Receiver Noise Stability Calibration for CV-QKD

Sjoerd van der Heide, João Frazão, Aaron Albores-Mejía and Chigo Okonkwo
High-Capacity Optical Transmission Laboratory, Eindhoven University of Technology, the Netherlands
s.p.v.d.heide@tue.nl

Abstract: A method to investigate CV-QKD receiver stability is proposed and experimentally validated. Comparing <100 kHz linewidth local oscillator lasers, we show long-term noise power variance differs more than tenfold, highlighting the importance of receiver hardware calibration.

1. Introduction

Public key cryptography, a cornerstone of modern communication, is being threatened by advances in quantum computing. A promising alternative to achieve security against quantum computer attacks is symmetric encryption, whereby the secret key is established using quantum key distribution (QKD). Continuous-variable quantum key distribution (CV-QKD) systems promise a broad use-case since they can be implemented with commercial, cost-effective devices used within coherent optical telecommunications. CV-QKD systems require a reliable estimation of the excess noise power contained in the quantum signal to ensure security and maximize both the secret key rate and the transmission distance. The accuracy of the excess noise estimate is strongly affected by the calibration of the coherent receiver noise power. Due to the inherent time lag between the calibration and the quantum signal measurement, the receiver noise power calculated by the calibration and that included in the actual quantum signal may differ, e.g. due to changes in the receiver over time. This leads to systematic errors in the excess noise estimate compromising security or degrading performance. Therefore, detailed characterization of receiver noise power and its temporal stability is paramount. Many recent CV-QKD papers mention receiver noise calibration, but do not investigate the temporal stability in detail [1–4]. However, some recent investigations of CV-QKD receiver noise stability by block wise comparison of total receiver noise power variations have been reported [5, 6].

In this paper, we experimentally investigate the temporal receiver noise power stability of a CV-QKD receiver. We propose a different calibration method based on Allan variance [7] and show its equivalence to the technique introduced in [5, 6], whilst our technique achieves better statistical confidence, especially for large sample sizes. Furthermore, we compare the short- and long-term stability of two distinct local oscillator (LO) lasers and find that the long-term variance differs by more than an order of magnitude, indicating the importance of calibration of CV-QKD receiver hardware. More stable LO lasers may decrease calibration overhead for CV-QKD and thus increase the secret key rate (SKR).

2. Methods

Fig. 1a shows the experimental CV-QKD receiver setup. A conventional single-polarization coherent receiver is used with a <100 kHz linewidth external cavity laser (ECL) used as LO. No signal is inserted into the signal port of the 90 degree hybrid during calibration. The electrical outputs of the two balanced photo-diodes (BPDs) are digitized using a 2-channel 2 GS/s analog-to-digital converter (ADC). The digital signal processing (DSP) chain consists of frequency shifting the received signal by 300 MHz, resampling to 2 samples per symbol (SPS), finite

