European Conference on Optical Communication (ECOC) 2022 © Optica Publishing Group 2022

Continuous-Variable Quantum Key Distribution Over 60 km Optical Fiber With Real Local Oscillator

Adnan A.E. Hajomer*, Hossein Mani, Nitin Jain, Hou-Man Chin, Ulrik L. Andersen, Tobias Gehring

Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark, * aaeha@dtu.dk

Abstract *We report the first continuous-variable quantum key distribution experiment that enables the generation of secure key over a 60 km fiber channel with locally generated local oscillator. This is achieved by controlling the excess noise using machine learning for phase noise compensation while operating the system at a low modulation variance.*

Introduction

Quantum key distribution (QKD) is an information-theoretically secure method to distribute secret keys between communication parties (Alice and Bob) based on the principles of quantum mechanics[1],[2]. Fundamentally, the secret key rate scales inversely with transmission distance[3] and as amplification of quantum states is incompatible with secret key generation, trusted or untrusted relays are required to achieve QKD over long distances. Naturally, it is desirable to extend the distance between relays as much as possible.

Since the first experiment of QKD over a 32-cm free space channel[4], considerable efforts have been devoted to perform QKD with channel lengths in the few 100s of km range[2]. Most of these experiments employed so-called discrete-variable schemes that use single photon detectors, which are not standard telecom equipment and require special cooling units during operation. In contrast, encoding the secret key bit information in the phase and amplitude quadratures of the electro-magnetic light field and then decoding it with a coherent receiver in so-called continuous-variable (CV) QKD, offers the use of standard telecom components that work at room temperature[5],[6]. However, long-distance CVQKD has been limited due to two main factors. One is excess noise[7], mainly attributed to the laser phase noise, and the other is limited information reconciliation efficiency[8].

To avoid phase noise, several CVQKD experiments have used the so-called transmitted local oscillator (TLO) scheme[9]–[13], in which the transmitter/Alice prepares both the weak quantum signal and a strong local oscillator (LO) from the same laser and sends them to the receiver/Bob on the same optical fiber channel, to provide a stable phase reference. However, this implementation allows the eavesdropper/Eve to manipulate the LO, resulting in different possible attacks[14],[15]. Moreover, to reduce in-band excess noise due to leakage from the strong TLO to the weak quantum signal, both polarization and time multiplexing are required, making the experimental realization of the system more complicated[16]. One way to deal with the security and implementation issues of TLO-based CVQKD is to use an independent laser at Bob to generate the LO. This real local oscillator (RLO) or local local oscillator (LLO) scheme[17]–[21], however, exhibits higher excess noise compared with TLO CVQKD because of the residual phase noise after the phase compensation procedure[22]. The maximum distance covered by a LLO-based CVQKD experiment has been 40 km[19],[21].

Here, we report the longest (to our knowledge) distance experiment of CVQKD with LLO over 60 km fiber channel. This remarkable range is made possible by operating the system at low modulation variance of 1.8 shot noise units (SNU), in which phase noise is not a dominant factor. Besides, we use a machine learning (ML) framework for phase noise compensation so that a small residual phase noise can be maintained at a low pilot power[20]. Our system employs a continuous-wave (CW) laser and digital mode shaping, obviating the need of an additional amplitude modulator for pulse carving. As for error correction, we perform information reconciliation (IR) based on a multi-dimensional scheme using a multi-edge-type low-density-parity-check error correcting code[23] with an efficiency of 94.31% .

