Continuous-variable quantum passive optical network

Adnan A.E. Hajomer,[1,*] Ivan Derkach[1,2], Vladyslav C. Usenko[2], Radim Filip[2], Ulrik L. Andersen[1] and Tobias Gehring[1,]**

[1] *Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark*

[2] *Department of Optics, Faculty of Science, Palacky University, 17. listopadu 12, 771 46 Olomouc, Czech Republic*

[*]*aaeha@dtu.dk*, [**] *tobias.gehring@fysik.dtu.dk*

Abstract: We report the first continuous-variable quantum passive optical network (CV-QPON), that supports secure key generation for 5 users simultaneously. This is achieved considering practical PON topology with an 11 km span of access links.

1. Introduction

Quantum key distribution (QKD) is a method of distributing cryptographic keys between two distant parties based on the principles of quantum mechanics [1]. This approach is highly effective for establishing information-theoretically secure data communication in point-to-point scenarios, particularly well-suited for backbone core networks spanning distances exceeding 100 km [2]. However, its compatibility is challenged when it comes to access networks where multiple users require simultaneous access to QKD infrastructure.

Passive optical networks (PONs) are widely adopted for access networks due to their cost-effectiveness, high capacity, and energy efficiency. In this network topology, users are connected to a central station via a downstream broadcasting structure that utilizes passive optical beam splitters and access links, covering distances of up to several kilometers. However, due to the broadcast nature of this network, discrete variable QKD protocols, which measure properties of single photons cannot be employed because single photons cannot be shared among multiple users simultaneously [3]. Conversely, continuous variable (CV) QKD, based on coherent states and coherent detection, naturally integrates into such a broadcasting structure since coherent states can be shared concurrently among all users.

Here, we report the first experimental continuous variable quantum passive optical network (CV-QPON) enabling the concurrent generation of independent keys for five users. The quantum correlation is established by encoding key information into the amplitude and phase quadratures of coherent states at the central station (Alice), and heterodyne detection is employed to decode the quantum information at the receiving end (Bobs). Our CV-QPON spans a distance of 11 km and operates at a symbol rate of 20 Mbaud.

2. Basic concept and system

In the prepare-and-measure scheme of CV-QPON, Alice prepares coherent states, whose amplitudes are randomly drawn from a Gaussian distribution. These prepared states are subsequently transmitted through quantum channels composed of passive optical beam splitter and fiber links, which are assumed to be fully accessible to a potential attacker (Eve). Each Bob generates independent keys with Alice after performing heterodyne detection followed by classical data processing that includes parameter estimation, information reconciliation, and privacy amplification.

For the security analysis, we assume that users are not trusted, but are not collaborating with an attacker either [4]. This implies they act faithfully, i.e. there's a single adversary that collects information from all quantum channels and uses it to obtain every single key that is generated in parallel in the network. Alice upon estimating all channels parameters and receiving classical communication from users can reconstruct the overall shared state and assess the mutual information $I(A:B_i)$ with user B_i and consequently the lower bound on the key rate K_i. The privacy amplification cost is determined by the maximum between the upper bound on the accessible information to an eavesdropper χ_{B_iE} and $I(B_i:B_k)$ the mutual information any non-reference user B_k can have on the particular key generated with B_i [4]:

$$K_i = \beta I(A:B_i) - \max\left\{\max_k I(B_i:B_k), \chi_{B_iE}\right\}, \tag{1}$$

