High-speed continuous-variable quantum key distribution with advanced digital signal processing

Matteo Schiavon, Yoann Piétri, Luis Trigo Vidarte, Damien Fruleux, Manon Huguenot, Baptiste Gouraud, Amine Rhouni, Philippe Grangier, Eleni Diamanti

High-speed continuous-variable quantum key distribution with advanced digital signal processing

Matteo Schiavon[1], Yoann Piétri[1], Luis Trigo Vidarte[2], Damien Fruleux[1], Manon Huguenot[3], Baptiste Gouraud[3], Amine Rhouni[1], Philippe Grangier[4] and Eleni Diamanti[1]

[1]*Sorbonne Université, CNRS, LIP6, F-75005 Paris, France*

[2]*ICFO - Institut de Ciènces Fotòniques, The Barcelona Institute of Science and Technology, Castelldefels (Barcelona) 08860, Spain*

[3] *Exail, Modulation Solution Division, Besançon, France*

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

e-mail: matteo.schiavon@lip6.fr

ABSTRACT

Continuous-variable quantum key distribution (CV-QKD) is a promising solution for providing high secure key rates in moderate loss channels. A great advantage with respect to discrete-variable (DV) systems is the use of a technology similar to the one used in classical coherent communication, in particular for the detection system, which can operate at room temperature and benefits from an easier integration process. In addition to this, the use of advanced digital signal processing (DSP) techniques developed for classical communication allows for bandwidth-efficient temporal shaping, which optimizes the performance of the CV-QKD system. These techniques applied to the detected signal are also fundamental for using a locally generated local oscillator, correcting frequency and phase differences using frequency-multiplexed pilots generated by the transmitter. In this presentation, we will describe how these DSP techniques can be applied to a CV-QKD system and show some recent experimental results obtained by our research group, including results for a receiver based on a Photonic Integrated Circuit (PIC).

Keywords: photonics, CV-QKD, DSP, PIC

1. INTRODUCTION

Quantum key distribution (QKD) is a protocol that allows two distant parties, Alice and Bob, to exchange a cryptographic key in an *unconditionally secure* way, meaning that an eavesdropper with infinite computational power but subject to the laws of physics will have a negligible amount of information about it. The security comes from the use of non-commutable observables for the encoding of the information. According to the type of observable, it is possible to divide the protocols between discrete-variable (DV), which use observables whose measurement gives a discrete number of outputs, such as the polarisation of a single photon, and continuous-variable (CV), using observables that take value on a real interval. Discrete-variable protocols have played and still play an important role in the development of quantum information, from the first quantum protocols [1], [2] to the current distance records, both in optical fiber [3] and on satellite [4]. These protocols are based on the use of single-photon detectors, which represent both an advantage, due to the post-selection on non-vacuum pulses, and a disadvantage, since these detectors are based on amplification mechanisms that require meta-stable states of the matter, such as a diode junction polarized above background or superconductivity, and limit the maximum detection rate, since after a detection event it is necessary to bring back the material to the meta-stable state. The use of continuous-variable protocols for quantum communication, on the other hand, relies on the measurement of the two quadratures of a single-mode electromagnetic field, which is based on coherent detection techniques that have been studied for a long time [5] and are currently used for classical communication [6]. These techniques consist in amplifying the quantum properties of the electromagnetic field to a classical regime by using a strong laser beam, the local oscillator (LO), at the receiver side. For this reason, their implementation uses standard photo-diodes, which can reach high efficiency and detection speed at a much lower cost with respect to single-photon detectors. This makes continuous-variable protocols more promising in the low-to-medium loss regime [7], [8], even though some preliminary studies have shown that they can also play a role in situations where losses have a stronger impact, such as satellite quantum communication [9], [10].

The use of the same measurement techniques as in classical optical communication represents a great advantage for the development of CV systems, thanks to the race towards reaching the highest possible transmission rate that characterises this field nowadays [11]. This translates to the development of high speed electronic components for the detection system and to the implementation of techniques for optimizing the use of these components, mainly concerning the shape of the pulses encoding the transmitted symbols and advanced digital signal processing (DSP) techniques for recovering them from the output of the measurement system [6]. The quantum protocol that got the highest advantage from these similarities is CV-QKD, since, differently from other CV protocols in quantum information that may require for instance squeezed states, it allows the encoding of

the information on coherent states [12], like in classical communication. In this article we will briefly describe the system under development at the LIP6 laboratory at Sorbonne University, in close collaboration with Institut d'Optique Graduate School and Exail, focusing on the techniques used and the reasons why we chose them. In addition to this, we will also present the results of the characterization of a receiver based on a Photonic Integrated Circuit (PIC), fabricated in a collaboration with CEA/Leti and C2N, which represents a promising solution towards the miniaturization of CV-QKD systems.

