Wavelength Division Multiplexing of 194 Continuous Variable Quantum Key Distribution Channels

Tobias A. Eriksson, Ruben S. Luís, Benjamin J. Puttnam, Georg Rademacher, Mikio Fujiwara, Yoshinari Awaji, Hideaki Furukawa, Naoya Wada, Masahiro Takeoka, and Masahide Sasaki

***Abstract*—We demonstrate the first continuous variable quantum key distribution (CV-QKD) system with fully digital phase and polarization tracking, enabling the first wavelength division multiplexing experiment for CV-QKD. We transmit 194 × 0.5 GHz channels with 25 GHz channel spacing, demonstrating an aggregate estimated asymptotic secret key rate of 172.6 Mbit/s over 25 km.**

***Index Terms*—Quantum key distribution, wavelength division multiplexing.**

I. Introduction

PROVIDING means of secure communication is a critical topic for next generation fiber-optical systems, especially for applications involving sensitive information such as governmental, military, banking or medical applications [1]. Current encryption technology is threatened by rapid technological advances, such as quantum computing [2]. No classical encryption technique can guarantee security against the so called "store now, decrypt later" attack in which an eavesdropper stores encrypted intercepted data until sufficient technological advance has been made to break the encryption. Relying on the laws of quantum mechanics, quantum key distribution (QKD) can provide means of unconditionally secure communication [1]. QKD can be divided into discrete variable (DV) and continuous variable (CV) technologies, where CV-QKD, although being less mature than DV-QKD, has the potential to be implemented with components that are common for coherent communication technologies thus providing a lower cost solution suitable for large-scale production. CV-QKD has been demonstrated over distances up to 100 km [3] and recently achieved secret key rates (SKRs) in the Mbit/s region [4]–[6]. Further, co-propagation of a single CV-QKD channel and classical data channels has been demonstrated in different settings with 56 [7] and 100 wavelength division multiplexing (WDM) channels [8], showing that CV-QKD can be integrated into the existing fiber-optical network architecture.

For CV-QKD, one of the main challenges is how to establish a phase reference between Alice and Bob. Early demonstrations transmitted a copy of the transmitter laser over the channel to be used as a local oscillator (LO) on Bob's side. This has two major drawbacks; it is a possible security loop hole if the transmitted LO is manipulated by any attacker of the channel [9], [10]. Further, the receiver performance is reduced with channel loss since the LO also experiences the loss of the channel. Due to these two issues, the use of a true LO has been proposed [11]–[14]. However, so far manual polarization alignment at the receiver side has been performed, or optical polarization tracking with feedback from the receiver has been applied [15].

WDM together with digital signal processing (DSP) has enabled the capacity of today's fiber-optical links [16]. It is highly likely that QKD systems will follow the same trend. A natural evolution to increase the SKRs for QKD systems is to employ WDM techniques in the low-loss spectral-window of the fiber [17]. WDM transmission of 8 [18] and 20 [19] DV-QKD channels has been experimentally demonstrated and up until now, WDM transmission of CV-QKD has not yet been demonstrated. One reason that WDM demonstrations of CV-QKD channels have so far been missing, is that employing optical solutions for phase and/or polarization tracking does not scale well with many WDM channels. DSP offers the possibility of moving functionality into the digital domain and hence removing the need for bulky and costly optical solutions. DSP is an enabling technology for massive WDM transmission of CV-QKD channels since, as will be shown in this paper, phase and polarization tracking can be moved to the digital domain, making the transmitter and receiver of each WDM channel more or less plug-and-play.

