Digital Filter Design For Experimental Continuous-Variable Quantum Key Distribution

Abdulmohsen Alsaui[1,2], Yazeed Alwehaibi[1,2], Anil Prabhakar[1], Deepa Venkitesh[1,*]

[1] *Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai 600036, India*
[2] *Research and Development Dept., Natl. Company of Telecomm. and Info. Security, Jeddah 23525, Saudi Arabia*
[*] *deepa@ee.iitm.ac.in*

Abstract: We explore the effect of digital filter design on enhancing the performance of an experimental CV-QKD system. The filtering procedure is anticipated to enable greater than 20 Mbaud/s at 20 km fiber length.

1. Introduction

With the anticipated advent of quantum computing, there is a possible security threat to communication networks that rely on the public key infrastructure. This has motivated the development of suitable countermeasures, such as post-quantum cryptography and quantum key distribution (QKD). QKD relies on the principles of quantum mechanics to establish symmetric keys between two mutually authenticated parties (Alice and Bob) to provide unconditional security. There are two main classes of QKD protocols - discrete variable (DV-QKD) and continuous variable (CV-QKD). DV-QKD protocols are more mature since they use discrete states to transmit the quantum key, making it easier to analyze. However, DV-QKD requires bulky and expensive photon counting modules often operated at low temperatures. On the other hand, CV-QKD systems are easier to implement with standard telecommunication technology and fit in a framework of probabilistic shaped and constellation-shaped modulations in traditional coherent communication. It is also convenient to use the commercially popular coherent transmitters and IQ receivers for CV-QKD implementation to blend it with classical coherent communication [1]. However, the caveat is that, the practical complexity is shifted to the analysis domain, thus requiring a more challenging security analysis [2] and sophisticated digital signal processing (DSP) algorithms [3].

CV-QKD is usually implemented in two flavors- by either carrying out discrete modulation or continuous modulation of low power light source. Specific signal processing algorithms need to be applied to correct the system impairments for both versions of CV-QKD [4]. One of the critical challenges to maintaining the operation in the quantum regime is that the shot noise of the system should dominate over all other sources of noise. This work presents the details of optimizing the post-measurement digital filtering parameters to ensure a positive secret key rate (SKR), when CV-QKD is implemented with commercial hardware. We believe the procedure explained here and the results presented in this work provide a crucial step toward the practical realization and maximization of key rates in an experimental setup.

2. Theoretical Framework

In essence, CV-QKD relies on communicating a coherent state with a particular fundamental uncertainty attributed to shot noise. The incoming states are sampled by analog to digital converters and represented as voltages. Measurement uncertainties, including the shot noise, are quantified by voltage variances. The security analysis of CV-QKD considers the relative value of the voltage variance from different origins with respect to the shot noise. This makes it convenient to normalize the measurements to the shot noise unit (SNU). Given a detector with quantum efficiency η_{det}, the measured variance per quadrature at the receiver, σ_{B}^2, is related to the transmitter's modulation variance σ_{A}^2 as [4]

$$\sigma_{\mathrm{B}}^2 = \frac{T_{\mathrm{c}} \cdot \eta_{\mathrm{det}}}{2} \cdot \sigma_{\mathrm{A}}^2 + N_0 + \xi_{\mathrm{det}} + \frac{T_{\mathrm{c}} \cdot \eta_{\mathrm{det}}}{2} \cdot \xi_{\mathrm{exc}} \qquad [\mathrm{V}^2], \tag{1}$$

where T_{c} is channel transmittance, N_0 is the shot noise variance, ξ_{det} is the detector's noise variance, and ξ_{exc} is the excess noise variance at the channel input corresponding to the optimal attack point of Eve. The factor of half appears due to the 3 dB coupler loss in the 90° optical hybrid. The secret key fraction,

$$\mathrm{SKF} = \beta I(A:B) - S(B:E), \tag{2}$$

where $\beta = 0.85$ is the reconciliation efficiency of the error correction procedure, $S(B:E)$ is the Holevo bound between Eve's quantum state and Bob's error-corrected classical data, and $I(A:B)$ is the Shannon mutual information between the classical data of Alice and Bob after error correction, and can be calculated as [5]

$$I(A:B) = \log_2\left(1 + \frac{\frac{T_c \cdot \eta_{\text{det}}}{2} \cdot \sigma_A^2}{1 + \xi_{\text{det}} + \frac{T_c \cdot \eta_{\text{det}}}{2} \cdot \xi_{\text{exc}}}\right). \tag{3}$$

In addition to the SKF, the SKR is directly correlated with the symbol frequency. Hence, we consider a product of the communication bandwidth and the SKF. Practical settings are simulated by reducing the achieved bandwidth by a roll-off factor of 1.4, mimicking a pulse shaping filter. We measure σ_B^2, σ_A^2, N_0, and ξ_{det} in an experiment and use Equation (1) to estimate the excess noise ξ_{exc}; from which we calculate and quantify the SKF and SKR.

