SAND2016-5186D

Self-Referenced Continuous-Variable Quantum Key Distribution

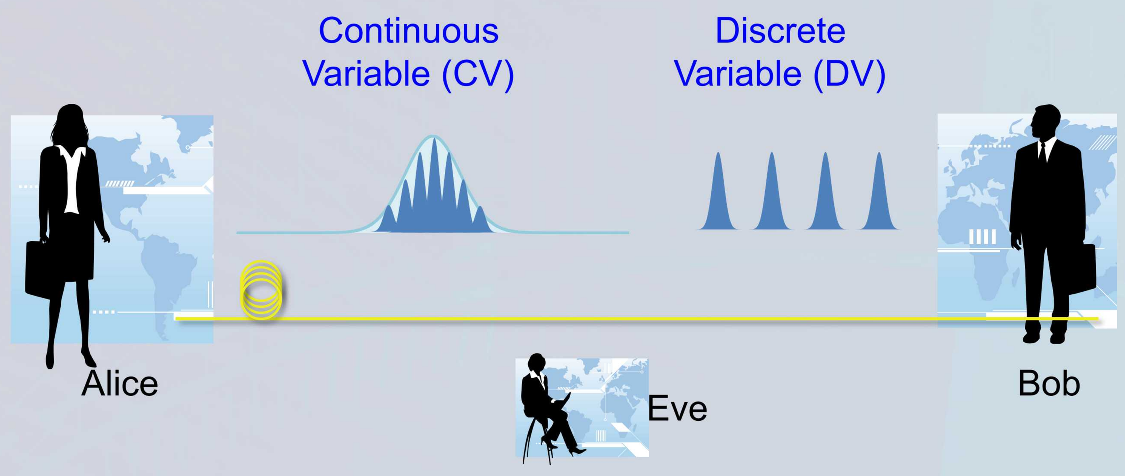
Sandia National Laboratories

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

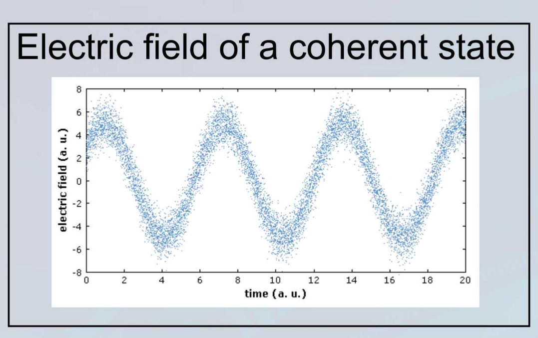
[1]Sandia National Laboratories, California 94551 [2]University of Waterloo, Canada [3]Sandia National Laboratories, New Mexico 87123

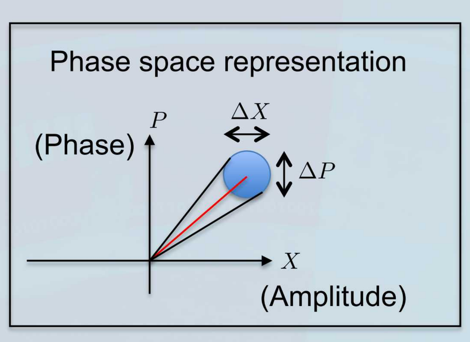
Problem

- This work is a part of the SECANT-QKD Grand Challenge LDRD project.
- Quantum key distribution (QKD) aims to distribute secret keys (one-time pads) that can be utilized for unconditionally secure communication.
- The main goal of the project is to put a QKD system on a photonic chip.
- Two approaches to QKD: CV and DV:



- CV-QKD approach is based on measuring two conjugate quantum observables: amplitude and phase of the optical field:

