InP-based CV-QKD PIC Transmitter

J. Aldama[(1,*)], S. Sarmiento[(1,*)], S. Etcheverry[(1)], I. López Grande[(1)], L. Trigo Vidarte[(1)], L. Castelvero[(1)], A. Hinojosa[(2)], T. Beckerwerth[(3)], Y. Piétri[(4)], A. Rhouni[(4)], E. Diamanti[(4)], and V. Pruneri[(1,5)]

(1) ICFO-Institut de Ciències Fotòniques, The Barcelona Institute of Science and Technology, Castelldefels, Barcelona, 08860, Spain
(2) VLC Photonics S.L–Ed. 9B–D2, UPV, Camino de Vera s/n, 46022 Valencia, Spain
(3) Fraunhofer Heinrich Hertz Institute (HHI), Einsteinufer 37, 10587 Berlin, Germany
(4) Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, F-75005 Paris, France
(5) ICREA-Institució Catalana de Recerca i Estudis Avançats, Barcelona, 08010, Spain
** These authors contributed equally to this work*
Author e-mail address: valerio.pruneri@icfo.eu

Abstract: An InP-based photonic integrated circuit (PIC) transmitter for pulsed Gaussian-modulated coherent-state (GMCS) CV-QKD protocol is presented and characterized. Results show potential asymptotic secret key rates of 0.4 Mbps at 11 km, and up to 2.3 Mbps in back-to-back configuration. © 2023 The Author(s)

1. Introduction

Quantum key distribution (QKD) allows two or more parties to share a secret key by distributing quantum signals. The security of the key is based on the fundamental laws of quantum physics [1]. On the one hand, continuous-variable QKD (CV-QKD), using coherent quantum states, is a promising solution for various reasons: easy integration with current telecommunications infrastructure, high scalability, and cost-effectiveness. On the other hand, photonic integrated circuits (PICs) can potentially offer enhanced system functionalities with respect to bulk systems, such as higher reproducibility, better stability, and reduced power consumption. Thus, photonic integration of CV-QKD systems may enable the mass deployment of this technology at large-scale telecommunication infrastructures in a cost-effective manner [2, 3].

Different PIC platforms have already been explored for quantum communication [4–6]. PIC-based QKD systems for discrete-variable QKD (DV-QKD) and CV-QKD applications have been reported in [7–11]. Over the last years, silicon photonics technology has been promoted to enable CV-QKD PIC systems since it offers many advantages such as low transmission loss, high coupling efficiency, and mature microfabrication techniques. However, fast modulators with 50 GHz bandwidth modulation and direct laser integration cannot be realized. Alternatively, InP-based PICs have already been used in DV-QKD implementations [10, 11]. However, to the best of our knowledge, no demonstration of InP-based CV-QKD PIC systems has been reported.

In this paper, an InP-based PIC transmitter (TX) for pulsed Gaussian-modulated coherent-state (GMCS) CV-QKD protocol is designed and characterized. A potential secret key rate value of 0.4 Mbps at 11 km (up to 2.3 Mbps in back-to-back configuration) is achieved in the asymptotic regime. We believe that the developed InP-based CV-QKD PIC TX could be used in real network environments to maintain compatibility with classical coherent communication systems.

2. Description of the InP-based CV-QKD PIC TX design and experimental setup

Fig. 1(a) shows the block diagram proposed for the InP-based PIC TX for the pulsed GMCS CV-QKD protocol [12]. It includes an electro-absorption modulator (EAM) providing an adequate extinction ratio, an IQ modulator to generate