978-1-6654-3868-1/21/$31.00 ©2021 IEEE

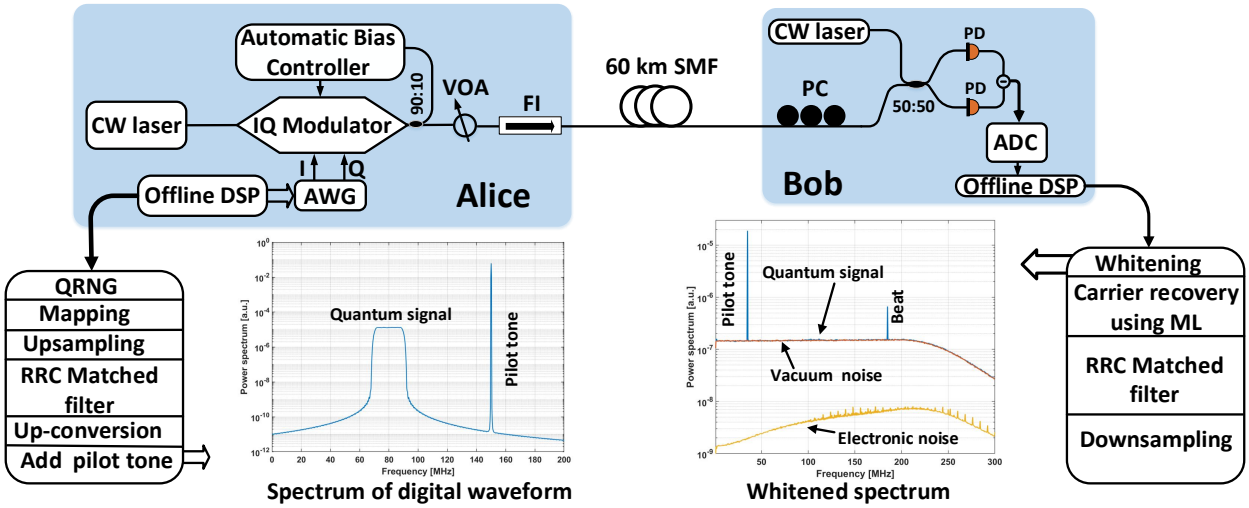

Fig. 1: Experimental setup and DSP routine. QRNG: quantum random number generator; CW: continuous-wave laser; AWG: arbitrary waveform generator; VOA: variable optical attenuator; PC: polarization controller; ADC: analog-to-digital converter; PD: photodiode, FI: Faraday isolator, RRC: root raised cosine.

Residual phase noise

To estimate the relative phase between Alice's and Bob's free running lasers in LLO CVQKD, pilot-aided techniques, in which a classical reference signal known as pilot tone is transmitted together with the quantum signal, have been used[17]–[20]. However, the estimated phase from these methods is not exactly equal to the actual relative phase of the quantum signal, which results in residual phase noise after phase compensation. This phase noise is the main contributor to the total excess noise that limits long-distance LLO CVQKD. In our case, where we use a Gaussian-modulated coherent state (GMCS) protocol, the phase noise can be expressed as[22],

$$\xi_{\text{phase}} = 2V_{\text{mod}}\left(1 - e^{-\frac{V_{\text{est}}}{2}}\right), \qquad (1)$$

where V_{est} is the variance of the residual phase, defined as the variance of the difference between the actual phase of the quantum signal and the estimated value, and V_{mod} is the modulation variance.

From equation 1 it is clear that one can quantitatively reduce the phase noise either by reducing V_{est}, for instance through better phase estimation, or by operating the system at a low modulation variance. While the quality of phase estimation depends on the signal-to-noise ratio of the pilot tone, the latter option requires careful optimization as the secret key rate has a V_{mod} dependence even without phase noise. It is nevertheless practical and simple to realize as the modulation variance can be easily fine tuned. However, as a pilot tone with low power is desirable in CVQKD (to minimise the leakage from the pilot tone to the quantum signal), maintaining a constant residual phase, while the optical loss increases with distance, is not possible using traditional phase estimation techniques[17],[18]. As an alternative, ML has been shown to be an effective way to maintain a relatively constant residual phase over a wide-range of optical loss for a fixed input pilot power[20]. We take the advantage of ML and operate in the low modulation variance regime to reduce the excess noise in our LLO CVQKD system, and therefore extend the channel distance.

Experimental setup

Our experimental setup is shown in Fig. 1. At Alice, a 20 Mbaud quantum signal was generated using offline digital signal processing (DSP). The transmitted symbols were drawn from a quantum number generator (QRNG)[24]. These symbols were upsampled to 1 Gsample/s and pulse-shaped by a root raised cosine (RRC) filter with a roll of factor of 0.2. The samples were then frequency shifted to 80 MHz and frequency multiplexed with a pilot tone at 150 MHz for carrier phase estimation. The spectrum of the digital waveform is shown in the inset of Fig. 1. The generated digital waveforms were uploaded to an arbitrary waveform generator (AWG) with 16 bit resolution and sampling frequency of 1 GSample/s. An in-phase and quadrature (IQ) modulator driven by the AWG was used to encode the ensemble of coherent states and the pilot tone onto a sideband of the optical carrier, generated from 1550 nm continuous-wave (CW) laser with $\approx$ 100 Hz linewidth. At the output of the IQ modulator, the quantum signal was attenuated using a vari-

