

Continuous-variable quantum key distribution with extended Kalman filter assisted by recurrent neural networks for phase estimation

P. KASTHURI¹, P. PRAKASH^{1,*}, M.S. SOWMYAA VATHSAN¹, A. SASITHRADEVI²

¹Department of Electronics Engineering, Madras Institute of Technology Campus, Anna University, Chennai, 600044, Tamil Nadu, India

²Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, 600127, Tamil Nadu, India

*Corresponding author: prakashp_mit@annauniv.edu

Continuous-variable quantum key distribution (CV-QKD) holds promise for enhancing security in communication networks. However, obtaining a higher secure key rate poses challenges, particularly in reliable phase estimation. So, it is very necessary for CV-QKD implementations with independent local oscillator (LO) to employ carrier recovery along with precise phase estimation. Our methodology combines extended Kalman filters (EKF) with recurrent neural networks (RNNs) to enhance the accuracy of phase recovery for locally generated LO signals. Using numerical simulations, we evaluate the achievable secret key rates for different transmission distances and line widths. The proposed method achieves a phase error of approximately 1×10^{-4} , leading to positive secure key rates for distances up to 40 km. This method of phase tracking solves the problem and is effective in real-time deployment of CV-QKD in communication networks.

Keywords: CV-QKD, quantum communication, phase estimation, recurrent neural networks, extended Kalman filter.

1. Introduction

With advancements in high-performance computing, there is a potential threat to existing classical cryptographic systems. Traditional cryptographic systems rely on mathematics which has been proven to be breakable by high performance computers in today's world. Quantum key distribution or QKD, by laws of quantum physics provide a reliable mechanism for exchanging cryptographic keys despite eavesdroppers with advanced computing capabilities [1, 2]. QKD lets Alice transmit information and Bob the recipient of the signal share secret keys for secure communication over a vulnerable

channel controlled by eavesdropper Eve with unbounded computational capacity. There are mainly two approaches to QKD: CV-QKD (continuous variable quantum key distribution) and DV-QKD (discrete variable quantum key distribution). Discrete variable quantum key distribution uses discrete quantum states, such as the polarization states of a single photon, whereas continuous variable quantum key distribution uses coherent detection technique.

DV-QKD is more mature and has been implemented in experimental setups. The qubits are encoded in properties of individual particles like photons and are decoded using single photon avalanche detectors (SPAD). The need for specialized hardware makes real-world implementation of DV-QKD very complex and expensive [3]. Also, factors affecting the transmission of quantum states are absorption and scattering thereby reducing the signal-to-noise ratio and impacting the reliability of this method. CV-QKD encrypts confidential key information in the states of the quadrature of light's amplitude and phase [4]. On the basis of Gaussian modulated coherent states (GMCS), the CV-QKD protocol is constructed. GMCS CV-QKD is the subject of extensive research due to its potential to provide an economical substitute for DV-QKD. CV-QKD uses PIN diode for coherent detection which makes CV-QKD compatible with standard optical communication infrastructure, and thereby facilitating the ease of deployment in practical communication scenarios.

When implementing CV-QKD, one of the biggest obstacles is finding an accurate phase reference that can connect Alice, the transmitter, and Bob, the receiver. In this work, we have presented a technique to estimate the phase of the reference pilot signal using recurrent neural network aided extended Kalman filtering (EKF). Recent improvements in CV-QKD involves transmitting a low-power reference signal called the reference pilot signal along with the quantum signal, and the reference signal is then used for tracking in receiver LO. However, as the transmitted power is very low, traditional methods of phase recovery cannot be relied upon in CV-QKD. For noisy systems, the estimation of unknown state variables is done by incorporating the extended Kalman filter. The performance of these methods relies on the characterization of the system state. Inability to characterize the system state can lead to degradation of performance. Deep neural networks (DNNs) such as recurrent neural networks (RNNs) perform well in time series related forecasting and has been proposed as a hybrid approach in aiding extended Kalman filter to estimate the unknown state variable without accurate characterization of the system [5]. In this paper we have come up with a novel technique to make use of the machine learning incorporating neural networks combined with extended Kalman filter. We have demonstrated that we would be able to estimate the phase of the reference signal with better accuracy. We have then performed secret key rate analysis on the received signal based on the estimated phase. Secret key rate is benchmark for analysing the performance of QKD systems and indicates its practicality in real world use. This method demonstrates the use of machine learning in estimating the phase of the reference pilot signal. Further work involves use of RNNs in estimating the phase of the reference signal by further increasing accuracy. This opens

up the use of CV-QKD making it a practical methodology for deploying QKD in long distance optical networks.

