# Savitzky-Golay-filter-based Phase Recovery for CV-QKD

**E. Llanos*, P. Adillon*, S. Sarmiento, J. Tabares, and S. Etcheverry**
*LuxQuanta Technologies S.L., Mediterranean Technology Park. Carrer d'Esteve Terradas, 1, Office 206,08860, Castelldefels (Barcelona), Spain*
*These authors contributed equally to this work*
*Author e-mail address: samael.sarmiento@luxquanta.com*

**Abstract:** A Savitzky-Golay filter (SGF) is employed to reduce the excess noise introduced by a pilot-tone-based phase recovery in CV-QKD. Results show an improvement of 29.2% in the secret key rate at 10.9 km when the SGF is used. © 2024 The Author(s)

## 1. Introduction

Quantum key distribution (QKD) allows two or more parties to share a secret key with information-theoretic security based on the fundamental laws of quantum physics [1, 2]. Continuous-variable QKD (CV-QKD), which encodes the information in the $X$- and $P$-quadrature of the electromagnetic field of light, has recently emerged as a cost-effective alternative to discrete-variable QKD (DV-QKD) for various reasons. Unlike DV-QKD, CV-QKD does not require single-photon detectors which need to be operated at very demanding temperature conditions. Instead, CV-QKD employs coherent detectors that can be implemented with off-the-shelf telecom components. Moreover, since coherent detectors can be integrated in an easier way [3-5], CV-QKD can potentially be mass-produced using photonic integrated circuits. This would push forward the adoption of this technology in heterogeneous network scenarios such as metro-access networks connecting 5G/6G-based radio stations, edge datacenters, businesses, and home users.

A coherent detector for CV-QKD requires a local oscillator (LO) laser to retrieve the signal containing the quantum information. To simplify and increase the security of practical CV-QKD systems, the LO must be independent from that used in the transmitter and generated locally at the receiver's side [6, 7]. Due to the phase mismatch between the two free-running lasers, optical phase-diversity detection followed by a carrier recovery procedure is required to shrink the system excess noise. Pilot-aided phase recovery techniques have been widely used to recover the phase of the transmitted quantum states [6, 8, 9]. In this technique, the phase information of a classical reference signal—usually multiplexed in time or frequency with the quantum signal—serves to estimate the phase error in the quantum symbols. Although this technique has been proved to be effective, the presence of a strong reference signal close to the quantum signal brings a remaining phase error after the carrier recovery procedure, that needs to be reduced. To solve this problem, Kalman filters have recently been proposed in [10-12]. In this paper, we experimentally study the use of a Savitzky-Golay filter (SGF) to reduce the noise introduced by a pilot tone for phase error estimation. Specifically, the measured phase of the pilot tone has been smoothened by the SGF before applying it to the quantum symbols. In our experimental setup, the pilot tone has been multiplexed in frequency with the quantum signal in a single sideband (SSB) configuration. Heterodyne detection that allows to measure the $X$- and $P$-quadrature simultaneously has been considered. For comparison, we have also implemented an Unscented Kalman filter (UKF) to estimate the phase of the quantum symbols. Results show an improvement of 29.2% in the secret key rate at 10.9 km when the SGF is used compared to the case without phase estimation filter, while when using the UKF the improvement is of 12.5%.

## 2. Savitzky-Golay and Unscented Kalman filtering

By using coherent heterodyne detection without frequency offset, the phase noise of a pilot tone can be efficiently estimated using $\theta = \tan^{-1}(P/X)$ for a high pilot tone power. However, due to low spectral separation, the high power of the pilot will increase the crosstalk over the quantum signal, reducing the signal-to-noise ratio (SNR) and, therefore, lessening the secret key rate. On the other hand, if we reduce the power of the pilot tone too much, $\theta$ will be strongly affected by the additive noise present in the system. To balance this power trade-off, the SGF and UKF can be applied to mitigate the crosstalk from the pilot tone to the quantum signal, while keeping high enough the pilot tone power to maximize its SNR at the detection. Note that these filters are featured to deal with non-linear measurements as $\theta$.

