Theoretical analysis and proof-of-principle demonstration of self-referenced continuous-variable quantum key distribution

Constantin Brif,[1] Daniel B. S. Soh,[1,2] Patrick J. Coles,[3] Norbert Lütkenhaus,[3]
Ryan M. Camacho,[4] Junji Urayama,[4] and Mohan Sarovar[1]

[1]*Sandia National Laboratories, Livermore, CA 94550, USA*
[2]*Edward L. Ginzton Laboratory, Stanford University, Stanford, CA 94305, USA*
[3]*Institute of Quantum Computing, University of Waterloo, N2L 3G1 Waterloo, Canada*
[4]*Sandia National Laboratories, Albuquerque, NM 87123, USA*

Quantum key distribution (QKD), which enables the generation of secure shared randomness between two distant parties (Alice and Bob), is the most advanced quantum technology to date. Discrete-variable QKD (DV-QKD) is the term for well-established protocols that involve generation and detection of extremely weak pulses of light (ideally, single photons). Unfortunately, significant technological challenges still remain in generation and detection of single photons, although important advances have been made over past three decades. Protocols for an alternative approach, continuous-variable QKD (CV-QKD), were developed more recently. CV-QKD utilizes conjugate continuous degrees of freedom (field quadratures) of a light pulse prepared in a Gaussian (coherent or squeezed) state to transmit the signals that constitute the shared randomness. At the receiver, the quadratures are measured using shot-noise limited balanced homodyne or heterodyne detectors, which have the advantage of not requiring single photon detection and operating at extremely high detection rates (on the order of GHz). In particular, the coherent-state CV-QKD protocol has received much attention because of its promise of achieving information-theoretically secure key distribution with modest technological resources. A particular reason for the appeal is the expectation that the integrated photonics implementation of CV-QKD will be easier than that of DV-QKD, and such implementations are critical for the next phase of QKD development that is focused on practicality and wide-spread utilization.

Conventional CV-QKD protocols require transmission of a high-intensity coherent pulse, called local oscillator (LO), between Alice and Bob. The shared LO is needed to ensure that Alice and Bob use the same reference frame for signal state preparation and quadrature measurement, respectively. The requirement for LO transmission is a major obstacle to the implementation of CV-QKD, especially in integrated photonics. Current fiber-based implementations co-transmit the LO with the signal states using techniques that involve combinations of time-division multiplexing (TDM), wavelength-division multiplexing (WDM), and polarization encoding. Free-space implementations of CV-QKD also multiplex using the polarization degree of freedom. Since the LO intensity dictates the quality of quadrature measurement at Bob's receiver, it is desirable to transmit a high-power LO that is many orders of magnitude more intense than the signal pulse. Due to this power disparity, multiplexing has to significantly separate the two components in order to minimize the contamination of the signal states by photons scattered from the LO (for example, this is the reason for combining polarization encoding with TDM). This degree of separation in multiplexing (and associated demultiplexing at Bob's receiver) greatly complicates the hardware required for CV-QKD, and is even a roadblock for integrated photonics implementations of CV-QKD since TDM and polarization manipulation and maintenance are more difficult on-chip. Another complication associated with the requirement of LO transmission is that a relative phase shift arises between the signal and LO due to the path separation during demultiplexing at the receiver. This shift can be compensated by precise calibration of the separated paths, which is however not

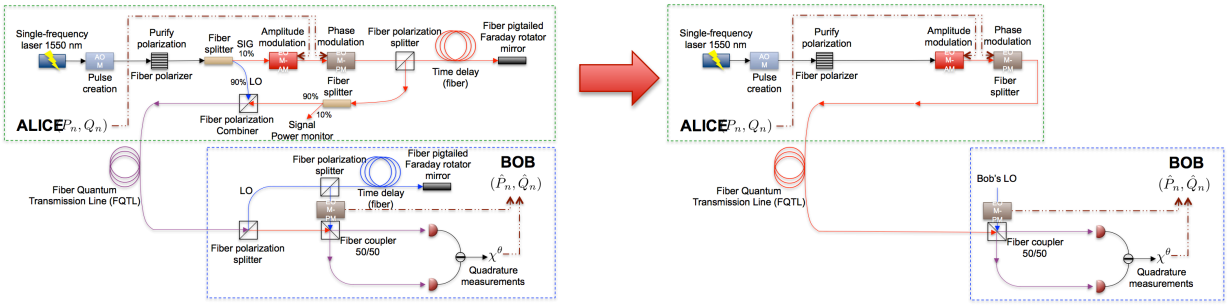

FIG. 1. Hardware schematic for a conventional CV-QKD implementation using LO transmission (on the left) and for the SR-CV-QKD protocol (on the right). The elimination of LO transmission dramatically simplifies the hardware requirements.

a robust solution, or by dynamic phase estimation at the receiver, in which case the speed at which this estimation can be done becomes a practical limitation on the rate of key generation.

