On the right of each plot, the histogram of the data with 20 bins.

efficiency on the signal input. This explains why the achieved efficiency was 17.5% and 16.1% respectively for the two experiments; see Table II that summarizes the estimated experimental parameters.

Our experiments yielded an average value of ξ_B of, respectively, 0.014 SNU and 0.009 SNU at Bob's side. As shown in Table II, we have all the parameters necessary to estimate the CV-QKD rate.

Parameter	10 km experiment	23 km experiment
V_A	4.10 SNU	5.45 SNU
T	0.632	0.346
ξ_B	0.014 SNU	0.009 SNU
η	0.175	0.161
V_{el}	0.086 SNU	0.097 SNU
FER	0.36	0.27
Asymptotic SKR	2.4 Mbit/s	220 kbit/s

Table II. **Average values of the estimated parameters for CV-QKD.** The average was calculated respectively on 193 frames and 218 frames for the 10 and 23 km experiments.

For the first experiment, taking the average values of the excess noise and of the transmittance yields a secret key rate (SKR) of 2.4 Mbit/s in the asymptotic case. It is also possible to compute the key rate for each frame, with each of the 193 frames giving a positive key rate, also averaging to 2.4 Mbit/s.

These calculations were performed in the asymptotic

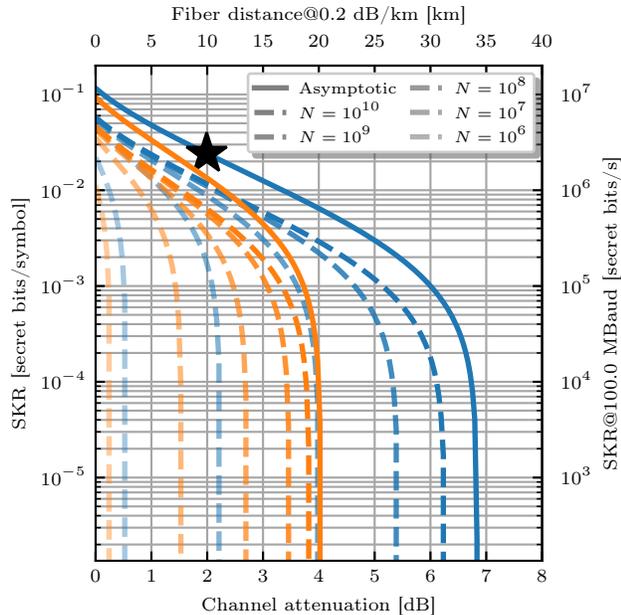


Figure 13. **Secret key rate estimation.** The blue and orange lines correspond to the 10 km and 23 km experiments respectively.

regime, which means that we make the assumption that we can perfectly estimate ξ and T and that we do not have leakage in the privacy amplification step (we still however consider the error correction efficiency). There are several methods to account for finite-size effects and one of them is to compute the variance of ξ and T over all the frames and then the worst case estimators T_{min} and ξ_{max} such that probability of $\xi_{real} > \xi_{max}$ (respectively $T_{real} < T_{min}$) is less than some ε (usually 10^{-10}). However this method here does not work mainly because the variations in the estimated transmittance and excess noise are high due to the unstable coupling. Instead, we conducted an analysis considering finite-size regime using the method in [30], with the same security parameters. We also take into account the fact that only half of the symbols are actually used for the key generation process while the other half is used for parameter estimation. The Frame Error Rate (FER) is not taken into account in these calculations.

The results for the first experiment are plotted in blue in Fig. 13. The plain lines correspond to the asymptotic case and the dashed lines to different level of finite-size scenarios, *i.e.*, the number of symbols that are considered for the parameter estimation.

We notice that the number of symbols used in our experiment (10^6) is not sufficient to obtain a positive key rate. Expected SKR values for $N = 10^7, 10^8, 10^9$ and 10^{10} symbols are respectively 0.17, 0.88, 1.10 and 1.18 Mbit/s but such a number of symbols is challenging for the DSP and the stability of the system, in particular since, as the DSP will require more time to be executed,

the frames would be more separated temporarily.

