# 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

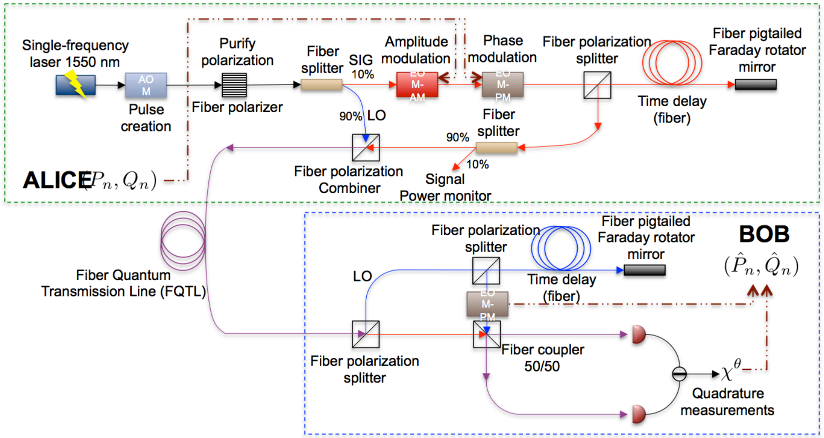
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

# Motivation

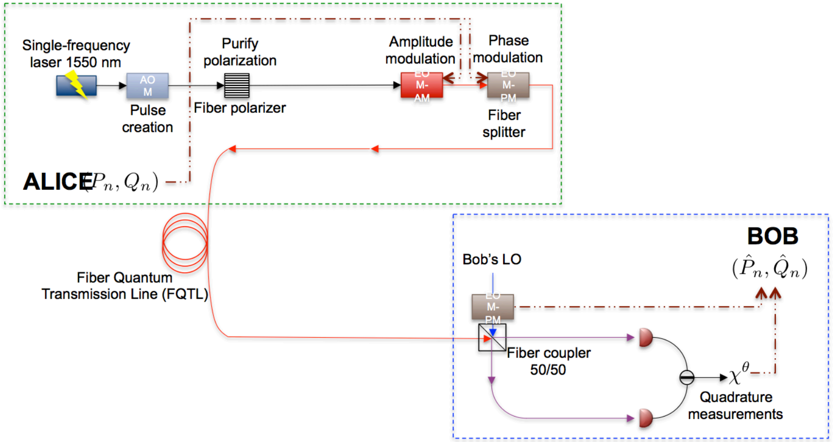
- **Coherent-state CV-QKD** can achieve information-theoretically secure key distribution with modest technological resources.
- It is particularly appealing due to the expectation that the integrated photonics implementation of CV-QKD will be easier than that of DV-QKD, resulting in greater practicality and wide-spread utilization.
- Conventional CV-QKD protocols require transmission of a high-intensity coherent pulse, **local oscillator (LO)**, between Alice and Bob. The shared LO is needed to ensure that Alice and Bob use the same reference frame.
- ***The requirement for LO transmission is a major obstacle to the implementation of CV-QKD.***
- **Security problems**: There exist side-channel attacks that exploit detection using a publicly shared high-power LO.
- **Technological issues**: Co-transmitting the LO with the signal states requires techniques that involve combinations of time-division multiplexing, wavelength-division multiplexing, and polarization encoding.

# Motivation

- Technological issues associated with LO transmission would be especially severe for **integrated photonics implementation** of CV-QKD, since time-division multiplexing and polarization manipulation and maintenance are more difficult on-chip.



