Receiver Calibration and Quantum Random Number Generation for Continuous-variable Quantum Key Distribution

Receiver Calibration and Quantum Random Number Generation for Continuous-variable Quantum Key Distribution

Sjoerd van der Heide[1,*], Aaron Albores-Mejía[1], João Frazão[1], and Chigo Okonkwo[1]

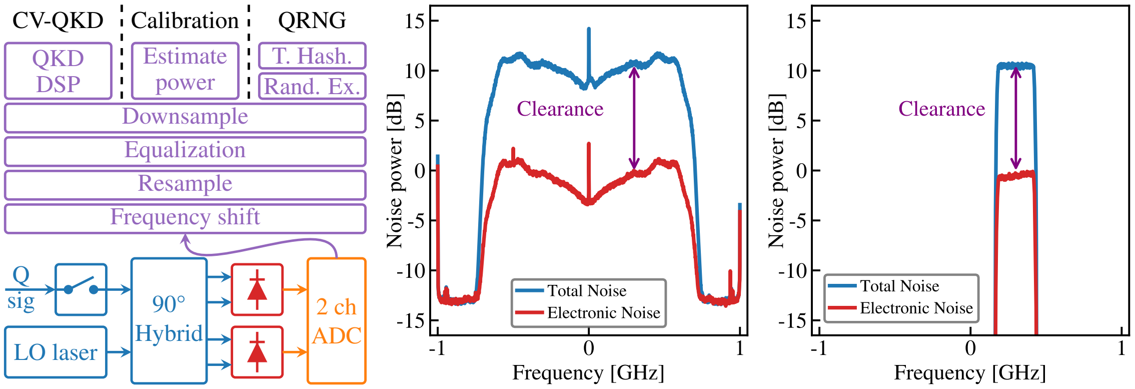
[1] High Capacity Optical Transmission Laboratory, Electro-Optical Communications Group,
Eindhoven University of Technology, the Netherlands [*] s.p.v.d.heide@tue.nl

The desire for secure communications and the advent of quantum computing has spurred innovation into key-distribution technologies that are secure against future quantum computers. Computationally secure solutions based on post-quantum algorithms and physically-secure solutions using either discrete-variable or continuous-variable quantum key distribution (CV-QKD) have been proposed. The attraction with CV-QKD systems in particular is the potential to leverage the vast knowledge base and access scaling benefits of photonic integration for conventional coherent optical communication for key distribution. CV-QKD requires detailed characterization of coherent receiver hardware, specifically noise generated by electronics and shot noise caused by the local oscillator (LO) laser. This work investigates the temporal stability of the receiver noise power which defines the amount of trusted noise in the quantum link used to compute the secret key rate (SKR). Depending on the noise power's stability, this characterization must be repeated often, typically in the order of seconds. Therefore, this work explores the possibility of using the shot noise measurement as a source of quantum random numbers, which is required by a CV-QKD transceiver. This work enables further integration of the CV-QKD hardware, removing the need for a separate quantum random number generator (QRNG).

Introduction

Current key-exchange mechanisms employed are based on public key cryptography and could be potentially compromised by future quantum computers. A proposed alternative secure method is QKD. In particular, CV-QKD is of interest because it utilizes hardware and digital signal processing (DSP) similar to conventional coherent optical communications. By leveraging knowledge and components from current classical fiber-optical communication systems, future CV-QKD systems may become highly-integrated and low-cost.

To ensure security, CV-QKD receivers require thorough characterization. Under the trusted noise assumption, they must be calibrated frequently[1], typically in the order of



(a) **(b)** **(c)**

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

seconds, but this can be traded off against raw SKR. It also depends on the temporal stability of receiver noise. Furthermore, a CV-QKD receiver requires secure random numbers, usually provided by a separate QRNG. Many QRNGs use vacuum-state fluctuations as a source of randomness by measuring shot noise using a balanced photo-diode (BPD)[2]–[4].

In this paper, a detailed characterization of CV-QKD receiver hardware is presented, including its noise spectrum and clearance. Furthermore, the temporal stability of noise sources is investigated, indicating that calibration needs to be performed every couple of seconds. A method is then introduced to generate quantum random numbers during the calibration procedure. Finally, the randomness of the QRNG is verified.

