254.6 Mb/s Secret Key Rate Transmission over 13.5 km SMF Using PCS-256QAM Super-Channel Continuous Variable Quantum Key Distribution

François Roumestan[(1)], Amirhossein Ghazisaeidi[(1)], Haik Mardoyan[(1)], Jérémie Renaudier[(1)], Eleni Diamanti[(2)], and Philippe Grangier[(3)]

(1) Nokia Bell Labs, Paris-Saclay, route de Villejust, F-91620 Nozay, France
(2) Sorbonne Université, CNRS, LIP6, 4 place Jussieu, F-75005 Paris, France
(3) Université Paris-Saclay, IOGS, CNRS, Laboratoire Charles Fabry, 2 avenue Fresnel, F-91127 Palaiseau, France
francois.roumestan@nokia.com

Abstract: We experimentally validate the feasibility of wavelength-division multiplexing for continuous-variable quantum-key-distribution, transmitting four 600 MBaud probabilistically-shaped 256-QAM signals with 4 GHz spacing, achieving total 254.6 Mb/s average secret key rate.

1. Introduction

Continuous-variable quantum-key-distribution (CV-QKD) based on coherent states is a promising solution to implement practical secure communications over insecure physical links, thanks to its compatibility with commercially available light sources and equipment [1]. Over the past years, several CV-QKD experiments showed the achievability of several Mb/s of secret key rates (SKR) [2,3]. Recently, we reported experimental demonstrations of a CV-QKD protocol based on polarization division multiplexed probabilistically shaped (PCS) QAM formats [4,5]. Relying on an analytical security proof for arbitrary discrete modulation formats [6], we showed the feasibility of average 68 Mb/s SKR over 9.5 km of single-mode fiber (SMF) using dual polarization PCS 64-QAM. In the present work, we extend our previous results by proposing a simple experiment to validate the possibility of wavelength division multiplexing (WDM) with our protocol. Several works address the issue of WDM of QKD channels with or without the presence of classical transmission channels [7,8]. Here, Alice simulates the transmission of four WDM QKD channels, without classical channels, using four laser sources, set at 4 GHz apart from each other, modulated by the same 600 MBaud signal with PCS 256-QAM format and transmitted to Bob through 13.5 km of SMF. Bob monitors each channel independently to estimate the transmission parameters, including excess noise. The total average achievable SKR is evaluated at 254.6 Mb/s, with average 63.7 Mb/s SKR on each WDM channel.

2. CV-QKD protocol based on probabilistic constellation shaping

In the CV-QKD protocol that we implement, the transmitter, Alice, prepares coherent states $|\alpha\rangle = |(p + iq)/2\rangle$, chosen at random from a discrete modulation. She sends them through an optical link to the receiver, Bob, who measures them using phase-diversity coherent detection. Afterwards, Alice and Bob reveal a fraction of their data on a public authenticated channel to evaluate the quantum channel parameters. These are used to infer the quantity of information obtained by the eavesdropper, Eve, and compute the length of the final key. Then, Alice and Bob correct transmission errors through a step called reconciliation. Finally, they perform privacy amplification to extract the final secret key from their common data sets. The quantum channel is characterized, after phase diversity coherent detection, by the equation $V_B = \frac{\eta T}{2} V_A + N_o + V_{el} + \xi_B$, where V_B is the variance of Bob's measured states in shot noise units (SNU), $V_A = 2\langle n \rangle$ is the variance of Alice's modulation, η is the quantum efficiency of the receiver, T is the channel transmittance, $N_o = 1$ is the shot noise variance, V_{el} is the receiver's electronic noise variance and ξ_B is the excess noise variance measured at Bob's site. To infer the final secret key rate using the different parameters involved in the above equation it is necessary to use a suitable security proof.

The modulation format implemented in this work is a probabilistic constellation shaping (PCS) 256-QAM. It is a regular QAM constellation with discretized Gaussian probability distribution, as illustrated in Fig. 1. Its theoretical security was established using an analytical security proof for CV-QKD protocols with any discrete modulation format [6]. Its practical security was further analyzed for our previous work [5], with trusted electrical noise V_{el} and quantum efficiency η, and worst-case estimation for finite size effects. In this paper, we use the same method to compute SKR of our WDM QKD channels.

