Impact of Shot Noise Estimation on the Secret Key Rate of a CV-QKD System

Daniel Pereira[1,2], **Nuno A. Silva**[1], **Armando N. Pinto**[1,2]

[1]Instituto de Telecomunicações, University of Aveiro,
Campus Universitário de Santiago, 3810-193, Aveiro, Portugal

[2]Department of Electronics, Telecommunications and Informatics, University of Aveiro,
Campus Universitário de Santiago, 3810-193, Aveiro, Portugal

danielfpereira@ua.pt, nasilva@ua.pt, anp@ua.pt

Abstract. *In this work we present the impact of the uncertainty of the shot noise estimate on the performance of a continuous variables quantum key distribution system using a probabilistically shaped 128-APSK constellation. We demonstrate that the performance of the system is greatly degraded by the uncertainty of the shot noise estimate, with a total loss of security being possible.*

1. Introduction

The near-future emergence of a practical quantum computer is a threat to classical cryptography, with prime number based classical cryptography being particularly affected [Sergienko 2018]. Quantum Key Distribution (QKD) tackles the problem of the generation and distribution of symmetric cryptographic keys without assuming any computational limitations [Sergienko 2018]. Continuous Variables QKD (CV-QKD) is a subset of QKD that uses weak coherent states to transmit the keys, thus allowing for implementation with current modulation methods and telecom-based equipment [Grosshans and Grangier 2002]. The security of CV-QKD systems is evaluated with recourse to the communication channel's parameters, and since their value is evaluated in relation to the receiver's shot noise, a precise characterization of the receiver is mandatory for the implementation of secure CV-QKD systems [Leverrier et al. 2010].

QKD was first proposed in 1984, using the polarization of single photons as a coding basis [Bennett and Brassard 1984]. Nevertheless, the use of single photons demands the use of specialized equipment for single photon generation and detection [Ralph 1999]. As an alternative, coherent-state CV-QKD was proposed. The first implementations of CV-QKD were carried out by using a transmitted local oscillator (LO) setup [Ralph 1999]. However, that was found to be a security flaw, because an eavesdropper could manipulate the LO, thus hiding their tampering on the quantum signal itself [Qi et al. 2015]. In that scenario, local LO (LLO) techniques, aided by digital signal processing (DSP), are today the most common implementations of CV-QKD [Qi et al. 2015]. These LLO techniques usually employ a relatively high power pilot tone, with the pilot being multiplexed with the quantum signal, to allow for frequency and phase recovery between the different lasers at the transmitter and receiver [Kleis et al. 2017, Pereira et al. 2021]. Lately, LLO CV-QKD implementations using single-sideband modulation with heterodyne detection have been proposed, avoiding low-frequency noise [Kleis et al. 2017, Pereira et al. 2021].

In order to further maximize noise rejection, CV-QKD implementations using root-raised-cosine (RRC) signal modulation have been explored [Kleis et al. 2017]. The security bounds of CV-QKD systems were established in [Leverrier 2009] and updated in [Denys et al. 2021], where the security is evaluated via the channel parameters (transmission and excess noise). In order to estimate the channel parameters, the receiver's shot noise has to have been precisely estimated [Leverrier 2009]. The fact that the channel parameters are estimated from a finite number of samples, thus being subjected to an imperfect estimation, needs to be taken into account [Leverrier et al. 2010]. However, the work in [Leverrier et al. 2010] does not tackle the problem of the imperfect estimation of the shot noise of the receiver, a problem that, to best of our knowledge, has not been approached before.

In this paper, we explore the need for precise estimations of the receiver's shot noise, and study the compounding effect of the estimation imperfections on the security of a CV-QKD system, employing true heterodyne detection and RRC modulation. This work is divided into four sections. In Section 2, we describe the generic system under analysis. In Section 3, we show the impact of the uncertainty of the shot noise estimate on the performance of the system. We finalize this work with a summary of the major conclusions in Section 4.

