Digital Self-Coherent Continuous Variable Quantum Key Distribution System

Tobias A. Eriksson[1,2], **Ruben S. Luís**[1], **Kadir Gümüş**[3], **Georg Rademacher**[1], **Benjamin J. Puttnam**[1], **Hideaki Furukawa**[1], **Naoya Wada**[1], **Yoshinari Awaji**[1], **Alex Alvarado**[3], **Masahide Sasaki**[1], **Masahiro Takeoka**[1]

(1) National Institute of Information and Communications Technology (NICT), 4-2-1 Nukui-kitamachi, Koganei, Tokyo 184-8795, Japan.
(2) Royal Institute of Technology (KTH), AlbaNova University Center, 106 91 Stockholm, Sweden.
(3) Eindhoven University of Technology, 5600 MB Eindhoven, The Netherlands.
eriksson@nict.go.jp

Abstract: We investigate a continuous variable quantum key distribution system with digital tracking of both polarization and phase. Stable operation over 25km for 36 hours with secret key rates between 1.9 and 2.8 Mbit/s is demonstrated.

OCIS codes: 060.5565 Quantum communications, 270.5568 Quantum cryptography

1. Introduction

Quantum key distribution (QKD) offers means to increase the security of next generation optical communication systems or even ensure unconditionally security in combination with one-time pad encryption [1]. The interest in QKD has risen in recent years, largely due to the rapid progress in computation hardware, lower cost of data storage, and quantum computing technologies [2]. The most mature QKD systems are based on single-photon detection schemes, however, continuous variable (CV) QKD has recently received a lot of interest for several reasons. It may be implemented with off-the-shelf hardware from coherent communication technology, promising low cost and/or integrability. It is also compatible with wavelength division multiplexing of classical channels and hence may use the existing network infrastructure. Long distance CV-QKD has been demonstrated [3] and recently the secret key rates (SKRs) have been pushed into the Mbit/s region [4–6]. Further, it has been experimentally demonstrated that CV-QKD can be co-propagated with classical channels in experiments with 56 [7] and 100 wavelength division multiplexing (WDM) channels [8].

One major challenge for CV-QKD systems is how to synchronize the phase between the transmitter and receiver. The phase tracking can be done using all-optical techniques [3, 8, 9] or relying on digital techniques based on pilot signals [4, 5, 7]. However, these systems have relied on manual polarization alignment or all-optical tracking solutions [9] which do not scale well with channel count and is not well suitable for commercial implementation.

In this paper we propose and evaluate a fully digital self-coherent CV-QKD systems based on dual-polarization and dual-quadrature detection using a polarization-multiplexed pilot tone [10], avoiding costly and bulky optical tracking systems. We also evaluate the performance using reconciliation based on multi-edge type low-density parity check codes. At 25 km, we show SKR of 2.3 Mbit/s estimated from the channel observations and 2.2 Mbit/s with the reconciliation applied. Long-term measurements over 36 hours show that the system can operate without manual tuning.

2. Experimental Setup and Digital Signal Processing

In Fig. 1, the experimental setup is outlined. The transmitter, Alice, uses a conventional tunable laser with $<$100 kHz nominal linewidth as light source tuned to 1547.3 nm. CV-QKD state modulation using four phase states is achieved using a dual-polarization I/Q-modulator, where one polarization is driven by an 12 GS/s arbitrary waveform generator (AWG) generating 0.5 Gbaud signals using a root-raised cosine pulse shape with a roll-off factor of 0.05. The second polarization is left unmodulated and used as a pilot tone in the receiver. The

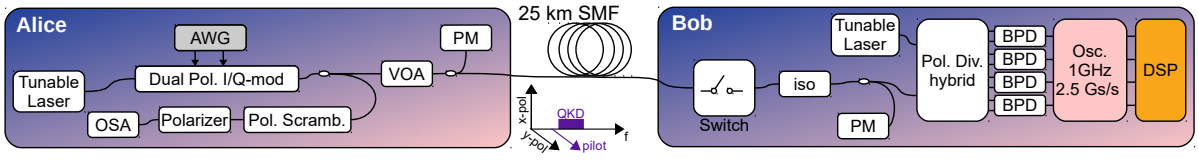

Fig. 1: Experimental setup for the self-coherent CV-QKD system.

