Proof-of-principle study of self-coherent continuous-variable quantum key distribution

Luis Trigo Vidarte, Adrien Marie, Romain Alléaume, and Eleni Diamanti

Laboratoire Traitement et Communication de l'Information, CNRS, Télécom ParisTech, Université Paris-Saclay, Paris 75103, France,
{luis.trigovidarte, adrien.marie, romain.alleaume, eleni.diamanti}@telecom-paristech.fr

Continuous-variable quantum key distribution systems allow the generation of secret keys between two parties (Alice and Bob) as follows: Alice randomly generates states following a certain distribution (for instance, Gaussian in GMCS [1]) and transmits them through an insecure quantum channel; and Bob recomposes the original state making the signal transmitted by Alice interfere with a powerful, classical signal - the local oscillator (LO). In order to have a good reconstruction of the original state, the LO at Bob's must have the same frequency and phase as the signal generated by Alice. This is difficult in practice, since two lasers do not typically have exactly the same characteristics and the channel can affect the original signal.

One option to obtain a signal of identical frequency and phase at Bob's is to send the LO along the insecure quantum channel. This has been the standard solution in implementations, as in [2] where Alice multiplexes the LO in time and polarization to be sent along with the quantum signal, operations that are inverted at Bob's side to obtain a good interference between LO and signal. This assures a good match in terms of frequency and phase at Bob's side, but also opens the way to side-channel attacks [3,4]. The LO also needs to be sufficiently powerful at Bob's side to perform the required coherent detection, hence limiting the communication range of the system, while its direct generation at Bob's is more sensible in terms of energy efficiency.

Several proposals have been introduced recently in order to allow the generation of the LO locally at Bob's side. In particular, Refs. [5] and [6] propose the transmission of reference pulses between the quantum signal in order to estimate the phase difference between Alice and Bob (due to laser imperfections and the channel). The reference is used only for estimation and does not contribute to the secret key rate. The optical power transmitted in the reference pulse can be higher than the quantum signal, but lower than the LO. These Refs. as well as [7] also provided proof-of-principle demonstrations of such proposals.

Although the aforementioned methods can deal with certain levels of phase noise, they typically require the use of very reliable lasers (in terms of high stability and narrow linewidth in particular) at both Alice's and Bob's sites. Ref. [8] has recently performed a theoretical analysis that studies the performance of these methods depending on parameters such as the laser linewidth. As narrow linewidth lasers remain a laboratory tool, it is interesting to extend the phase estimation methods to standard lasers. One possibility for that, as proposed in [8], is to avoid the phase mismatch between two consecutive pulses obtaining them from the same original laser pulse using a Franson interferometer (self-coherent delay line scheme, or *LLO-delayline* in [8]). Doing this at both sides ideally guarantees that a consecutive reference-signal pair will have the the same phase, independently of the linewidth of the laser. So if the phase difference can be correctly estimated from the reference pulse it can be applied to the signal in order to recover the original state.

The purpose of this work is to assess the viability of this scheme. The optical part of the experiment is indicated in figure 1. Alice splits the pulses of her laser (generated with a frequency f) to obtain two branches; one serves as a reference for the phase estimation at Bob's side and the other carries the quantum signal. The reference-signal pulse pair then share the same frequency and phase, since they come from the same original pulse, even if they are now separated in time by $1/(2f)$. At Bob's side the LO is generated locally and goes through the same Franson interferometry procedure. Both pairs of pulses have to be matched at Bob's side via a delay line that serves as a synchronization mechanism. Heterodyne detection is then performed using a 90° hybrid and two homodyne detectors. This allows the estimation of the phase from the reference pulses, difference that is then applied to the signal. Using this setup, we test the viability of the scheme in particular as a function of the linewidths of the lasers involved, mainly with respect to their capability to recover the phase of the original state, but also to their tolerance to possible differences in the optical delay lines.

References

1. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan 2002.

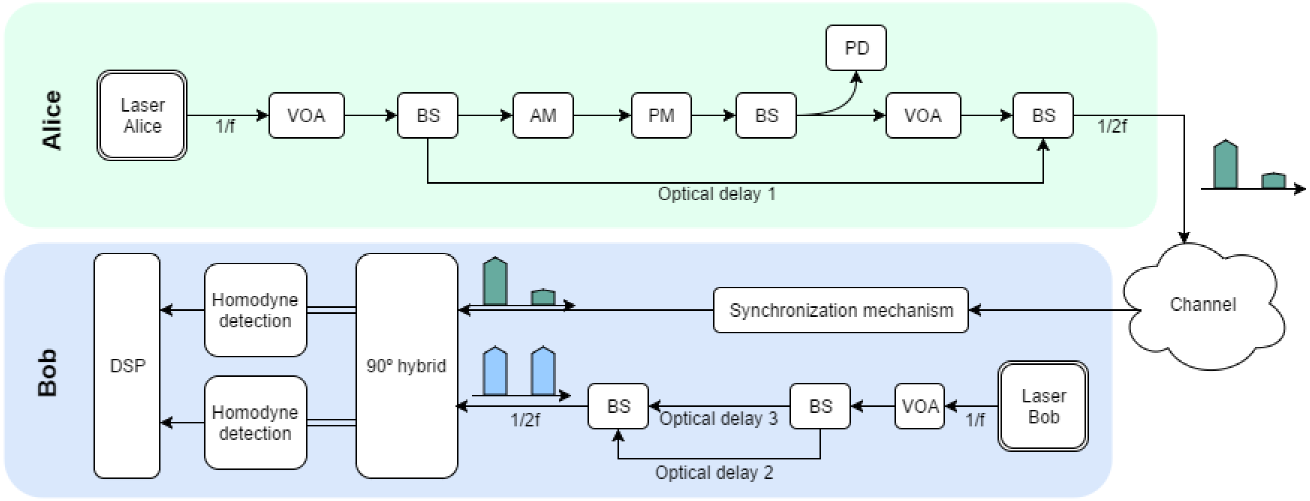

Fig. 1. Scheme of the experiment. The optical delays have to be matched so that the splitting of the pulses is equivalent in Alice and Bob. The delay between both entities has to be controlled by some synchronization mechanism, like a variable delay line. The experiment relies on a 90° hybrid to perform the heterodyne detection. VOA: Variable Optical Attenuator; BS: Beam Splitter; AM: Amplitude Modulator; PM: Phase Modulator; PD: Photodiode; DSP: Digital Signal Processing.

2. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of continuous-variable quantum key distribution over 80 km of standard telecom fiber," in *CLEO: 2013*, p. QTu2C.4, Optical Society of America, 2013.
3. X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems," *Phys. Rev. A*, vol. 88, p. 022339, Aug 2013.
4. P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 87, p. 062313, Jun 2013.
5. B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," *Phys. Rev. X*, vol. 5, p. 041009, Oct 2015.
6. D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol," *Phys. Rev. X*, vol. 5, p. 041010, Oct 2015.
7. D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," *Opt. Lett.*, vol. 40, pp. 3695–3698, Aug 2015.
8. A. Marie and R. Alléaume, "Self-referenced continuous-variable quantum key distribution protocol," *arXiv:1605.03642*, May 2016.