2. System Description

A simplified block diagram of the experimental CV-QKD system assumed in this work is presented in Fig. 1. Alice starts by modulating the optical signal that she extracts from her

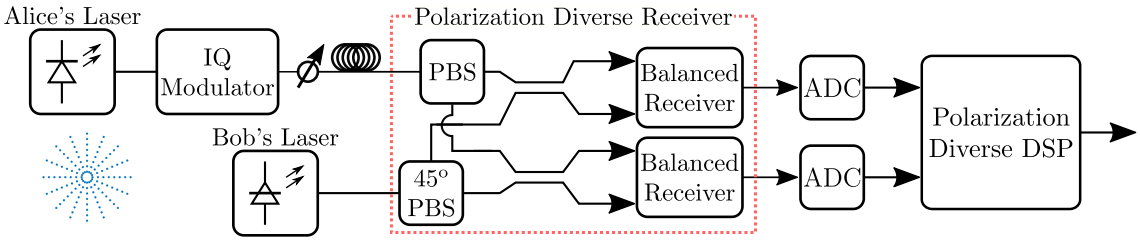

Figura 1. Block diagram of the CV-QKD system assumed in this work, including a representation of the employed constellation.

local coherent source, which consists of a Yenista OSICS Band C/AG TLS laser, tuned to 1550.004 nm. RRC modulation is chosen because of the possibility of using matched filtering at the receiver without inter-symbolic interference [Faruk and Savory 2017], thus allowing for optimum Gaussian white-noise minimization. The symbol rate was set at 153.6 MBd, with a 128-amplitude and-phase-shift keying (128-APSK) constellation, the security of which was established in [Almeida 2021]. An image of the employed constellation is included in Figure 1 as an inset. The RRC signal is then up-converted in the transmitter to an intermediate frequency, $f_Q = 153.6$ MHz. Furthermore, this signal is frequency multiplexed with a DC pilot tone, i.e. $f_P = 0$ Hz, which will be used for frequency and phase recovery at the receiver. This signal is fed into a Texas Instruments DAC39J84EVM digital to analog converter (DAC), which in turn drives a u2t Photonics 32 GHz IQ modulator coupled with a SHF807 RF amplifier. The signal is then sent through a single-mode fibre spool with a length of 40 km before arriving at the receiver.

The LLO consists of a Yenista OSICS Band C/AG TLS laser tuned to 1549.999 nm, in this situation the signals have a frequency shift of $f_S \approx 800$ MHz. The outputs of each coherent receiver, which consist of a pair of Thorlabs PDB480C-AC balanced optical receivers, are digitized by a Texas Instruments ADC32RF45EVM analog to digital converter (ADC) board, which is running at a sample rate of 2.4576 GS/s. The digitized signals are then fed into the digital signal processing (DSP) stage, where they are subjected to frequency, phase and clock recovery, steps which are aided by the pilot tone inserted at f_P, and matched filtering. For a more detailed description of the polarization diverse receiver, see [Pereira et al. 2021].

The shot noise estimation is made with recourse to a capture of the receiver output with the transmitter laser turned off. Due to the non-flatness of the spectral response of the receiver, the shot noise value is highly dependent on the spectral position of the signal. Due to this, as the difference between the frequencies of the two lasers fluctuates, to obtain a precise shot noise estimation, the same DSP that was previously applied to the quantum signal is applied to the shot noise capture obtained previously, being down converted, phase compensated and filtered before its variance is computed. Since we cannot measure the shot noise without also including the thermal noise, the latter was obtained first and its value was subtracted from the variance of the former, yielding an estimate for the shot noise, s^2_{shot}. After estimation of the receiver's shot noise, the signal output by Bob's DSP can be converted to Shot Noise Units (SNU), this is accomplished by dividing the ADC count output by $\sqrt{s^2_{\text{shot}}}$. Bob's and Alice's states, b and a respectively, are related by the normal linear model [Kleis et al. 2017]:

$$b = ta + z, \tag{1}$$

where a is assumed to be normalized such that $\mathrm{E}\{|a|^2\} = 1$, $t = \sqrt{\eta T 2 \langle n \rangle}$, where η is the quantum efficiency of Bob's detection system, T is the channel transmission and $\langle n \rangle$ is the average number of photons per symbol. z is the model's noise contribution, which follows a normal distribution with null mean and variance $\sigma^2 = 2 + 2\epsilon_{\text{thermal}} + \eta T \epsilon$, where ϵ is the excess channel noise and $\epsilon_{\text{thermal}}$ is the receiver's thermal noise. In (1), a is generated by Alice when she chooses the symbols to send, while b corresponds to Bob's output constellation after it has been converted to SNU. Moreover in (1), t and σ^2 can be estimated through [Kleis et al. 2017]

$$\tilde{t} = \mathrm{Re}\left\{ \frac{\sum_{i=1}^{N} a_i b_i^*}{N} \right\}, \qquad \tilde{\sigma}^2 = \frac{\sum_{i=1}^{N} |b_i - \tilde{t} a_i|^2}{N}, \tag{2}$$

the transmission and excess noise are then estimated through

$$\tilde{T} = \frac{\tilde{t}^2}{\eta 2 \langle n \rangle}, \qquad \tilde{\epsilon} = \frac{\tilde{\sigma}^2 - 2 - 2\epsilon_{\text{thermal}}}{\eta \tilde{T}}. \tag{3}$$

