SAND2014-18551PE

SECANT QKD Grand Challenge

Sandia Enabled Communications and Authentication Network using Quantum Key Distribution

Sandia National Laboratories

LORD

CV-QKD and on-chip coherent quantum feedback

Scott Bisson, Constantin Brif, David Farley, Matthew Grace, Mohan Sarovar, Daniel Soh, Kevin Young

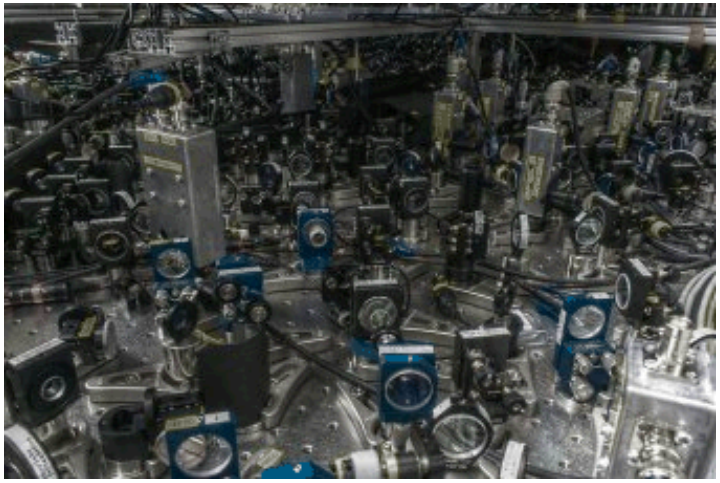
U.S. DEPARTMENT OF ENERGY

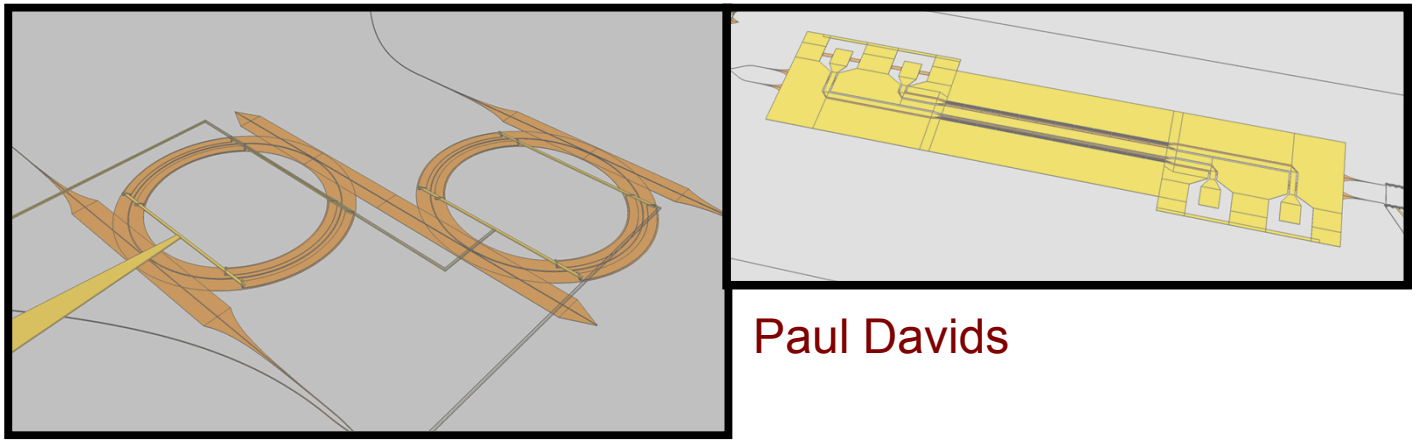
National Nuclear Security Administration

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 No. 2014-XXXXP

Moving optical networks on-chip

Sandia National Laboratories



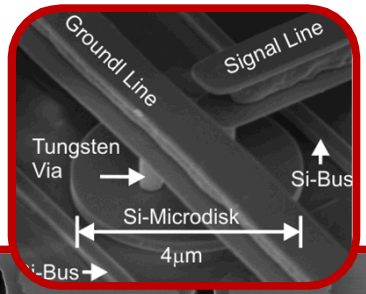


Paul Davids

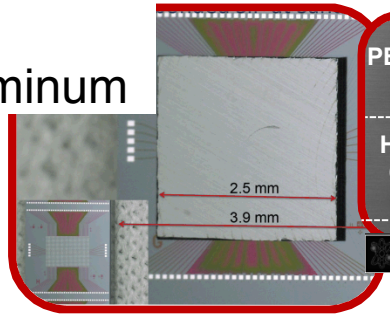
SNL Photonics Fabrication

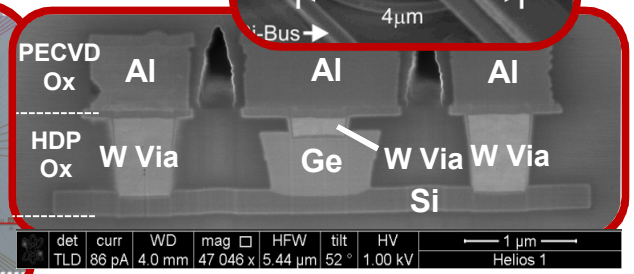
Sandia National Laboratories

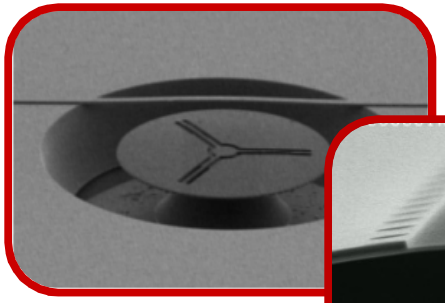
- Low-energy modulators[1], detectors[2], low-loss waveguides, SiN edge couplers, travelling wave Mach-Zehnder modulators, grating couplers, advanced CMOS flip-chip / direct CMOS integration

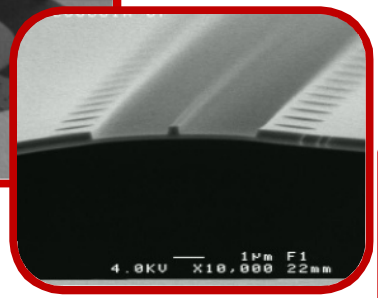


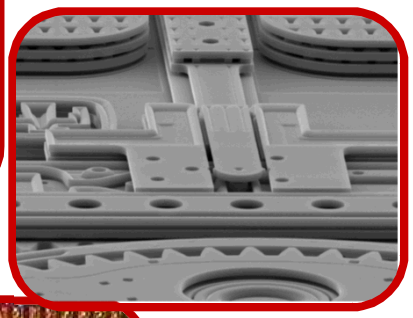
- Suspended Si/SiN resonators phononic/photonic crystals[3], aluminum nitride resonators and transducers.



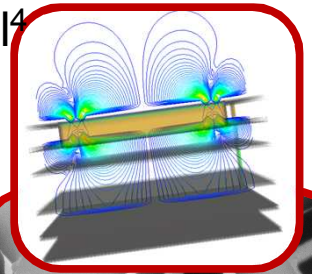




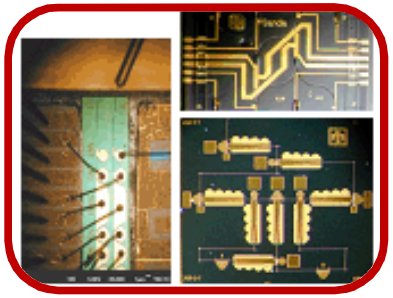


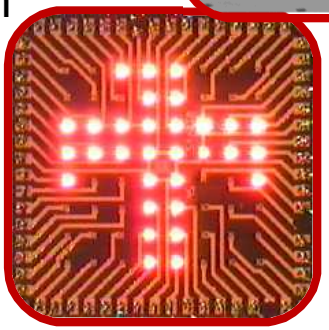


- Near to long-wave IR plasmonics and metamaterial[4] based devices.