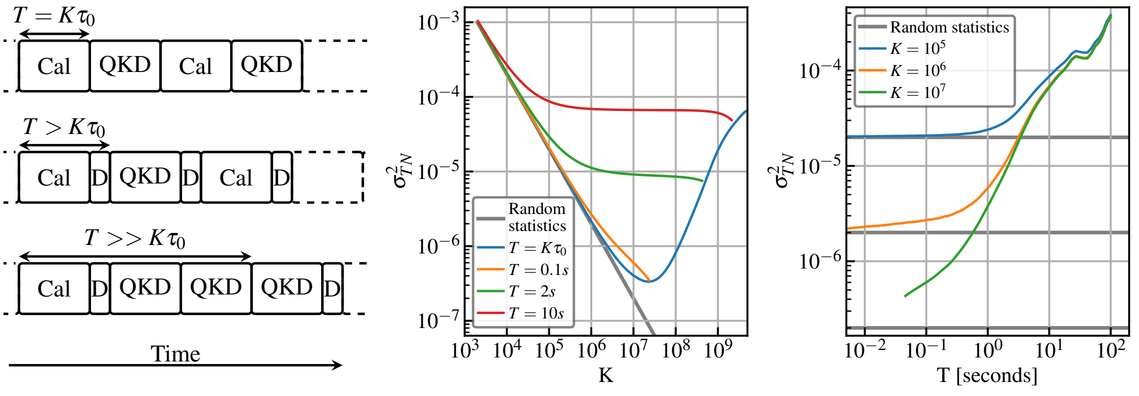
Experimental setup

Fig. 1a shows the experimental CV-QKD setup with a conventional single-polarization coherent receiver. A <100 kHz external cavity laser (ECL) is used as LO. During calibration, the quantum signal into the 90-degree hybrid is blocked by an optical switch. Two BPDs detect the optical signals, whose electrical signals are then digitized using a 2-channel 2 GS/s analog-to-digital converter (ADC). Note that the experimental setup can be easily extended to be polarization-diverse, but we did not have the extra ADC channels to do so. Furthermore, the employed 90-degree hybrid is a dual-polarization model, thus, half of the optical power is directed towards unused ports.

Fig. 1a also shows most signal processing steps are common for CV-QKD transmission, calibration, and QRNG. DSP starts by frequency shifting the digitized signal by 300 MHz. Then, the signal is resampled to 2 samples per symbol (SPS), filtered by a static equalizer to a 250 MBaud 10% rolloff root-raised-cosine (RRC) pulse shape, and downsampled to 1 SPS. Fig. 1b and Fig. 1c show the spectra of electronic noise and total noise, i.e. shot noise plus electronic noise, before and after DSP, respectively. Note that the spectrum of Fig. 1c is upshifted for illustrative purposes to show the assumed quantum signal is modulated on a digital subcarrier to avoid disturbances around direct current (DC), similar to[5].

Calibration

Fig. 2a outlines three scenarios for CV-QKD calibration with varying time delay T. The required temporal stability is at least equal to the QKD block length K multiplied by the symbol time τ_0, but may be longer if switching delay causes dead time D between



(a) (b) (c)

Fig. 2: (a) Three scenarios with varying required calibration time delays T, depending on the calibration (Cal), quantum key distribution (QKD), and switching delay (D). Allan variance of total noise (σ^2_{TN}) as a function of block size K (b) and as a function of time delay T (c).

QKD and calibration. Finally, a much greater temporal stability enables multiple QKD transmission blocks for each calibration block, greatly decreasing calibration overhead.

