# Practical Challenges in Classical Coherent Receivers for Detecting High Speed CV-QKD Signals

Xinke Tang[1], Rameez Asif[1], Rupesh Kumar[1,2], Adrian Wonfor[1], Seb Savory[1], Ian White[1], and Richard Penty[1]

[1]Centre for Photonic Systems, Electrical Engineering Division, Department of Engineering, University of Cambridge, UK
[2]Quantum Communication Hub, University of York, UK

**Abstract**

Quantum key distribution (QKD) is a method to disseminate encryption codes between two distant nodes, i.e. Alice and Bob, via photons. The unconditional security of QKD is based on the intrinsic laws of quantum mechanics [1, 2]. The quest for long distance high-speed encrypted transmission has led researchers to delve into new methods to improve security and performance [3]. The all-important factors in restricted implementation of classical QKD protocols in field deployable networks is the inadequacy of efficient single photon sources and detectors [4]. An alternative approach that offers compatibility with off-the-shelf telecommunication technologies, is continuous-variable quantum key distribution (CV-QKD) protocol. In this technique the information is encoded on the quadrature of the coherent state of the light pulse that constitute the shared randomness [5]. It is envisioned that this approach will become a viable candidate for commercial large-scale secure quantum access networks because of the assurance of attaining high secure key distribution with modest technological resources.

However, the performance of CV-QKD signals is highly dependent on the noise characteristics of the classical coherent receivers. Moreover, the repetition rate of CV-QKD is mainly limited by the bandwidth of balanced homodyne detector, the speed of data acquisition modules, and the performance of reconciliation scheme [6]. In this work, we have analytically investigated the electronic noise induced by Bob's classical coherent receiver and it's impact on achievable secure key rates. We have developed a realistic analytical model considering all noise sources associated with the coherent receiver as well as excess noise and reconciliation efficiency. Furthermore, noise equivalent power (NEP) and gain from the transimpedance amplifiers (TIA) as well as noise contribution from analogue-to-digital converter (ADC) are investigated. From the analysis, it is concluded that 10Mbit/s secure key rates can be achieved over 20km transmission distance by using 1GHz receiver at 300MHz repetition rate. Detailed results will be presented in poster.

# References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, pp. 145195, March 2002.

[2] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Phot., vol. 8, pp. 595604, July 2014.

[3] B. Frolich, J. Dynes, M. Lucamarini, A. Sharpe, S. Tam, Z. Yuan, and A. Shields, "Quantum secured gigabit optical access networks," Sci. Rep., vol. 5, pp. 18 121(1)18 121(7), December 2015.

[4] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," Phys. Rev. A, vol. 76, p. 052323, November 2007.

[5] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Phot., vol. 7, pp. 378381, April 2013.

[6] Y. M. Chi, B. Qi, W. Zhu, L. Qian, H. K. Lo, S. H. Youn, A. I. Lvovsky and L. Tian, "A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution," NEW J. PHYS., vol. 13, pp. 13 (013003), January 2011.