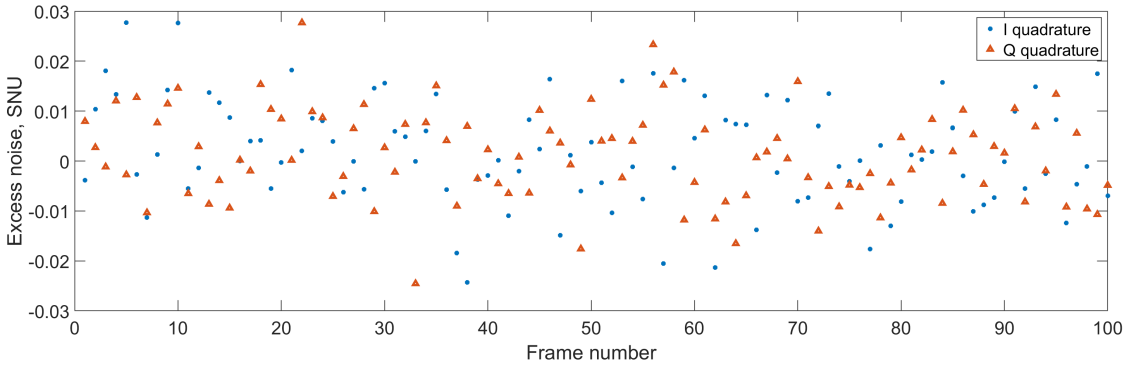

Fig. 2: Measured excess noise.

able optical attenuator (VOA), so that the modulation variance of the thermal state at the input of the 60 km single mode fiber (SMF) channel was 1.8 SNU. To avoid Trojan-horse attacks from the channel a Faraday isolator (FI) was added.

At Bob, the polarization of the optical signal was adjusted using a manual polarization controller (PC). A radio frequency (RF) heterodyne detector, with a 3 dB bandwidth of 365 MHz, measured the optical signal after interference with the LLO on a 50:50 beam splitter. The LLO itself was generated from a CW laser with frequency shift of $\approx$ 180 MHz with respect to Alice's laser. The output of the detector was digitized using an analog-to-digital converter (ADC) with a sampling rate of 1 GSample/s, whose clock was synchronised together with that of the AWG to an external 10 MHz reference clock. The measurement time was divided into frames, each containing 10^7 samples. To recover the transmitted symbols, offline DSP was applied to the recorded frames as follows: A whitening filter was first applied to the modulated signal, vacuum noise trace and electronic noise trace. The output of the whitening filter is depicted as an inset of Fig. 1. The carrier phase estimation was performed using an unscented Kalman filter on the pilot tone[20]. Temporal synchronization was then achieved through a cross correlation between transmitted and received reference symbols, the RRC matched filtering and downsampling were applied to recover the quantum symbols. Finally, Alice and Bob perform IR and parameter estimation.

Results

Fig. 2 shows the measured excess noise variance at the output of the channel for 100 frames, each with 2×10^5 symbols. The average excess noise of *I* and *Q* quadrature is 1.1×10^{-3} and 1.7×10^{-3} SNU, respectively. The corresponding secret key rate fraction is computed in the asymptotic limit according to Ref.[20]. Tab. 1 summarizes the experimental parameters used for secret key generation. Based on these parameters, we achieved a secret key faction of 0.0024 bits/symbol, corresponding to 0.0471 Mbits/s for a symbol rate of 20 Mbaud.

Tab. 1: Experimental parameters. τ: Trusted efficiency, η: Untrusted efficiency, t: trusted detection noise, u: untrusted channel noise, FER: frame error rate, β: IR efficiency.