2. THE SYSTEM

2.1 Description of the setup

A scheme setup used for the characterizations described in this article is shown in Figure 1.

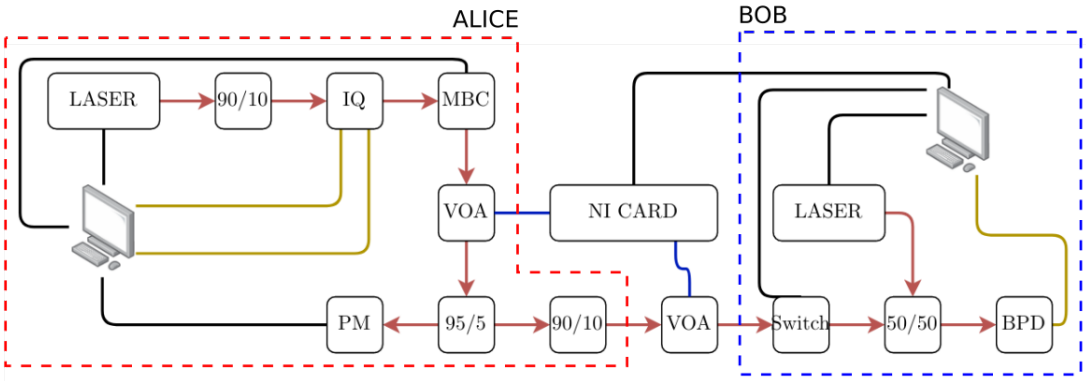

Figure 1: Scheme of the CV-QKD setup. IQ: IQ modulator, MBC: modulator bias controller, VOA: variable optical attenuator, PM: power meter, BPD: balanced photo-detector.

Alice is composed of a continuous-wave laser (PurePhotonics PPCL590), which is split by a 90:10 beam-splitter. The 10% output is sent to an IQ modulator (Exail), which is composed of two amplitude modulators with a relative phase shift of $\pi/2$. The amplitude of each quadrature is modulated by an electronic signal generated by Alice's computer and sent through a digital-to-analog converter (DAC) working at 500 MSPS and with a bandwidth of 200 MHz. The bias voltage of the two amplitude modulators and the relative phase shift are controlled by the Modulator Bias Controller (MBC), exploiting low frequency dither signals to implement a feedback loop. After a first attenuation by a variable optical attenuator (VOA), the signal is sent to a 95:5 beam-splitter, whose 95% output is sent to a power meter (PM) which is used to measure Alice's modulation variance V_A. The 5% output is further attenuated by using a 90:10 beam-splitter, whose 10% output, at the level of few photons per symbol, is sent to the quantum channel. All components of the source are connected by polarization maintaining single-mode fibers. We implement a fixed transmittance quantum channel by using a variable optical attenuator (VOA). The losses of the channel can be converted to a distance knowing the attenuation of the fiber, typically around 0.2 dB/km at 1550 nm. At the entrance of Bob's setup, a switch is used to switch off the signal during the rounds of calibration of the shot noise. The signal arrives then to the coherent detection system, described in the next section.

2.2 Coherent detection

A coherent detection system is based on the interference between the signal with a local oscillator (LO) on a 50:50 beam-splitter. The difference between the two outputs of the beam-splitter provides a signal that is proportional to one quadrature of the signal, "amplified" by the power of the local oscillator. The measured quadrature depends on the relative phase between the signal and the local oscillator. This is the reason why in most earlier generation CV-QKD systems the local oscillator was sent together with the signal. In order to use a different laser, generated locally at Bob's side, as a local oscillator, it is necessary to use some technique for recovering the phase between the two lasers. This can be done by sending some intense pilot tones, originating from the same laser used for the signal, and measuring them using the local LO.