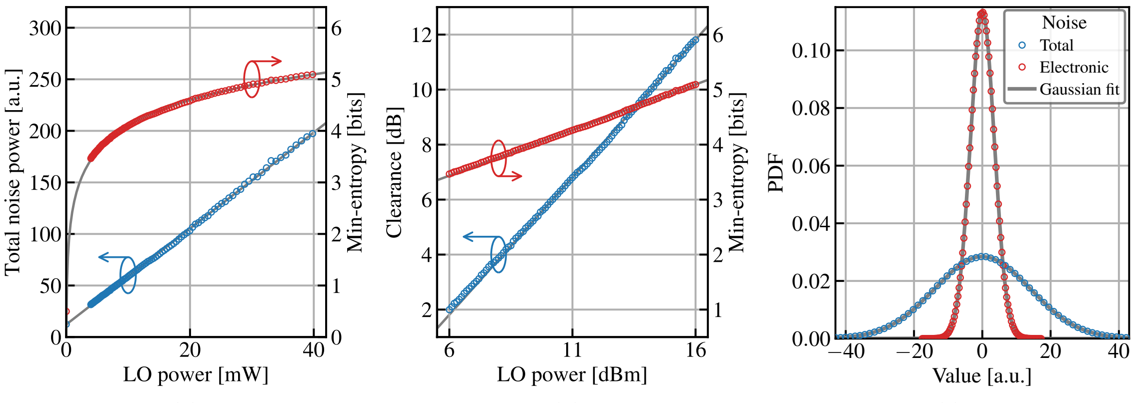
Temporal receiver stability T is investigated using the overlapped Allan variance method[6]. After DSP as explained in the previous section, the power of the extracted noise symbols is calculated (y_n) and the cumulative sum is taken using $x_n = \sum_{i=0}^{n} y_i$. Then, the Allan variance is given by $\sigma_{TN}^2 = \frac{1}{(N-K-L)K^2} \sum_{n=0}^{N-K-L-1} (x_{n+K+L} - x_{n+L} - x_{n+K} + x_n)^2$ with $L = \frac{T}{\tau_0}$. Fig. 2b and Fig. 2c show the Allan variance of the total noise versus QKD block length K and time delay T, indicating that for the tested hardware, calibration needs to be performed at least every 2 seconds if $K = 10^7$ and $\sigma_{TN} = 10^{-5}$ are assumed. Note that underestimating the Allan variance σ_{TN}^2 is a security concern and overestimation lowers SKRs. Therefore, SKR and time between calibrations can be traded off.

Fig. 3a demonstrates a linear relation between LO power and observed total noise power after DSP. This one-time characterization is required to ensure the BPDs are adequately balanced. Unbalanced operation is a security concern and would violate this linearity. Fig. 3b shows the clearance, the ratio between shot and electronic noise, achieving 12 dB clearance at 16 dBm LO power into the 90-degree hybrid.

Quantum random number generation

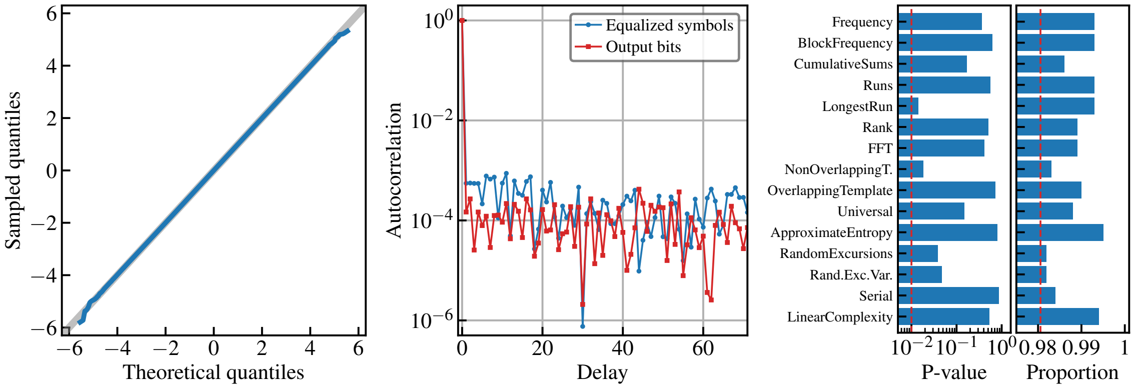
A QRNG based on vacuum-state fluctuations is implemented using the same noise symbols as used for calibration. The min-entropy per symbol can be calculated using $H_{min} = \text{erf}\left(\frac{\delta}{2\sqrt{2}\sigma_q}\right)$, with σ_q the standard deviation of the shot noise and δ the sampling resolution[4]. Figs. 3a and 3b show that more than 5 random bits can be extracted per 1D-symbol at highest LO power. Extraction requires re-binning with identical sampling resolution as initially used by the ADC, here performed using 8 bits. Note that this equation for min-entropy only holds if the noisy symbols are Gaussian distributed and the sampling range is sufficiently large to capture the tails. Fig. 3c shows excellent agreement between a Gaussian fit and the observed probabilities and Gaussianity is further confirmed by the quantile-quantile plot of Fig. 4a.