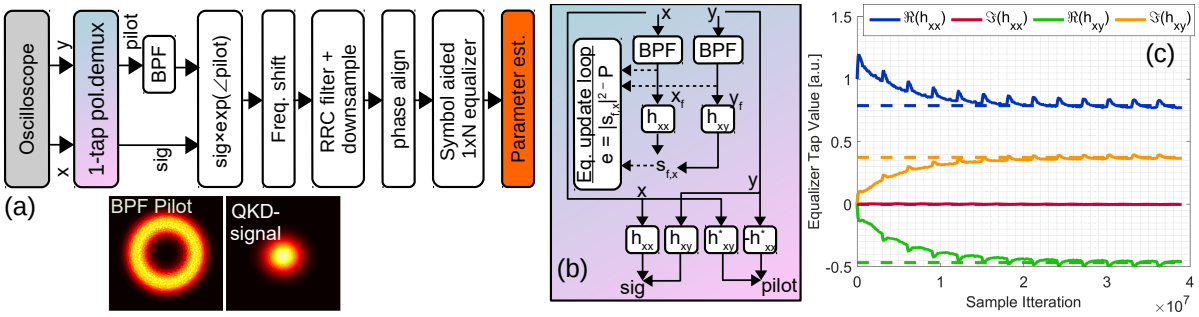

Fig. 2: (a) Schematics of the digital signal processing procedure. (b) Illustration of the polarization demultiplexing stage. (c) Convergence of the taps for the polarization dumultiplexing stage for one batch of data of experimental data.

CV-QKD signal is upshifted by 0.67 GHz to avoid polarization crosstalk from the pilot signal. To monitor the ratio between the CV-QKD signal and the pilot signal, a portion of the signal after the I/Q-modulator is sent to a polarization scrambler followed by a polarizer where an optical spectrum analyzer (OSA) is measuring the optical power using min/max hold. We note that this function could also be performed after calibrating the modulators internal photodetectors typically used in auto bias circuity. The power ratio is set to 12 dB.

The signals are transmitted over 25 km of conventional single-mode fiber. The receiver starts with an optical switch, which is synchronized to the trigger of the oscilloscope. The switch blocks all incoming signals in order to estimate the shot-noise variance of the receiver. This is always measured in the same trace as the CV-QKD signal. A second free-running laser is used as a local oscillator, operating at 15.5 dBm output power. An optical polarization diverse 90-degree hybrid is used followed by four sets of balanced photodetectors (BPDs) with electrical amplifiers and 1.6 GHz bandwidth. The signals are digitized using a 1 GHz real-time oscilloscope with 2.5 GS/s sampling rate. Note that no polarization control is used at the receiver.

The digital signal processing is outlined in Fig. 2(a). The two complex signals constructed from the digitized signals are first sent to a 1-tap polarization demultiplexing stage where the error is calculated based on the knowledge that one polarization should contain a strong pilot tone, i.e. a constant modulus signal. As illustrated in Fig. 2(b), the equalizer taps are updated based on error calculated from narrowly bandpass-filtered versions of the signals where the center of the bandpass filter is adapted based on finding a peak in the combined spectrum of the x- and y-pol polarization signals. The convergence of the taps for one measured batch is shown in Fig. 2(c). The average of the equalizer taps over the final iteration, shown as dashed lines in Fig. 2(c)., are then applied on the non-filtered signal. The pilot tone signal is then narrowly filtered and the phase is extracted from the pilot and removed from the CV-QKD signal followed by a frequency down-shift corresponding to the applied shift in the transmitter. After this, a root-raised cosine filter with roll-off 0.05 is applied followed by downsampling to 4 samples per symbol. The constant phase offset between the transmitted and received data is removed followed by a symbol aided equalizer with 9 taps from which the output is 1 sample per symbol. The symbols are then sent to a parameter estimation stage [7] and/or a reconciliation stage.