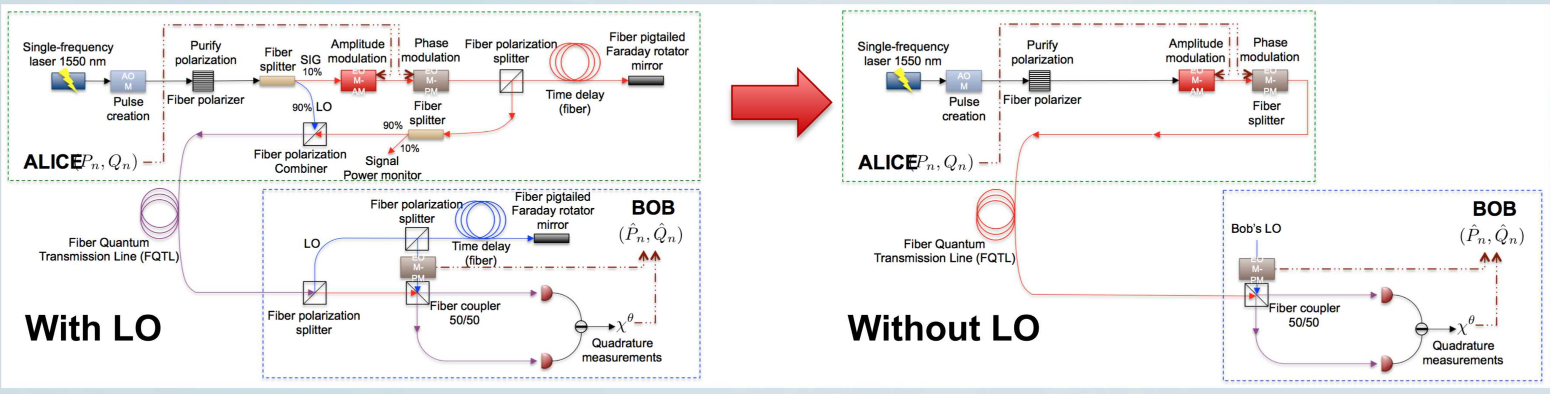




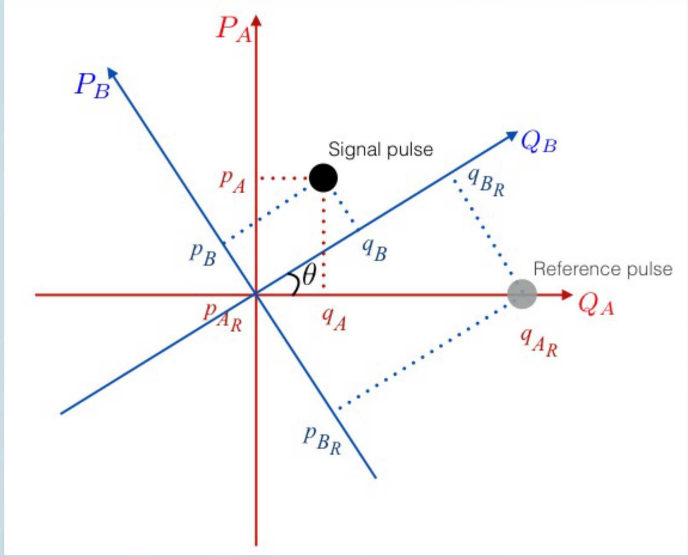
- A major problem of CV-QKD: it requires transmission of a high-intensity coherent pulse, called local oscillator (LO).

Approach

- We have developed a new CV-QKD protocol that eliminates the transmission of an LO.
- Instead of transmitting an LO, Alice sends 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 since it enables them both to employ independent (truly local) LOs.