For the second experiment, computing the SKR from the average values gives a null result in the asymptotic case as can be seen from the plain orange line in Fig. 13; in particular, we see that it falls at zero at 20 km using the average values of ξ and T . However, we can make the analysis by averaging the frames where the key rate was positive, asymptotic or with finite-size effects. Out of the 218 frames, 99 yielded a positive key rate and taking the average of these values yields a rate of 485 kbit/s, while averaging over all 218 frames gives 220 kbit/s.

We can also compute the finite-size key rate and the frames that gave a positive excess noise and we get the following results: for $N = 10^7, 10^8, 10^9$ and 10^{10} we had among the 218 frames, respectively 1, 28, 70 and 94 frames that gave positive SKR values yielding an average (over the frames with a positive key rate) of 232, 199, 217 and 221 kbit/s, while averaging over all the frames, we obtain 1, 26, 70 and 96 kbit/s.

We also remark that with the parameters used in the 10 km experiment, we would expect to be able to reach a range greater than 20 km. However this would only be true if all the parameters were constant (which is not the case for η for instance) and if the excess noise was indeed coming entirely from the channel (which again is not the case, for instance the DSP is less efficient at lower SNR). We remark as well that the excess noise increases when Alice's variance increases which makes it harder to find the optimal value for the number of photons at Alice's side. In our experiment we made, for each attenuation, a sweep for Alice's variance and took the value that was giving the best key rate on average.

V. CONCLUSION

In this work, we presented a coherent receiver platform based on a Si photonic integrated device with promising intrinsic characteristics for CV-QKD. The measured excess noise was in a valid range for CV-QKD exchange and an asymptotic secret key rate in the order of hundred of kbit/s was computed for attenuation corresponding to metropolitan distances. The receiver is based on a technology that is CMOS compatible, simple and can achieve scaling with low size and low cost.

The performance of the experiment is currently limited by a few factors including the packaging of the chip, especially the optical packaging that limits the efficiency of the receiver, by the electronic chain that can be improved to obtain a higher bandwidth and hence symbol rate, and by the DSP process, where both the memory consumption and computation time can be optimised. The limitations are however not intrinsic to the photonic circuit, thus our results constitute a strong proof-of-principle for PIC-based CV-QKD.

Future versions of integrated receiver platforms could benefit from additional components, including a switch (or fast VOA) on the signal path, to block light during shot noise calibration, on-chip laser generation by

using other PIC platforms such as InP [31], direct 90° mixing for phase-diverse heterodyne detection, and better optical packaging, which is critical for stability and efficiency. On the system level, future perspectives include full CV-QKD transmission, with implementation of error correction and privacy amplification, and experiments with a PIC-based transmitter [32] and receiver.

VI. ACKNOWLEDGMENTS

The authors acknowledge fruitful discussions with the partners of the concluded European Quantum Technologies Flagship project CiViQ. ED, LV and PG deeply thank Delphine Marris-Morini, Mauro Persechino and Melissa Ziebell for essential contributions at early stages of this work [33] and Jean Marc Fédéli from CEA-Leti for circuit fabrication. We acknowledge financial support from the European Union’s Horizon Europe research and innovation program under the grant agreement No 101114043 (QSNP).