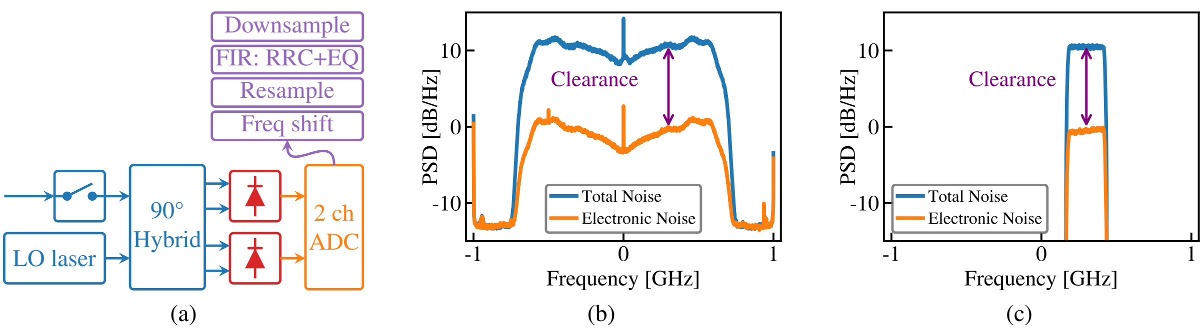
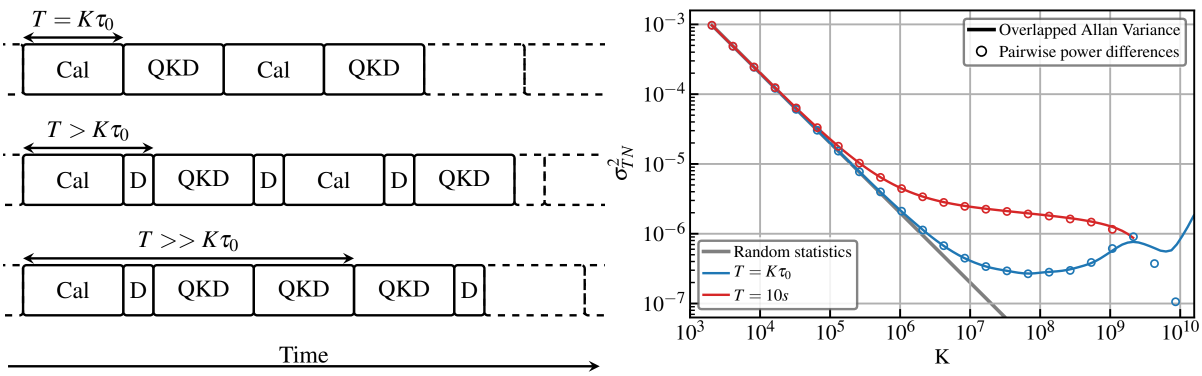


Figure 1: Experimental CV-QKD receiver (a) with measured spectra before (b) and after (c) DSP.

impulse response (FIR) filtering with a 250 MBaud root-raised-cosine (RRC) pulse shape with 10% rolloff and static equalization, and finally downsampling to 1 SPS. Fig. 1b and Fig. 1c show measured spectra of the total noise, i.e. LO shot noise plus electronic noise, and electronic noise before and after DSP, respectively. Note that the spectrum depicted in Fig. 1c is upshifted for illustrative purposes to show that the assumed quantum signal is modulated on a digital subcarrier to avoid disturbances around direct current (DC), similar to [8]. In the actual system, the signal depicted in Fig. 1c is downshifted to baseband. Note that the employed 90 degree hybrid is actually a dual-polarization hybrid, but only a single polarization is connected to the ADC since we only had access to 2 ports. This does not change any of the results and the setup can easily be extended to include both polarizations if more ADC ports are available.

Under the trusted noise assumption CV-QKD requires receiver calibration to estimate the electronic and shot noise power [9]. If the system drifts after calibration, the assumed shot noise may be either too high or too low. There is a security concern in assuming too high a shot noise power value, whilst a too low value leads to lower SKR. Therefore, this calibration needs to be performed regularly, depending on the temporal stability of the employed receiver hardware. Noise powers are estimated for a block size of K, which corresponds to the block size used in the CV-QKD algorithm. To minimize the finite-size effects, it is beneficial to keep increasing K to the largest value the system can handle, although this may not always be practical. Temporal stability is defined as the variance of the normalized total noise power difference between two of those blocks (σ^2_{TN}), as will be described in the next paragraph. Some implementations assume that the receiver alternates between QKD transmission and noise calibration, as depicted in the top row of Fig. 2a. In this case, the temporal stability T should be at least the duration of such a block, i.e. $T = K\tau_0$. In a realistic implementation, there is always a slight delay between the calibration and QKD transmission due to the switching time of the optical switch in front of the signal port of the 90 degree hybrid. Therefore, slightly longer temporal stability is required, i.e. $T > K\tau_0$. Finally, one can envision a system where a single calibration block can be followed by multiple QKD transmission blocks, decreasing calibration overhead, thus increasing net SKR, if receiver stability allows for such operation, i.e. $T >> K\tau_0$.