**With LO transmission**



**Without LO transmission**

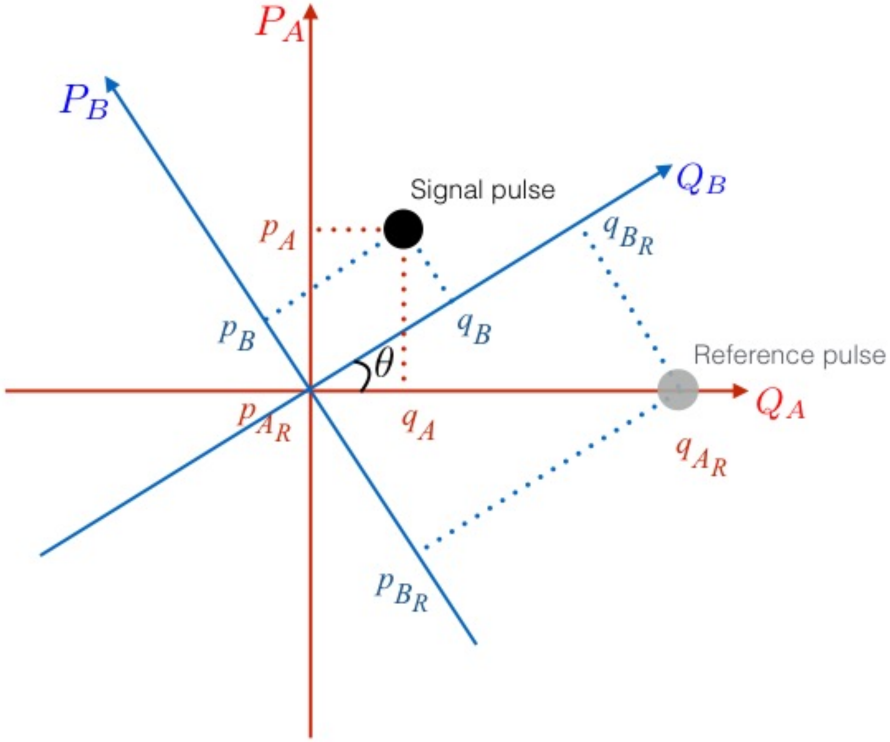
**When LO transmission is eliminated, the hardware simplification is a real advantage for on-chip implementation**

# New approach: SR-CV-QKD

- ***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.
- We call this new protocol **self-referenced CV-QKD (SR-CV-QKD)**
- **Key advantages of SR-CV-QKD**:
  - ✓ It greatly simplifies the hardware requirements at Alice's and Bob’s since it enables them both to employ independent (truly local) LOs.
  - ✓ It 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.
  - ✓ It is manifestly compatible with chip-scale implementation since it only requires (low-loss and low-noise) classical optical communication components.

# How it works

- 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.

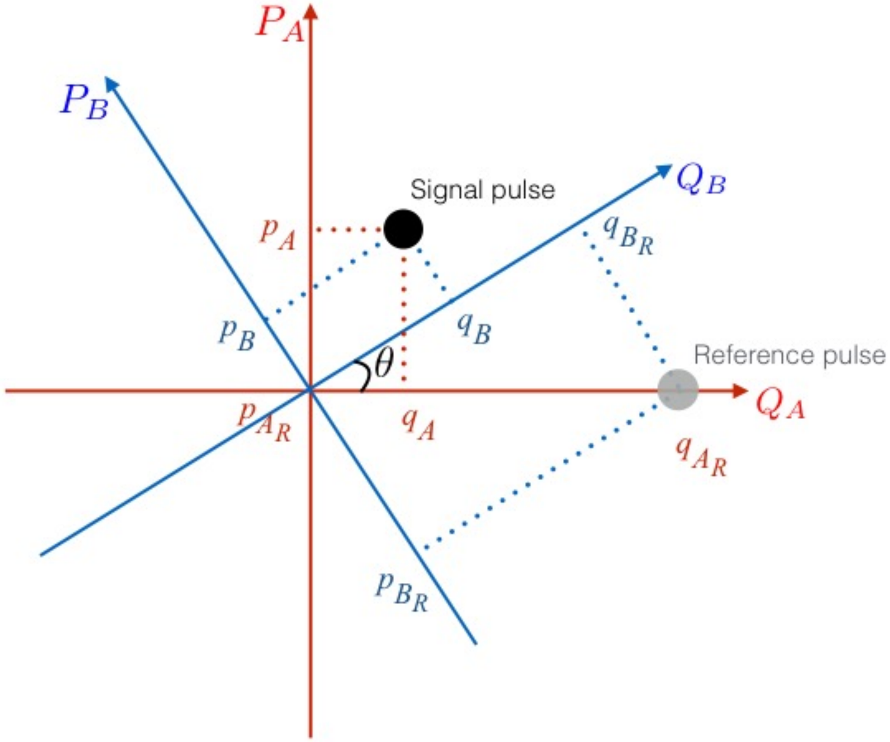


- In each round, Bob performs homodyne measurement of one of the quadratures of the received signal pulse.
- He also performs heterodyne measurement of both quadratures of the received reference pulse.
- The key operation is the **estimation of the phase difference** $\theta$ between Alice's and Bob's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

