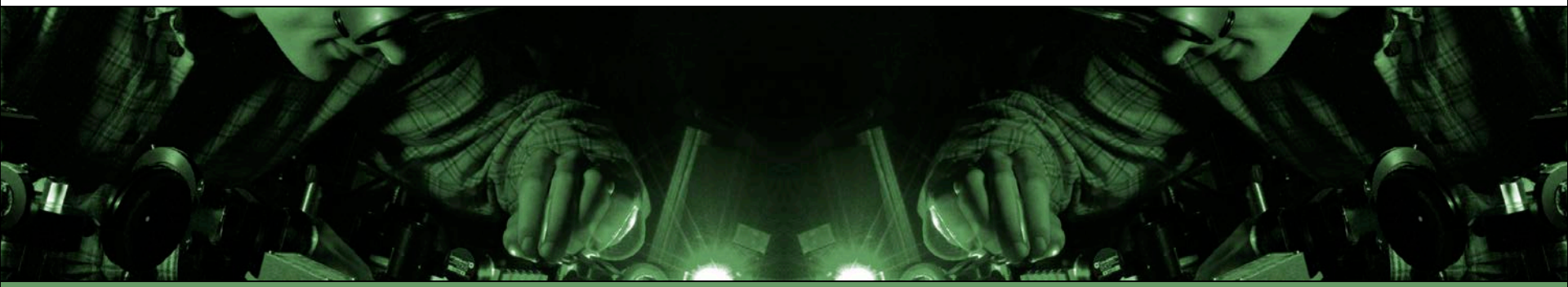


September 29, 2015

Ultrabroadband Quantum-Secured Communication

5th International Conference on Quantum Cryptography

Quntao Zhuang, Zheshen Zhang, Justin Dove, Franco N.C. Wong, and **Jeffrey H. Shapiro**

RESEARCH LABORATORY OF ELECTRONICS
Massachusetts Institute of Technology

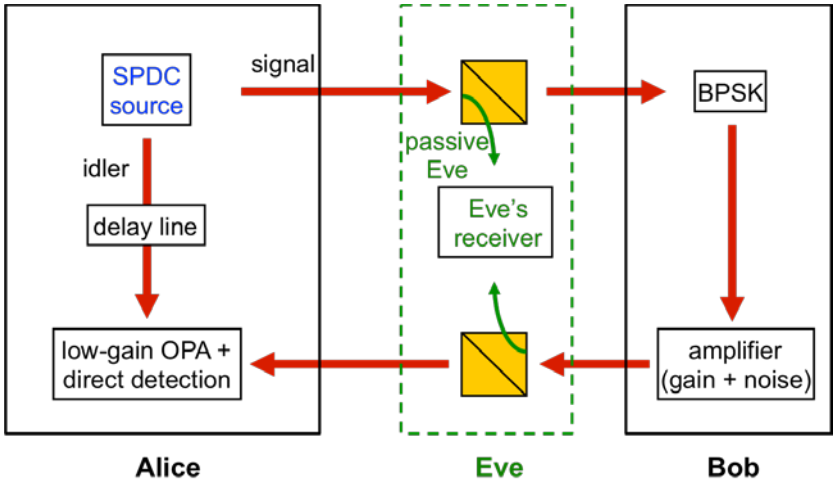
Optical and Quantum Communications Group
www.rle.mit.edu/qoptics

Ultrabroadband Quantum-Secured Communication

- Defeating passive eavesdropping with quantum illumination
  - security from entanglement on an entanglement-breaking channel
  - high secure rate from multiple modes per bit ➔ many photons per bit
  - weakness of the quantum illumination (QI) protocol: idler-storage loss
  - vulnerability of the QI protocol: active-eavesdropping attack
- Amplified spontaneous emission quantum communication
  - security from low-brightness signal transmission + no-cloning theorem
  - high secure rate from multiple modes per bit ➔ many photons per bit
  - high-brightness reference eliminates QI's idler-storage loss problem
  - entanglement-based channel monitoring defeats active eavesdropping
- Conclusions