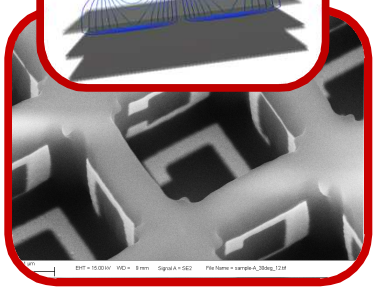


- Compound semiconductor devices and fabrication





- MEMS processing

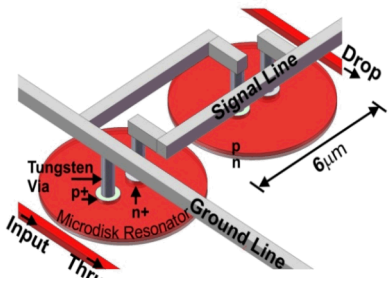


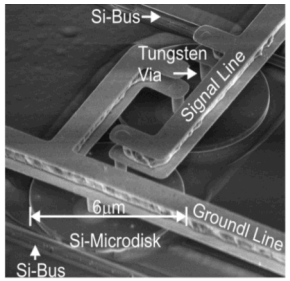
[1]M.R. Watts, et al. OPEX **19** 21989 (2011)
[2]C.T. DeRose, et al. OPEX **19** 24897 (2011)
[3]P.T. Rakich, et al. Nature Comm. **4** 1 (2013)
[4]D.B. Burckel, et al. Advanced Mat. **22** 5053 (2010)

Core Silicon Photonics

Sandia National Laboratories

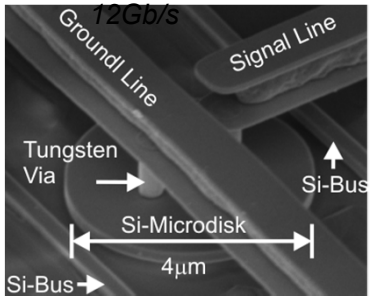
Free-carrier Effect (high-speed)

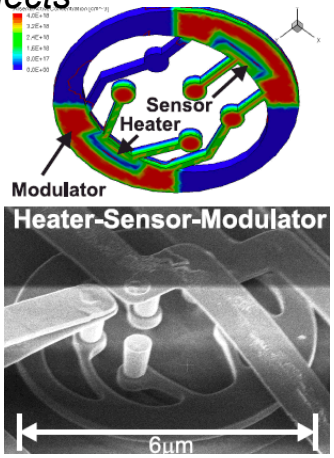




Fast Reconfigurable Interconnects

3.2fJ/bit at 12Gb/s



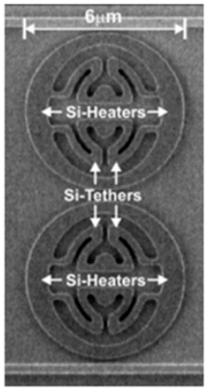


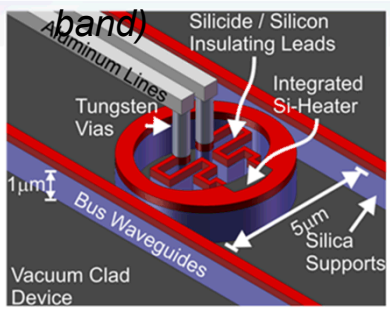
Resonant Optical Modulator/Filter

Thermally stabilized modulator

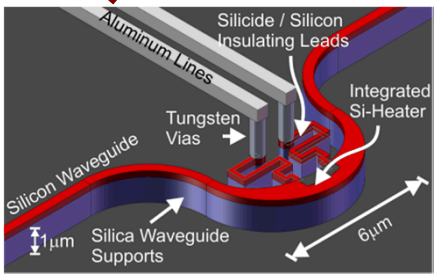
Broadband Mach-Zehnder Filter/Switch < 1V-cm at 10 Gb/s

Thermal Optic Effect (wide-band)