# Estimation of phase difference

Since Bob knows the mean quadrature values of the reference pulse both in Alice's frame, ($q_{AR}$, $p_{AR}$), and in his own frame, ($q_{BR}$, $p_{BR}$), he can calculate an estimate of the phase difference:

$$\hat{\theta} = \tan^{-1}\left(\frac{p_{B_R} q_{A_R} - q_{B_R} p_{A_R}}{q_{B_R} q_{A_R} + p_{B_R} p_{A_R}}\right)$$



Assuming, without loss of generality, that Alice's reference pulse has

$$p_{AR} = 0,$$

we obtain:

$$\hat{\theta} = \tan^{-1}\left(\frac{p_{B_R}}{q_{B_R}}\right)$$

# Effect of quantum uncertainty

- Since the reference pulse has a relatively small amplitude, its quantum uncertainty will produce an error in the phase difference estimate: $$\hat{\theta} = \theta + \varphi$$
- The estimation error *φ* is a random variable distributed according to some probability distribution *P*(*φ*). We assume that *θ* and *φ* are independent random variables, since they arise from separate physical processes.
- The density matrix for the state shared between Alice and Bob before they perform any measurements: $$\rho_{AB} = \mathcal{E}(\rho_{SV})$$
- The effect of the (mismatched) reference frame alignment between Alice and Bob:

$$\rho_{AB}(\hat{\theta}, \theta) = U_A(-\hat{\theta})U_B(\theta)\rho_{AB}U_A^{\dagger}(-\hat{\theta})U_B^{\dagger}(\theta)$$

- The effect of averaging over distributions of random variables *θ* and *φ*:

$$\overline{\rho}_{AB} = \overline{\rho_{AB}(\hat{\theta}, \theta)} = \int_{-\pi}^{\pi} d\varphi \mathcal{P}(\varphi) \int_{-\pi}^{\pi} \frac{d\theta}{2\pi} \rho_{AB}(\hat{\theta}, \theta)$$

# Effect of quantum uncertainty

- In terms of the covariance matrix, only off-diagonal elements are affected:

$$\langle Q_A Q_B \rangle = \int_{-\pi}^{\pi} d\varphi \mathcal{P}(\varphi) \int_{-\pi}^{\pi} \frac{d\theta}{2\pi} \mathrm{Tr}\left[\rho_{AB}(\hat{\theta},\theta) Q_A Q_B\right]$$

$$= \sqrt{T\eta(V^2-1)}\,\overline{\cos\varphi}$$

- $T$ is the channel transmittance, $\eta$ is the detector efficiency, $\chi$ is the channel noise (referred to the input of the channel), and $V = V_A + 1$.
- The effect on asymptotic key rates secure against individual and collective attacks is through the parameter:

$$\xi = 1 - (\overline{\cos\varphi})^2$$

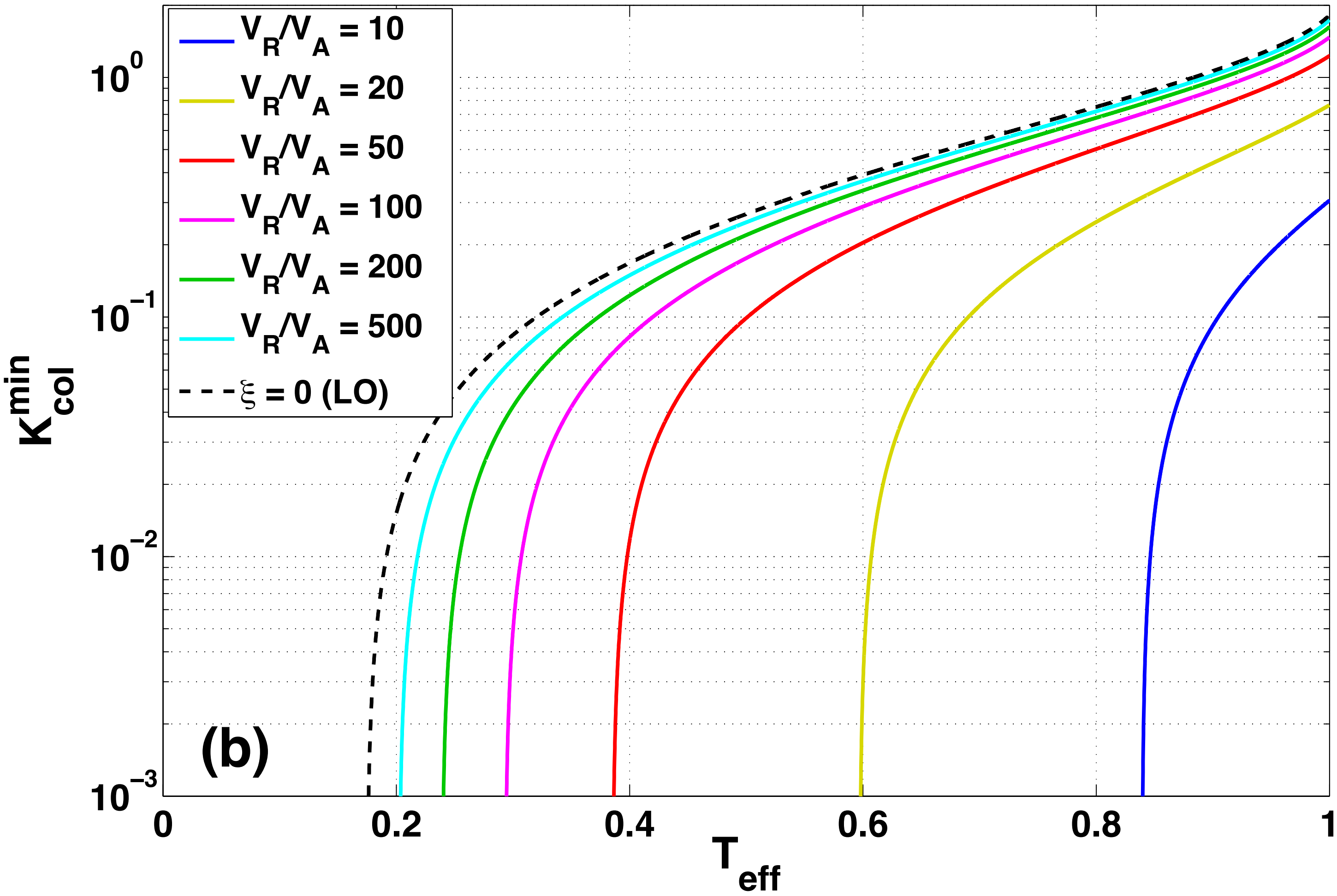
- Under reasonable assumptions on $P(\varphi)$ (symmetric and tight), we derive a tight bound on $\xi$:

$$\xi \lessapprox \overline{\varphi^2} = V_{\hat{\theta}} = \frac{\chi + 1}{V_R} + \frac{\delta_R}{T\eta V_R}$$

- $\delta_R = 1$ in the single-reference-pulse mode, $\delta_R = 0$ in the twin-reference-pulse mode.