2. Continuous-variable quantum key distribution utilizing locally generated LO signals

The Gaussian modulated coherent state (GMCS) protocol is among the most studied methods for using CV-QKD [6, 7]. GMCS involves modulation of coherent states that have a well-defined phase and amplitude that follow Gaussian probability distribution.

It appears that the eavesdropper Eve has complete control over the unsecured route over which the resultant states are communicated. The receiver selects either the phase or the amplitude of the quadrature randomly either using balanced homodyne or heterodyne detection. The measurements of Bob are shared with Alice over a secure channel. Alice and Bob will proceed with privacy amplification and mistake correction if their mutual information is higher than Eve's. Noise photons are suppressed by the strong LO signals used in coherent detection. This characteristic renders it as an attractive solution for integration of GMCS into traditional optical networks.

GMCS protocol uses transmitted local oscillator (TLO) scheme to broadcast a powerful LO signal with quantum signal [8]. In recent research, it has been proven that Eve may exert influence over the local oscillator by initiating attacks [9, 10]. Additionally, to accomplish noise-free detection, the strength of local oscillator signal must be seven to eight times larger than the power of the quantum signal. Due to these drawbacks, recent studies have revolved around the use of LO signals that are generated locally at the receiver's end, referred to as the locally generated local oscillator scheme [11, 12].

However, to have a locally generated LO signal, a trustworthy reference phase is needed between Alice and Bob. A relatively low-power reference pulses have been transmitted alongside quantum signals and the reference pulses are used for carrier recovery as shown in Fig. 1. Traditional communication systems have been doing the task of recovering the phase of the received signal. This is known as carrier recovery [13, 14]. However, in order to preserve the quantum signal, the reference pilot signal is transmitted at a relatively low power. This low-power nature of the reference pilot signal makes the traditional carrier recovery methods in communication systems useless in CV-QKD applications.

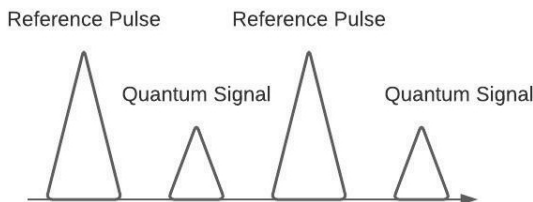


Fig. 1. Enhanced phase recovery scheme using pilot assistance with concurrent reference pulse and quantum signals.

3. Enhanced phase recovery using EKF

3.1. Pilot aided phase recovery

Pilot aided phase recovery is a method employed to estimate phase information from the incoming QKD signals. In the local local oscillator (LLO), there are two separate, independently operating local oscillators (LO) generating two separate but identical LO signals at the transmitter and the receiver [11]. A phase reference signal is provided with QKD signals for phase recovery. As they both travel on the same optical medium, the phase noise on both signals is equal therefore, the channel phase noise is equal to 0. The phase noise experienced by the signals could be expressed by [15],

$$\varphi_{\text{noise}} = \varphi_{\text{error}} + \varphi_{\text{drift}} \quad (1)$$

where φ_{error} denotes the phase difference between the LO signal at the receiver and the signal at the transmitter and φ_{drift} denotes the phase difference between two laser frequencies which results from inaccuracies between two lasers. For optimal key rate, it is necessary to keep the phase difference between LO signals as minimal as possible. We recover the phase signal from the reference pulse that is broadcast concurrently with the quantum signal. The reference signal is a strong unmodulated signal with relatively high power when compared to the QKD signal. We try to estimate the phase of the reference signal at the receivers end with the help of neural network aided Kalman filter.