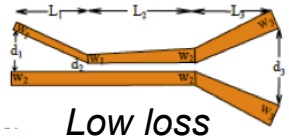




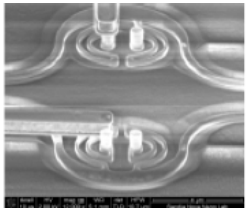
Tunable Resonant Filt



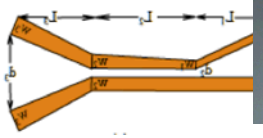
Thermo-optic Phase Shifter

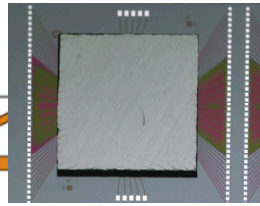


Low loss optical coupler

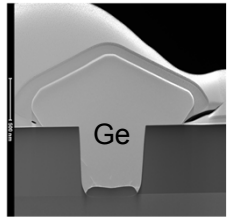


Switch Arrays

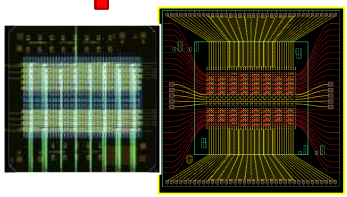




High-speed Ge Detector in

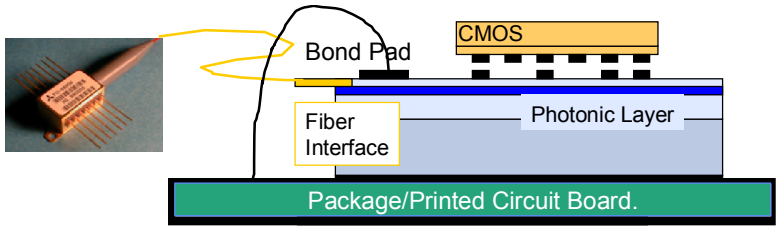


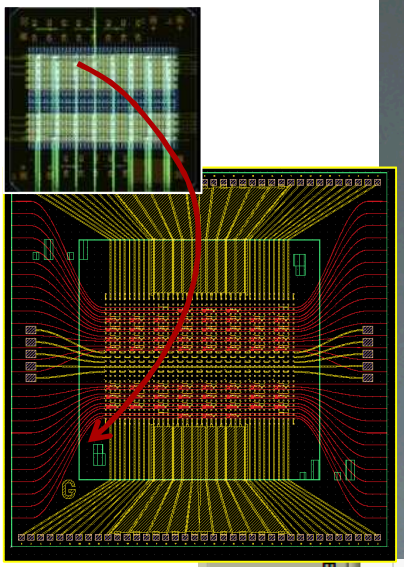
Si Photonics-CMOS Integration

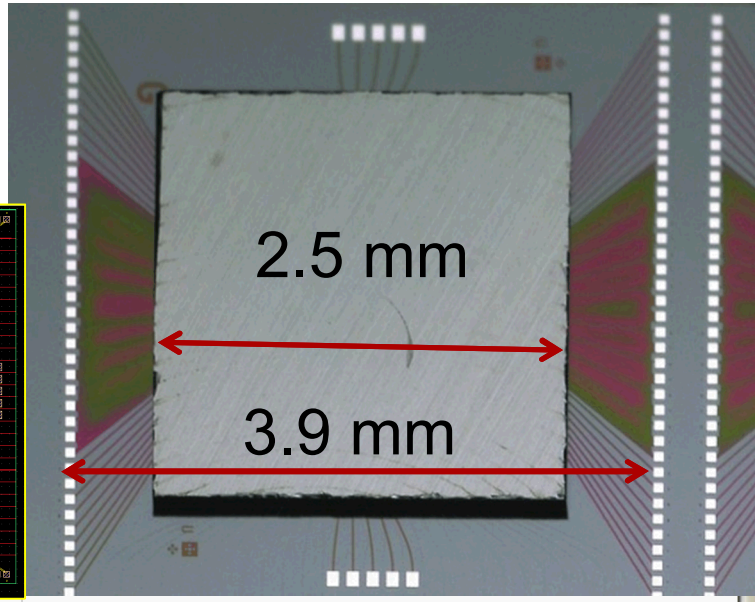


Electronic-Photonics Integration

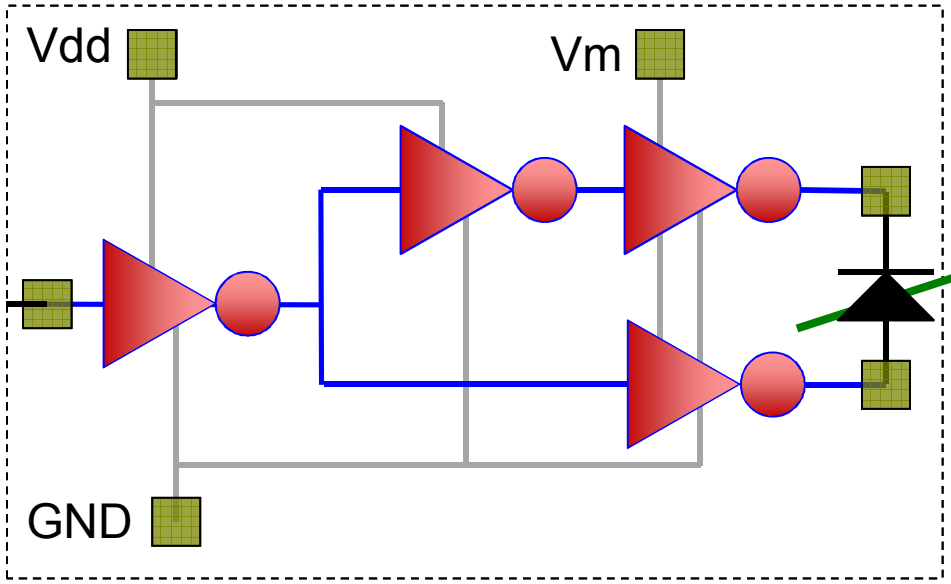
Sandia National Laboratories

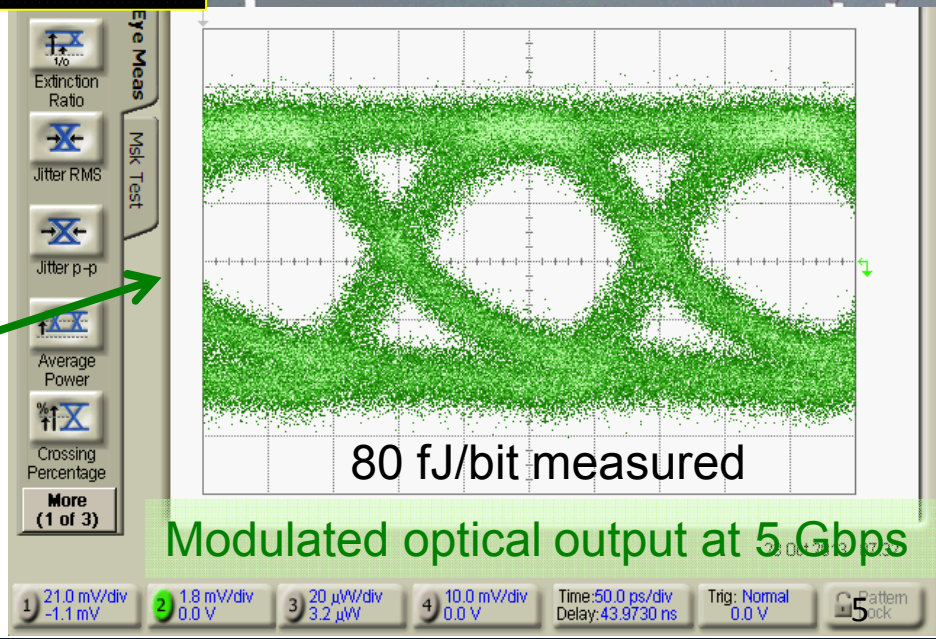






- Heterogeneous integration
  - Independent optimization of electronics & photonics
  - Challenge: Need high yields and small bond size

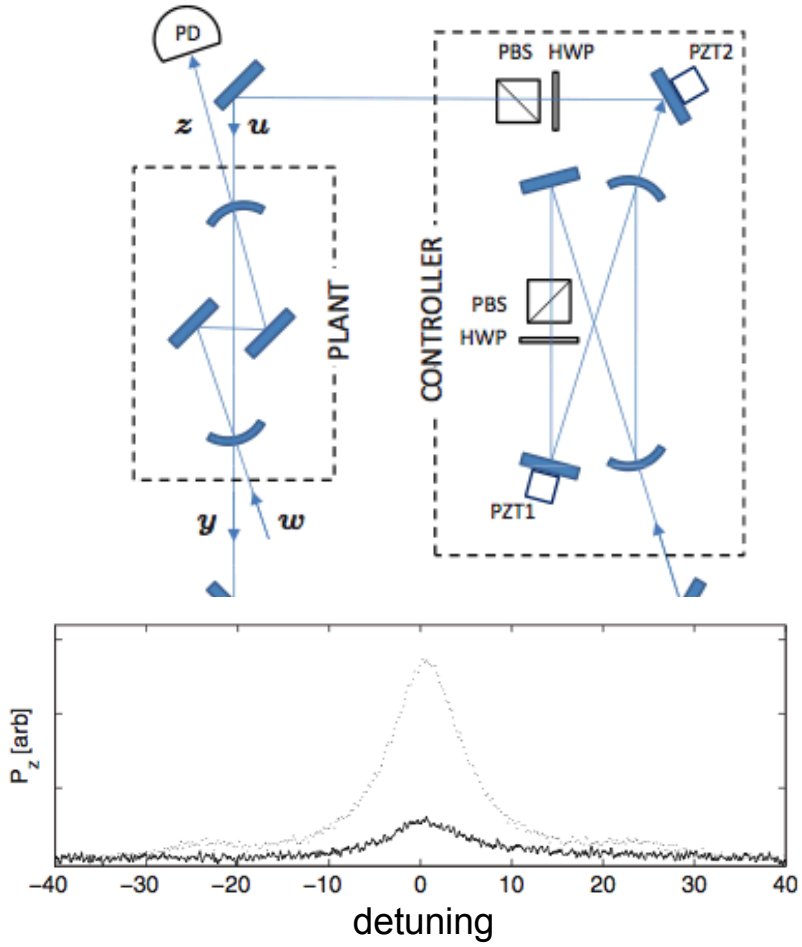




Coherent quantum feedback

Example: disturbance rejection

Example: disturbance rejection by dynamic compensation



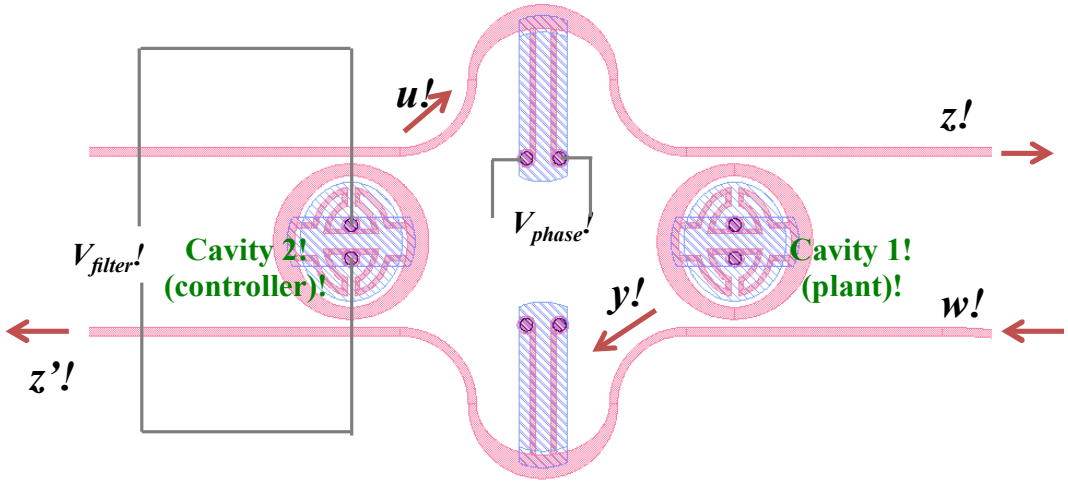
Goal: maintain z(t)=0 in the presence of w(t)

Feedback: use cavity output y(t) and actuate with u(t)

Mabuchi, H. *Phys. Rev. A*, *78*, 032323 (2008).