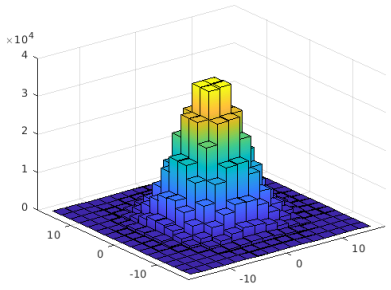

Fig. 1. Histogram of a PCS 256-QAM.

3. Experimental WDM system for CV-QKD

The experimental CV-QKD system, outlined in Fig. 2, is built using off-the-shelf telecom equipment. Alice uses a 16 bits and 5 GSample/s arbitrary waveform generator (AWG) to generate a dual polarization,

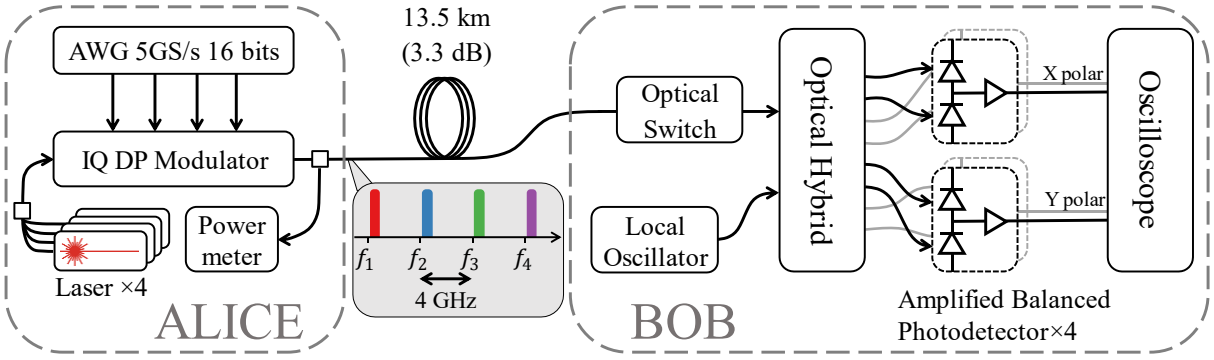

Fig. 2. Experimental WDM CV-QKD testbed. It features Alice's 30 kHz linewidth lasers sources, a conventional I/Q dual polarization (DP) optical modulator, and a 5GS/s 16 bits arbitrary waveform generator (AWG). On Bob's side, a 180° Hybrid with four amplified balanced photodetectors, a 10 kHz linewidth local oscillator, and a 1 GHz 10 bits oscilloscope with 5 GS/s sampling rate.

PCS 256-QAM, and 600 MBaud signal. The pulse shape of the signal is digital root-raised cosine (RRC) with roll-off factor 0.4. To avoid low frequency noise from the hardware, both from Alice and Bob, the baseband signal was digitally upshifted by 500 MHz. Thus, the useful analog bandwidth extends from 120 MHz to 880 MHz. The four outputs of the AWG are fed to the analog part of a standard dual polarization I/Q optical modulator. The optical input of the modulator is a frequency comb made with four external cavity laser sources with 30 kHz nominal linewidth. Their frequencies are respectively tuned to 193 396 GHz, 193 400 GHz, 193 404 GHz, and 193 408 GHz. The output is a super channel with 4 WDM carriers.