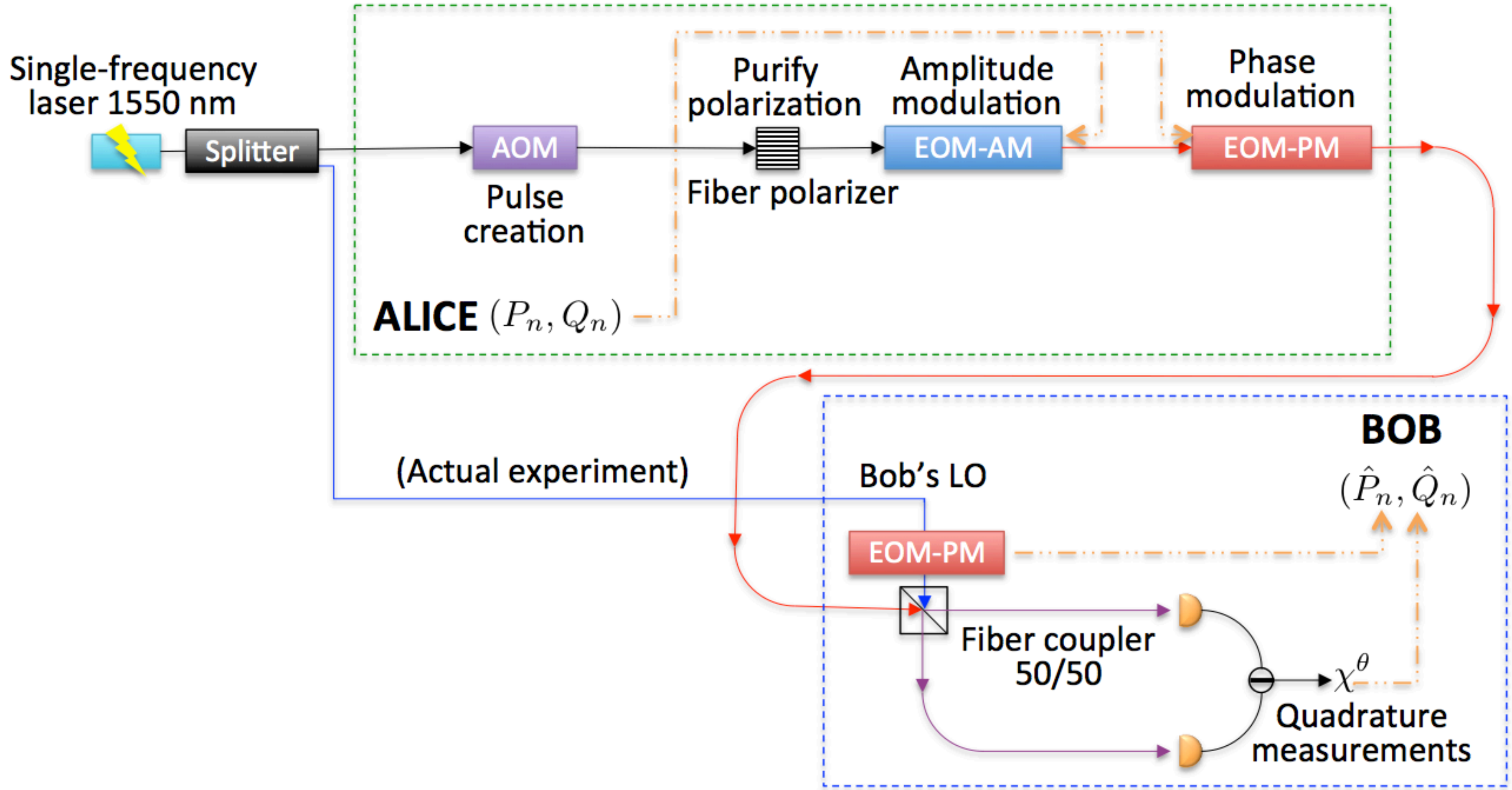
# Expected secure key rates

- Using the analysis outlined above, we obtain analytic expressions for asymptotic key rates secure against individual and collective attacks.