The SGF smooths a noisy signal by fitting a subset of data points to a polynomial function as $\theta'_j = \sum_{i=(1-m)/2}^{(m-1)/2} C_i \theta_{j+i}$ with $(\mathrm{m}+1)/2 \le j \le n - (\mathrm{m}-1)/2$, being $m$ the polynomial order, $n$ the window length, and $C_i$, the convolutional coefficients computed through least squares minimization [13]. The selection of $m$ and $n$ is subject to the inherent characteristics of the system. The UKF relies on Bayesian inference and an unscented transform to determine $\theta'_j$ from $\theta_j$ [10, 11]. It is a five-step process: calculate sigma points, propagate sigma points, predict $\theta_j$, calculate error, and update parameters [10]. The sigma points—mean and variance—are calculated assuming that the noise process is $\theta_j = \theta_{j-1} + q_j$ and $q \sim N(0, Q)$, with $Q = 2\pi \Delta v_t T_S$. Here, $\Delta v_t$ represents the combined linewidths

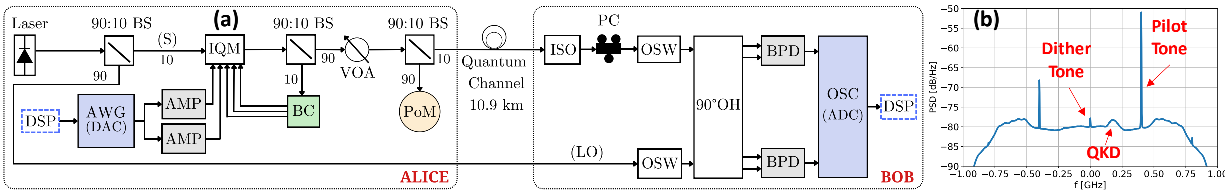


**Fig. 1.** (a) Experimental setup. (Acronyms) S: signal laser; LO: local oscillator laser; IQM: in-phase-and-quadrature modulator; BS: beam splitter; VOA: variable optical attenuator; AWG: arbitrary waveform generator; DAC: digital-to-analog converter; AMP: RF amplifier; BC: bias controller; ISO: optical isolator; PC: polarization controller; OSW: optical switch; 90º OH: 90-degree optical hybrid; BPD: balanced photodetector; OSC: oscilloscope; ADC: analog-to-digital converter; PoM: power meter; DSP: digital signal processing. (b) Power spectral density of the received signal.

of transmitter and LO lasers, and $T_S$ is the symbol period. The sigma points are then propagated through the measurement model $\theta$, and the new predicted mean and variance are obtained. Similarly, the mean and variance ($R$) of the measurement noise are calculated to estimate the error between the predicted state and the measured pilot. The variance $R$ can be estimated from the first-order term of the Taylor series expansion for $\theta$. Finally, the filter parameters are updated using a Metropolis-Hastings algorithm [10].