James, M. R., Nurdin, H. I., & Petersen, I. R. *IEEE Transactions on Automatic Control*, *53*, 1787 (2008).

On-chip CQFC



Paul Davids
Jonathan Cox

Free parameters in device (in linear mode)

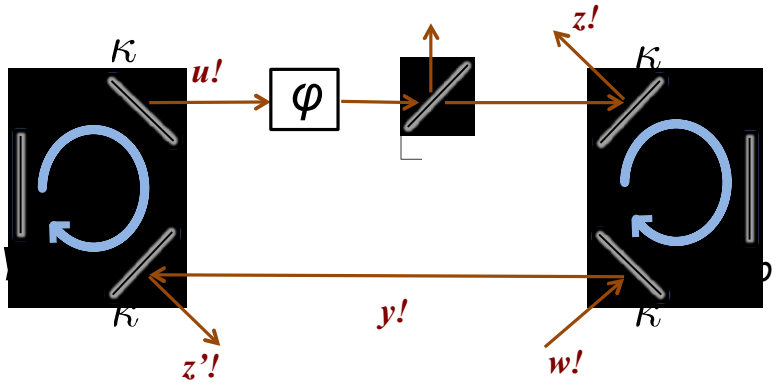
Resonance frequencies of two cavities (ω_p, ω_c)

Cavity-waveguide coupling κ

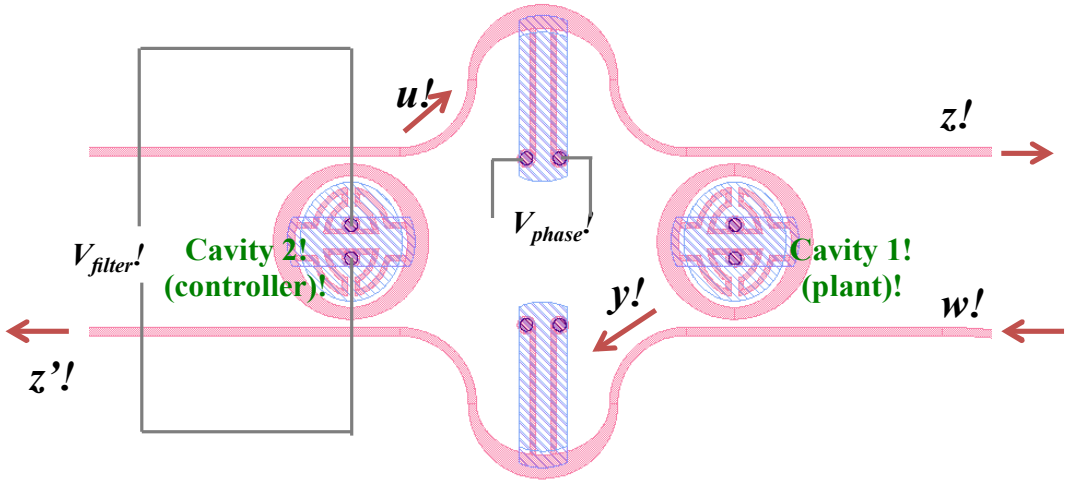
Intrinsic cavity losses (γ_p, γ_c)

Feedback phase ϕ

Losses in waveguide coupling η



On-chip CQFC

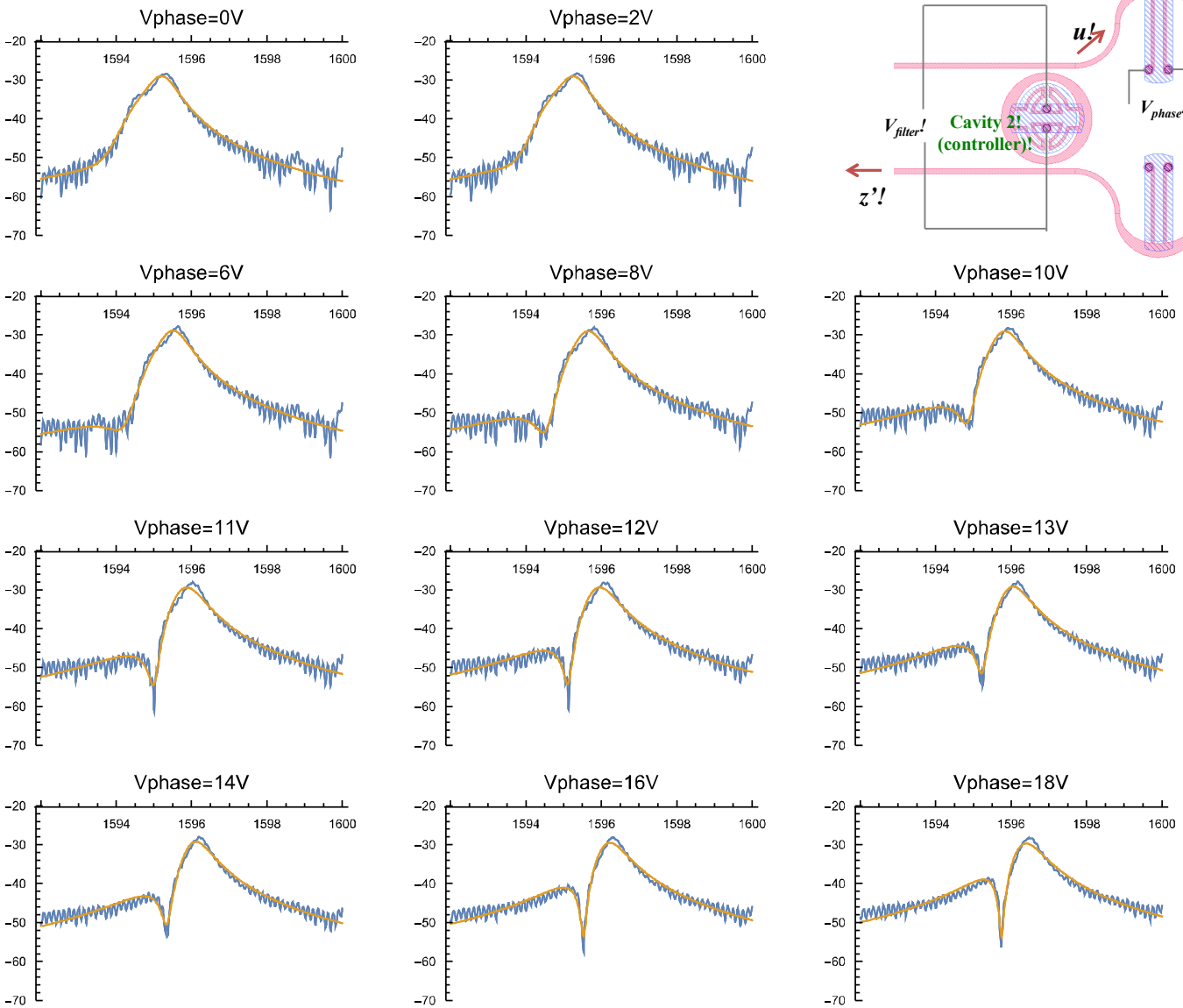


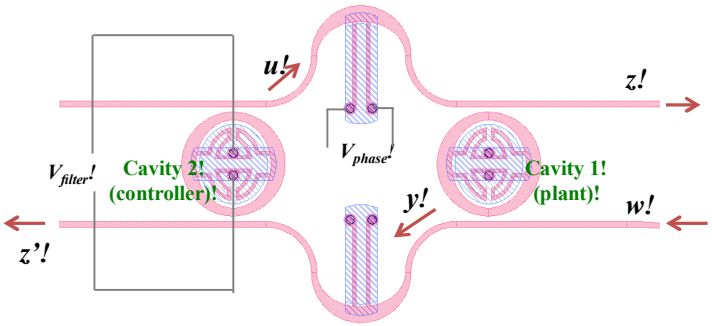
Built SLH model for this device.