The quantum channel is a 13.5 km standard SMF link with 3.3 dB characterized channel loss. Bob uses a dual polarization optical hybrid based on two single polarization 90° hybrids, with four amplified balanced photodiodes to detect the quadratures of the received coherent states. The measured value of the quantum efficiency of the receiver was $\eta = 0.65$ and of its trusted electronic noise $V_{el} = 0.10$ SNU. The local oscillator (LO) at Bob's site is a tunable laser source with 10 kHz nominal linewidth. The received analog signal is sampled using a 1 GHz real-time oscilloscope with 5 GSample/s sampling rate and 10 bits vertical resolution. The sampled waveforms are finally stored on a hard-drive for offline digital signal processing (DSP). Calibration of the shot noise is performed periodically using a fast optical switch to turn on and off the signal light. The bandwidth of Bob's hardware, especially the oscilloscope, allows us to measure only one WDM channel per acquisition. Bob can select the WDM channel he wishes to receive by tuning the frequency of the LO to the center frequency of the desired channel.

To retrieve the QKD symbols at low SNR, the QKD signal is interleaved in time with a deterministic sequence of QPSK pilot symbols, with 14 dB higher power than the QKD symbols. The pilots are public information shared by Alice and Bob. They are used by the DSP to correct the optical channel impairments. Outlined in Fig. 3 is the DSP suite, which uses standard algorithms common in classical optical coherent transmissions [9]. The waveforms sampled by the oscilloscope are assembled as two complex signals, one for each orthogonal polarization. A matched filter (RRC) is applied to the samples, and constant amplitude zero autocorrelation (CAZAC) sequences are used to synchronize the pilot sequence. Polarization demultiplexing is performed with a constant modulus algorithm (CMA) with coefficients updated on the pilots. Carrier frequency estimation is performed using a periodogram method. Pilot-aided maximum-likelihood estimation applied on the pilots and combined with linear interpolation for carrier phase estimation. All DSP parameters, most notably the learning coefficient and filter lengths of the pilot-aided CMA and the moving average filter length of the carrier phase estimation, are carefully optimized to minimize the excess noise during the off-line processing. Once the best parameters are determined, all waveforms are processed with the same set of parameters. This optimization greatly improved the performance of PCS 256-QAM compared to our previous work. That is the reason why we use it in this work, instead of PCS 64-QAM. Finally, the QKD parameters are estimated using the QKD symbols, according to the equation of Section 2.

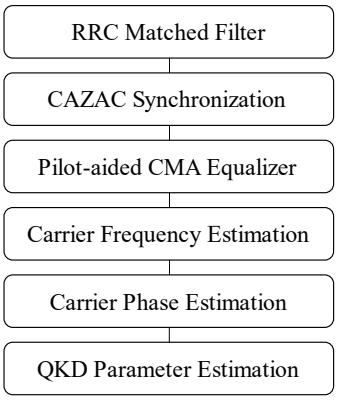

Fig. 3. Digital signal processing.

4. Experimental results

For each of the four WDM channels, we perform 100 acquisitions of 20 ns over 1 hour. For each acquisition, we apply the DSP and estimate the QKD parameters, including modulation variance V_A and excess noise ξ_B. The estimation is done with 5×10^6 QKD symbols. Fig. 4. gives the corresponding SKR for each acquisition, computed using the proof mentioned in Section 2, with trusted electronic noise and worst-case estimator for the

	193 396 GHz	193 400 GHz	193 404 GHz	193 408 GHz
V_A [SNU]	7.61	7.11	7.07	7.44
ξ_B [SNU]	3.93×10^{-3}	3.12×10^{-3}	4.01×10^{-3}	3.74×10^{-3}
SKR [Mb/s]	62.5	66.5	62.1	63.5

Tab. 1. Experimental values of modulation variance V_A in SNU, average excess noise ξ_B in SNU, and average secret key rate in Mb/s, for each WDM channel.