## 3. Experimental setup

Fig. 1(a) shows the experimental setup. At Alice, a 100 MBd Gaussian-modulated quantum signal was generated using offline digital signal processing (DSP). It included up-sampling to 2 GSa/s and pulse-shaping with a 0.65 roll-off-factor root-raised-cosine filter. Moreover, the quantum signal was frequency shifted to 200 MHz and frequency multiplexed with a pilot tone at 400 MHz for carrier phase estimation. The digital signal was uploaded to an arbitrary waveform generator with 14-bit nominal resolution and 2 GSa/s digital-to-analog converters. An in-phase-and-quadrature modulator (IQM) was used to modulate a laser beam at 1550 nm and with 10 kHz linewidth, yielding optical SSB modulation. An electronic variable optical attenuator (VOA) was used to adjust the modulation variance ($V_{mod}$), which was estimated using an optical power meter (PoM). Alice's output was connected to 10.9 km single-mode fiber with attenuation coefficient of 0.2 dB/km. At Bob's side, the state of polarization was manually adjusted with a polarization controller (PC). A 90° optical hybrid (90° OH) in conjunction with two 1 GHz bandwidth balanced photodetectors (BPDs) performed the heterodyne detection, although we remark that this receiver configuration might be simplified by using a 50:50 beam splitter (BS) and a BPD. For simplicity, the LO was derived from the transmitter laser using a 90:10 BS. Note that, since the quantum channel distance is longer than the laser coherence length, this configuration is equivalent to having two independent lasers. Two optical switches (OSW) were employed to perform electronic and shot noise calibration. Moreover, to avoid LO laser leakage towards the quantum channel, an optical isolator (ISO) was placed at Bob's input. The detected signals were digitized with a 10 GSa/s real-time oscilloscope (OSC), whose bandwidth was set to 800 MHz. Fig. 1(b) shows the power spectral density of the optical SSB modulation containing the quantum signal along with the aggregated pilot tone. Moreover, the small tone close to the baseband in Fig 1(b) corresponds to a dither signal used for automatically biasing the IQM. The DSP performed in Bob included the bandpass filtering for quantum and pilot signals respectively, phase recovery for the quantum symbols using the SGF and UKF, down-sampling, and pattern synchronization using cross-correlation. The QKD parameters were estimated according to $V_B = 0.5\eta T(V_{mod} + \varepsilon) + \nu_{elec} + 1$, where $V_B$ is the variance of the quadrature distribution measured at Bob's output, $\eta$ is the detection efficiency, $T$ is the channel transmittance, $\varepsilon$ is the excess noise at the channel input, and $\nu_{elec}$ is the electronic noise variance. The secret key rate ($SKR$) was estimated considering the asymptotic limit, trusted electronic noise at the receiver, and reverse reconciliation. Finally, the channel loss was assumed to be controlled by an eavesdropper.

## 4. Experimental results

Table 1 summarizes the parameters used for the QKD transmission over a 10.9 km fiber link. Fig. 2(a) and 2(b) show the $\varepsilon$ and $SKR$ for 28 consecutive measurements, each featuring a block size of $10^5$ coherent states. In particular, $\varepsilon$ and $SKR$ are shown when SGF- and UKF-based phase recovery are applied to the same set of measurements. Fig. 2(a) and 2(b) also show $\varepsilon$ and $SKR$ when no phase estimation filter is considered. As observed in Fig. 2(a), the SGF shows the lowest $\varepsilon$ values, leading to the highest $SKR$ values in Fig. 2(b). From Fig. 2(b), it can also be computed the average

**Table 1.** Transmission parameters summary

| Parameter | Value | Parameter | Value |
|---|---|---|---|
| Modulation variance, $V_{mod}$ | 4.58 SNU | Detection efficiency, $\eta$ | 0.21 |
| Electronic noise variance, $\upsilon_{elec}$ | 26 mSNU | Reconciliation efficiency, $\beta$ | 0.95 |
| Power ratio between pilot and quantum signal | 17 dB | Quantum symbol rate, $R_s$ | 100 MBd |

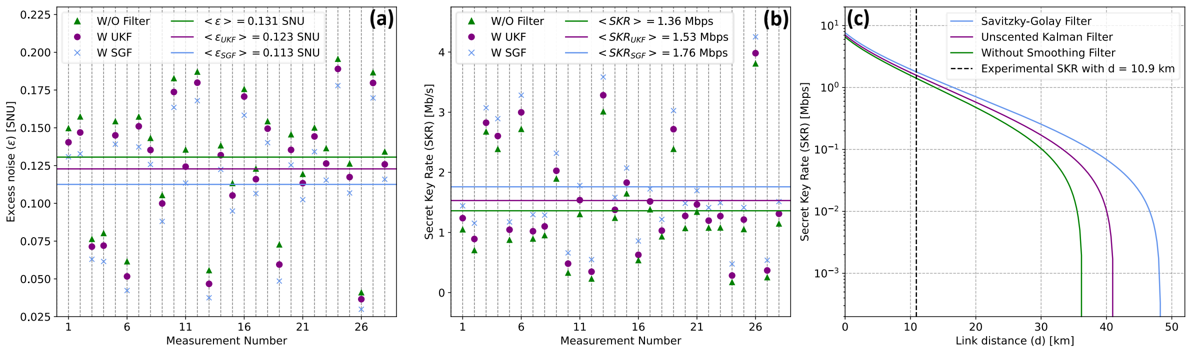


**Fig. 2.** Experimental result: (a) excess noise, and (b) secret key rate for 28 consecutive measurements, when employing different phase recovery procedures for a fiber link distance of 10.9 km. (c) Simulation of the $SKR$ as a function of link distance in the asymptotic regime, for the three phase recovery methods considered in this work.