It is also possible to measure both quadratures of the field at the same time, as currently done in classical optical communication [6]. However, since the two quadratures of a single-mode field are non-commuting quantities, this comes at the expense of extra noise added to the system. A first method for a simultaneous measurement of both quadratures is *phase-diverse heterodyne*, which uses the 90° mixer shown in Figure 2. Here the extra noise is introduced by the beam-splitter on the signal at the entrance of the system. This technique

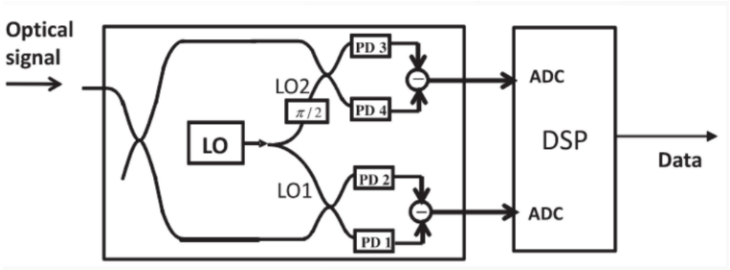

Figure 2: A 90° mixer used to implement a phase-diverse heterodyne [6].

requires two pairs of balanced homodyne detectors. A second technique for a simultaneous measurement of both quadratures is the *RF-heterodyne*. It consists of shifting the signal by a frequency f_c such that $f_c > B/2$, where B is the bandwidth of the signal, as shown in Figure 3. The noise added by RF-heterodyne is the same as with

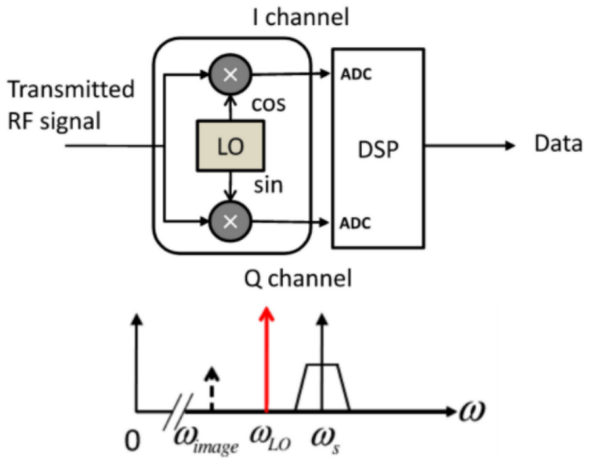

Figure 3: A 180° mixer used for the implementation of an RF-heterodyne [6]. The added noise comes from the mixing of the signal band with the image band, symmetric with respect to the frequency of the local oscillator.

phase diversity, since the vacuum fluctuations of the image band are added to the signal [6]. Our system uses RF-heterodyne detection, hence we measure the two quadratures using a single pair of balanced detectors. This is obtained by shifting the signal at the transmitter side, using the so-called optical single sideband (OSSB) modulation. A similar scheme has recently given good results in a setup built by the Technical University of Danemark (DTU) [17], but it requires particular attention in order to prevent leakage of information in the negative part of the spectrum, which is not monitored [18]. The signal coming from the balanced photo-detector (BPD) is amplified by a trans-impedance amplifier (TIA) and digitized by a analog-to-digital converter (ADC), at a sampling rate of 2.5 GSPS for a bandwidth of 1.25 GHz. The digitized signal is the sent to Bob's computer, which performs the required digital signal processing (DSP) to extract a sequence of symbols, correlated to the ones sent by Alice, which will be used for the extraction of the secret key.

2.3 Digital signal processing

The digital signal processing (DSP) is the collection of software procedures that transform the discrete sequence of quadrature values into a modulated optical signal (Alice DSP) and then back from a modulated optical signal into a discrete sequence of quadrature values (Bob DSP). A scheme of the different steps of the DSP is shown in Figure 4.

We developed a CV-QKD system using the Gaussian Modulated Coherent State (GMCS) protocol, an evolution of the first coherent-state protocol proposed by Grosshans and Grangier in 2002 (GG02) [12]. According to this protocol, a single-mode electromagnetic field must be modulated as a coherent state with the mean value of the quadratures $\langle I \rangle$ and $\langle Q \rangle$ chosen randomly from a Gaussian distribution of mean 0 and variance V_A. The single mode is defined by the temporal shape of the pulse being modulated, which is repeated at the repetition rate of the transmission. The ideal temporal shape would be a bounded pulse, as short as possible. However, an important result of Fourier analysis states that if a function is bounded in time domain, its Fourier transform in the frequency domain is unbounded, meaning that a bounded pulse requires an infinite bandwidth detector in order to be retrieved without distortion. In order to minimize distortions in the signal measured by a finite