Defeating Passive Eavesdropping with Quantum Illumination: Theory

- QI setup for immunity to passive eavesdropping



- Alice and Eve's Error Probabilities

Alice's best known receiver

$$\Pr(e)^{\text{OPA}}_{\text{Alice}} \sim \exp(-2W\kappa_S^3 G_B N_S / R N_B)/2$$

Eve's optimum quantum receiver

$$\Pr(e)^{\text{opt}}_{\text{Eve}} \sim \exp(-4W\kappa_S G_B N_S^2 / R N_B)/2$$

$N_S =$ Alice's SPDC signal brightness (photons/sec-Hz) $\ll 1$

$W =$ Alice's SPDC phase-matching bandwidth (Hz)

$\kappa_S =$ one-way channel transmissivity $\ll 1$

$G_B =$ Bob's amplifier gain $\gg 1$

$N_B =$ Bob's amplified spontaneous emission output-noise brightness $\gg 1$

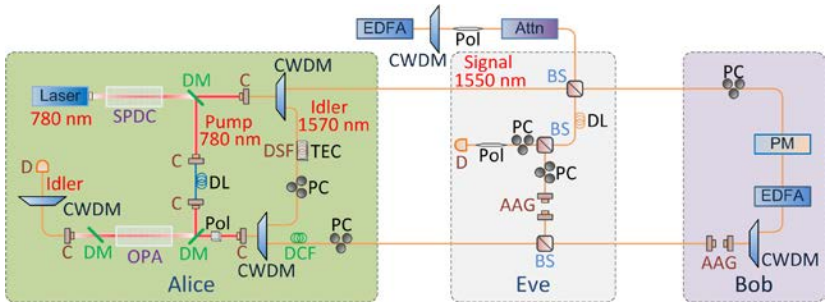
$R =$ Bob's BPSK bit rate

$W/R =$ modes per bit $\gg 1$

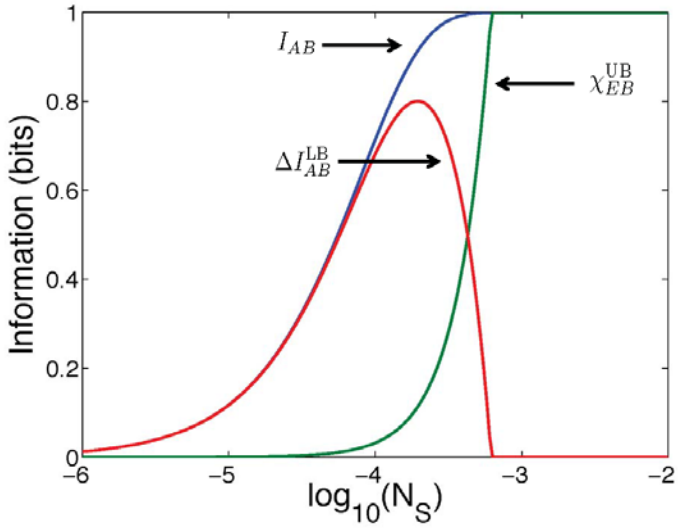
Shapiro, *Phys. Rev. A* **80,** 022320 (2009)

Defeating Passive Eavesdropping with Quantum Illumination: Proof-of-Principle Experiment