We have created a simulation setup to train and verify the accuracy and feasibility of our phase recovery method for CV-QKD applications (see Fig. 2). The optical signal generated by the continuous wave laser is sent to the beam splitter to divide the signal

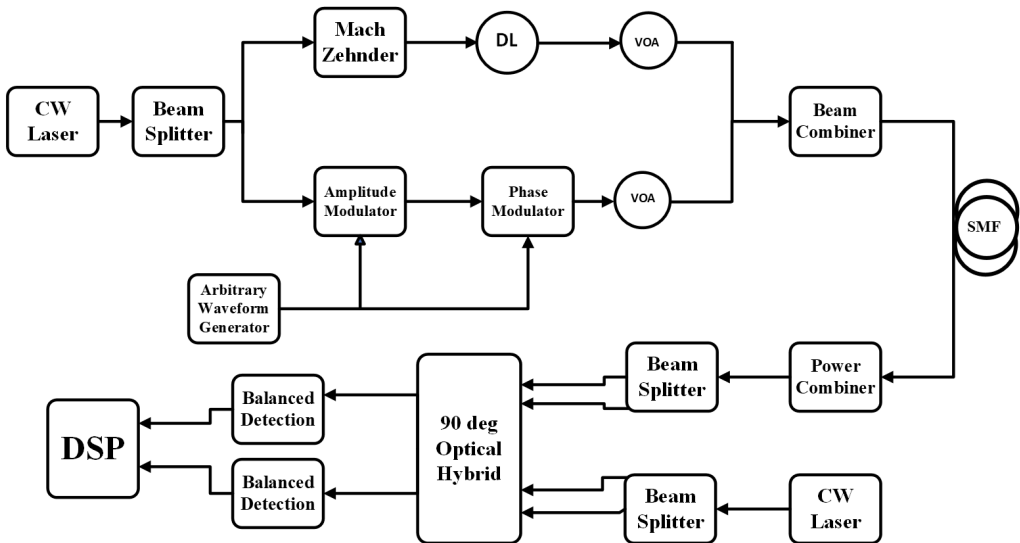


Fig. 2. Simulation setup of phase recovery.

into two components, with one component serving as the reference pulse and the other as the signal. The optical signal in the signal arm is modulated by a Mach–Zehnder (MZ) modulator, utilising the modulated signals generated by an arbitrary waveform generator. The same signals from the arrayed waveguide grating (AWG) are then used to modulate the signal further using a phase modulator (PM). Then it is subsequently sent to an attenuator (VOA) in order to get the desired quantum signal strength. A delay line (DL) is utilised to synchronise successive reference and signal pulses.

Optical fibre lines with different link lengths, the combined signals are sent to their receiving station. Bob's signal is subjected to polarisation control (PC) and then the receiver detects the transmission. The detection of homodyne is carried out by means of a locally produced LO signal at Bob's end, which is then followed by phase estimation by the use of an extended Kalman filter operation on the reference pulses that have been received.

3.2. Neural network based Kalman filtering

Kalman filter is a linear recursive estimator. The estimate of the system x_t at instant t is based on the previous estimate of the system, x_{t-1} and the new observation of the system y_t at that instant.

The phase of the signal is defined by the state-space model, which can be expressed as,

$$X_K = \varphi_k = \varphi_{k-1} + q_{k-1} \quad (2)$$

The symbol's state at instant k , denoted by X_K , is determined by the phase φ_k , where the phase incorporates both the current system phase and the previous instant's unknown phase noise q_{k-1} . As a result of the LO laser's throbbing in conjunction with vacuum fluctuations, the phase of the LO signal within a system may fluctuate at random. The process noise introduced into the Kalman filtering procedure is the phase noise due to the random fluctuations of the laser.

The expression that shows the system's noisy measurement is

$$Y_K = A \sin(\Delta\omega T_s + \varphi_k) + n_k \quad (3)$$

Here n_k denotes the shot noise from the photo-detector, $\Delta\omega$ shows the frequency difference between the pilot and LO, A indicates the amplitude of the signal, and also $\Delta\omega = 0$ for homodyne detection. Two phases comprise the extended Kalman filter (EKF): prediction and update.