In [5] the temporal stability of the shot noise as the variance of normalized shot noise power estimates in subsequent blocks of size K is introduced. Ref [6] labels this ”pairwise power differences” and calculates it using the total noise, rather than the shot noise. When only LO is inserted, the output symbols of the DSP chain of Fig. 1a contain ”total noise” symbols. The normalized absolute value squared of these symbols are the normalized total noise power estimates y. First, these estimates y are averaged in blocks of size K: $P_{TN}[i] = \frac{1}{K}\sum_{k=0}^{K-1} y_k$. Then, the variance of difference between subsequent blocks is calculated: $\sigma^2_{TN} = \mathrm{var}(P_{TN}[i+1] - P_{TN}[i])$. It is noted in [5] that this technique is similar to the Allan deviation in clock-stability theory. Here, we argue it is not just similar, but actually identical to the Allan variance. In our proposed method, first, we take the cumulative sum of the per-symbol total noise power estimates: $x_n = \sum_{n=0}^{n} y_n$. Then, the overlapped Allan variance can be calculated using $\sigma^2_{TN} = \frac{1}{(N-2K)K^2}\sum_{n=0}^{N-2K-1}(x_{n+2K} - 2x_{n+K} + x_n)^2$ [7]. Note that both techniques assume $T = K\tau_0$. The pairwise power differences can be calculated for different T by comparing blocks further apart, for example $\sigma^2_{TN} = \mathrm{var}(P_{TN}[i+4] - P_{TN}[i])$ for $T = 4K\tau_0$. The Allan variance can be modified for longer T as follows: $\sigma^2_{TN} = \frac{1}{(N-K-L)K^2}\sum_{n=0}^{N-K-L-1}(x_{n+K+L} - x_{n+L} - x_{n+K} + x_n)^2$ with $L = \frac{T}{\tau_0}$.



(a) (b)

Figure 2: (a) Three scenarios with varying required calibration time delays T, depending on the calibration (Cal), quantum key distribution (QKD), and switching delay (D). (b) Allan variance as a function of calibration length K for two time delays T calculated using the overlapped Allan variance (solid lines) and pairwise power differences (open circles).

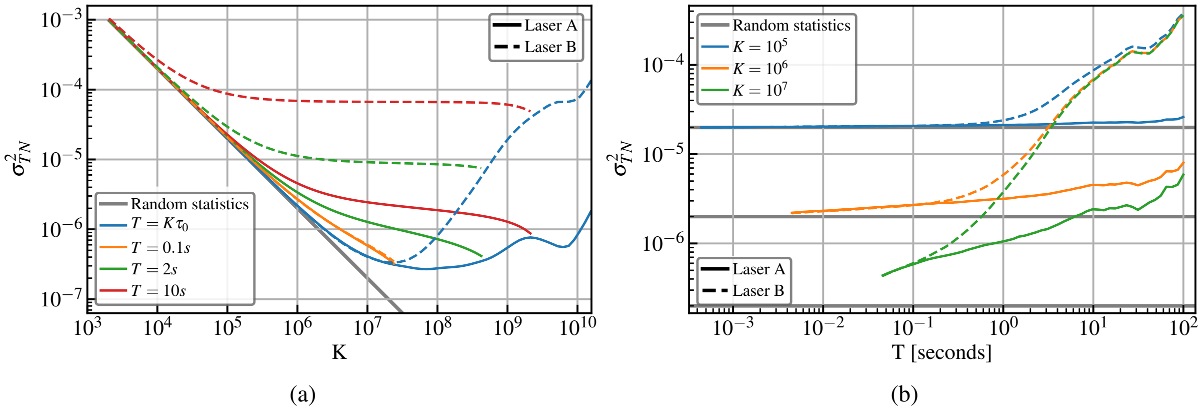


Figure 3: Allan variance of total noise (σ^2_{TN}) as a function of block size K (a) and as a function of time delay T (b)