In this paper, we propose and experimentally demonstrate for the first time a fully digital polarization and phase tracking scheme for CV-QKD, using a true local oscillator. The system is using a polarization multiplexed pilot signal together with a 1-tap polarization demultiplexing stage. By avoiding the use of all-optical tracking solutions, this system has the potential for on-chip implementation similar to conventional coherent communication systems. Further, the system is fully WDM compatible and we demonstrate the first WDM experiment for

Manuscript received October 15, 2019; revised December 20, 2019; accepted January 10, 2020. Date of publication January 29, 2020; date of current version April 15, 2020. Originally submitted to the 45th European Conference on Optical Communications on September 13, 2019. This work was supported in part by the Swedish Research Council under Grant 2017-06179, in part by the Council for Science and CSTI, SIP, and in part by the Photonic and Quantum Technology for Society5.0. *(Corresponding author: Tobias Eriksson.)*

T. A. Eriksson is with the National Institute of Information and Communications Technology, Tokyo 184-8795, Japan, and also with the Department of Applied Physics, Royal Institute of Technology (KTH), AlbaNova University Center, 106 91, Stockholm, Sweden (e-mail: tobias.a.eriksson@gmail.com).

R. S. Luís, B. J. Puttnam, G. Rademacher, M. Fujiwara, Y. Awaji, H. Furukawa, N. Wada, M. Takeoka, and M. Sasaki are with the National Institute of Information and Communications Technology, Tokyo 184-8795, Japan (e-mail: rluis@nict.go.jp; ben@nict.go.jp; georg.rademacher@nict.go.jp; fujiwara@nict.go.jp; yossy@nict.go.jp; furukawa@nict.go.jp; wada@nict.go.jp; takeoka@nict.go.jp; psasaki@nict.go.jp).

Digital Object Identifier 10.1109/JLT.2020.2970179

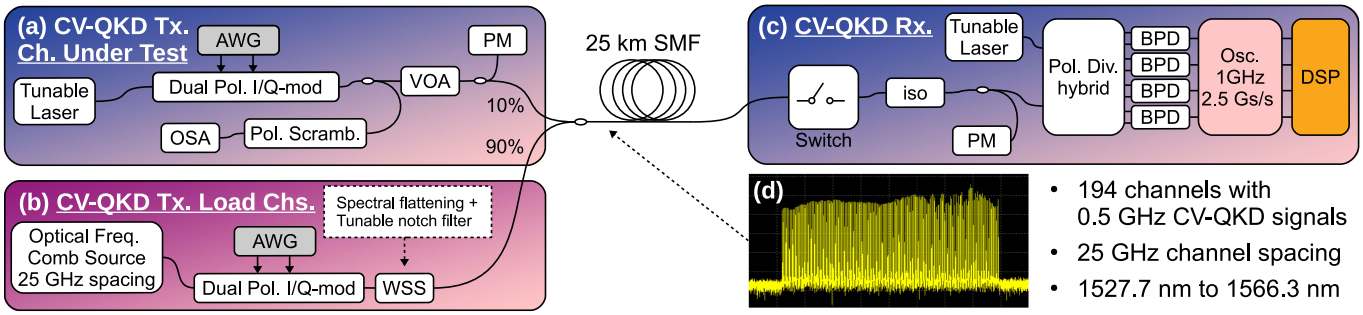

Fig. 1. Experimental setup showing (a) the CV-QKD channel under test based generating 0.5 GHz four-state (QPSK) CV-QKD channels. (b) The transmitter for generating 193 load channels with a tunable notch filter to remove the load channel at the channel under test. (c) The CV-QKD receiver with a switch that is synchronized to the oscilloscope trigger to measure the shot-noise and CV-QKD signal in the same trace. (d) The measured spectra of the 194 transmitted CV-QKD channels.

CV-QKD. We transmit 194 WDM channels of CV-QKD, which is a record for any QKD system. We demonstrate an estimated aggregated asymptotic SKR of 172.6 Mbit/s for a transmission distance of 25 km.

II. Fully Digital CV-QKD System

The CV-QKD system is applying a digital self-homodyne approach [20]. The four-state (QPSK) CV-QKD signal is transmitted on one polarization while a copy of the transmitter laser is transmitted on the orthogonal polarization. This signal is generated using an integrated dual-polarization I/Q-modulator as shown in Fig. 1, which effectively preserves the phase relation between the signal and pilot. The QKD signal is shifted in frequency compared to the pilot to avoid crosstalk due to non-perfect polarization extinction in the Tx. and Rx [7], [21].