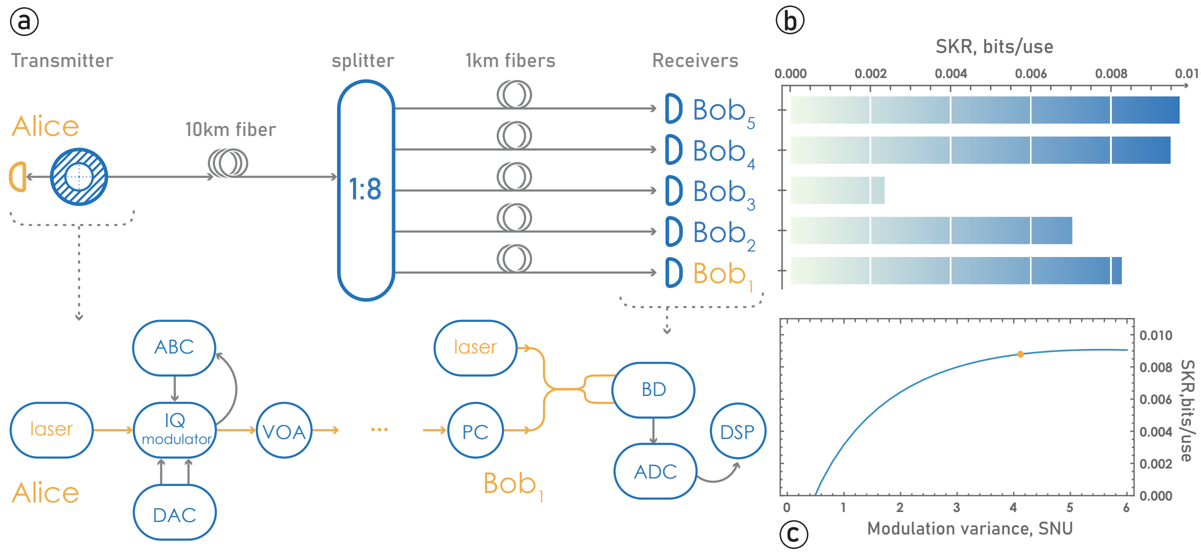

Fig. 1. Scheme and performance of the continuous variable quantum passive optical network. *(a)* Overall layout of the experiment. Transmitter components: 1550 nm **laser**, **ABC**: automatic bias controller, **IQ**-modulator, **DAC**: 16-bit digital-to-analog converter, **VOA**: variable optical attenuator; Receiver components: free running **laser**, **PC**: polarization controller, **BD**: custom balanced detector, **ADC**: 16-bit analog-to-digital converter, and **DSP**: digital signal processing. *(b)* Secure key rate in bits per channel use for each user. *(c)* Dependence of the key rate on the modulation variance (in SNU) for averaged observed security parameters. Modulation variance of choice (single point shown) during the experiment is 4.12 SNU. Reconciliation effiecncy $\beta = 95\%$.

where β accounts for limited efficiency of information reconciliation. Due to considerable total loss the correlations between users in our setup were sufficiently small, hence $\max_k I(B_i : B_k) \ll \chi_{B_i E}$.

Figure 1 (a) shows the schematic of our CV-QPON. Alice prepared coherent states in the single sideband frequency of the optical carrier. These states were generated by drawing random numbers at a rate of 20 MBaud from Gaussian distribution obtained from a vacuum-based quantum random number generator [7]. The quantum symbols were upsampled to 1 GSample/s and pulse-shaped using a root-raised cosine filter with a roll-off of 0.2. A 205 MHz pilot tone was frequency-multiplexed with the broadband signal, centered at 170 MHz, to facilitate the carrier phase recovery. This waveform was then loaded into a digital-to-analog converter (DAC) with a sampling rate of 1 GSample/s. The corresponding optical signal was produced by modulating a 1550 nm continuous wave (CW) laser with a linewidth of 100 Hz. The modulation was achieved using an in-phase and quadrature (IQ) modulator driven by the DAC. The IQ modulation was operated in optical single sideband carrier suppression mode, achieved by controlling the direct current bias voltages with an automatic bias controller (ABC). Following the IQ modulator, a variable optical attenuator (VOA) was employed to fine-tune the modulation variance of the thermal state. The quantum signal then propagated through quantum channels, made of a shared 10 km standard single mode fiber (SMF), a 1:8 optical beam splitter, and 1 km SMF channels connecting the beam splitter to the various Bob stations. The average physical loss of each channel is ≈ -13 dB.

Each Bob measured the coherent states using radio frequency (RF) heterodyne detection, which was performed by overlapping the incoming signal with a free-running local oscillator (LO) generated from an independent CW laser. To maximize the visibility of the interference, a manual polarization controllers were used to align the polarization of the quantum signal with that of the LO. Subsequently, the end user employed a custom-made broadband balanced detector (BD) with a bandwidth of approximately 250 MHz and a 1 GSample/s analog-to-digital converter (ADC) for the purposes of detection and digitization. All ADCs and the DAC were clock synchronized using a 10 MHz reference clock.