3. System Description

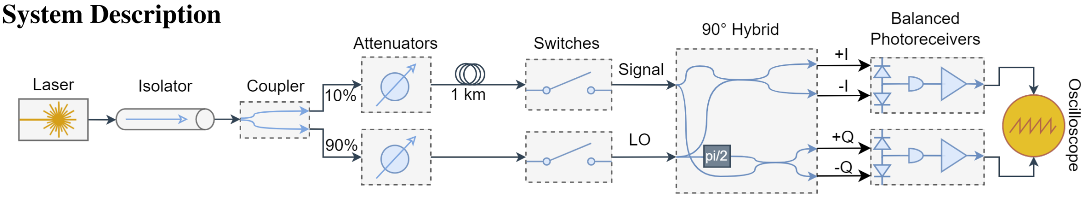

Fig. 1: Illustration of the utilized experimental setup.

A schematic of the experimental setup used to transmit a CVQKD signal is shown in Figure 1. Initially, a 90:10 optical coupler is utilized to split the light from a 1550 nm laser with 100 kHz linewidth. The optical isolator serves to prevent decoherence and damage to the laser. The higher power output is transmitted directly to the receiver to emulate a homodyne detection. In reality, the LO could be generated at Bob's side, with appropriate signal processing to correct the frequency offset between the transmitted laser and LO [6]. Alternatively, the LO can be transmitted in another fiber in the same bundle or another core if the transmission is through a multicore fiber. Nevertheless, the configuration discussed here suffices for the current scope of the work. The signal is transmitted through a one km standard single-mode fiber with 0.25 dB/km attenuation.

At the receiver, a 90° optical hybrid is used, followed by two 500 MHz bandwidth and AC-coupled balanced photoreceivers with a 45 dB common-mode rejection ratio (CMRR). The low 28 pW/$\sqrt{\text{Hz}}$ noise-equivalent power (NEP) makes this receiver potentially useful for operation in the shot-noise dominated regime, which is a requirement in CV-QKD. Finally, the analog output is sampled at 5 GSa/s with a 39 μV resolution enabled by the high-resolution 13-bit oscilloscope. Even though the photo receiver is ac coupled, there is a significant low- frequency pink noise due to the electronics, and this needs to be eliminated for achieving positive key rates. Hence, the sampled output is first passed through a band-pass filter (Bessel filter of order 10) to eliminate the low-frequency electronic noise.

4. Results and Discussion

Table 1

	LO Switch	Signal Switch	Measured Variance [V^2]
Stage I	OFF	OFF	ξ_{det}
Stage II	ON	OFF	$N_0 + \xi_{\text{det}}$
Stage III	ON	ON	$\frac{T_c \cdot \eta_{\text{det}}}{2} \cdot \sigma_A^2 + N_0 + \xi_{\text{det}} + \frac{T_c \cdot \eta_{\text{det}}}{2} \cdot \xi_{\text{exc}}$

The experimental stages are outlined in Table 1. At first, the detector noise (ξ_{det}) is measured by blocking both switches. Then, the LO switch is turned ON to estimate the shot noise variance (N_0). High clearance between the shot and detector noises is desired, quantified by the logarithmic difference of their powers. An optical attenuator was used to vary the LO power to maximize the clearance while ensuring the linear power dependence, corresponding to the quantum regime where the shot noise is dominant over other classical noises (e.g., thermal and laser intensity fluctuation). Figure 2a shows the measured noise variance as a function of LO power after filtering the low-frequency electronic noise, where 8 dB clearance is achieved at around 13 mW LO power. We use this optimized LO power for further experiments. The clearance is further improved by optimizing the band-pass filter used in the post-processing stage. Specifically, the high-frequency components exhibit a much smaller clearance, as shown in Figure 2b. To measure the excess noise (ξ_{exc}) for different modulation powers, an optical attenuator is used while keeping the Signal switch ON.