-
- [1] 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, and P. Wallden, *Advances in Optics and Photonics* **12**, 1012 (2020).
- [2] C. E. Shannon, *The Bell System Technical Journal* **28**, 656 (1949).
- [3] C. Bennett and G. Brassard (1984) pp. 175–179.
- [4] F. Grosshans and P. Grangier, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [5] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [6] H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [7] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, *Nature* **557**, 400 (2018).
- [8] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussièrès, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, *Phys. Rev. Lett.* **121**, 190502 (2018).
- [9] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, *Phys. Rev. Lett.* **125**, 010502 (2020).
- [10] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, A. Leverrier, E. Diamanti, and P. Grangier, *arXiv:2207.11702 [quant-ph]* (2022), 10.48550/arXiv.2207.11702.
- [11] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, *Nature Photonics* **16**, 154 (2022).
- [12] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, *Nature* **549**, 43 (2017).
- [13] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, *npj Quantum Information* **7**, 3 (2021).
- [14] R. Sax, A. Boaron, G. Boso, S. Atzeni, A. Crespi, F. GrÜnenfelder, D. Rusca, A. Al-Saadi, D. Bronzi, S. Kupijai, H. Rhee, R. Osellame, and H. Zbinden, *arXiv:2211.11560 [quant-ph]* (2022), 10.48550/arXiv.2211.11560.
- [15] J. A. Dolphin, T. K. Paraiso, H. Du, R. I. Woodward, D. G. Marangon, and A. J. Shields, *arXiv:2308.02238 [quant-ph]* (2023), 10.48550/arXiv.2308.02238.
- [16] Q. Liu, Y. Huang, Y. Du, Z. Zhao, M. Geng, Z. Zhang, and K. Wei, *Entropy* **24**, 1334 (2022).
- [17] S. Ferrari, C. Schuck, and W. Pernice, *Nanophotonics* **7**, 1725 (2018).
- [18] C. Bruynsteen, M. Vanhooecke, J. Bauwelinck, and X. Yin, *Optica* **8**, 1146 (2021).
- [19] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, *Quantum Science and Technology* **3**, 025003 (2018).
- [20] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, *Nature Photonics* **13**, 839 (2019).
- [21] A. A. E. Hajomer, C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, S. Bastiaens, U. L. Andersen, X. Yin, and T. Gehring, “Continuous-variable quantum key distribution at 10 gbaud using an integrated photonic-electronic receiver,” (2023), *arXiv:2305.19642 [quant-ph]*.
- [22] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, C. Pacher, T. Gehring, and U. L. Andersen, *Nature Communications* **13** (2022), 10.1038/s41467-022-32161-y.
- [23] L. Vivien and L. Pavesi, *Handbook of Silicon Photonics*, Series in Optics and Optoelectronics (CRC Press, 2016).
- [24] K. Gümüş, T. A. Eriksson, M. Takeoka, M. Fujiwara, M. Sasaki, L. Schmalen, and A. Alvarado, *Scientific Reports* **11**, 10465 (2021).
- [25] E. Bai, X.-q. Jiang, and Y. Wu, *Electronics* **11**, 377 (2022).
- [26] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, *Advanced Quantum Technologies* **1**, 1800011 (2018).
- [27] A. Denys, P. Brown, and A. Leverrier, *Quantum* **5**, 540 (2021).
- [28] J. Lin, T. Upadhyaya, and N. Lütkenhaus, *Phys. Rev. X* **9**, 041064 (2019).
- [29] I. Devetak and A. Winter, *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* **461**, 207 (2005).

- [30] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
- [31] J. Aldama, S. Sarmiento, I. H. López Grande, S. Signorini, L. T. Vidarte, and V. Pruneri, Journal of Lightwave Technology **40**, 7498 (2022).
- [32] J. Aldama, S. Sarmiento, S. Etcheverry, I. L. Grande, L. T. Vidarte, L. Castelvero, A. Hinojosa, T. Beckerwerth, Y. Piétri, A. Rhouni, E. Diamanti, and V. Pruneri, in *2023 Optical Fiber Communications Conference (OFC)* (2023) pp. 1–3.
- [33] M. Ziebell, M. Persechino, N. Harris, C. Galland, D. Marris-Morini, L. Vivien, E. Diamanti, and P. Grangier, in *2015 European Conference on Lasers and Electro-Optics - European Quantum Electronics Conference* (Optica Publishing Group, 2015) p. JSV_4_2.
- [34] A. A. E. Hajomer, N. Jain, H. Mani, H.-M. Chin, U. L. Andersen, and T. Gehring, npj Quantum Information **8**, 136 (2022).