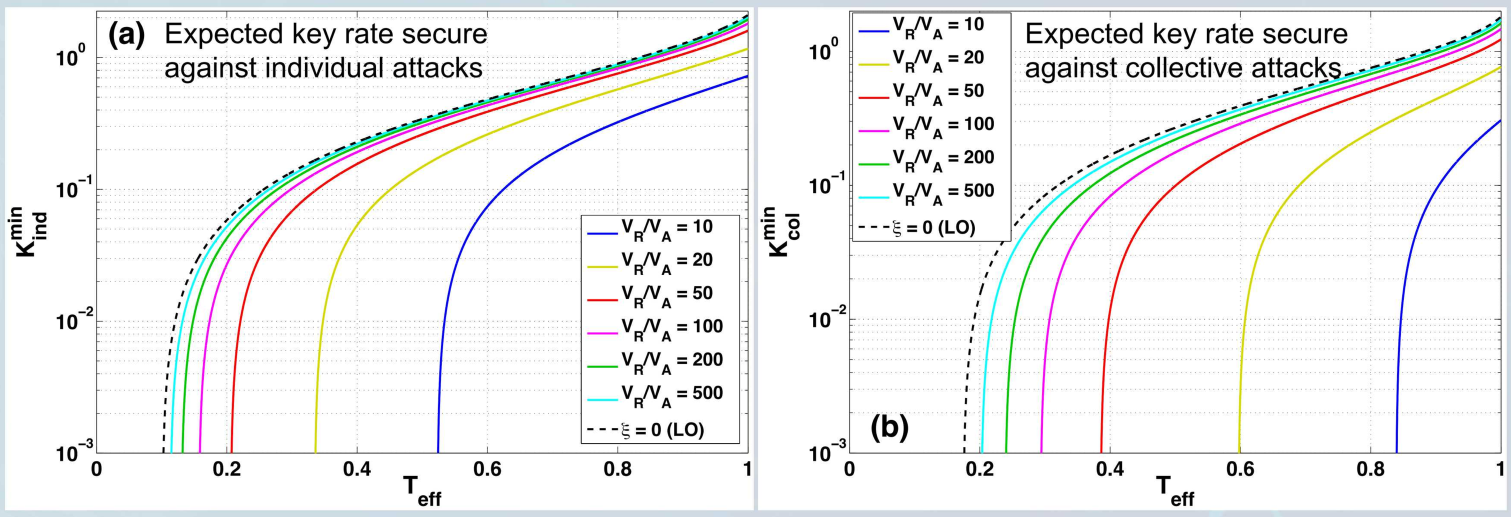
- In a physical implementation of the SR-CV-QKD protocol, Alice chooses two independent Gaussian random variables (q_A, p_A), both normally distributed with zero mean and a fixed variance V_A, and sends Bob a coherent-state signal pulse with amplitude $q_A + i\,p_A$.
- She also sends a coherent-state reference pulse with publicly known fixed amplitude $V_R^{1/2}$, which is much smaller than that of a typical LO.



- In each round, Bob performs homodyne measurement of one of the quadratures of the received signal pulse.
- He also performs heterodyne measurement of both quadratures of the received reference pulse.
- The key operation is the estimation of the phase difference θ between Alice's and Bob's frames.