For the optimized LO power, we capture the variance at the output (σ_B^2) for different values of input signal power levels. We also vary the first stage band-pass filter's lower and upper cutoff frequencies. The SKR for each case is shown in the heat map in Figure 2c. In case of low signal powers, irrespective of the filter used, SKR is close to zero because the electronic noise dominates. At very high signal power levels, the system moves to classical operation. In the optimal range of optical powers, the filters' cutoff frequencies are found to significantly influence the maximal achievable key rates, shown in Figure 2c. Note that the filter bandwidths change with a change in the shot noise (optical power). Figure 2d shows the achievable transmission lengths and the corresponding SKR

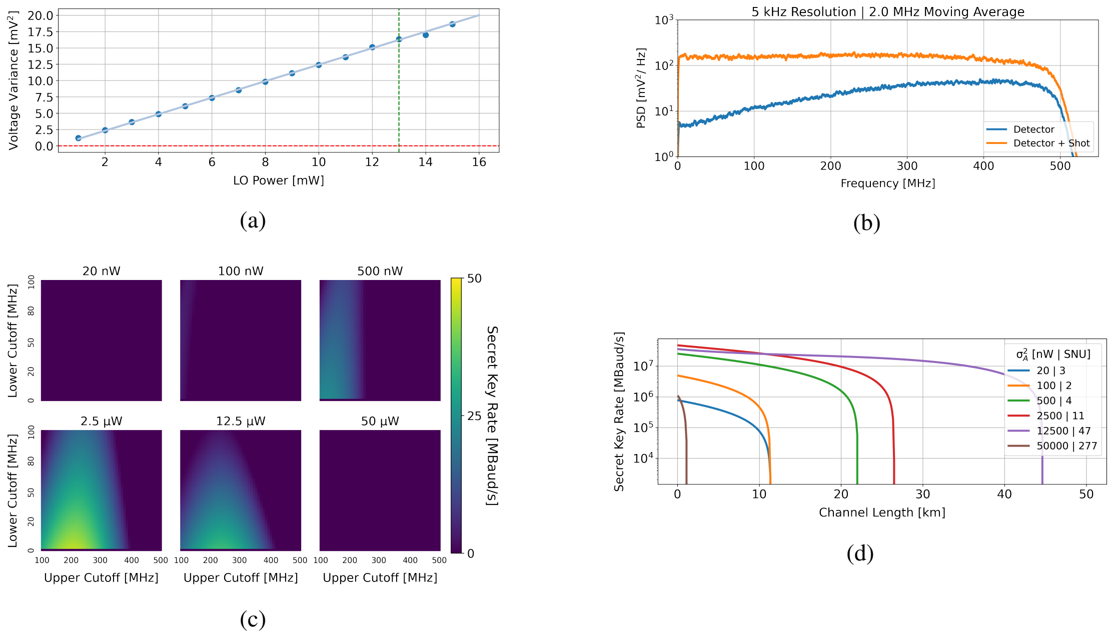

Fig. 2: (a) Measured voltage variance as the LO power is increased after blocking the electronic noise. Dashed red and green lines indicate the detector noise and optimal operation point, respectively. (b) Power spectral density contributions of the detector and Shot noises at the chosen 13 mW LO operation point where the electronic noise has been blocked. (c) Achieved results of varying the band-pass cutoff frequencies. (d) Extrapolated SKR for the optimum cutoff frequencies at each modulation power.

for the possible combination of the lower and upper cutoff frequencies indicated in the legend. At 20 km, around 20 MBaud/s is possible for $\sigma_A^2 = 12.5\ \mu$W. Note that the possible symbol rate for modulation gets limited as the bandwidth decreases. These plots highlight the importance of the correct choice of filter cutoff frequencies in the band-pass filter used as a first post-processing step to achieve a positive SKR in a practical experiment.

5. Conclusion

In this paper, we demonstrated a crucial post-processing step in processing CV-QKD signals to correct the hardware properties of the used components. We show that optimizing the band-pass filter's lower and upper cutoff frequencies at the front end is critical to achieving positive SKR. These results will be vital for achieving the optimal key rates in a practical CV-QKD implementation.

6. Acknowledgement

The authors were supported, in part, by a grant from Mphasis F1 Foundation to the Centre for Quantum Information, Communication, and Computing (CQuICC).

References

1. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.
2. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, no. 2, p. 621, 2012.
3. F. Roumestan, A. Ghazisaeidi, H. Mardoyan, J. Renaudier, E. Diamanti, and P. Grangier, "6 Mb/s secret key rate transmission over 13.5 km SMF using PCS-256QAM super-channel continuous variable quantum key distribution," in *Optical Fiber Communication Conference*, pp. Tu3I–4, Optica Publishing Group, 2022.
4. L. Trigo Vidarte, *Design and implementation of high-performance devices for continuous-variable quantum key distribution*. PhD thesis, Université Paris-Saclay (ComUE), 2019.
5. F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, no. 1, p. 1800011, 2018.
6. F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, F. Karinou, A. Poppe, M. Peev, and H. Hübel, "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," *Quantum*, vol. 3, p. 193, 2019.