Alice	Bob	Channel	IR
B = 20 MBaud	$\tau = 0.68$	$\eta = 0.049$	FER $= 50\%$
V_{mod} =1.8 SNU	$t = 58$ mSNU	$u = 1.3$ mSNU	$\beta = 94.31\%$

Tab. 2: Summary of notable CVQKD demonstrations

Ref.	Pulsed/CW	LO	distance	modulation
[9]	Pulsed	TLO	25 km	Gaussian
[11]	Pulsed	TLO	50 km	Gaussian
[10]	Pulsed	TLO	80 km	Gaussian
[12]	Pulsed	TLO	100 km	Gaussian
[13]	Pulsed	TLO	202.18 km	Gaussian
[17],[18]	Pulsed	LLO	25 km	Gaussian
[21]	Pulsed	LLO	40 km	Discrete
[19]	CW	LLO	40 km	Discrete
[20]	CW	LLO	20 km	Gaussian
current work	CW	LLO	60 km	Gaussian

Tab. 2 summarizes recent fiber based CVQKD demonstrations. For distances beyond 60 km, all demonstrations used TLO and pulse carving, in which an additional amplitude modulator is required. So far, the reported maximum distance of LLO CVQKD with CW laser was 40 km, however this system used a 8-state protocol[19] instead of the GMCS protocol, which has a more mature security proof[6].

Conclusions

We have reported a long-distance experiment that extends the security range of LLO CVQKD systems to record length of 60 km. This was made possible by taking advantage of a machine learning framework for phase noise compensation and operating the system with low modulation variance to minimize system excess noise. This work is a step forward to close the gap between LLO- and TLO-CVQKD systems' performance, while maintaining a high level of security and lowering the implementation complexity.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution", *Rev. Mod. Phys.*, vol. 81, no. 3, p. 1301, 2009.

[2] S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in quantum cryptography", *Adv. Opt. Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[3] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications", *Nat. commun.*, vol. 8, no. 1, pp. 1–15, 2017.

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography", *J. cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[5] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states", *Phys. Rev. Lett.*, vol. 88, no. 5, p. 057 902, 2002.

[6] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching", *Phys. Rev. Lett.*, vol. 93, no. 17, p. 170 504, 2004.

[7] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Controlling excess noise in fiber-optics continuous-variable quantum key distribution", *Phys. Rev. A*, vol. 72, no. 5, p. 050 303, 2005.

[8] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution", *Phys. Rev. A*, vol. 77, no. 4, p. 042 325, 2008.

[9] J. Lodewyck, M. Bloch, R. García-Patrón, *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system", *Phys. Rev. A*, vol. 76, no. 4, p. 042 305, 2007.

[10] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution", *Nat. Photonics*, vol. 7, no. 5, pp. 378–381, 2013.

[11] C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, "25 mhz clock continuous-variable quantum key distribution system over 50 km fiber channel", *Scientific Reports*, vol. 5, no. 1, pp. 1–8, 2015.

[12] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise", *Scientific Reports*, vol. 6, no. 1, pp. 1–9, 2016.

[13] Y. Zhang, Z. Chen, S. Pirandola, *et al.*, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber", *Phys. rev. lett.*, vol. 125, no. 1, p. 010 502, 2020.

[14] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems", *Phys. Rev. A*, vol. 88, no. 2, p. 022 339, 2013.

[15] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution", *Phys. Rev. A*, vol. 87, no. 6, p. 062 313, 2013.

[16] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers", *Phys. Rev. A*, vol. 76, no. 5, p. 052 323, 2007.

[17] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator âlocallyâ in continuous-variable quantum key distribution based on coherent detection", *Phys. Rev. X*, vol. 5, no. 4, p. 041 009, 2015.

[18] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator", *Optics lett.*, vol. 40, no. 16, pp. 3695–3698, 2015.

[19] 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.

[20] H.-M. Chin, N. Jain, D. Zibar, U. L. Andersen, and T. Gehring, "Machine learning aided carrier recovery in continuous-variable quantum key distribution", *npj Quantum Inf.*, vol. 7, no. 1, pp. 1–6, 2021.

[21] F. Laudenbach, B. Schrenk, C. Pacher, *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] A. Marie and R. Alléaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution", *Phys. Rev. A*, vol. 95, no. 1, p. 012 316, 2017.

[23] H. Mani, T. Gehring, P. Grabenweger, B. Ömer, C. Pacher, and U. L. Andersen, "Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution", *Phys. Rev. A*, vol. 103, no. 6, p. 062 419, 2021.

[24] T. Gehring, C. Lupo, A. Kordts, *et al.*, "Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information", *Nat, Commun.*, vol. 12, no. 1, pp. 1–11, 2021.