A. Digital Signal Processing

The processing flow of the DSP is shown in Fig. 2(a) where the input consists of two complex data-streams which are samples from the optical signal, with random polarization orientation, using a free-running laser with 15 dBm optical power as LO. The DSP starts with a 1-tap polarization demultiplexing stage outlined in Fig. 2(b) [20]. This algorithm is based on the knowledge that one polarization contains a pilot tone which appears as a constant modulus signal when beating with the local oscillator. The other polarization containing the CV-QKD signal should have very low power in comparison to the pilot. The equalizer taps are updated using a gradient descent algorithm with error calculated on only one output signal as follows

$$e = |s_{f,x}|^2 - P, \tag{1}$$

where $s_{f,x}$ is the output of the equalizer applied to the band-pass filtered signals. $P = 1$ is the target power of the constant modulus signal. The bandpass filters greatly helps the convergence of th equalizer and is applied by finding a peak in the combined spectra of the x- and y-polarization signal to center the filter around the pilot tone. The equalizers are updated as

$$h_{xx} = h_{xx} - \mu e s_{f,x} x_f^*, \tag{2}$$

$$h_{xy} = h_{xy} - \mu e s_{f,x} y_f^*, \tag{3}$$

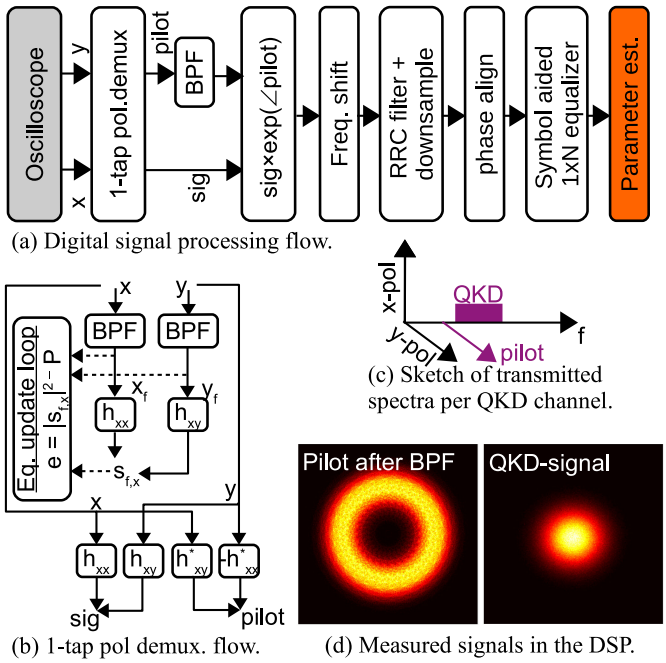

Fig. 2. Outline of the digital signal processing showing: (a) The digital signal processing flow from digitized signals in the oscilloscope to the parameter estimation stage. (b) The update flow of the 1-tap polarization demultiplexing stage where the input signals are sent through bandpass filters (BPFs) in the update of the equalizer taps. The converged taps are applied to the non-filtered signals. (c) A sketch of the transmitted spectra where the pilot tone is polarization multiplexed with a frequency shifted CV-QKD signal. (d) Measured signals in the i/q-plans of the two polarizations after the polarization demultiplexing stage.

where μ is the step size, $s_{f,x}$ the output of the equalizer applied to the band-pass filtered signals. Further, x_f^* and y_f^* are the conjugated band-pass filtered inputs. The filters are initialized as $h_{xx} = 1$ and $h_{xy} = 0$. The step size μ is set to 10^{-5} and is decreased as $\mu = \mu/1.1$ over 13 iterations over each data batch. Note that iterations over the same batch is needed due to the limited number of samples per experimental batch, and in a real-time system the equalizer would be continuously updated using a fixed μ. The final converged equalizer is then applied to the original (non-bandpass filtered) signals. To get the output of the CV-QKD polarization, the following tap relations are used