1) Prediction: The system's predicted phase $x_{k|k-1}$ is obtained by,

$$m_{\bar{k}} = f(x_{k-1}, k-1) \quad (4)$$

$$P_{\bar{k}} = F(m_{k-1}, k-1)P_{k-1}F^T(m_{k-1}, k-1) + q_{k-1} \quad (5)$$

The system's innovation difference is calculated based on the current observation and the estimate of the current observation,

$$\tilde{y}_k = y_k - y_{k|k-1} \quad (8)$$

Here $y_{k|k-1}$ indicates the estimate of the current observation. The estimate of the current observation is represented in terms of $h(x_k, k)$ function. And $h(x_k, k)$ is obtained by equating the current phase estimate obtained in $y_{k|k-1}$ in Eq. (8).

The forward evolution difference of the system, *i.e.*, the difference the two consecutive posterior state estimates. The posterior state estimate is obtained from the prediction step of Kalman filtering,

$$\tilde{x}_k = x_{k|k} - x_{k-1|k-1} \quad (9)$$

The forward update difference of the system – this quantity represents the difference between the current posterior state estimate and prior state estimates. This can be equated as,

$$\tilde{x}_k = x_{k|k} - x_{k|k-1} \quad (10)$$

where $x_{k|k-1}$ is the prior estimate of the system obtained during prediction state of previous observation.

The above input features are fed into the RNN model to predict the Kalman gain of the system. The Kalman gain K , computed from the RNN is then used to obtain the updated prediction of the system as,

$$P_k = (I - KH)P^- \quad (11)$$

The architecture of the RNN consists of a fully connected input layer that is followed by an GRU layer and a fully connected output layer. In the inputs, the innovation difference and forward update difference represents the uncertainty in the state estimates while the observation difference and the forward evolution difference represents the state evolution process.

The RNN network is trained with normalised data. The data for training is captured from running simulations in the setup mentioned in Fig. 2, in various different system configurations.

4. Secret key rate analysis

Alice constructs the coherent states $|\alpha\rangle = |X_A + iP_A\rangle$ in Gaussian-modulated CV-QKD. Here, X_A and P_A are quadrature values having V_A as covariance and zero mean. Alice transmits a series of states to Bob via an unsecured transmission channel. Eve, the eavesdropper, is presumed to have absolute control over the transmission channel. Bob selects quadrature X or quadrature P at random to measure. Subsequently, he apprises Alice of his measurements, which are utilised to calculate the amount of information

that Eve has been privy to and the mutual information that Alice and Bob exchange. The protocol is terminated if the quantity of known information shared by Alice and Bob is minimal compared with the maximum information disclosed to Eve, specifically the maximum information constrained by Holevo information. Bob has carried out error correction whereas Alice uses a privacy amplification technique. Secret key rate analysis for long distance continuous variable QKD is described below [16].

For collective attack, the secret key rate for reverse reconciliation would be expressed as,

$$\delta I = \gamma I_{AB} - \chi_{BE'} \quad (12)$$

where $\chi_{BE'}$ is the maximum possible Holevo information contained by Eve and Bob, I_{AB} represents the mutual information between Alice and Bob and γ is the reconciliation efficiency provided γI_{AB} exceeds $\chi_{BE'}$.

The mutual information between Alice and Bob may be mathematically represented as,

$$I_{AB} = \frac{1}{2} \log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}} \quad (13)$$

The total noise χ_{tot} and V should be expressed as follows,

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{ohm}}}{T} \quad (14)$$

$$V = V_A + 1 \quad (15)$$

where χ_{line} represents the noise from the channel, χ_{ohm} indicates the noise due to the homodyne detector. The channel's transmittance T for a distance L , determined by an attenuation coefficient α , follows $10^{(-\alpha L)/10}$, while the noise that is produced by the channel may be represented as,

$$\chi_{\text{line}} = 1/T - 1 + \varepsilon \quad (16)$$

$$\varepsilon = \varepsilon_{\phi} + \varepsilon_r \quad (17)$$

Here ε denotes the system's excess noise, ε_r indicates the noise incurred by Raman's scattering effect and ε_{ϕ} represents the phase noise of the system.