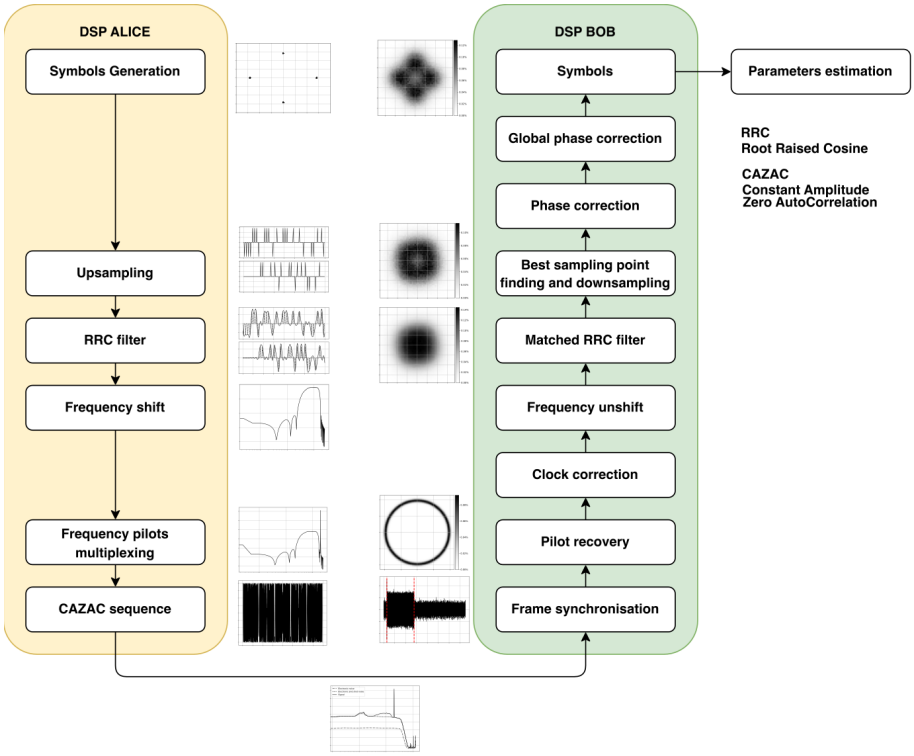

Figure 4: Scheme of the digital signal processing (DSP) used in the CV-QKD setup. This illustration corresponds to a QPSK modulation [19], but the steps of the DSP are the same as the ones used in our setup.

bandwidth detector, which gives rise to *inter-symbol interference* (ISI) [14], classical communication protocols have started to use pulse shapes that are bounded in frequency. The most widely used pulse shape is the *root-raised cosine* (RRC), whose bandwidth is larger than the minimum one not showing ISI, for a given transmission rate, by a factor called *roll-off* [15]. Its limited bandwidth makes this temporal mode also well suited for being used as the single-mode for quantum key distribution [16]. The signal is then frequency shifted in order to be able to retrieve both quadratures using a single detector by using RF-heterodyne, then two frequency multiplexed pilot tones are added, in order to correct both the clock and phase difference between Alice and Bob system and a Zadoff-Chu sequence is added at the beginning of each frame for synchronization. This signal is then sent by Alice's computer to the IQ modulator, which transforms the electronic signal into the optical one that will be sent through the quantum channel.

The aim of the coherent detection system is to transform the optical signal back into an electronic one, that is then sampled by the ADC and transmitted to Bob's computer. The first step of the DSP consists in looking for the synchronisation sequence in order to isolate the transmission frame. The frequency of both pilot tones is measured and since the frequency difference between the two tones is determined by Alice's clock, its measurement at Bob's side allows to recover the difference between the two clocks. After adjusting the clock difference, the difference between the frequency of the pilot tone measured at Bob's side and the one sent by Alice is used to determine the frequency difference between the two lasers. Using this value, the quantum data are shifted towards the base-band and they are filtered using another RRC filter, which determines the temporal mode at the receiver side, and down-sampled at the best sampling point [14]. The instantaneous phase difference is estimated using the measured tone and used to apply a phase rotation to the symbols. The global phase is then corrected by applying a phase rotation to all the symbols.