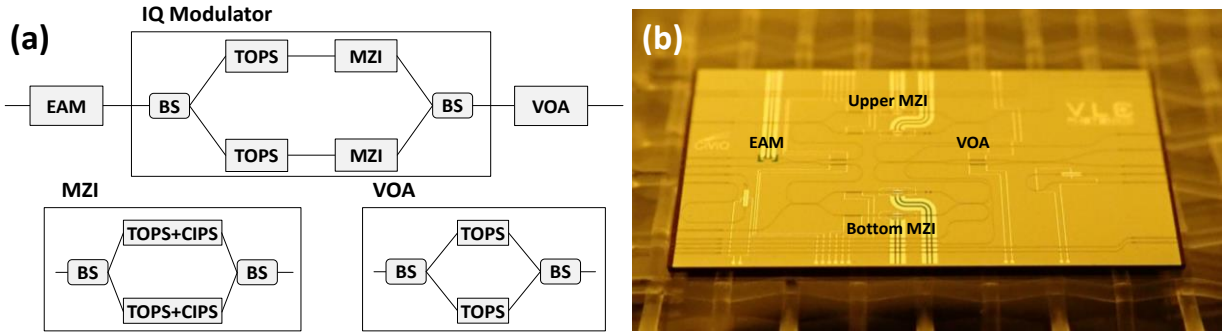

Fig. 1. (a) Block diagram of the CV-QKD PIC TX. (Acronyms) EAM: electro-absorption modulator, BS: beam splitter, MZI: Mach-Zehnder interferometer, TOPS: thermo-optic phase shifter, CIPS: current-injection phase shifter, VOA: variable optical attenuator. (b) Top view of the fabricated 6 × 12 mm^2 InP-based CV-QKD PIC TX, Fraunhofer HHI Foundry.

the GMCSs, and a variable optical attenuator (VOA) to reduce the signal power to the quantum level. The IQ modulator is a Mach-Zehnder interferometer (MZI) structure with one MZI nested on each of its arms. The phase shift of $\pi/2$ between the arms of the IQ modulator is set with two thermo-optic phase shifters (TOPSs). Each arm of the MZI combines a TOPS and a current-injection phase shifter (CIPS). The VOA is also based on a MZI where the interference is controlled by two TOPSs. Finally, the input and output coupling to and from the chip are performed with spot-size converters. Fig. 1(b) shows the top view of the fabricated CV-QKD PIC TX. Table 1 shows the main parameters characterizing the InP-based CV-QKD PIC TX in terms of the extinction ratio of the EAM (ER_{EAM}) and IQ modulator (ER_{IQM}), the maximum attenuation of the VOA (Att_{VOA}), the bandwidth of the system (BW), and linearity. Although the EAM showed a relatively high ER, its measured insertion loss was very high, preventing its use. Thus, the light source was pulsed externally with an amplitude modulator (AM). Note that the EAM is not an essential component for the protocol implementation, as the system could operate entirely in continuous wave mode using pulse shaping in the signal modulation [13].

Table 1. Summary of main parameters characterizing the InP-based CV-QKD PIC TX.

ER_{EAM}	ER_{IQM}	Att_{VOA}	BW	Linearity
24 dB @ DC	25 dB @ DC	30 dB	> 1 GHz	High

Fig. 2(a) shows the experimental setup used. The light source consisted of a 10 kHz nominal linewidth continuous-wave external cavity laser followed by a 90:10 beam splitter (BS). For simplicity, the 90% BS output was directly used as the local oscillator (LO). The other BS output was pulsed with a 30 dB ER AM. The laser was biased to emit 48 mW at 1550 nm. The AM, IQ modulator, and VOA were driven by a field-programmable gate array (FPGA) electronic board with a 16-bit nominal resolution 1 GSa/s digital-to-analog converter unit. Two independent sequences of 2040 pseudo-random values were used to cyclically generate the GMCSs. Fig. 2(b) shows the normalized histogram of the transmitted symbols including references. To ensure high phase recovery accuracy, references and quantum symbols were interleaved in time. The modulation variance (V_{mod}), defined as two times the mean photon number at Alice's output, was measured using a 99:1 BS and a power meter. An 11 km single-mode fiber (SMF) with a coefficient of 0.2 dB/km was used. The receiver consisted of a 90° optical hybrid (90° OH) and two 350 MHz bandwidth balanced photodetectors. Detected signals were digitized with a 10 GSa/s real-time oscilloscope (RTO). The RTO bandwidth was fixed at 50 MHz. Digital signal processing (DSP) was performed offline. It included downsampling, quantum state phase recovery [14], and pattern synchronization using cross-correlation. The QKD parameters were estimated according to $V_B = (\eta T V_{mod} + \varepsilon)/2 + \nu_{elec} + 1$, where V_B is the variance of the quadrature distribution measured at Bob's site, η is the detection efficiency, T is the channel transmittance, ε is the excess noise at Bob's site, and ν_{elec} is the electronic noise variance. The secret key rate (SKR) was estimated considering the asymptotic limit, trusted receiver electronic noise, and reverse reconciliation; $SKR = (\beta I_{AB} - \chi_{BE})R_{eff}$, where β is the reconciliation efficiency, I_{AB} is the mutual information between Alice and Bob, χ_{BE} is the Holevo bound, and R_{eff} is the effective quantum pulse rate. Finally, the channel loss was considered to be controlled by an eavesdropper.