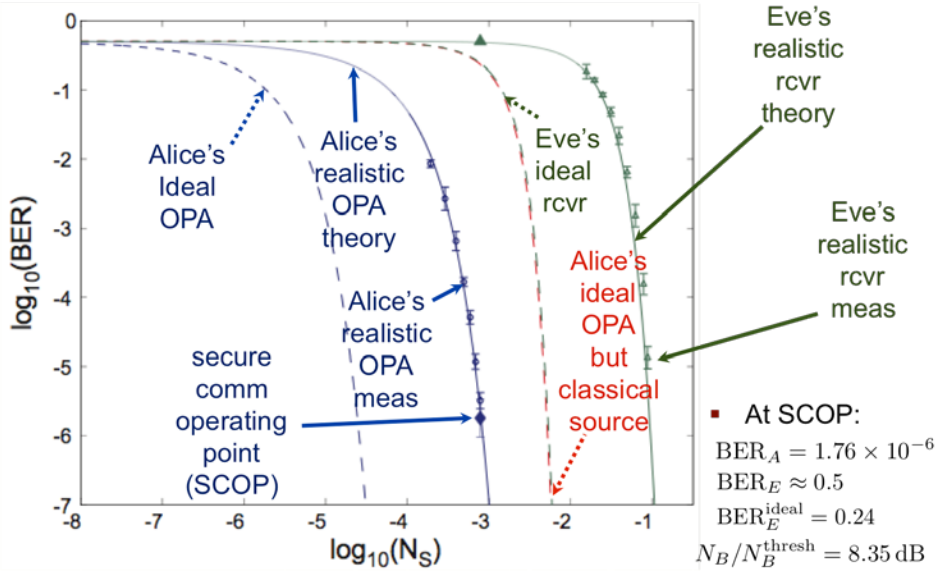
- QI experimental setup



- Alice and Bob's information advantage over Eve



- Alice versus Eve's Pr(e)'s

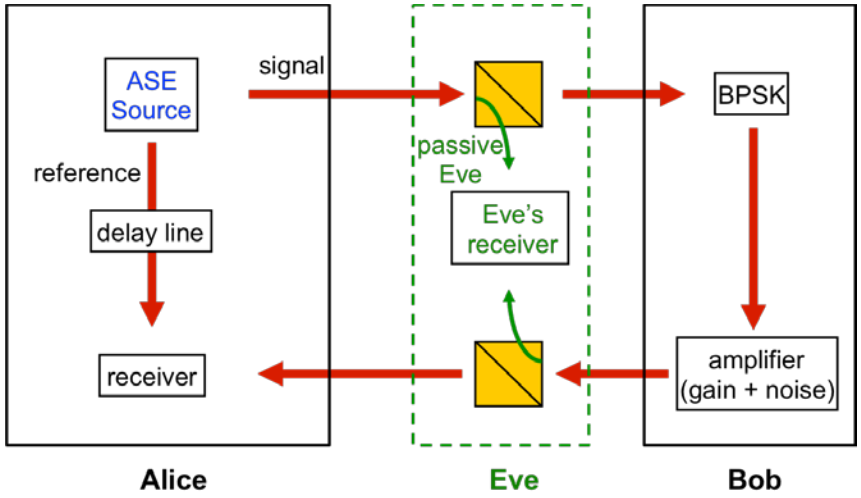


- *All* bits are received
  - direct communication possible
  - QKD possible
- Idler-storage loss a problem
- Active-eavesdropping a problem

Zhang, Tengner, Zhong, Wong, and Shapiro, *Phys. Rev. Lett*. **111,** 010501 (2013)

Defeating Passive Eavesdropping with Amplified Spontaneous Emission (ASE) + Homodyne Detection

- ASE-homodyne setup for passive eavesdropping immunity



- Alice and Eve's Error Probabilities

Alice's homodyne receiver

$$\Pr(e)^{\text{ASE}}_{\text{Alice}} \sim \exp(-W\kappa_S G_B N_S / R N_B)/2$$

Eve's optimum quantum receiver

$$\Pr(e)^{\text{Opt}}_{\text{Eve}} \sim \exp(-4W\kappa_S G_B N_S^2 / R N_B)/2$$

N_S = Alice's ASE signal brightness (photons/sec-Hz) $\ll 1$

W = Alice's ASE bandwidth (Hz)