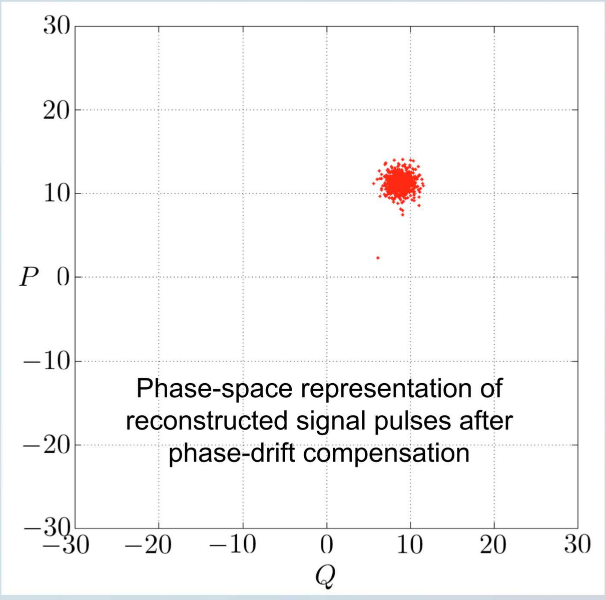
Results

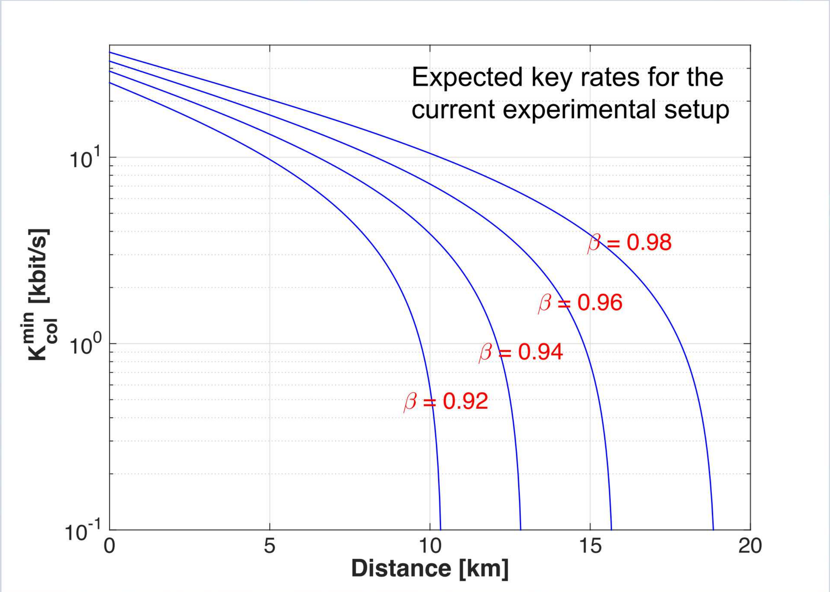
- Our theoretical analysis focused on obtaining expected asymptotic key rates, secure against individual and collective attacks.
- A principal feature of our security analysis is the incorporation of the inherent quantum uncertainty of reference pulses.



- Our experimental work focused on:

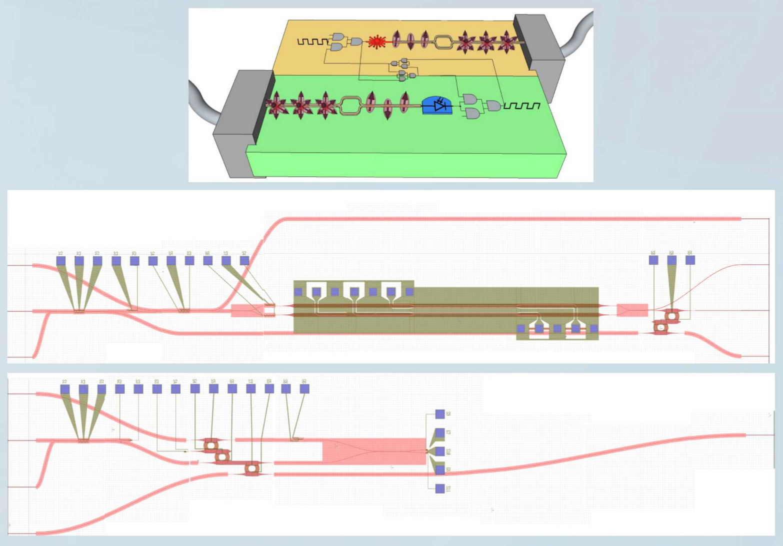
1. Characterizing the performance of the central element of SR-CV-QKD – signal reconstruction through compensation of the drifting phase;
2. Performing a proof-of-principle demonstration of key distribution using the new protocol.





Significance

- 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.
- SR-CV-QKD is manifestly compatible with chip-scale implementation since it only requires classical optical communication components. This enables miniaturization of CV-QKD hardware:



Transmitter design

Receiver design

- Our results [1], along with demonstrations by other groups [2, 3], establish SR-CV-QKD as a practical protocol with significant benefits in terms of hardware simplification and compatibility with integrated photonics.

References

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).

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.

SAND 2010-xxxP