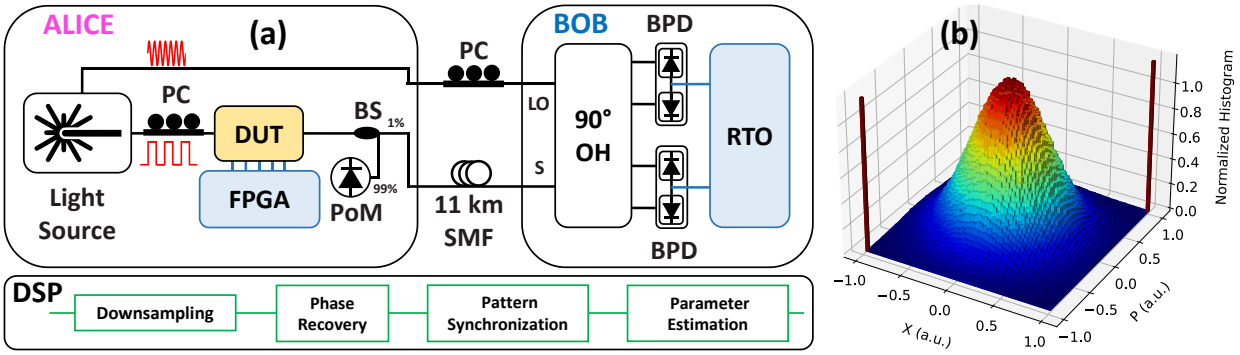

Fig. 2. (a) Experimental setup, including DSP chain. The bulk AM is included in the light source and provides the pulsed signal output. (Acronyms) BS: beam splitter, BPD: balanced photodetector, DUT: device under test, LO: local oscillator port, OH: optical hybrid, PC: polarization controller, PoM: power meter, S: signal port, SMF: single-mode fiber, RTO: real-time oscilloscope. (b) Normalized histogram of the transmitted symbols, including the GMCSs and the phase references.

3. Experimental results

Table 2 summarizes the parameters used for the QKD transmission over an 11 km link. Figs. 3(a) and 3(b) present 20 consecutive measurements of ε and T with SKR, respectively, obtained over 15 min. Each measurement featured a

block size of 10^5 coherent states. Moreover, the values of ε, T, and SKR were independently estimated for each block of coherent states. The calibration of the electronic and shot noise were manually performed before each measurement. The mean values of ε and T were 16.5 mSNU (SNU: shot noise unit) and 0.586, respectively. From Fig. 3(b), it can be observed that the T parameter was stable with a relative standard deviation of 6.6%. A mean SKR value of 0.4 Mbps was achieved, as shown in Fig. 3(b). Finally, Fig. 3(c) shows a simulation of SKR versus the transmission distance, using the experimental parameters estimated above. From Fig. 3(c), a positive SKR could be obtained up to 20 km.

Table 2. Transmission parameter summary.