κ_S = one-way channel transmissivity $\ll 1$

G_B = Bob's amplifier gain $\gg 1$

N_B = Bob's ASE output-noise brightness $\gg 1$

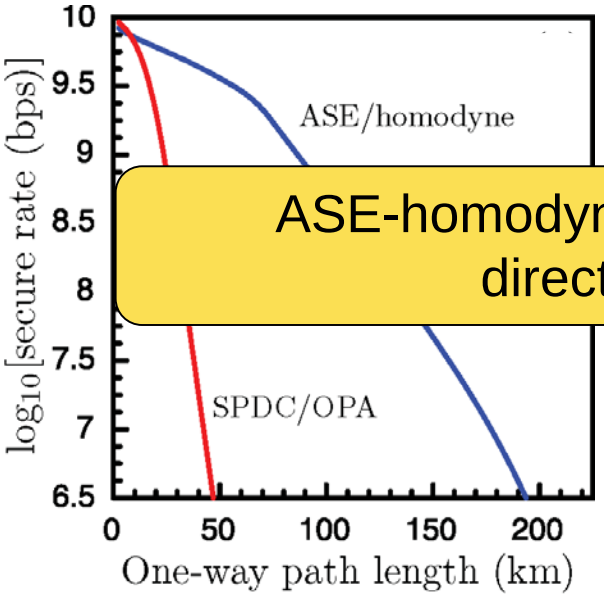
R = Bob's binary phase-shift keying bit rate

W/R = modes per bit $\gg 1$

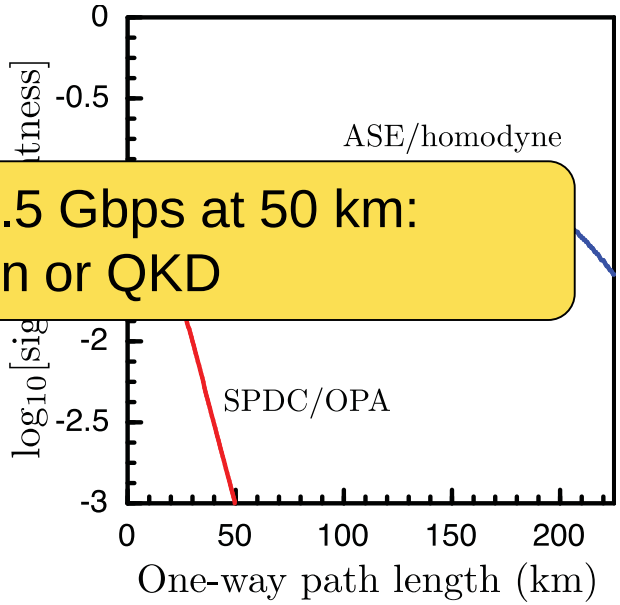
Zhuang, Zhang, Dove, Wong, and Shapiro, arXiv:1508.01471 [quant-ph]

Defeating Passive Eavesdropping: Quantum Illumination versus ASE-Homodyne

- Secure-rate comparison



- Optimum signal brightness



ASE-homodyne capable of 3.5 Gbps at 50 km: direct communication or QKD

N_S = Alice's SPDC and ASE signal brightness, chosen for maximum secure rate

W = Alice's SPDC and ASE bandwidth = 2 THz

κ_S = one-way channel transmissivity for 0.2 dB/km fiber

G_B = Bob's amplifier gain = 10^4

N_B = Bob's ASE output-noise brightness = 10^4

R = Bob's BPSK bit rate $\leq$ 10 Gbps, chosen for maximum secure rate with $\Pr(e)^{\text{ASE}}_{\text{Alice}} \leq 0.1$