Protocol security is evaluated following the methodology presented in [Denys et al. 2021]. The achievable secret key rate is given by

$$K = \beta I_{\text{BA}} - \chi_{\text{BE}}, \tag{4}$$

where β is the reconciliation efficiency, I_{BA} is the mutual information between Bob and Alice, given by [Kleis et al. 2017]

$$I_{\text{BA}} = \log_2 \left(1 + \frac{2\tilde{T}\eta \langle n \rangle}{2 + \tilde{T}\eta\tilde{\epsilon} + 2\epsilon_{\text{thermal}}} \right). \tag{5}$$

In (4), χ_{BE} describes the Holevo bound that majors the amount of information that Eve can gain on Bob's recovered states, being obtained through equation (5) in [Almeida et al. 2021]. For the results presented in this work $\langle n \rangle$ was set at 1.91 photons per symbol, η was measured at 0.72 and $\epsilon_{\text{thermal}}$ was assumed to be 0.35 SNU.

3. Impact of receiver noise imperfect estimation

The formula for the $(1 - \alpha)$ confidence interval of a variance estimate, s^2, done with recourse to a sufficiently large number of samples, N, is given by the inequalities

$$s^2 \left(1 - z_{\alpha/2}\sqrt{\frac{2}{N}} \right) \leq \sigma^2 \leq s^2 \left(1 + z_{\alpha/2}\sqrt{\frac{2}{N}} \right), \tag{6}$$

where $z_{\alpha/2}$ is the $100(1 - \frac{\alpha}{2})$th percentile of a standard normal distribution. In order to ensure security with certain degree of confidence α, the worst case scenario value, i.e. the values that give the most advantage to Eve, for each value in the given confidence interval needs to be taken. For the case of the shot noise, this corresponds to obtaining the channel transmission estimation using the upper bound of the shot noise estimation to convert Bob's DSP output to SNU, and to obtaining the excess noise estimation using the lower bound. In doing this, we are splitting the linear model (1) in two

$$b_{\text{upper}} = t_{\text{upper}} a + z_{\text{upper}}, \tag{7}$$

$$b_{\text{lower}} = t_{\text{lower}} a + z_{\text{lower}}, \tag{8}$$

and computing $\tilde{T}$ from the upper one and $\tilde{\epsilon}$ from the lower one (while using the channel transmission estimation obtained previously). Furthermore, the uncertainty of the channel parameter estimations themselves need to be taken into account. The confidence interval for the variance of z_{i} will follow the same behavior as shown in (6), meanwhile the channel transmission estimate will have the confidence interval:

$$\tilde{t} - z_{\alpha/2}\sqrt{\frac{\tilde{\sigma^2}}{N}} \leq t \leq \tilde{t} + z_{\alpha/2}\sqrt{\frac{\tilde{\sigma^2}}{N}} \tag{9}$$

For the channel parameters, the worst case scenarios correspond to the lower bound of the channel transmission and the upper bound of the excess noise.

In Figure 2, we present results showing the worst case scenario secure key rate in function of confidence level of the estimates. In obtaining these results, the average values for the channel transmission and excess noise observed in our experimental system, 0.1418 and 0.0258 [SNU] respectively, were taken, and the worst case scenario estimates were computed assuming that three different numbers of symbols were used in their estimation. We take into account that, due to the symbol- and sampling-rate used in our