SUPPLEMENTARY MATERIAL

Appendix A: Amplification chain circuit design

The architectures that we considered for the TIA of our PIC were based on RF amplifiers, mainly from Texas Instruments (TI). The design methodology involved AC/DC small-signal and noise analysis using SPICE models, Monte-Carlo simulations, then lab validation on-PCB to confirm the performances using scopes and spectrum analyzers. The electronics was tested alone using electronic inputs and with a bulk BHD made of photodiodes from Hamamatsu (G9801-22) before a final test with the PIC. We noticed for instance, that the RF amplifier OPA855, which offers a high gain bandwidth product (8 GHz) and a low voltage input voltage noise ($0.98 \text{ nV}/\sqrt{\text{Hz}}$) has an important contribution to the total output noise of the detector. This is due to its bipolar input transistors suffering from a high input current noise, which increases with frequency. Also, managing the stability of the OPA855 in a closed-loop topology was not trivial and required a coarse tuning of its (already) large feedback capacitor, thus limiting the frequency bandwidth. We also considered the FET input OPA858 as an alternative solution to the OPA855 due to its interesting announced noise performance, but it is intended for operations in single-supply (e.g. time flight measurement with a single photodiode). Our investigation converged finally to the OPA818 to be a good candidate. It has FET input transistors and could operate at both single (10 V) and dual ($-5 \text{ V}/+5 \text{ V}$) supplies. Despite its lower gain-band product (2.7 GHz) compared to the OPA855 and to the OPA858, it achieves a very low input current noise $3 \text{ fA}/\sqrt{\text{Hz}}$ at 10 kHz ($3 \text{ pA}/\sqrt{\text{Hz}}$ at 100 MHz) and offers a low common-mode input capacitance (1.9 pF) and a wide dynamic output range allowing flexibility for amplification gain setting.

To optimize the amplification chain circuit shown in Fig. 3, we set the TIA gain to $R_f = 10 \text{ k}\Omega$ to reach

a closed-loop FC_{-3dB} -bandwidth of about 150 MHz in simulations for a maximum detector capacitance of 5 pF. The non-inverting gain was set to $R_2/R_1 + 1 = 11$ offering a total chain gain (I to V) of 110 kV/A over the voltage output range of $V_+ = 5 \text{ V}$, $V_- = -5 \text{ V}$. C_f was first determined by simulation regarding the estimated maximum detector capacitance (parasitic, TIA's input and junction capacitors). The total parasitic capacitor is minimized due to appropriate PCB routing skills, by improving electrical bonding and selecting small packages (QFN, WSON,...). The photodiode's junction capacitor depends on the manufacturing process, and its value is inversely proportional to the applied reverse voltage. In our case, under 500 mV, the equivalent Silicon-Germanium BHD capacitor (two parallel junction capacitances) is estimated to be of some dozens of femto-Farad and by far, not the limiting factor of the TIA's frequency bandwidth. Indeed, the feedback capacitance estimated by simulation, requires a review and a fine tuning on PCB to achieve the largest bandwidth while ensuring system stability versus the detector total equivalent capacitance.

Appendix B: Optical coherent detection

A Balanced Homodyne Detector (BHD) can be seen as an amplified quadrature measurement, and usually the term *homodyne optical detection* or simply *homodyne* is used, at least in CV-QKD, to describe the detection of one quadrature, which can be done with one balanced detector.

On the other hand, the term *heterodyne* refers, in CV-QKD, to the simultaneous measurement of the two quadratures. The more straightforward way to do this is by using a 90° instead of a 180° mixer. This is sometimes referred to as *phase-diverse heterodyne*. This however requires two BHDs and extra steps in the DSP (such as equalization for instance).

The technique of measuring both quadratures with only a single balanced detector is called *RF-heterodyne*. It consists of making a frequency displacement of the signal by a frequency f_c . To ensure however that there is no overlap in the frequency spectrum, one has to impose that $f_c > \frac{B}{2}$, where B is the bandwidth of the signal. Also, one has to ensure that only one sideband is modulated on Alice's side; improper sideband suppression can lead to errors and information leakage creating a side channel [34]. This also means that half of the bandwidth is not available and the use of phase-diverse heterodyne would allow a doubling in the SKR.

The RF-heterodyne method was used in the experiments reported in the present work, but we are also investigating the use of multiple BHDs, either to perform phase diversity heterodyne and/or polarisation diversity detection, notably with a power supply board capable of powering up to 4 cards and with the additional required external discrete components. This would however also require a custom fiber array or several coupling stages.