For the information reconciliation, we used multi edge type low parity check codes (MET-LDPC) with a block length of 10^6 decoding using the sum-product algorithm with 500 iterations. The base code that was used is a rate 0.02 code adhering to the distribution described in [11]. Shortening of the code was applied in order to achieve a variable rate. The estimated SKRs with and without reconciliation is given as

$$SKR_{est} = \beta I(A|B) - \chi(E|B), \qquad SKR_{recon} = (1-FER)(R-\chi(E|B)), \tag{1}$$

where β is the reconciliation efficiency, $I(A|B)$ is the mutual information between Alice and Bob, $\chi(E|B)$ the Holevo information between Eve and Bob [12]. Further, FER is the frame error rate, and R the rate of the error correction. Note that for the reconciliation case, the frames containing errors are considered to be discarded.

3. Results

The measured SKR over the 25 km of fiber as a function of transmitted modulation variance is shown in Fig. 3(a) together with the theoretical calculation with parameters matching the experiment. The DSP parameters, such as step-size and convergence time, were optimized at a modulation variance of 0.5. For very low modulation variances the DSP had issues with convergence, however this could possibly be addressed by optimizing the DSP parameters for every modulation variance. The SKR with a modulation variance of around 0.375 and 0.5 were approximately the same. However, we choose to perform the rest of the experiments using the latter to avoid having issues with mis-convergence at lower power. Fig. 3(b) depicts the SKR using modulation variance of 0.5 and the reconciliation based on MET-LDPC codes using different code rates. Note that each point is associated with a certain code rate and a frame error rate (FER). The highest SKR is achieved with a rate of 0.01745 and

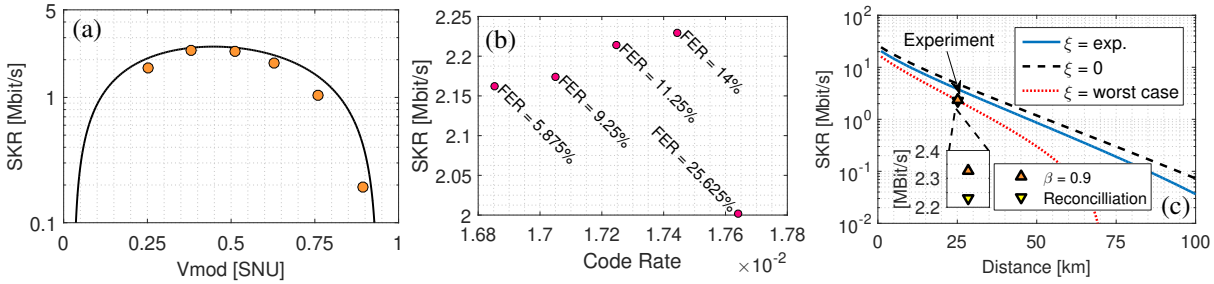

Fig. 3: (a) Measured secret key rate as a function of transmitted variance. (b) The secret key rates as a function of the applied code rate of the MET-LDPC on the experimental results with modulation variance of 0.5. Text labels shows the frame error rate (FER). (c) Calculated secret key rates as a function of distance for three cases: no excess noise, excess noise matching experiment, and worst case excess noise estimated from long term measurements with 95% confidence. The two markers shows the experimental results with assumption of a reconciliation efficiency of 90% and with the performance from the actual reconciliation. The inset shows a zoom in to differentiate the difference. The reconciliation results is 0.1 Mbit/s lower than the estimated results.