# Proof-of-principle experiment

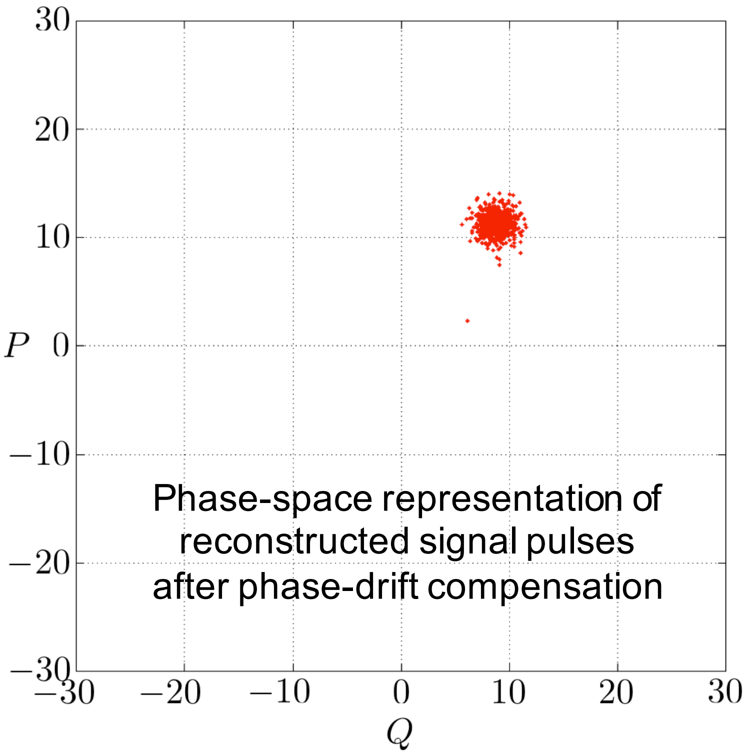
Schematic of our experimental setup (for simplicity, the same laser was used for both Alice's and Bob's LOs):



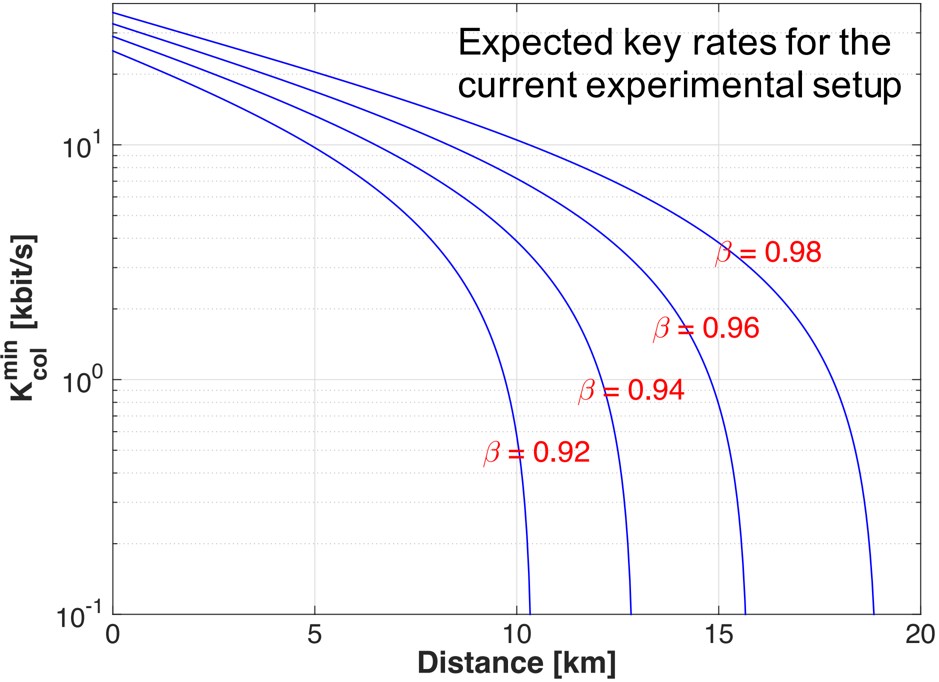
# Proof-of-principle experiment

- 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.