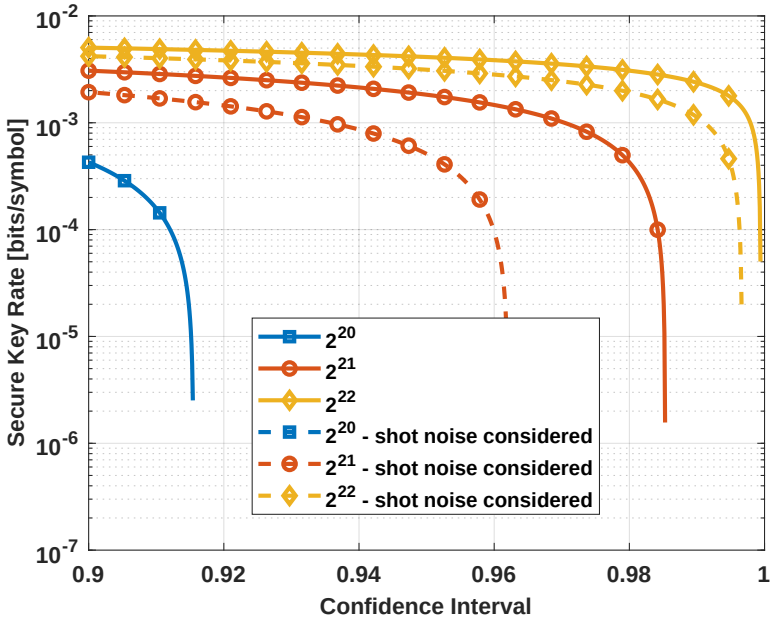

Figura 2. Worst case scenario secure key rate in function of confidence level. The different numbers of symbols used in their estimation are identified by color and by the different markers used, while the consideration or not of the shot noise uncertainty is identified by the use of full or dashed lines.

experimental setup, $8\times$ more samples are available for the estimation of the shot noise than are available for the estimation of the channel parameters. First, it was assumed that only the uncertainty of the channel parameters themselves was taken into account, results which are presented in full-line, then the uncertainty inherent to the shot noise estimate was included in the results, presented here in dash-line. We see that, when considering the uncertainty of the shot noise estimate, there is a clear degradation in the achievable secure key rate, with the situation using 2^{20} symbols in the estimation not being able to generate a key with even 90% confidence of its security. Meanwhile, for the results assuming 2^{21} and 2^{22} symbols used in the estimation process, we see a reduction of 2.4% and 0.3% in the maximum admissible confidence interval. These results, in conjunction with the smaller distance observed between the curves corresponding to a higher number of symbols used in the estimation, show that as more samples are used in the estimation of the shot noise, the less the impact of its uncertainty will be, due to the combined effect of the decrease of the width of the shot noise's and channel parameters' uncertainty intervals, which will cause the worst case scenario performances to approach the system's maximum performance. The optimal number of samples for use in each situation will depend on the observed channel parameters, as the lower the system's performance is, the less it will be able to withstand the impact on performance and thus more samples will be necessary, and on the desired confidence interval.

4. Conclusion

In this work, we show the importance of taking into account the uncertainty of the estimation of the shot noise while evaluating the security of a CV-QKD system. We present experimental results showing that the performance of the system is greatly degraded by the uncertainty of the shot noise estimate, something that can be mitigated by either using

more symbols in the estimation or by using a higher sampling-rate in the acquisition, which will result in a higher number of samples available for estimating the shot noise while maintaining the same number of symbols.

Acknowledgments: This work was supported in part by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework, under the PhD Grant SFRH/BD/139867/2018, projects UIDB/50025/2020, UIDP/50025/2020 , UIDB/50008/2020-UIDP/50008/2020 (action QuRUNNER and QUESTS).

Referências

Almeida, M. (2021). Practical security limits of continuous-variable quantum key distribution. Master's thesis, University of Aveiro.

Almeida, M., Pereira, D., Muga, N., Facão, M., Pinto, A. N., and Silva, N. A. (2021). Secret key rate of multi-ring m-apsk continuous variable quantum key distribution. *Optics Express*.

Bennett, C. H. and Brassard, G. (1984). Quantum cryptography: Public key distribution and con tos5. In *Proceedings of the International Conference on Computers, Systems and Signal Processing*.

Denys, A., Brown, P., and Leverrier, A. (2021). Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540.

Faruk, M. S. and Savory, S. J. (2017). Digital signal processing for coherent transceivers employing multilevel formats. *Journal of Lightwave Technology*, 35(5):1125–1141.

Grosshans, F. and Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):057902.

Kleis, S., Rueckmann, M., and Schaeffer, C. G. (2017). Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Optics letters*, 42(8):1588–1591.

Leverrier, A. (2009). *Theoretical study of continuous-variable quantum key distribution*. PhD thesis, Télécom ParisTech.

Leverrier, A., Grosshans, F., and Grangier, P. (2010). Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6):062343.

Pereira, D., Silva, N. A., and Pinto, A. N. (2021). A polarization diversity cv-qkd detection scheme for channels with strong polarization drift. In *2021 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 469–470. IEEE.

Qi, B., Lougovski, P., Pooser, R., Grice, W., and Bobrek, M. (2015). Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Physical Review X*, 5(4):041009.

Ralph, T. C. (1999). Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303.

Sergienko, A. V. (2018). *Quantum communications and cryptography*. CRC press, .