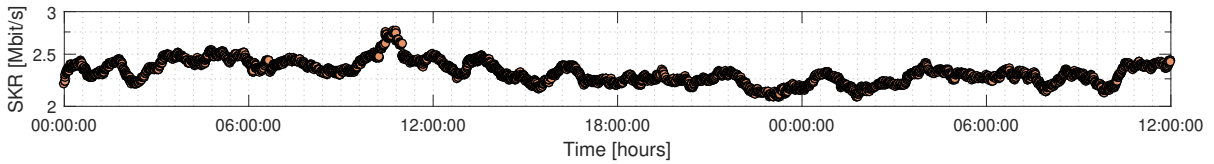

Fig. 4: Long term measurements of the secret key rate at 25 km over 36 hours using a sliding window of 60 batches each consisting of approximately 0.6M channel observations per point.

an associated FER of 14%. In Fig. 3(c) we plot our experimental results in comparison with calculated SKRs as a function of distance for different scenarios: excess noise matching the experiment, no excess noise, and finally excess noise = 0.015 corresponding to the worst case scenario with 95% confidence interval.

To evaluate how the system is performing over time where the polarization state is expected to vary, we perform continuous measurements over 36 hours without any manual control of polarization or frequency offset between transmitter and receiver laser. The measured SKR is shown in Fig. 4. The SKR ranges between 1.9 and 2.8 Mbit/, we attribute the variations to several factors including modulator bias drift, polarization dependent loss in receiver components, and frequency offset drift which changes performance due to roll-off of the oscilloscope bandwidth.

4. Conclusions

We have demonstrated a CV-QKD receiver capable of digital phase and polarization tracking based on a digital self-coherent scheme. Long term measurements over 36 hours shows a secret key rate between 1.9 and 2.8 Mbit/s. We also evaluate the performance using reconciliation based on MET-LDPC codes.

5. Acknowledgments

Tobias would like to thank Sebastian Kleis for discussion on the receiver. This work was funded by the Swedish Research Council Grant No 2017-06179 and Council for Science, Technology and Innovation (CSTI), Crossministerial Strategic Innovation Promotion Program (SIP), Photonics and Quantum Technology for Society5.0 (Funding agency : QST)..

References

1. E. Diamanti, et al., "Practical challenges in quantum key distribution," npj Quantum Information, vol. **2**, p. 16025, 2016.
2. C. Cesare, "Encryption faces quantum foe," Nature, vol. **525**, (7568), p. 167, 2015.
3. D. Huang, et al., "Long-distance continuous-variable quantum key distribution by controlling excess noise," Scientific Reports, vol. **6**, p. 19201, 2017.
4. Q. Zhen, et al., "RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection." Optics Letters, vol. **41**, (23), pp. 5507–5510, 2016.
5. M. Rueckmann, et al., "1 GBaud continuous variable quantum key distribution using pilot tone assisted heterodyne detection," Photonic Networks; 19th ITG-Symposium. VDE, 2018.
6. D. Huang, et al., "Continuous-variable quantum key distribution with 1 Mbps secure key rate," Optics Express, vol. **23**(13), pp. 17511-17519, 2015.
7. S. Kleis, et al., "Experimental investigation of heterodyne quantum key distribution in the S-band or L-band embedded in a commercial C-band DWDM system," Optics Express, vol. **27**(12), pp. 16540–16549, 2019.
8. T. A. Eriksson, et al., "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels," Communications Physics, vol. **2**(1), p. 9, 2019.
9. T. Hirano, et. al., "Implementation of continuous-variable quantum key distribution with discrete modulation," Quantum Science and Technology, vol. **2**(2), p. 024010, 2018.
10. R. Luis, et al., "Digital self-homodyne detection," IEEE Photonics Technology Letters, vol. **27**(6), pp. 608–611, 2015.
11. P. Jouguet, et al., "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," Physical Review A, vol. **84**(6), p. 062317, 2011.
12. H. Zhang, et al., "Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers," Physical Review A, vol. **86**(2), p. 022338, 2012.