Phase-space representation of reconstructed signal pulses after phase-drift compensation

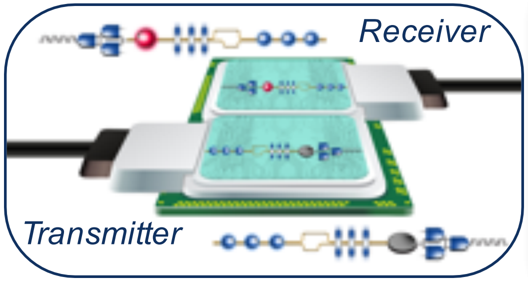


Expected key rates for the current experimental setup

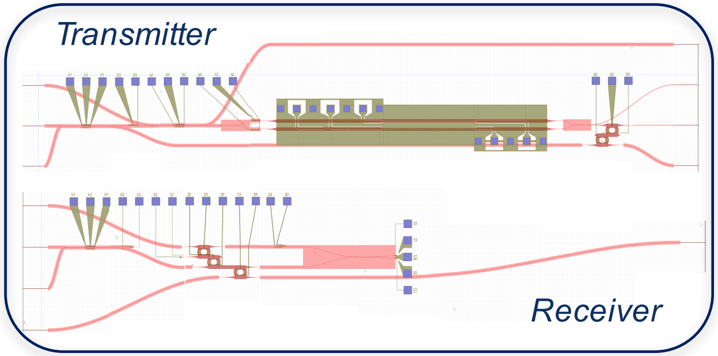
# Summary

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

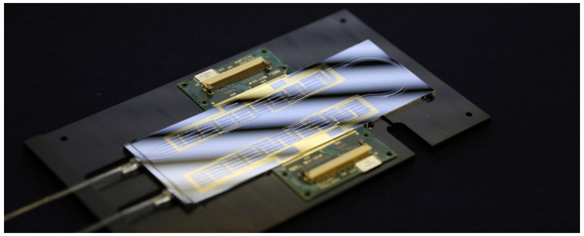
## Silicon photonics transceiver



**Idea**

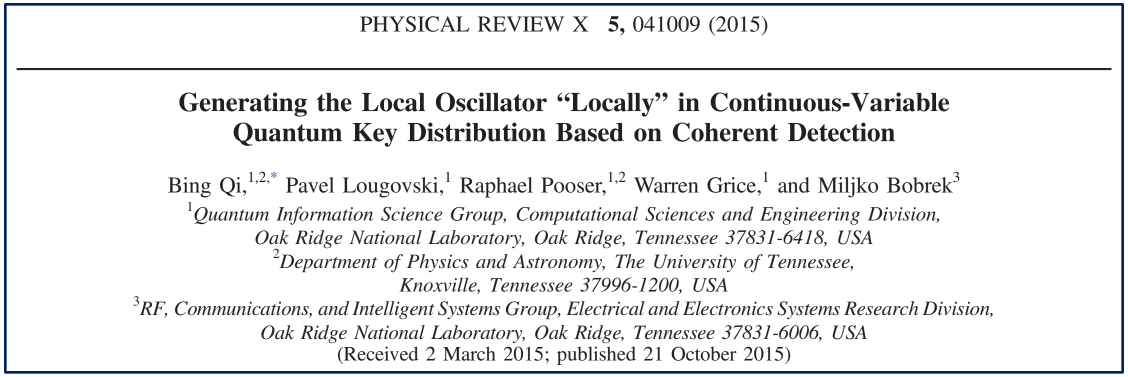


**Design**



**Implementation**

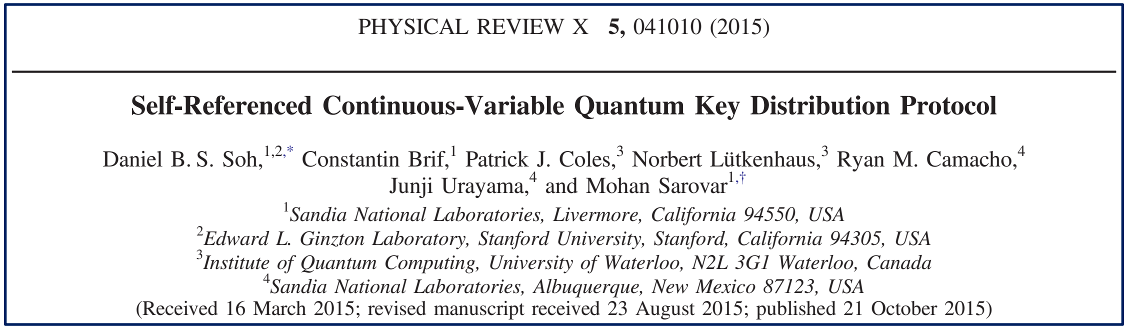
# References



PHYSICAL REVIEW X **5,** 041009 (2015)

### Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection

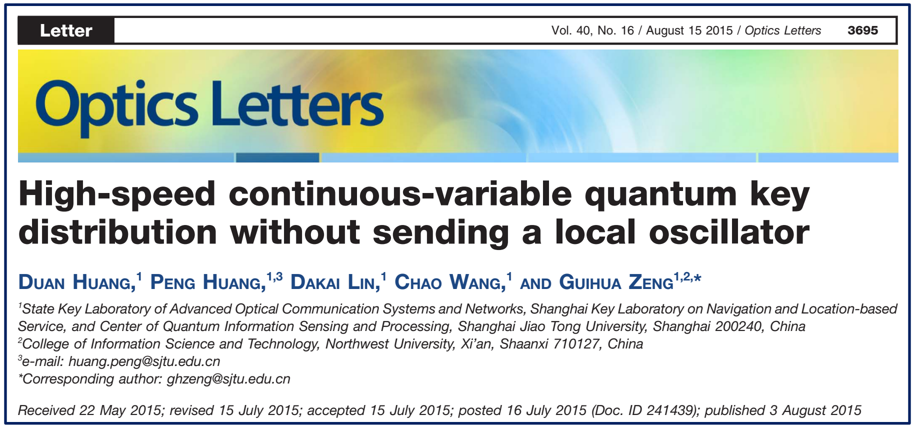
Bing Qi,[1,2,*] Pavel Lougovski,[1] Raphael Pooser,[1,2] Warren Grice,[1] and Miljko Bobrek[3]
[1]*Quantum Information Science Group, Computational Sciences and Engineering Division,*
*Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831-6418, USA*
[2]*Department of Physics and Astronomy, The University of Tennessee,*
*Knoxville, Tennessee 37996-1200, USA*
[3]*RF, Communications, and Intelligent Systems Group, Electrical and Electronics Systems Research Division,*
*Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831-6006, USA*
(Received 2 March 2015; published 21 October 2015)



PHYSICAL REVIEW X **5,** 041010 (2015)

### Self-Referenced Continuous-Variable Quantum Key Distribution Protocol

Daniel B. S. Soh,[1,2,*] Constantin Brif,[1] Patrick J. Coles,[3] Norbert Lütkenhaus,[3] Ryan M. Camacho,[4]
Junji Urayama,[4] and Mohan Sarovar[1,†]
[1]*Sandia National Laboratories, Livermore, California 94550, USA*
[2]*Edward L. Ginzton Laboratory, Stanford University, Stanford, California 94305, USA*
[3]*Institute of Quantum Computing, University of Waterloo, N2L 3G1 Waterloo, Canada*
[4]*Sandia National Laboratories, Albuquerque, New Mexico 87123, USA*
(Received 16 March 2015; revised manuscript received 23 August 2015; published 21 October 2015)



**Letter** Vol. 40, No. 16 / August 15 2015 / *Optics Letters* **3695**

Optics Letters

### High-speed continuous-variable quantum key distribution without sending a local oscillator

DUAN HUANG,[1] PENG HUANG,[1,3] DAKAI LIN,[1] CHAO WANG,[1] AND GUIHUA ZENG[1,2,*]
[1]*State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Key Laboratory on Navigation and Location-based Service, and Center of Quantum Information Sensing and Processing, Shanghai Jiao Tong University, Shanghai 200240, China*
[2]*College of Information Science and Technology, Northwest University, Xi'an, Shaanxi 710127, China*
[3]*e-mail: huang.peng@sjtu.edu.cn*
**Corresponding author: ghzeng@sjtu.edu.cn*

*Received 22 May 2015; revised 15 July 2015; accepted 15 July 2015; posted 16 July 2015 (Doc. ID 241439); published 3 August 2015*