All Bobs performed three distinct types of measurements, namely the quantum signal measurement, vacuum noise measurement, and electronic noise measurement. The measurement process was structured into frames, with a frame size of 10^7 samples. Following the measurements, the Bobs proceeded to recover their quantum symbols through an offline digital signal processing (DSP) routine [5]. This routine involved several key steps, including the application of a whitening filter to eliminate any correlations between the quantum symbols, carrier phase recovery based on machine learning technique [6], temporal synchronization facilitated by cross-correlation with

Table 1. Estimated channel parameters (at the output) along with detector electronic noise for each user.

Parameters	**Bob$_1$**	**Bob$_2$**	**Bob$_3$**	**Bob$_4$**	**Bob$_5$**
Transmittance	0.037	0.0307	0.0312	0.056	0.045
Excess noise, mSNU	0.966	0.765	2.321	2.56	1.334
Electronic noise, mSNU	103	87	98	98	94

reference symbols, matched filtering, and downsampling.

3. Results

To generate keys, Alice prepared an ensemble of 1×10^7 coherent states, characterized by a modulation variance of 4.1 shot-noise units (SNU). Fig. 1(c) shows the secret key rate (SKR) as a function of modulation variance, with an assumed information reconciliation efficiency of $\beta = 95\%$. The optimal modulation variance falls within the range of 4 to 6 SNU, which aligns with our chosen value of 4.1 SNU.

Table 1 summarizes the channel parameters and electronic noise in our experiment for each Bob. The average transmittance was ≈ -16 dB primarily attributed to the utilization of a 1:8 beam splitter and suboptimal polarization alignment. The excess noise varies for each user because it relies on the received modulation variance and thus the unique channel transmittance for each user [5]. Moreover, due to limitations in detector clearance, imposed by the limited optical power of the laser shared as the LO between the Bobs, a relatively high level of electronic noise was observed.

Figure 1(b) illustrates the obtained SKR by all users. Among the users, Bob$_5$ achieved the highest SKR of ≈ 0.01 bits/use, which corresponds to 0.2 Mbit/s. On the other end, Bob$_3$ attained the lowest SKR of ≈ 0.0024. These variations in SKR arise due to differences in the transmittance and the noise encountered by each user.

4. Discussion

In this work, we demonstrated the first CV-QPON with five users, enabling the simultaneous generation of independent keys over 11 km access links. Unlike prior research in quantum access networks [3, 9], our CV-QPON takes into account the inherent broadcasting nature of downstream traffic and employs cost-effective and off-the-shelf components, seamlessly integrating with classical PON infrastructure. While our demonstration focused on only five users, the network's capacity can be readily expanded [4]. Furthermore, improvements in the secret key rate can be achieved by using broadband balanced detectors and higher symbol rates [10]. Our successful demonstration marks a significant step towards the realization of large-scale quantum networks.

Acknowledgments This work was supported by QuantERA II Programme (project CVSTAR, agreement no. 101017733), the Danish National Research Foundation, Center for Macroscopic Quantum States (bigQ, DNRF142), the European Union's Digital Europe programme under Grant agreement No 101091659 (QCI.DK), and the Czech Science Foundation (project 22-28254O).

References

1. S. Pirandola, *et al.*, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012 (2020).
2. A. Boaron, *et al.*, "Secure quantum key distribution over 421 km of optical fiber," Phys. Rev. Lett. **121**, 19 (2018).
3. B. Fröhlich, *et al.*, "A quantum access network" Nature **501**, 7465 (2013).
4. Y. Bing, *et al.*, "High-Rate Point-to-Multipoint Quantum Key Distribution using Coherent States," arXiv preprint arXiv:2302.02391, (2023).
5. A. A. E. Hajomer, *et al.*, "Long-distance continuous-variable quantum key distribution over 100 km fiber with local local oscillator," arXiv preprint arXiv:2305.08156, (2023).
6. H.-M. Chin *et al.*, "Machine learning aided carrier recovery in continuous-variable quantum key distribution", npj Quantum Inf. **7**, (2021).
7. T. Gehring, *et al.*, " Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side information," Nat. Commun. **12**, (2021).
8. X. Wang, *et al.* "Experimental upstream transmission of continuous variable quantum key distribution access network," Opt Lett. **48**, 12 (2023).
9. X. Wang, *et al.* "Experimental upstream transmission of continuous variable quantum key distribution access network," Opt Lett. **48**, 12 (2023).
10. A. A. E. Hajomer, *et al.*, "Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receive," arXiv preprint arXiv:2305.19642, (2023).