$SKR$ improvement as a percentage relative to the case where no phase estimation filter is employed. In this way, the average $SKR$ improvement is of 29.2% when using SGF, while in the case of using UKF is of 12.5%. Compared to the UKF, the SGF shows average $SKR$ improvement of 15%. Finally, Fig. 2(c) depicts a simulation of $SKR$ as a function of the transmission distance. The results show that positive $SKR$ values could be obtained up to 48 km and 41 km for the SGF and UKF, respectively. When no phase estimation filters are used, the distance limit is 36 km.

## 5. Conclusion

We have proposed and experimentally assessed a SGF-based phase recovery method for CV-QKD that outperforms the state-of-the-art UKF-based method for a link distance of 10.9 km. The SGF showed an average excess noise reduction of 8% compared to the UKF, and 13.7% when no phase estimation filter is used. As a result, the $SKR$ has been improved 29.2% when using the SGF. Simulations have also been conducted to find potential fiber distance limits for positive $SKR$. When using the SGF, the distance limit was extended from 36 km to 48 km. We believe that after deeper system optimization, the proposed SGF-based phase recovery will allow us to reach fiber distance longer than 100 km. Finally, we attribute the better performance of SGF with respect to UKF, to stronger non-linear characteristics on the phase noise process $\theta$ when using lasers with significant linewidth. For lasers with lower linewidth, we expect the UKF and SGF to show similar performances.

**Funding.** This work was supported in part by the European Union through the Digital Europe Work Programme 2021-2022 [DIGITAL-2021-QCI-01-INDUSTRIAL/QuarterProject/101091588], Spanish Ministry Grants PTQ2021-012121 and PTQ2021-012123 [MCIN/AEI/10.13039/50110001103], as well as Pla de Doctorats Industrials del Departament de Recerca i Universitats de la Generalitat de Catalunya under Grant 2022-DI-0118.

## References

[1] S. Pirandola, U. L. Andersen, L. Banchi, et al., "Advances in quantum cryptography," Adv. Opt. Photon. 12, 1012-1236 (2020).
[2] F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. 92, 025002 (2020).
[3] G. Zhang, J. Y. Haw, H Cai, et al., "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," Nat. Photonics 13, 839–842 (2019).
[4] A. A. E. Hajomer, C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, S. Bastiaens, U. L. Andersen, X. Yin, and T. Gehring, "Continuous-Variable Quantum Key Distribution at 10 GBaud using an Integrated Photonic-Electronic Receiver," arXiv:2305.19642 (2023).
[5] C. Bruynsteen, M.Vanhoecke, J. Bauwelinck, and X.Yin, "Integrated balanced homodyne photonic–electronic detector for beyond 20 GHz shotnoise-limited measurements," Optica, vol. 8(9),1146 (2021).
[6] 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," Phys. Rev. X 5, 041009 (2015).
[7] D. Huang et al., "High-speed continuous-variable quantum key distribution without sending a local Oscillator," Optics Lett., 40(16), 3695 (2015).
[8] S. Kleis, et al., "Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals," Opt. Lett. 42, 1588 (2017).
[9] F. Laudenbach, et al., "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," Quantum, 3, 193 (2019).
[10] 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 Information, 7, 20 (2021).
[11] A. A. E. Hajomer, I. Derkach, N. Jain, H. M. Chin, U. L. Andersen, and T. Gehring, "Long-distance continuous-variable quantum key distribution over 100 km fiber with local local oscillator," arXiv:2305.08156v2 (2023).
[12] S. Kleis and C. G. Schaeffer, "Improving the Secret Key Rate of Coherent Quantum Key Distribution with Bayesian Inference," J. Lightw. Tech., 37(3), 722 (2019).
[13] A. Savitzky, A. Golay, and J. E. Marcel, "Smoothing and differentiation of data by simplified least squares procedures," Analytical Chemistry, 36, 1627 (1964).