$h_{yy} = -h_{xx}^*$ and $h_{yx} = h_{xy}^*$ where h_{yy} and h_{yx} are applied to the non-filtered x-signal and y-signals, respectively. Note that the operation of the polarization de-multiplexing filter acts as a rotation in the four-dimensional optical field. If the optical hybrid is perfect all detectors are identical this operation should have no impact noise per polarization. However, in an implementation this is never the case and hence we apply the same rotation to the measured shot noise and electrical noise. After this stage, the signal-polarization can be treated as conventional single-polarization heterodyne (double quadrature) detection.

The pilot output of the pol. demux. stage is sent to a narrow bandpass filter with 7.75 MHz bandwidth and then the phase of the pilot signal is removed from the QKD signal, which effectively removes the frequency and phase offset between the Tx. and Rx. laser. Then the known frequency offset of 0.67 GHz between the pilot and the QKD signal is removed and a root-raised cosine filter with roll-off 0.05 is applied. From here on, a data-aided approach is applied where the idea is that the data that the Tx. reveals publicly for parameter estimation also can be used for the DSP. The residual fixed phase-offset of the processed batch is estimated based on knowledge of the transmitted symbols. The final part of the DSP is a data-aided equalizer with 145 taps for which the function is two-folded; removing any residual inter-symbol interference and also downsample the QKD-signal to 1 sample/symbol. The measured shot-noise and electrical noise is passed through the same DSP functions as the QKD signal.

III. Experimental Setup

The experimental setup is shown in Fig. 1. The CV-QKD wavelength channel under test is generated by one transmitter and the remaining 193 channels by a load channel setup. The test channel uses a tunable laser with $<$100 kHz nominal linewidth as light source which is modulated by a dual-polarization I/Q-modulator. One polarization is modulated with 0.5 Gbaud quadrature phase shift keying (QPSK) signals with root-raised cosine pulse shape with 0.05 roll-off using an arbitrary waveform generator with 12 GS/s sample-rate generating repeated random sequences. The signals are up-shifted by 0.67 GHz. The second polarization is left unmodulated and used as a pilot as described in the previous section. The power ratio between the pilot and the QKD signal is controlled by adjusting the bias of the unmodulated polarization. To monitor the ratio between the CV-QKD signal and the pilot signal, a portion of the signal after the I/Q-modulator is directed to a polarization scrambler followed by a polarizer where the optical power is measuring using min/max hold function of an optical spectrum analyzer (OSA). We note the monitoring of the pilot-to-signal ratio may possibly also be performed using the DP-I/Q-modulator's internal photodetectors, typically used in auto bias circuity. The pilot-to-signal power ratio is kept between 11.5 and 12.5 dB. The transmitted variance is adjusted to be 0.5 SNU using a variable optical attenuator (VOA) where the power measurement is calibrated to the input of the fiber.

A second transmitter setup is used to generate the load channels using an optical frequency comb with 25 GHz spacing as light source [22]. The loading channels are modulated by a second dual-polarization I/Q-modulator driven with the same signal shape as the channel under test, but with independent sequence, generating 194 channels. After the modulator, a wavelength selective switch (WSS) flattens the spectrum and creates a tunable notch that removes one channel at the wavelength of the channel under test. The WSS also controls the launched power of the load channels. For the measurements, the wavelength of the channel under test and the notch filter is swept such that all 194 wavelength channels are measured. The signals are combined using a passive 90/10 fiber coupler before being launched into a 25 km span of standard single-mode fiber (SMF). The spectrum of the combined signals is shown in the inset of Fig. 1. Note that the spectrum is not perfectly flat since we could not achieve high enough power for all the channels if more flattening was applied. The power difference can be seen as different channels using slightly different pilot-to-QKD power ratios.