3. Results

Fig. 2b shows the overlapped Allan variance and pairwise power differences for $T = K\tau_0$ and $T = 10\,\mathrm{s}$, for a 300 s long measurement. The results are identical, except for very high values of K where the number of blocks is low, leading to poor confidence. Note that the pairwise power difference method is identical to the Classic Allan variance, which is not recommended for general use due to poor confidence [7]. The overlapped Allan variance has better confidence, especially for large K. At some point the curves deviate from the statistical variance $\sigma^2_{TN} = 2/K$ [6], indicating that total noise power systematically deviates over time, for example due to instability in LO power or receiver electronics.

Fig. 3 further investigates this instability by comparing two different LO lasers. Laser A and B are both ECLs with linewidth $<100\,\mathrm{kHz}$. Laser A is a reserach grade laser, while laser B is a typical laser module used for telecommunication research. Fig. 3a shows both lasers perform virtually identical when $T = K\tau_0$ and $K < 10^7$. This indicates that short-term stability of both lasers is equally good. However, for larger T or K, laser A performs significantly better than laser B. For example, for $T = 10\,\mathrm{s}$ and $K = 10^8$, the Allan variance of laser A is over an order of magnitude better than laser B, meaning the instrument-grade laser has much better longer-term stability. Depending on the envisioned use case as explained in the previous section and in Fig. 2a, this may be a major advantage. Fig. 3b shows the Allan variance as a function of T for various K, highlighting that the Allan variance is dominated by laser instability for larger T for laser B.

4. Conclusion

The temporal stability of a CV-QKD receiver is experimentally investigated using different LO lasers, with the long-term stability of one laser shown to be more than an order of magnitude better than another. Since LO shot noise is a trusted noise source and miscalibration is a security concern, these results highlight the importance of detailed characterization of CV-QKD receiver hardware. Also, better hardware may lead to lower calibration overhead and thus higher SKR. Furthermore, a more accurate method to calculate temporal stability is proposed and compared to previous methods.

This work was supported by the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme.

References

1. N. Jain *et al.*, “Practical continuous-variable quantum key distribution with composable security,” Nat. communications **13** (2022). doi:10.1038/s41467-022-32161-y.
2. D. Milovančev *et al.*, “High Rate CV-QKD Secured Mobile WDM Fronthaul for Dense 5G Radio Networks,” in *Journal of Lightwave Technology,* vol. 39 (2021), pp. 3445–3457. doi:10.1109/JLT.2021.3068963.
3. T. A. Eriksson *et al.*, “Wavelength Division Multiplexing of 194 Continuous Variable Quantum Key Distribution Channels,” in *Journal of Lightwave Technology,* vol. 38 (2020), pp. 2214–2218. doi:10.1109/JLT.2020.2970179.
4. F. Laudenbach *et al.*, “Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator,” in *Quantum,* vol. 3 (2019). doi:10.22331/q-2019-10-07-193.
5. H. H. Brunner *et al.*, “Precise Noise Calibration for CV-QKD,” in *2020 22nd International Conference on Transparent Optical Networks (ICTON),* (2020), pp. 1–4. doi:10.1109/ICTON51198.2020.9203405.
6. M. Rueckmann and C. G. Schaeffer, “Calibration of Receiver Noise in CV-QKD Systems,” in *Photonic Networks; 21th ITG-Symposium,* (2020), pp. 1–4.
7. W. J. Riley, “NIST Special Publication 1065,” Handb. frequency stability analysis (2008).
8. F. Roumestan *et al.*, “Demonstration of Probabilistic Constellation Shaping for Continuous Variable Quantum Key Distribution,” in *Optical Fiber Communication Conference (OFC) 2021,* (2021), p. F4E.1. doi:10.1364/OFC.2021.F4E.1.
9. A. Leverrier, “Theoretical study of continuous-variable quantum key distribution,” Theses, Télécom ParisTech (2009).