In our work, we have performed a thorough optimization of the DSP parameters, including in particular the amplitude of the pilot tones, the temporal mode of the signal and the roll-off factor. This optimization aims at minimizing the excess noise of the system, namely the noise beyond the fundamental shot noise of coherent states, and at maximizing the secret key rate. We have started studying the system in the back-to-back configuration and obtain typical values of an average of 0.15 secure bits per sent symbol in the asymptotic limit, corresponding to about 15 Mbit/s at the repetition rate of the system.

3. A NEW INTEGRATED PHOTONIC RECEIVER FOR CV-QKD

The setup described in the above section is based on a discrete receiver, composed of a fiber beam-splitter, mixing the signal with the local oscillator, and a balanced photo-detector. However, one of the main advantages

of CV-QKD receivers is the fact that the required technology can be integrated more easily than for DV-QKD systems. Classical communication makes wide use of integrated detectors, which, despite providing a useful cost-effective solution, are designed to maximize the bandwidth at the cost of other characteristics like linearity. Since linearity is fundamental for CV-QKD, this requires the use of a low power local oscillator, giving a quite high electronic noise. For this reason, CV-QKD receivers based on the photonic integrated circuits (PIC) technology are usually designed to privilege linearity at the expense of the bandwidth.

In this work, we have performed the characterization of a PIC fabricated in a collaboration with the CEA/Leti and the C2N on a Silicon-Germanium integrated circuit, which contains several coherent detectors comprised of a 50:50 beam-splitter and a pair of balanced photo-diodes, with a variable optical attenuator (VOA) in front of each detector in order to balance them and increase the common mode rejection ratio (CMRR). The chip is wirebonded to an electronic board comprising of a low noise trans-impedance amplifier (TIA) to amplify the output of the detector, as shown in Figure 5.

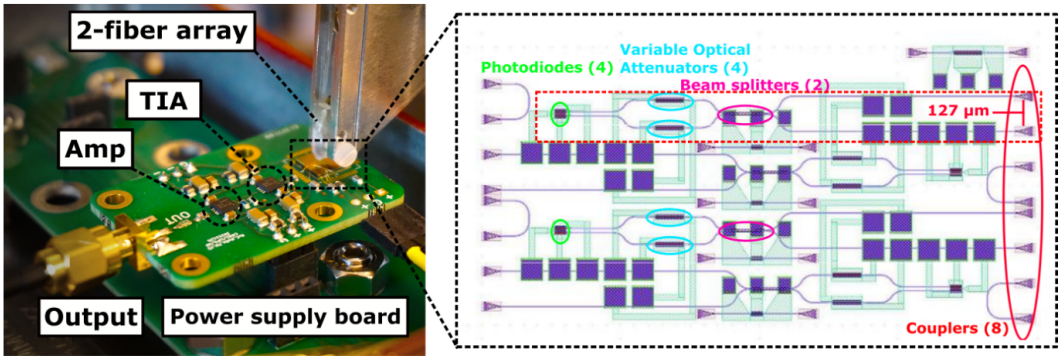

Figure 5: (Left) Electronic board and integrated receiver and (right) layout of the chip [22].

The light is injected into the chip using a 5-axis coupling station with a 2-fiber array, using the grating coupler of the integrated circuit and optimizing on the photocurrent measured by each detector.

The receiver has been tested in a setup similar to the one described in the previous section, with the only difference that the local oscillator originates from the same laser as the signal and is taken from the 90% output of the first beam-splitter at Alice's side. The results of excess noise estimation are shown in Figure 6.

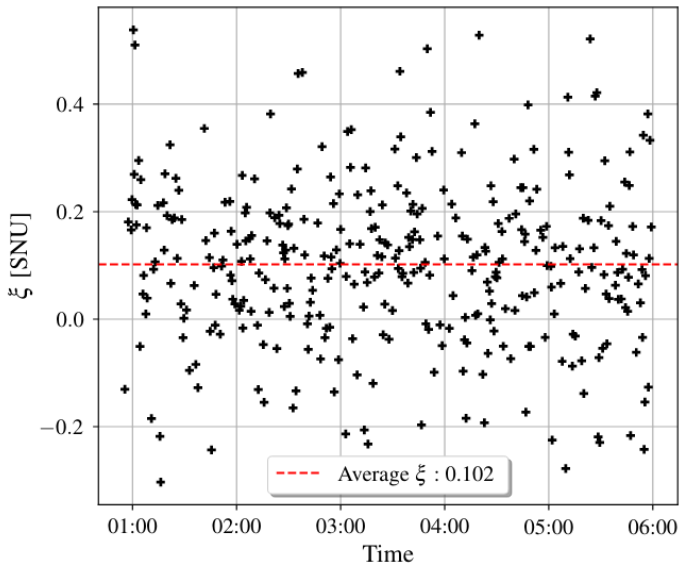

Figure 6: Excess noise estimation during a 5 hour acquisition [22].