The CV-QKD receiver starts with an optical switch that blocks the input to the receiver to measure the shot-noise variance followed by an optical isolator to avoid any reflections. The received signal is mixed with the LO, also a $<$100 kHz laser, in a polarization diversion optical hybrid and detected by four balanced photo-detectors (BPD) with 1.6 GHz bandwidths. The electrical signals are digitized by a 2.5 GS/s real-time oscilloscope with 1 GHz bandwidth. The received signal and the shot-noise are always measured in the same oscilloscope trace while the electrical noise captured before the measurements. The signals are sent to the DSP outlined in the previous section followed by parameter estimation [14], [23], [24] and SKR calculation for reverse reconciliation, using the common assumption of a trusted receiver with calibrated receiver electrical noise, based on the estimated mutual information between Rx. and Tx. and Holevo information between the Rx. and the eavesdropper [25], [26].

In this work, we estimate the asymptotic SKR as follows. The SKR per pulse used for QKD in bit/pulse is given as

$$SKR' = \beta I(A|B) - \chi(E|B) \tag{4}$$

where β is the reconciliation efficiency which is assumed to be 0.9. Further, $I(A|B)$ is the mutual information between Alice and Bob and $\chi(E|B)$ the Holevo information between Eve and Bob. Given the raw pulse repetition rate R_p of 0.5 GHz, the SKR in bit/s is given as

$$SKR = R_p(1 - P_{est})(1 - P_{SN})SKR' \tag{5}$$

where P_{est} is the percentage of pulses used for parameter estimation and P_{SN} the percentage of pulses where the input is closed for shot noise and electrical noise estimation. We assume half of the pulses are used for parameter estimation, i.e. $P_{est} = 50\%$ and that the shot noise measurements take up 10% of the measurement time, i.e. $P_{SN} = 10\%$.

IV. Results

The measured SKRs using Eq. (5), i.e. after the assumed percentage of pulses used for parameter estimation and pulses removed due to shot noise measurements has been deducted, for

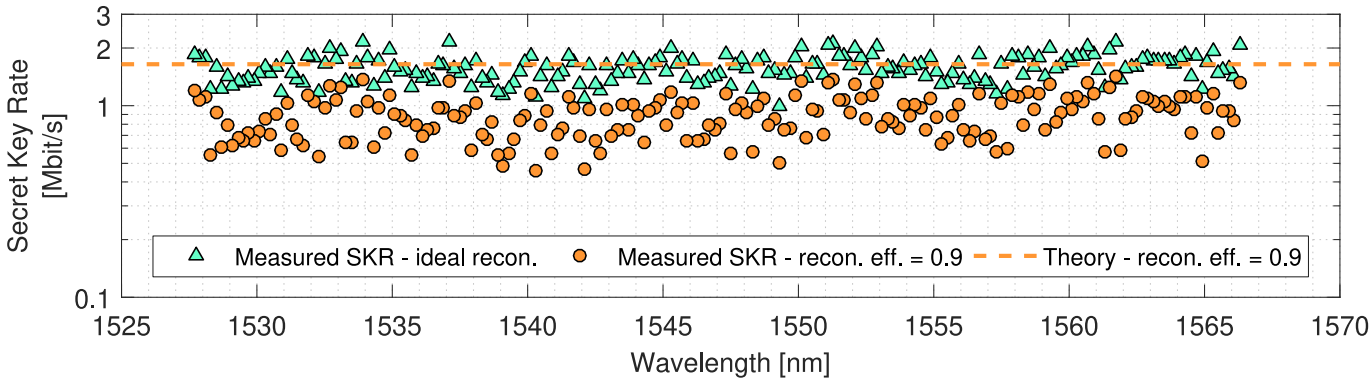

Fig. 3. Secret key rates of all 194 WDM channels on a 25 GHz spacing. Triangles show the SKR with ideal reconciliation efficiency and circles show the SKR assuming a realistic reconciliation efficiency of 0.9. Dashed line shows calculated SKR for 25 km with the parameters given in the text.