Weak probe power => all components in their linear regime

Equivalent to the transfer function approach used by Mabuchi
[Mabuchi, H. *Phys. Rev. A*, *78*, 032323 (2008)].

Transmission spectra

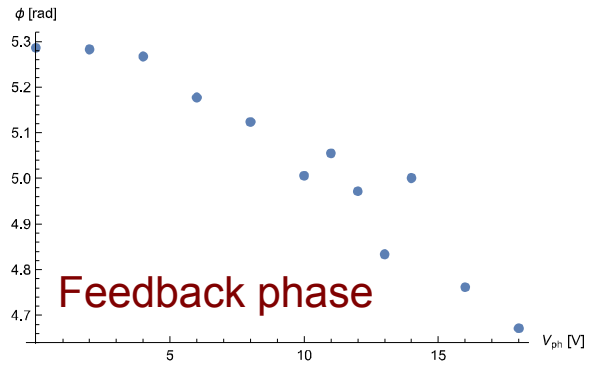


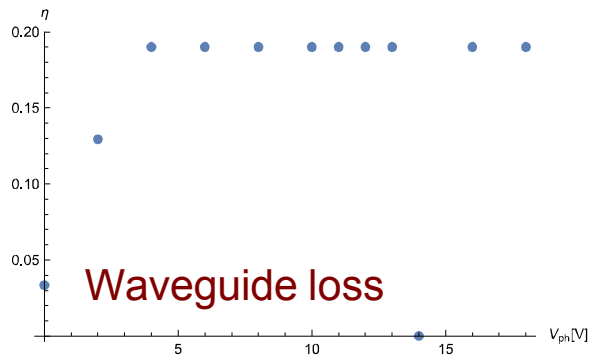


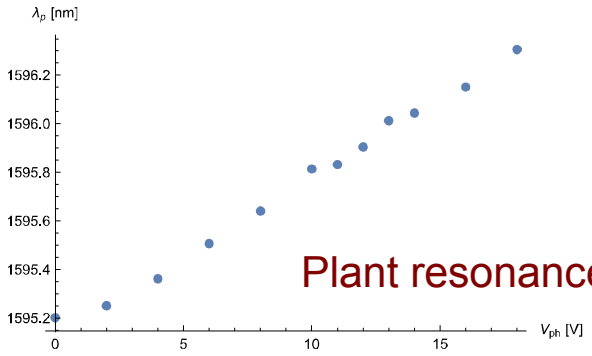
Experiment

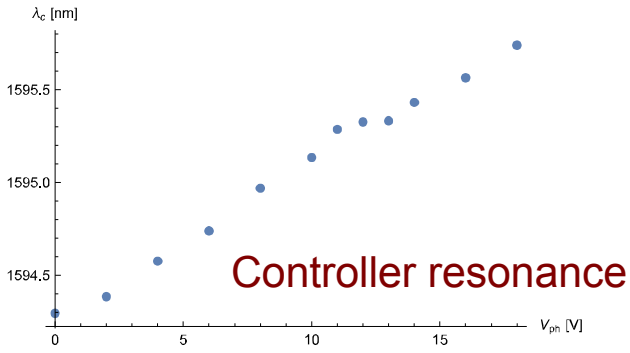
Theory

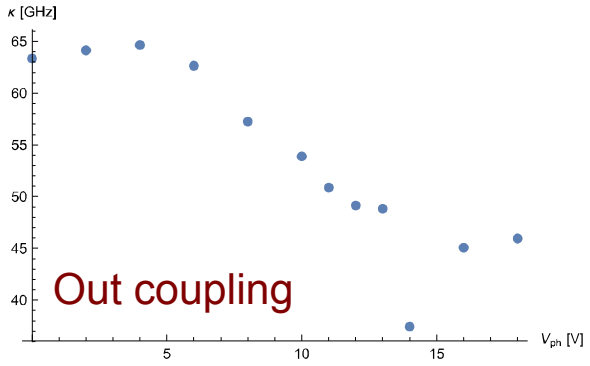
Theoretical fit to experiment











Thermal effect induced by thermo-optic phase shifter is not localized

No independent control over parameters

Integrated optics implementation of CQFC: issues

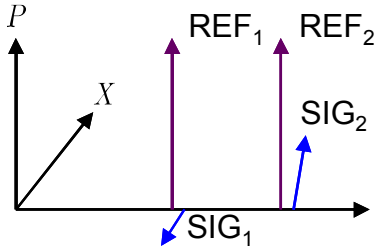
Sandia National Laboratories

- *Experimental challenges:*
  - In-situ control must be well localized and thermal effects contained
  - High quality nonlinear elements (e.g. OPO) necessary

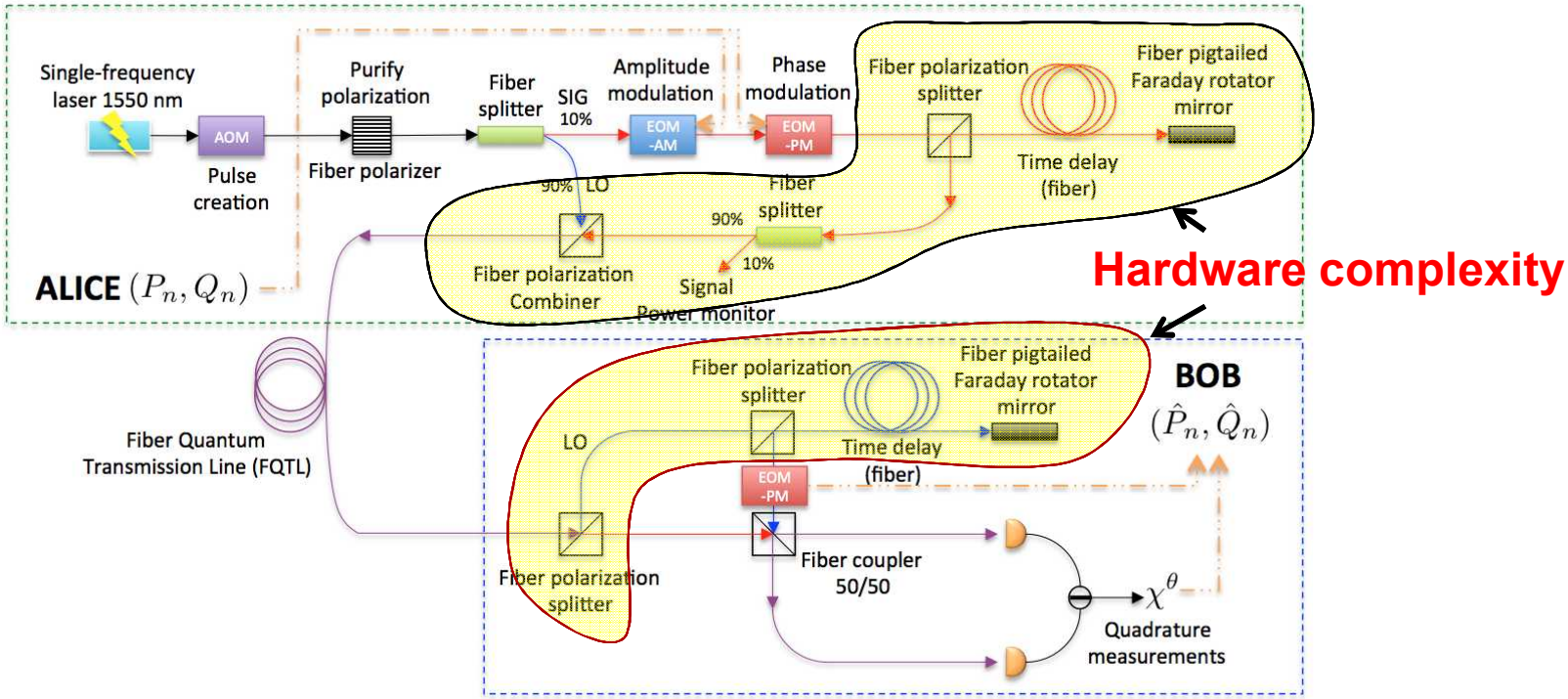
- *Theory challenges*:
  - Nonlinear effects (losses, Raman/Brillouin scattering) must be taken into account in resonant structures (if Q factor is large or probe power is large)
  - Two-photon absorption: can cause dynamical parameter changes (due to carrier concentration change, heating)
  - Thermal shifts of material properties