Suppose the phase of the quantum signal is denoted as ϕ_s , and the phase of the LO signal at reception is represented by ϕ_{LO} . The phase error between local oscillator and quantum signal phase is expressed as,

$$\phi_{\text{error}} = \phi_{LO} - \phi_s \quad (18)$$

Extended Kalman filter estimation algorithm could be used to obtain phase error. In order to rectify Alice's data in the reverse reconciliation scheme, it is necessary to utilise a rotation matrix that is specified as [12],

$$\begin{pmatrix} \cos \varphi_{\text{err}} & \sin \varphi_{\text{err}} \\ -\sin \varphi_{\text{err}} & \cos \varphi_{\text{err}} \end{pmatrix} \quad (19)$$

The corrected data for Alice is represented by the covariance matrix,

$$\begin{pmatrix} \tilde{x}_A \\ \tilde{p}_A \end{pmatrix} = \begin{pmatrix} \cos \varphi_{\text{err}} & \sin \varphi_{\text{err}} \\ -\sin \varphi_{\text{err}} & \cos \varphi_{\text{err}} \end{pmatrix} \begin{pmatrix} x_A \\ p_A \end{pmatrix} \quad (20)$$

Under the assumption of Gaussian phase noise, the estimated phase noise can be expressed as [12],

$$\varepsilon_\varphi = 2V_A \left[1 - \exp\left(-\frac{v_{\text{est}}}{2}\right) \right] \quad (21)$$

where V_A denotes the covariance of Alice's quadrature modulation.

To optimise the rate of the secret key, it is imperative to minimise the phase noise emitted by the system. The system's phase noise is generated by two distinct components. The noise produced during the homodyne detection can be described as,

$$\chi_{\text{ohm}} = \frac{1 - \eta + v_{\text{ele}}}{\eta} \quad (22)$$

where η represents the efficiency and v_{ele} is the electronic noise of the photo-detector.

5. Evaluation of phase estimation using EKF

Local oscillator (LO) signal generated at the sender is transmitted through a single mode fibre for a distance of 20 km and at the receiver's end uses homodyne detection. The phase of the signal is then estimated from the received reference signals using an RNN-based EKF estimator.

5.1. Mean phase error

The mean phase error incurred in estimating the phase of the LO signal produced during a 20 km transmission via optical fibre is displayed in Table 1. For the purpose of cal-

T a b l e 1. Mean phase error where the phase is estimated with RNN-based phase estimation.

Initial phase	Line width [kHz]	Mean phase error
0.350892	100	0.000078
0.350892	50	0.000142
0.350892	10	0.000173
0.350892	2	0.000128
0.350892	0.1	0.000236

T a b l e 2. Mean phase error with respect to signal-to-noise ratio for line width of 100 kHz.

Signal-to-noise ratio [dB]	Mean phase error
6	0.000236
10	0.000632
14	0.000543

culating T , certain assumptions were made like attenuation coefficient has a value of $\alpha = 0.2$ dB/km, $V_A = 2.5$, $\beta = 90\%$ (0.9), the detector efficiency η is 0.6, and electronic noise $v_{ele} = 0.1$. Table 2 shows the mean phase error and SNR in dB for reference signal that is transmitted in 50 kHz line width.

The phase error in RNN-based EKF phase estimate is typically approximately 10^{-4} . The phase error covariance is around 10^{-3} .

5.2. Secret key rate analysis

The secret key rate analysis is conducted using the mean phase error obtained in Table 1. By assessing phase estimation using the mean phase error, secret key rate has been determined for the linewidth of the LO signal as 100 kHz.

In this case, the attenuation coefficient is $\alpha = 0.2$ dB/km and Fig. 4 shows the various key rates that can be achieved for different distances in km.

Assuming a value of φ_{drift} as 0.2, a secure key rate was achieved for approximately 40 km. Figure 5 illustrates the secret key rate for a couple of linewidths of the LO laser signal, assuming a value of φ_{drift} as 0.2.

When the value of φ_{drift} is minimised, it is possible to enhance the distance using locally generated LO signal based CV-QKD. Utilising lasers with a low line width and increased repetition rate can effectively reduce the value of φ_{drift} . The phase noise φ_{drift}

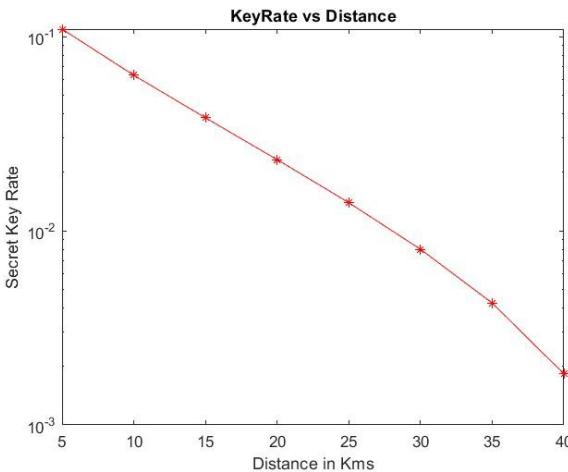


Fig. 4. Secret key rate *versus* distance.