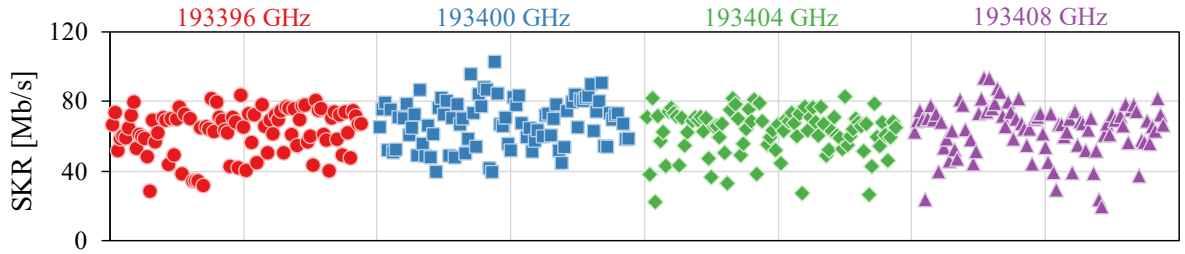

Fig. 4. (a) Experimental achievable SKR [Mb/s] for each acquisition of each WDM channel, with trusted noise, finite size effects, and reconciliation efficiency assumption $\beta = 0.95$.

excess noise with security parameter $\epsilon = 10^{-8}$ and $N = 5 \times 10^6$ symbols. We assumed reconciliation efficiency $\beta = 0.95$. The averaged estimated values for each channel are summarized in Tab. 1. The average excess noise over the different WDM channels is $\xi_B = 3.7 \times 10^{-3}$ SNU. The sum of the achievable SKR of the 4 WDM channels is 254.6 Mb/s, with average 63.7 Mb/s SKR on each WDM channel.

We remind that the baseband signal at the output of the AWG has been upshifted by 500 MHz, to avoid low frequency noise sources. Therefore, only positive frequencies are modulated on the optical carriers, as illustrated in the insert of Figure 2. Similarly, it is possible to create an only negative frequencies signal, that can be digitally multiplexed. This digital dual-carrier method should help us increase the SKR by a factor up to two.

As described in Section 3, the experiment uses only one modulator. Therefore, the four WDM channel carry the same signal. This could potentially offer more favorable conditions than real WDM and challenge the conclusions of the experiment. However, our system works at low launch power (lower than -40 dBm) and low distance. In these conditions, nonlinear impairments can be considered as negligible. This fact corroborates the conclusion of our experiment: the implementation of WDM techniques with PCS 256-QAM CV-QKD protocol is possible with high performance. However, new experiment with real WDM channels should be conducted to confirm the results and SKR.

5. Conclusion

We successfully conducted an experimental validation of WDM for CV-QKD protocols using PCS QAM formats. The experiment consisted of four WDM channels spaced at 4 GHz, transmitting a 600 MBd dual polarization PCS 256-QAM signal through 13.5 km of SMF. The total average achievable SKR was evaluated at 254.6 Mb/s, with average 63.7 Mb/s on each WDM channel. We believe this work to be an important step towards high-rate CV-QKD systems and their integration into classical telecommunication systems. Further improvements of the SKR are expected, for example using digital dual carrier signals.

Acknowledgement: This work has received funding from the European Union's Horizon 2020 research and innovation under grant agreements No 820466 CiViQ and No 857156 OpenQKD.

References

[1] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: principle, security and implementations," *Entropy* **17**, 6072 (2015).
[2] D. Huang et. al., "High-speed continuous-variable quantum key distribution without sending a local oscillator," *Opt. Lett.* **40**(16), 3695–3698 (2015).
[3] F. Laudenbach et. al., "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," *Quantum* 3, 193 (2019).
[4] F. Roumestan et. al., "Demonstration of Probabilistic Constellation Shaping for Continuous Variable Quantum Key Distribution," in *OFC 2021*, paper F4E.1 (2021).
[5] F. Roumestan et. al., "High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM," in *ECOC 2021*, paper Th2G-3 (2021).
[6] A. Denys et. al., "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum* **5**, 540 (2021).
[7] R. Alléaume et. al., "Technology Trends for Mixed QKD/WDM Transmission up to 80 km," in *OFC 2020*, paper M4A.1 (2020).
[8] T. A. Eriksson *et al.*, "Wavelength Division Multiplexing of 194 Continuous Variable Quantum Key Distribution Channels," *J. Light. Technol.*, **38**(8), 2214–2218 (2020).
[9] K. Kikuchi, "Fundamentals of Coherent Optical Fiber Communications," *J. Light. Technol.*, **34**(1), 157–179 (2016).