Year 1 research highlights

- Single OPO squeezed light apparatus almost complete
- Analysis and optimization of coupled OPO CQF network
- Implementation and analysis of on-chip optical feedback device
- New CV-QKD protocol without local oscillator transmission



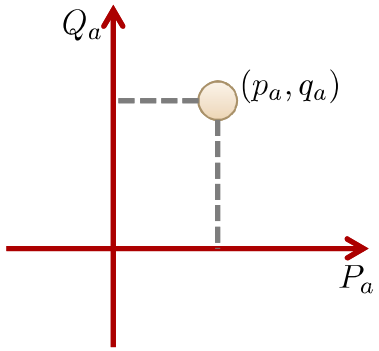
Sending a LO is expensive



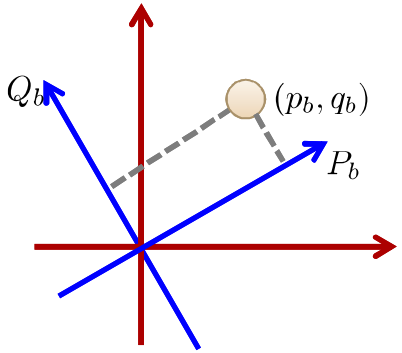
- Must multiplex SIG and LO
  - Strong LO added onto tiny SIG (50 dB power difference)
  - Multiple, simultaneous separation through – Time, Polarization, and Frequency (heterodyne)
- Complex phase tracking & control algorithm is needed for dynamic compensation of phase drift

LO = reference frame alignment

- Alice's encoding



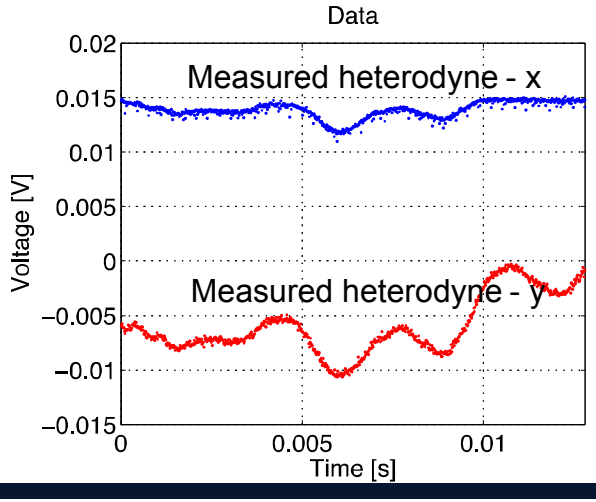
- Bob's decoding (homodyne)



$$(p_b, q_b) \neq (p_a, q_a)$$

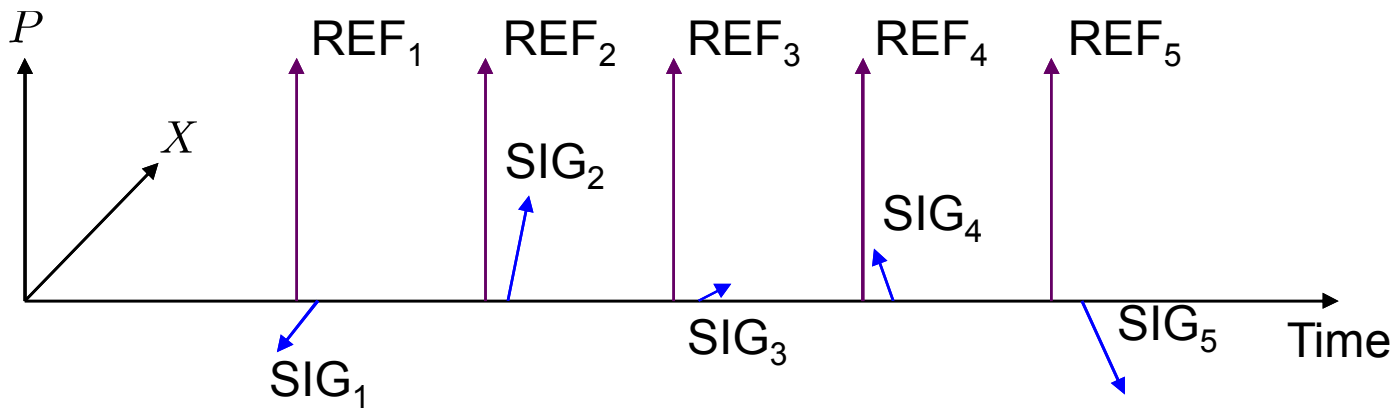
- Aligning Bob's quadrature angle with Alice's is important.
  - Quadrature angle is defined by phase difference between LO and SIG
  - If there is path-length difference between LO and SIG, Alice's angle may be different from Bob's angle.

Example: Alice transmits constant signal, signal measured by Bob:



Our solution: real-time referencing

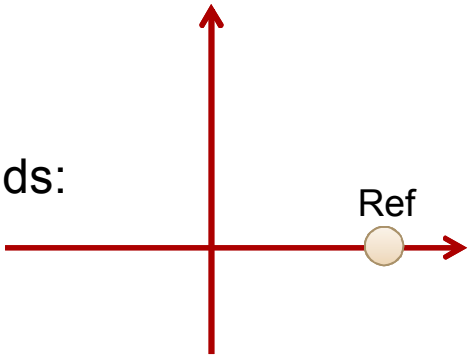
- Every signal pulse accompanied by a reference pulse
- Replaces LO phase reference

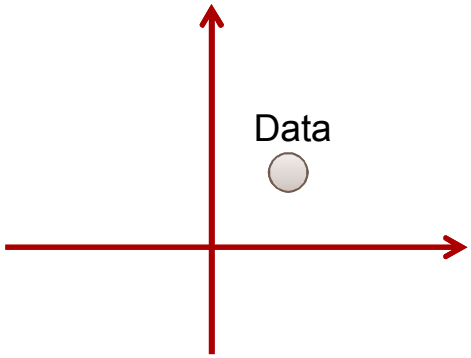


Our solution: real-time referencing

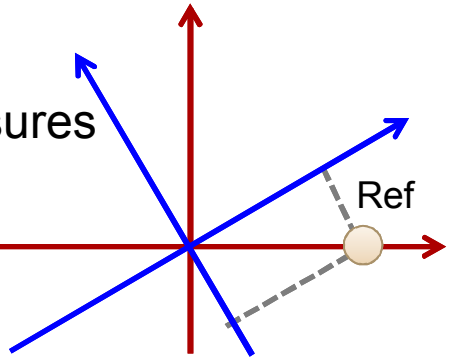
Sandia National Laboratories

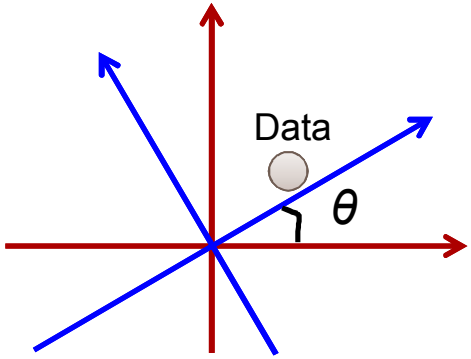
Alice sends:





Bob measures





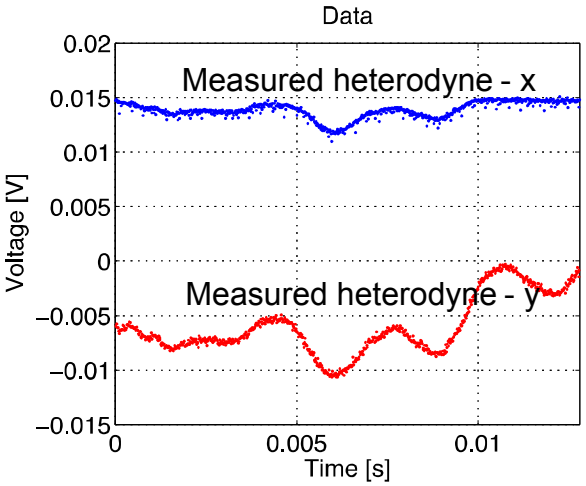
Using the Ref measurements, Bob computes rotation angle θ that relates original Data value to measured Data value

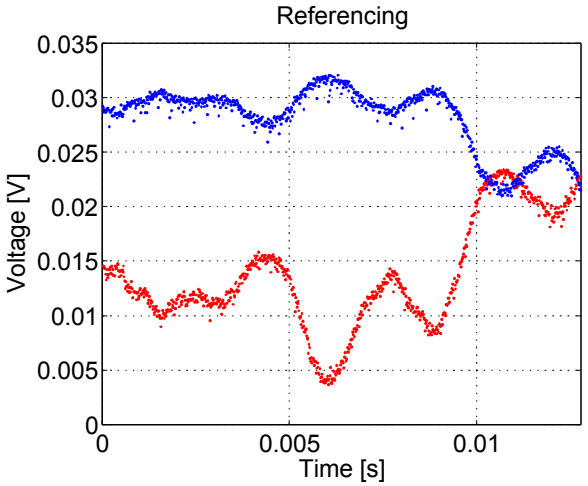
Then Bob corrects the measured Data value or transmits measurement angle to Alice

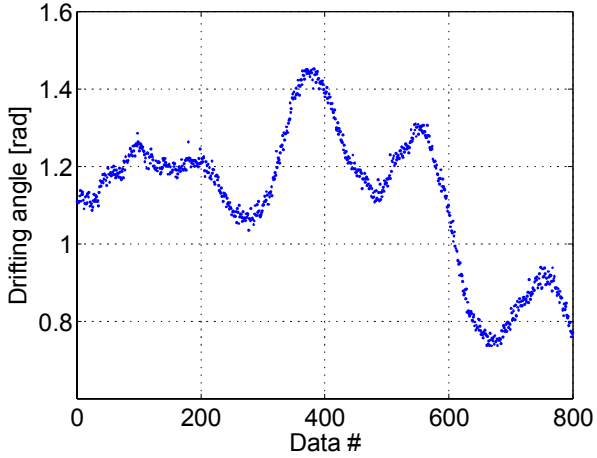
Phase drift compensation in action

Sandia National Laboratories

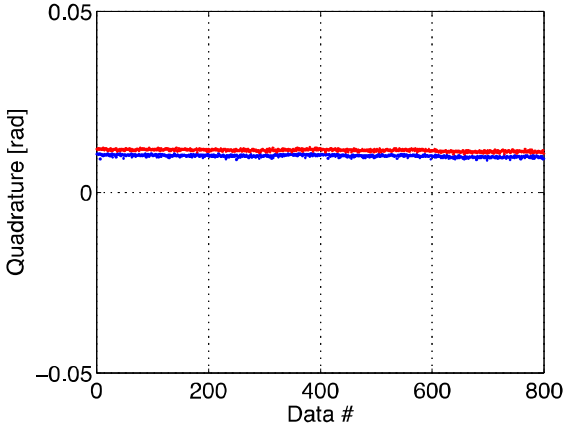
Alice transmits constant signal



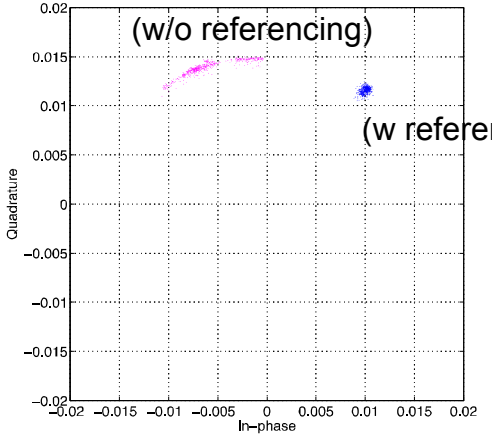




(Phase drift compensation)

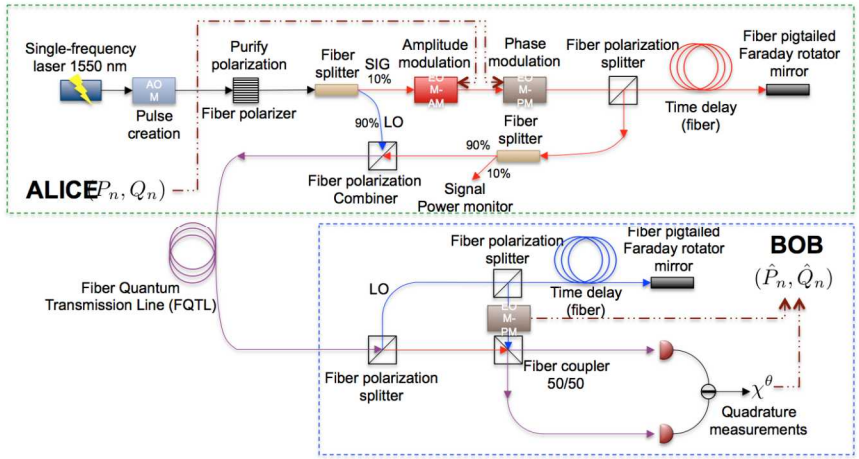


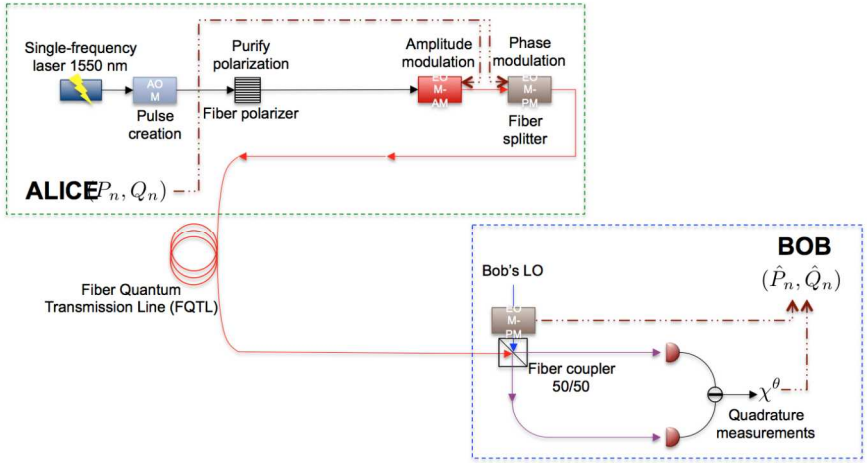
(Phase plane)



Benefits of new method

- Transmitting local oscillator no longer necessary
- Simplification of hardware
  - A real advantage for on-chip implementation





- No sacrifice in bandwidth
  - Real-time phase tracking & control also requires bandwidth for tracking and control sessions.
- REF pulses can be used for additional real-time calibration
  - e.g. time stamping, channel analysis, frequency locking