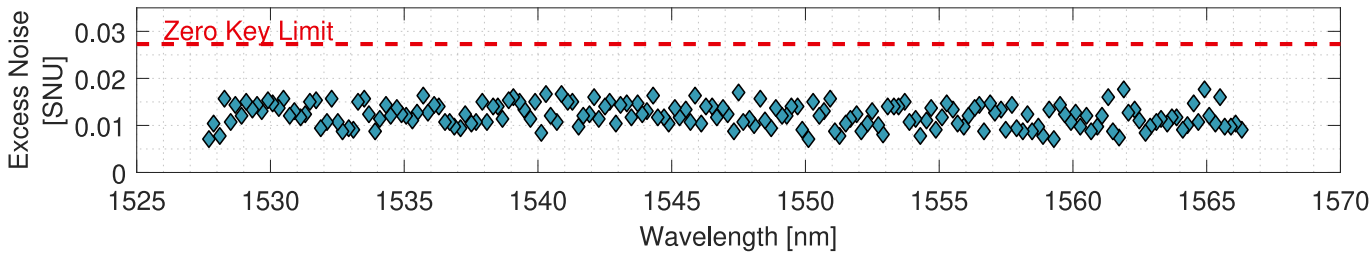

Fig. 4. Measured excess noise in shot noise units (SNU) for all 194 channels. Dashed line shows the excess noise limit where the SKR is zero, for 25 km and the parameters given in the text.

all 194 channels are shown in Fig. 3. The lowest measured SKR for any channel is 0.46 Mbit/s and the maximum 1.43 Mbit/s. The average SKR over all channels is 0.90 Mbit/s per channel. The total aggregated SKR is estimated to be 172.6 Mbit/s. For comparison, we also plot the SKR assuming perfect reconciliation efficiency in Fig. 3. We do not observe any significant wavelength dependence on the measured SKR. Also shown in the plot is the theoretically calculated SKR at 25 km plus 1 dB extra coupling loss, assuming 0.012 SNU excess noise, 0.9 SNU electrical noise, detection efficiency of 0.635, modulation variance 0.5 SNU, and reconciliation efficiency of 0.9.

The varying SKRs for different channels may originate from several effects. Even though we measure at least 5e6 channel observations per wavelength channel, we still expect some variance of the results. Further, the performance of the receiver is found to be dependent on the frequency offset between the Tx. and Rx. lasers which varies when the measured channel is changed. If the offset is large, the signal is attenuated due to the bandwidth limitation of the Rx. To show that the system is working with free-running lasers, we do not finely tune this offset.

The measured excess noise for all the channels is shown in Fig. 4 and ranges between 0.007 and 0.018 SNU, and is on average 0.01 SNU. All channels are below the zero key limit of 0.027 SNU. The measured electrical noise variance was on average 0.09 SNU. In Fig. 5 the calculated SKR for different modulation variances with the parameters given above for 25 km,

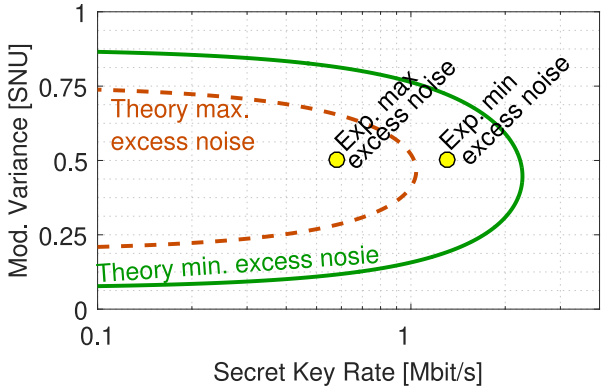

Fig. 5. Calculated SKRs for minimum and maximum excess noise measured for any of the 194 channels as a function of modulation variance with the other parameter set as explained in the text. Circles shows the corresponding measured SKR for the channels with minimum and maximum excess noise.