The system has been tested during a 5-hour acquisition, using Gaussian modulation, and shows an average excess noise at Alice's side of 0.1 SNU, for a channel transmittance of 1.4 dB equivalent to a fiber channel of roughly 7 km. With this level of excess noise, it is possible to extract a secret key rate of 280 kbit/s in the

asymptotic regime, corresponding to 123 kbit/s in the finite-size regime, assuming that the post-processing can be done in real time using blocks of 10^{10} symbols.

4. CONCLUSIONS

In this article, we described a digital signal processing technique for implementing high-speed CV-QKD. In addition to this, we also showed an integrated receiver developed for CV-QKD and we showed how it can be used for providing a valid alternative with respect to a system built with bulk detectors.

REFERENCES

[1] S. Wiesner, Conjugate Coding, SIGACT News 15, 78 (1983)

[2] C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, Theoretical Computer Science 560, 7 (2014)

[3] S. Wang et al., Twin-Field Quantum Key Distribution over 830-Km Fibre, Nat. Photon. 16, 154 (2022)

[4] S.-K. Liao et al., Satellite-to-Ground Quantum Key Distribution, Nature 549, 43 (2017)

[5] H. P. Yuen and V. W. S. Chan, Noise in Homodyne and Heterodyne Detection, Opt. Lett. 8, 177 (1983)

[6] K. Kikuchi, Fundamentals of Coherent Optical Fiber Communications, J. Lightwave Technol. 34, 157 (2016)

[7] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, E. Diamanti, and P. Grangier, High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM, arXiv:2111.12356 (2021)

[8] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and B. Xu, Sub-Mbps Key-Rate Continuous-Variable Quantum Key Distribution with Local Local Oscillator over 100-Km Fiber, Opt. Lett. 48, 1766 (2023)

[9] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, Feasibility of Satellite-to-Ground Continuous-Variable Quantum Key Distribution, Npj Quantum Inf 7, (2021)

[10] V. Marulanda Acosta, D. Dequal, M. Schiavon, A. Montmerle-Bonnefois, C. B. Lim, J.-M. Conan, and E. Diamanti, Analysis of Satellite-to-Ground Quantum Key Distribution with Adaptive Optics, arXiv:2111.06747 (2021)

[11] B. J. Puttnam, R. S. Luis, G. Rademacher, Y. Awaji, and H. Furukawa, 1 Pb/s Transmission in a 125μm Diameter 4-Core MCF, Conference on Lasers and Electro-Optics (2022)

[12] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. 88, (2002)

[13] A. Davis, M. Pettitt, J. King, and S. Wright, Phase Diversity Techniques for Coherent Optical Receivers, J. Lightwave Technol. 5, 561 (1987)

[14] J. G. Proakis and M. Salehi, Digital Communications, McGraw-Hill (2008)

[15] A. Lapidoth, A foundation in digital communication, Cambridge University Press (2017)

[16] H.-M. Chin, N. Jain, D. Zibar, T. Gehring, and U. L. Andersen, Effect of Filter Shape on Excess Noise Performance in Continuous Variable Quantum Key Distribution with Gaussian Modulation, arXiv:1808.04573 (2018)

[17] N. Jain et al., Practical Continuous-Variable Quantum Key Distribution with Composable Security, Nat Commun 13, (2022)

[18] N. Jain, I. Derkach, H.-M. Chin, R. Filip, U. L. Andersen, V. C. Usenko, and T. Gehring, Modulation Leakage Vulnerability in Continuous-Variable Quantum Key Distribution, Quantum Sci. Technol. 6, 045001 (2021)

[19] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation, Phys. Rev. X 9, (2019)

[20] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations, Adv. Quantum Technol. 1, 1800011 (2018)

[21] F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, F. Karinou, A. Poppe, M. Peev, and H. Hübel, Pilot-Assisted Intradyne Reception for High-Speed Continuous-Variable Quantum Key Distribution with True Local Oscillator, Quantum 3, 193 (2019)

[22] Y. Pietri et al., CV-QKD Receiver Platform Based On A Silicon Photonic Integrated Circuit, OFC 2023