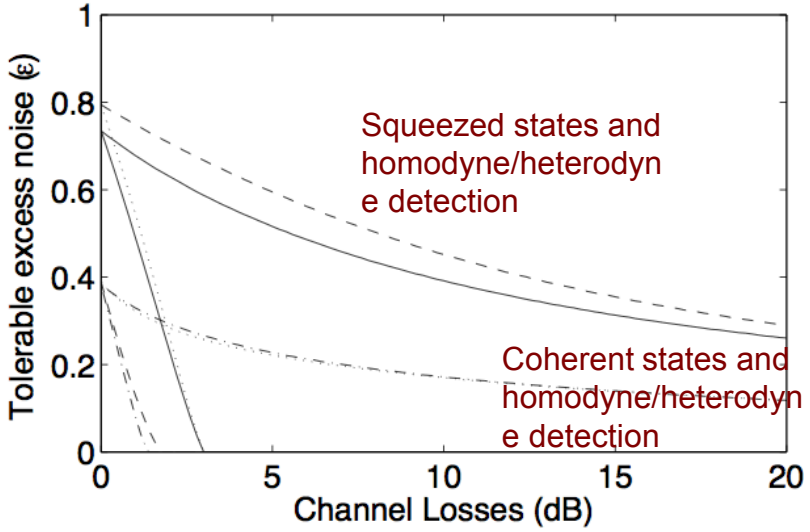
Security analysis

- Currently under way
- Similar information leakage as LO transmission
- Noise induced by imperfect phase compensation will impact key rate, especially in high loss channels

Task Objectives

To mature CV-QKD technology and protocols

1. Produce a stable source of squeezed light suitable for CV-QKD deployment
   - Demonstrate advantages of squeezed light for CV-QKD: Tolerance to excess noise



[Raul Garcia-Patron, Ph.D thesis, 2008]

2. On-chip realization of CV-QKD hardware

   (with CSI team, Paul Davids)

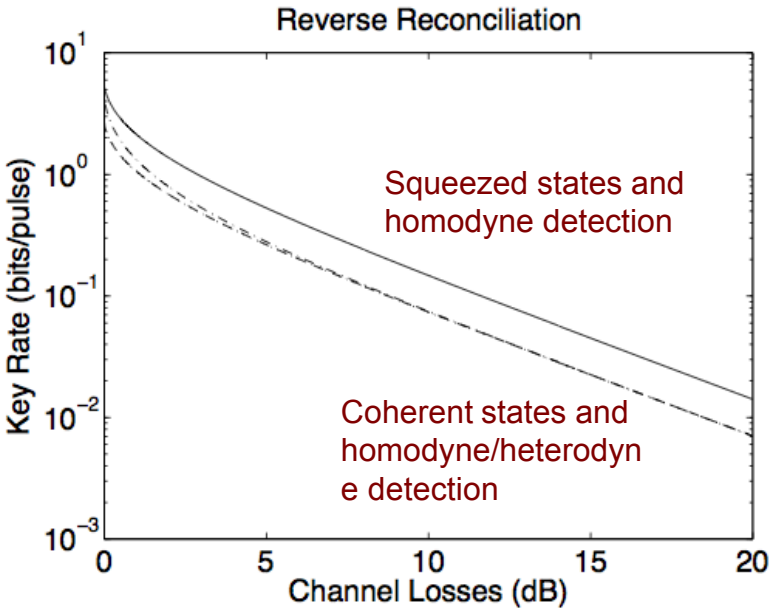
3. New protocols for CV-QKD

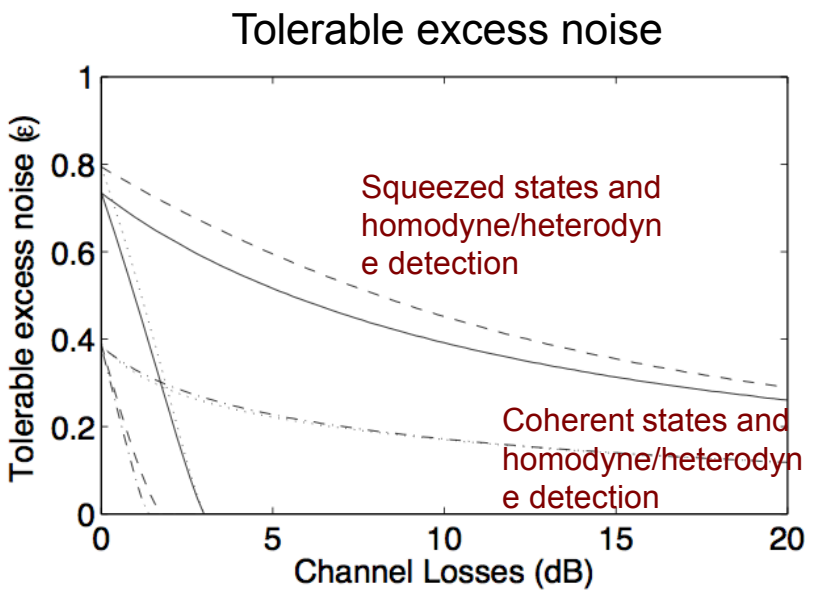
   (with QTL team, Junji Urayama)

Backup slides

Advantages of squeezed light encoding

- Squeezed light encoding can enable higher key rate/longer distance CV-QKD, and be more robust against excess noise





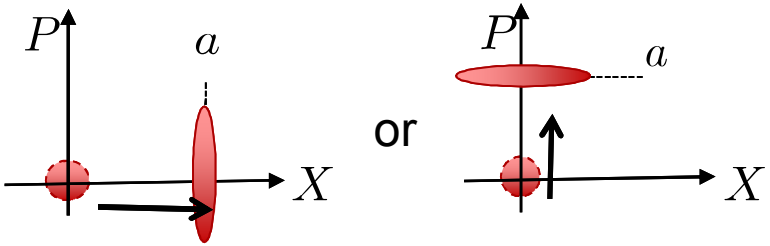
[Raul Garcia-Patron, Ph.D thesis, 2008]

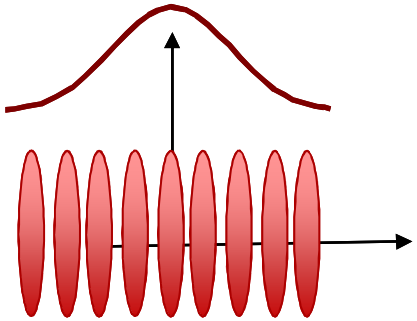
- Possible to generate squeezed light with high degree of squeezing, high bandwidth, in a portable package?

CV-QKD with squeezed light encoding

Sandia National Laboratories

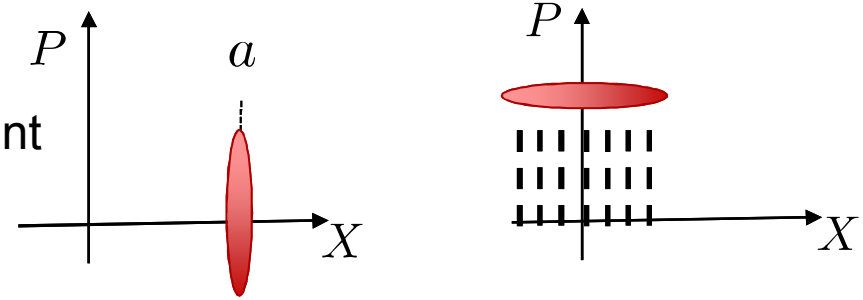
1) Alice generates a random real number (a) from a Gaussian distribution of variance V_A and a random bit (b) from a binary distribution. Bob generates a random bit (b′).
2) Depending on the value of the random bit (b) Alice sends a x-squeezed state with first moment d = (a, 0) or a p-squeezed state with first moment d = (0, a), where the squeezing r satisfies $V_A = 2 \sinh 2r$.





3) Bob, depending on his random bit (b′), measures either X or P.

Suppose an X measurement



4) Sifting: Alice discloses for each pulse the value of b (whether she displaced X or P). Bob keeps only the cases where he measured the right quadrature (b = b′).
5) Channel identification, **key discretization**, error correction, privacy amplification.