and using the minimum and maximum measured excess noise for any channel. As seen, the chosen modulation variance of 0.5 SNU gives close to optimal SKR for both cases. We should note that using a modulation variance lower than 0.25 SNU caused the DSP to fail frequently. However, this could possibly be solved by optimizing the parameters of the DSP at lower modulation variance as this was done only for the theoretically optimal value of around 0.5 SNU. We also note that it may be beneficial to

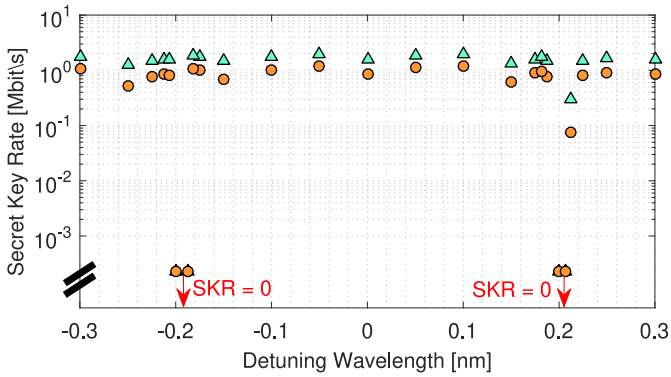

Fig. 6. Secret key rates as a function of wavelength detuning of one of the two center channel of the 194 WDM channels when all WDM channels are transmitting. Note that the two neighboring channels are spaced at approximately ±0.2 nm from the center of the measured channel. Note that the axis is discontinuous to indicate measurements where the SKR was 0.

operate the system at slightly higher then theoretically optimal modulation variance, to aid the DSP convergence. However, this requires more detail investigations outside the scope of this paper.

In our experiment the main reason for using 25 GHz channel spacing is due to the fact that the comb source driving the load channels is designed for this spacing. However, since the CV-QKD signal bandwidth is only 0.5 GHz, much narrower channel spacing may possibly be used. To indicate this, we investigate the SKR as a function of wavelength detuning for one of the two center channels of the WDM system. The results are plotted in Fig. 6. Note that the two neighboring channels are spaced at approximately ±0.2 nm from the center of the channel under test. This shows that we do not see any apparent penalty from spacing two channels closer than 25 GHz and it is only when the channel under test is extremely close to a neighboring channel that the SKR is affected. Hence, we note the CV-QKD system studied in this paper, has the potential of transmitting many more channels in the same optical bandwidth compared to what we show with 25 GHz spacing.

V. Conclusion

We have proposed and demonstrated a digital self-coherent CV-QKD technique based on a transmitted pilot tone and a polarization diverse receiver with a true LO. To the best of our knowledge, this is the first demonstrated fully digital QKD solution, capable of polarization and phase tracking in the digital domain. We show the first WDM experiment with CV-QKD channels and successfully transmit 194 × 0.5 GHz WDM channels, the highest reported number for any QKD system, over 25 km fiber with an estimated aggregate SKR of 172.6 Mbit/s assuming 50% of pulses used for parameter estimation and 10% for shot noise measurements.

Acknowledgment

Tobias would like to thank Sebastian Kleis for discussion on the receiver structure and shot noise measurements.