After re-binning, Toeplitz hashing with 2^{19} input bits and 2^{18} output is performed to remove any correlations left after equalization or introduced by binning. This reduces the number of extracted bits from 8 to 4 per 1D-symbol, leaving a large safety margin to the



(a) (b) (c)

Fig. 3: (a) Total noise power and min-entropy versus LO power. (b) Clearance and min-entropy versus LO power. (c) Empirical and fitted probability density function (PDF) for the total and electronic noise.



(a) **(b)** **(c)**

Fig. 4: (a) Quantile-quantile plot showing Gaussianity of normalized equalized symbols. (b) Autocorrelation of equalized symbols and QRNG output bits. (c) NIST-STS randomness test results.

min-entropy. Fig. 4b confirms that correlations are removed by the equalizer and Toeplitz hashing. To reduce computational complexity, Toeplitz hashing is performed using fast Fourier transforms (FFTs) instead of matrix multiplications[7].

Finally, Fig. 4c shows the result of the National Insitute of Standards and Technology: Statistical Test Suite (NIST-STS) randomness test[8]–[10] for 1000 sequences of 1 Mbit, indicating the generated bits are statistically random. Note that some sub-tests occasionally fail, as is to be expected, even for truly random numbers[11].

Conclusion

A CV-QKD receiver capable of performing calibration and quantum random number generation simultaneously is presented. Furthermore, a detailed analysis into its noise characteristics and the temporal stability thereof is given, indicating calibration needs to be performed every couple of seconds. Finally, the QRNG implementation is described and its successful operation is verified.

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

References

[1] A. Leverrier, "Theoretical study of continuous-variable quantum key distribution", Theses, Télécom ParisTech, Nov. 2009.

[2] T. Gehring *et al.*, "Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information", *Nature Communications*, 2021. DOI: `10.1038/s41467-020-20813-w`.

[3] A. Kordts *et al.*, "Security verification for vacuum fluctuation based quantum random number generator", *CLEO*, 2018. DOI: `10.1364/CLEO_AT.2018.JTh2A.10`.

[4] J. Y. Haw *et al.*, "Maximization of Extractable Randomness in a Quantum Random-Number Generator", *Phys. Rev. Applied*, 2015. DOI: `10.1103/PhysRevApplied.3.054004`.

[5] F. Roumestan *et al.*, "Demonstration of Probabilistic Constellation Shaping for Continuous Variable Quantum Key Distribution", *OFC*, 2021. DOI: `10.1364/OFC.2021.F4E.1`.

[6] W. J. Riley, "NIST Special Publication 1065", *Handbook of frequency stability analysis*, 2008.

[7] M. Hayashi *et al.*, "More Efficient Privacy Amplification With Less Random Seeds via Dual Universal Hash Function", *IEEE Trans. Inf. Theory*, 2016. DOI: `10.1109/TIT.2016.2526018`.

[8] L. Bassham *et al.*, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, 2010.

[9] M. Sýs *et al.*, *Faster randomness testing*, `https://randomness-tests.fi.muni.cz/`.

[10] M. Sýs *et al.*, "Algorithm 970: Optimizing the NIST Statistical Test Suite and the Berlekamp-Massey Algorithm", *ACM Trans. Math. Softw.*, vol. 43, 2016. DOI: `10.1145/2988228`.

[11] K. Marton *et al.*, "On the interpretation of results from the NIST statistical test suite", *Science and Technology*, vol. 18, no. 1, pp. 18–32, 2015.