We present a coherent-state CV-QKD protocol that avoids all of the issues outlined above by eliminating the transmission of an LO between Alice and Bob [1]. This is possible to achieve due to the fact that a common reference frame between Alice and Bob can be established by a method that, instead of transmitting an LO, uses regularly spaced *reference pulses* whose quadratures are measured by Bob to estimate Alice's phase reference. This new protocol, which we call *self-referenced* CV-QKD (SR-CV-QKD), greatly simplifies the hardware requirements at Alice's and Bob's stations (as shown in Figure 1) since it enables them both to employ independent (truly local) LOs. In addition, SR-CV-QKD obviates a key assumption of most CV-QKD security proofs — namely that the LO is trusted — and thus provides a more secure implementation of CV-QKD. Recent experimental demonstrations of SR-CV-QKD [1–3] used fiber-based setups utilizing fiber-pigtailed bulk-optics components. However, we stress that this protocol is manifestly compatible with chip-scale implementation since it only requires (low-loss and low-noise) classical optical communication components. We thus believe that this new protocol will play a key role in enabling the miniaturization of CV-QKD hardware, which has the potential to significantly enhance the applicability of quantum communications.

In a physical implementation of the SR-CV-QKD protocol, Alice chooses two independent Gaussian random variables (q_A, p_A), both normally distributed with zero mean and a fixed variance V_A, and sends Bob the coherent state with amplitude $q_A + ip_A$, which we refer to as the *signal pulse*. In addition, she sends a coherent-state *reference pulse* in the next time bin. The mean quadrature values of the reference pulse in Alice's reference frame are publicly known. The amplitude of the reference pulse is fixed and may be several times larger than $V_A^{1/2}$, but much smaller than that of a typical LO. Using reference pulses with a relatively small amplitude is a practically important aspect of SR-CV-QKD, which helps to reduce the interference with the signal pulse, as compared to the effect of a large-amplitude (classical) pulse, whose "long tail" cannot be completely suppressed and hence would interfere with the signal if time multiplexed at the same rate. In each round, Bob performs a homodyne measurement of one of the quadratures of the received signal pulse to estimate its mean value, where these quadratures are defined relative to his own high-power LO. He also performs a heterodyne measurement on the received reference pulse to obtain both of its mean quadrature values (again, with respect to his LO). Alternatively, Alice can send a pair of closely spaced twin reference pulses, and Bob will perform homodyne measurements on them sequentially, obtaining one quadrature's mean value from the measurement on one

reference pulse and the conjugate quadrature's mean value from the measurement on the other. The central element of SR-CV-QKD is the estimation of the phase difference θ between Alice's and Bob's frames. Since Bob knows the mean quadrature values of the reference pulse both in Alice's frame and in his own frame, he can calculate an estimate of the phase difference using an elementary trigonometric analysis. Since the phase difference θ is a time-dependent random variable, the key assumption is that the time delay between signal and reference plus the duration of both pulses is much shorter than the characteristic timescale on which θ changes.

A way to view the difference between conventional CV-QKD and SR-CV-QKD is that while the former physically transmits a reference frame (in the form of the LO), the latter only transmits *information* about the reference frame. As a result, SR-CV-QKD is immune against recently identified side-channel attacks that exploit detection using a publicly shared high-power LO. Of course, it remains to be seen whether new side channel attacks that target SR-CV-QKD are possible.

Our theoretical analysis of SR-CV-QKD focuses on obtaining analytical results for expected asymptotic key rates, secure against individual and collective attacks under a passive Gaussian channel assumption. The usefulness of such a theoretical analysis is in revealing the effects of various design parameters on the achievable key rate. This calculation is particularly important in our case since it allows us to compare the expected performance of SR-CV-QKD against the respective conventional protocol that requires LO transmission. A principal feature of our security analysis is the incorporation of the inherent quantum uncertainty of reference pulses. Specifically, we quantify how the error of the phase difference estimation associated with the quantum uncertainty of reference pulses changes the covariance matrix shared between Alice and Bob and, consequently, reduces the expected key rates. We show that as the reference pulse amplitude increases, the key rate of SR-CV-QKD approaches that of conventional CV-QKD with LO transmission, but that this rate can be achieved with much simpler hardware.

In our experimental work, we focus on (1) thoroughly characterizing the performance of the central new element of SR-CV-QKD, signal reconstruction through compensation of the drifting phase, and (2) performing a proof-of-principle demonstration of key distribution using the new protocol. We demonstrate a good agreement of the experimentally reconstructed covariance matrix with theoretical predictions. While the transmission distance is negligible in our proof-of-principle demonstration, we use measured data to estimate the achievable key rates as a function of transmission distance using our experimental setup for a range of post-processing efficiencies. In independent experimental studies, Qi et al. [2] and Huang et al. [3] reported demonstrations of protocols essentially identical to SR-CV-QKD over 25-km fiber links. Our results, along with the demonstrations in Qi et al. [2] and Huang et al. [3], establish SR-CV-QKD as a practical protocol with significant benefits in terms of hardware simplification and potential compatibility with integrated photonics.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

---

[1] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5**, 041010 (2015).

[2] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015).

[3] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, Opt. Lett. **40**, 3695 (2015).