Parameter	Symbol	Value
Modulation variance	V_{mod}	2.89 SNU
Electronic noise variance	ν_{elec}	13 mSNU
Reconciliation efficiency	β	0.95 [15]
Intensity ratio between reference and quantum pulses	ρ	340
Detection efficiency	η	0.30
Effective quantum pulse rate	R_{eff}	8 Mpulses/s

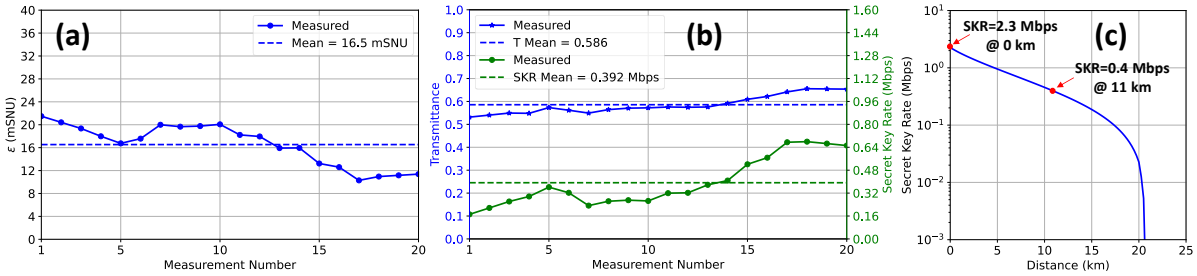

Fig. 3. Experimental results of (a) excess noise (ε), and (b) channel transmittance (T) with secret key rate (SKR) for 20 measurements acquired over 15 min. (c) Simulation of the SKR as a function of link distance in the asymptotic regime.

4. Conclusion

We have reported the design and the experimental characterization of a cost-effective InP-based PIC transmitter for the pulsed GMCS CV-QKD protocol. Reported results push forward the use of InP platform for integrating CV-QKD systems.

Funding. This work was supported in part by the Horizon 2020 Framework Programme (820466), H2020 Marie Skłodowska-Curie Actions (713729), the MCIN with funding from European Union NextGenerationEU (PRTR-C17.I1), and DGR-NextGeneration Catalonia, CEX2019-000910-S [MCIN/AEI/10.13039/501100011033], Fundació Cellex, Fundació Mir-Puig, and Generalitat de Catalunya through CERCA.

References

[1] V. Scarani et al., "The security of practical quantum key distribution," Reviews of Modern Physics, vol. 81, no. 3, pp. 1301–1350, 2009.
[2] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," Entropy, vol. 17, no. 9, pp. 6072–6092, 2015.
[3] H. Wang et al., "High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation," Optics Express, vol. 28, no. 22, pp. 32882-32893, 2020.
[4] S. Tanzilli, et al., "On the genesis and evolution of integrated quantum optics," Laser and Photonics Reviews, vol. 6, no. 1, pp. 115–143, 2012.
[5] G. Moody et al., "Roadmap on Integrated Quantum Photonics," 2021. [Online]. Available: http://arxiv.org/abs/2102.03323
[6] A. Orieux and E. Diamanti, "Recent advances on integrated quantum communications," Journal of Optics, vol. 18, no. 8, p. 083002, 2016.
[7] G. Zhang et al., "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," Nature Photonics, vol. 13, pp. 839–842, 2019.
[8] P. Sibson et al., "Chip-based quantum key distribution," Nature Communications, vol. 8, no. 1, pp. 1–6, 2017.
[9] P. Zhang et al., "Reference-Frame-Independent Quantum-Key-Distribution Server with a Telecom Tether for an On-Chip Client," Physical Review Letters, vol. 112, no. 13, p. 130501, 2014.
[10] H. Semenenko et al., "Chip-based measurement-device-independent quantum key distribution," Optica, vol. 7, no. 3, pp. 238–242, 2020.
[11] T. K. Paraïso et al., "A modulator-free quantum key distribution transmitter chip," npj Quantum Information, vol. 5, no. 42, 2019.
[12] F. Xu et al., "Secure quantum key distribution with realistic devices," Rev. Mod. Phys., vol. 92, no 2, p. 025002, 2020.
[13] F. Roumestan et al., "Experimental Demonstration of Discrete Modulation Formats for Continuous Variable Quantum Key Distribution," 2022. [Online]. Available: http://arxiv.org/abs/2207.11702, 2022.
[14] R. Valivarthi et al., "Plug-and-play continuous-variable quantum key distribution for metropolitan networks," Opt. Express, vol. 28, no. 10, pp. 14547-14559, 2020.
[15] P. Jouguet et al., "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nature Photon, vol 7, 378–381, 2013.