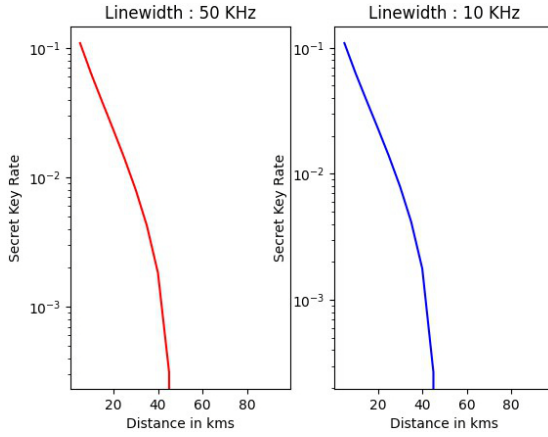


Fig. 5. Secret key rate *versus* distance with $\varphi_{\text{drift}} = 0.2$.

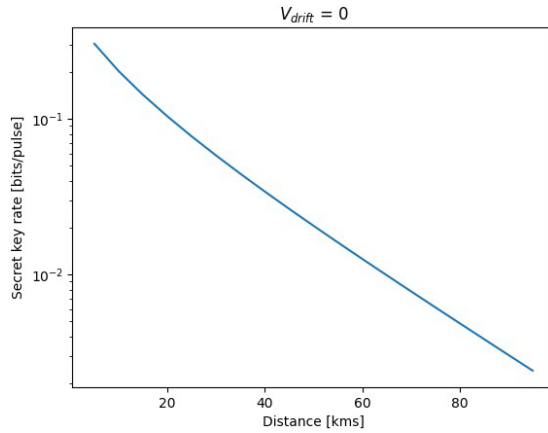


Fig. 6. Secret key rate with varying distances with $\varphi_{\text{drift}} = 0$ and line width of 100 kHz.

can be mitigated by employing an LLO (local local oscillator) technique that relies on a delay interferometer [12].

Figure 6 displays the secret key rate considering $\varphi_{\text{drift}} = 0$. It is evident that 80 km link range could be achieved with a favourable key rate with the assumption of $\varphi_{\text{drift}} = 0$ and line width of 100 kHz.

6. Conclusion

In this paper, we have proposed a novel phase estimation technique for continuous-variable quantum key distribution (CV-QKD) systems by integrating extended Kalman filter (EKF) with recurrent neural networks (RNNs). The key achievement of this approach is the significant improvement in phase recovery accuracy, reducing the phase

error to approximately 1×10^{-4} , which enables positive secure key rates for distances up to 40 km with different line widths.

This will overcome one of the major challenges in CV-QKD systems accurate phase estimation for locally generated LO signals. Our approach not only improves the precision of phase estimation but also enhances the practicality of deploying CV-QKD in real-world communication networks. By reducing phase estimation errors and improving the robustness of the key rate for longer distances, our work contributes to the ongoing development of secure quantum communication systems, especially in high-noise environments. Future research could extend this work by exploring its scalability in larger networks or integrating it with other forms of quantum cryptography for enhanced security.