References

[1] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, 2016, Art. no. 16025.
[2] C. Cesare, "Encryption faces quantum foe," *Nature*, vol. 525, no. 7568, 2015, Art. no. 167.
[3] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Scientific Rep.*, vol. 6, 2017, Art. no. 19201.
[4] Q. Zhen, I. B. Djordjevic, and M. A. Neifeld, "RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection," *Opt. Lett.*, vol. 41, no. 23, pp. 5507–5510, 2016.
[5] M. Rueckmann, S. Kleis, and C. G. Schaeffer, "1 GBaud continuous variable quantum key distribution using pilot tone assisted heterodyne detection," *Photon. Netw. 19th ITG-Symp. VDE*, 2018.
[6] D. Huang *et al.*, "Continuous-variable quantum key distribution with 1 Mbps secure key rate," *Opt. Express*, vol. 23, no. 13, pp. 17511–17519, 2015.
[7] S. Kleis, J. Steinmayer, R. H. Derksen, and C. G. Schaeffer, "Experimental investigation of heterodyne quantum key distribution in the S-Band embedded in a commercial DWDM system," in *Proc. Opt. Fiber Commun. Conf.*, 2019, paper Th1J.3.
[8] T. A. Eriksson *et al.*, "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels," *Commun. Phys.*, vol. 2, no. 1, 2019, Art. no. 9.
[9] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous variable quantum key distribution," *Physical Rev. A*, vol. 87, 2013, Art. no. 062313.
[10] J.-Z Huang *et al.*, "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack," *Physical Rev. A*, vol. 87, 2013, Art. no. 062329.
[11] D. B. S Soh *et al.*, "Self-referenced continuous-variable quantum key distribution protocol," *Physical Rev. X*, vol. 5, no. 4, 2015, Art. no. 041010.
[12] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator 'locally' in continuous-variable quantum key distribution based on coherent detection," *Physical Rev. X*, vol. 5, 2015, Art. no. 041009.
[13] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," *Opt. Lett.*, vol. 40, no. 16, pp. 3695–3698, 2015.
[14] S. Kleis, M. Rueckmann, and C. G. Schaeffer, "Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals," *Opt. Lett.*, vol. 42, no. 8, pp. 1588–1591, 2017.
[15] T. Hirano *et al.*, "Implementation of continuous-variable quantum key distribution with discrete modulation," *Quantum Sci. Technol.*, vol. 2, no. 2, 2018, Art. no. 024010.
[16] E. Agrell *et al.*, "Roadmap of optical communications," *J. Opt.*, vol. 18, no. 6, 2016, Art. no. 063002.
[17] G. Brassard *et al.*, "Multiuser quantum key distribution using wavelength division multiplexing," in *Proc. SPIE Appl. Photon. Technol.*, vol. 5260, 2003, pp. 149–153.
[18] K. I. Yoshino *et al.*, "High-speed wavelength-division multiplexing quantum key distribution system," *Opt. Lett.*, vol. 37, no. 2, pp. 223–225, 2012.
[19] J. Mora *et al.*, "Simultaneous transmission of 20x2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON," *Opt. Express*, vol. 20, no. 15 pp. 16358–16365, 2012.
[20] R. S. Luis *et al.*, "Digital self-homodyne detection," *IEEE Photon. Technol. Lett.*, vol. 27, no. 6, pp. 608–611, Mar. 2015.
[21] F. Laudenbach *et al.*, "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," *Quantum*, vol. 3, p. 193, 2019.
[22] B. P.-Kuo, E. Myslivets, V. Ataie, E. G. Temprana, N. Alic, and S. Radic, "Wideband parametric frequency comb as coherent optical carrier," *J. Lightw. Technol.*, vol. 31, no. 21, pp. 3414–3419, 2013.
[23] P. Jouguet, S. K.-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," *Physical Rev. A*, vol. 86, no. 3, 2012, Art. no. 032309.
[24] F. P. Laudenbach *et al.*, "Continuous-variable quantum key distribution with Gaussian modulation-The theory of practical implementations," *Adv. Quantum Technol.*, vol. 1, no. 1, 2018, Art. no. 1800011.
[25] H. Zhang, J. Fang, and G. He, "Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers," *Physical Rev. A*, vol. 86, no. 2, 2012, Art. no. 022338.
[26] A. Leverrier and P. Grangier, "Continuous-variable quantum key distribution protocols with a discrete modulation," 2010, *arXiv:1002.4083*.