References

- [1] SHOR P.W., *Algorithms for quantum computation: discrete logarithms and factoring*, [In:] *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994: 124–134. <https://doi.org/10.1109/SFCS.1994.365700>
- [2] BENNETT C.H., BRASSARD G., *Quantum cryptography: Public key distribution and coin tossing*, *Theoretical Computer Science* **560**, 2014: 7–11. <https://doi.org/10.1016/j.tcs.2014.05.025>
- [3] CHOI I., ZHOU Y.R., DYNES J.F., YUAN Z., KLAR A., SHARPE A., PLEWS A., LUCAMARINI M., RADIG C., NEUBERT J., GRIESSER H., EISELT M., CHUNNILALL C., LEPERT G., SINCLAIR A., ELBERS J.-P., LORD A., SHIELDS A., *Field trial of a quantum secured 10Gb/s DWDM transmission system over a single installed fiber*, *Optics Express* **22**(19), 2014: 23121–23128. <https://doi.org/10.1364/OE.22.023121>
- [4] RALPH T.C., *Security of continuous-variable quantum cryptography*, *Physical Review A* **62**(6), 2000: 062306. <https://doi.org/10.1103/physreva.62.062306>
- [5] REVACH G., SHLEZINGER N., NI X., ESCORIZA A.L., VAN SLOUN R.J.G., ELДАР Y.C., *KalmanNet: Neural network aided Kalman filtering for partially known dynamics*, *IEEE Transactions on Signal Processing* **70**, 2022: 1532–1547. <https://doi.org/10.1109/tsp.2022.3158588>
- [6] GROSSHANS F., GRANGIER P., *Continuous variable quantum cryptography using coherent states*, *Physical Review Letters* **88**(5) 2002: 057902. <https://doi.org/10.1103/physrevlett.88.057902>
- [7] HUANG P., HUANG J., ZHANG Z., ZENG G., *Quantum key distribution using basis encoding of Gaussian-modulated coherent states*, *Physical Review A* **97**, 2018: 042311. <https://doi.org/10.1103/PhysRevA.97.042311>
- [8] LAUDENBACH F., PACHER C., FUNG C.-H.F., POPPE A., PEEV M., SCHRENK B., HENTSCHEL M., WALTHER P., HÜBEL H., *Continuous-variable quantum key distribution with Gaussian modulation —The theory of practical implementations*, *Advanced Quantum Technologies* **1**(1), 2018: 1800011. <https://doi.org/10.1002/qute.201800011>
- [9] MA X.-C., SUN S.-H., JIANG M.-S., LIANG L.-M., *Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems*, *Physical Review A* **88**, 2013: 022339. <https://doi.org/10.1103/PhysRevA.88.022339>
- [10] SHOR P.W., PRESKILL J., *Simple proof of security of the BB84 quantum key distribution protocol*, *Physical Review Letters* **85**, 2000: 441–444. <https://doi.org/10.1103/PhysRevLett.85.441>
- [11] QI B., LOUGOVSKI P., POOSER R., GRICE W., BOBREK M., *Generating the local oscillator “locally” in continuous-variable quantum key distribution based on coherent detection*, *Physical Review X* **5**(4), 2015: 041009. <https://doi.org/10.1103/physrevx.5.041009>
- [12] ZHANG Y., CHEN Z., PIRANDOLA S., WANG X., ZHOU C., CHU B., ZHAO Y., XU B., YU S., GUO H., *Long-distance continuous-variable quantum key distribution over 202.81 km of fiber*, *Physical Review Letters* **125**, 2020: 010502. <https://doi.org/10.1103/PhysRevLett.125.010502>

- [13] IP E., KAHN J.M., *Feedforward carrier recovery for coherent optical communications*, Journal of Lightwave Technology **25**(9), 2007: 2675-2692. <https://doi.org/10.1109/JLT.2007.902118>
- [14] JHON Y.M., KI H.J., KIM S.H., *Clock recovery from 40 Gbps optical signal with optical phase-locked loop based on a terahertz optical asymmetric demultiplexer*, Optics Communications **220**(4-6), 2003: 315-319. [https://doi.org/10.1016/S0030-4018\(03\)01408-1](https://doi.org/10.1016/S0030-4018(03)01408-1)
- [15] TANG X., KUMAR R., REN S., WONFOR A., PENTY R.V., WHITE I.H., *Performance of continuous variable quantum key distribution system at different detector bandwidth*, Optics Communications **471**, 2020: 126034. <https://doi.org/10.1016/j.optcom.2020.126034>
- [16] GHALAIH M., OTTAVIANI C., KUMAR R., PIRANDOLA S., RAZAVI M., *Long-distance continuous-variable quantum key distribution with quantum scissors*, IEEE Journal of Selected Topics in Quantum Electronics **26**(3), 2020: 6400212. <https://doi.org/10.1109/JSTQE.2020.2964395>

*Received May 10, 2024
in revised form October 21, 2024*