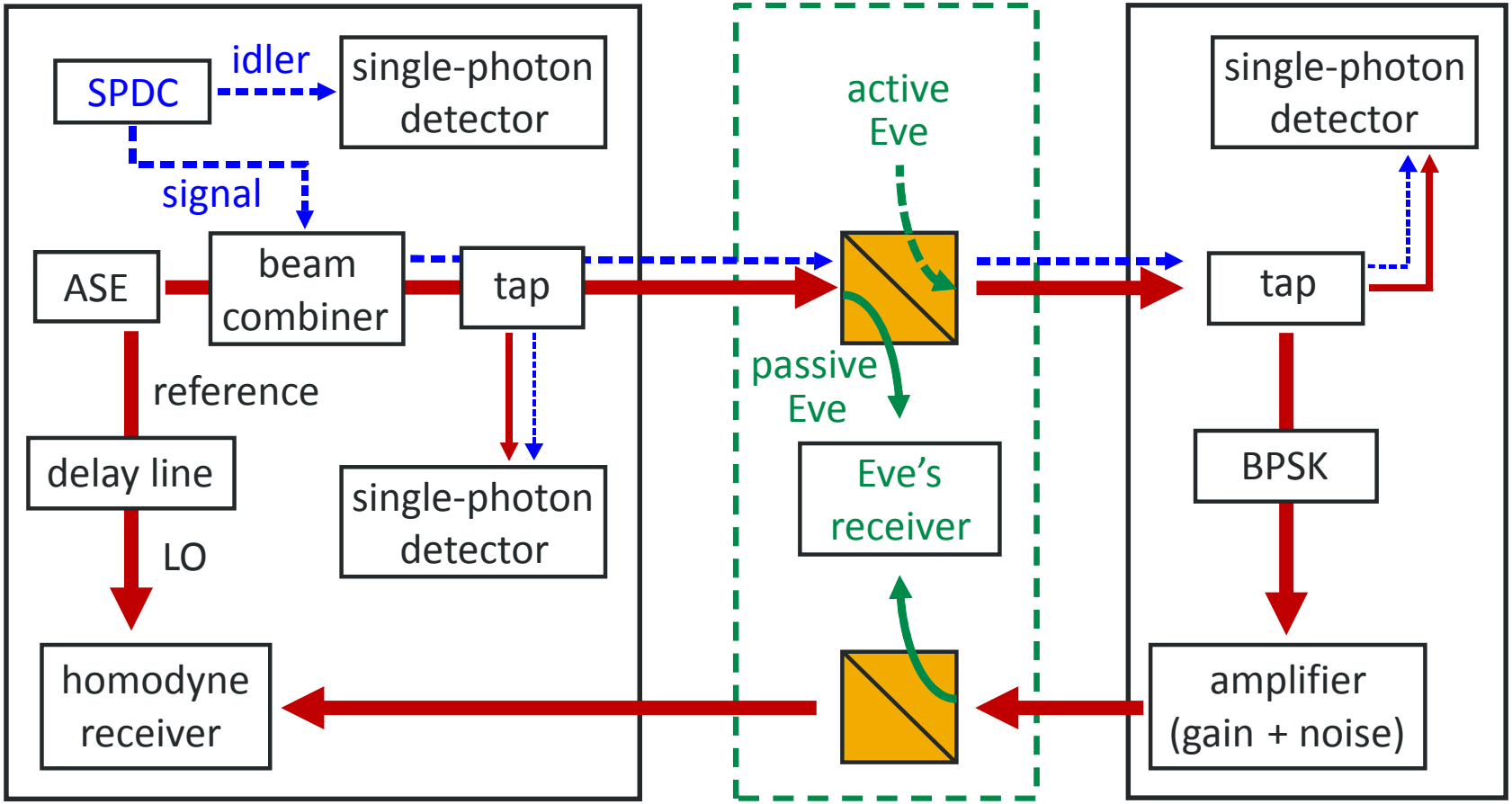
β = ASE-homodyne's reconciliation efficiency = 0.94

Zhuang, Zhang, Dove, Wong, and Shapiro, arXiv:1508.01471 [quant-ph]

Defeating Active Eavesdropping on ASE-Homodyne Communication using Channel Monitoring

Eve injects her own light (SPDC, optimally) to decode Bob's message

Active monitor of channel integrity:
inject SPDC light; measure singles and coincidences; Alice's reference tap



Bounding Eve's SPDC Injection

- Singles and coincidence rates

S_I = Alice's idler singles rate

S_A = Alice's signal-tap singles rate

S_B = Bob's signal-tap singles rate

C_{IA} = Alice's idler×signal coincidence rate

C_{IB} = Alice's idler × Bob's signal-tap coincidence rate

- Light injection fraction

$$f_E = \frac{\text{Eve's optical power into Bob}}{\text{total optical power into Bob}}$$

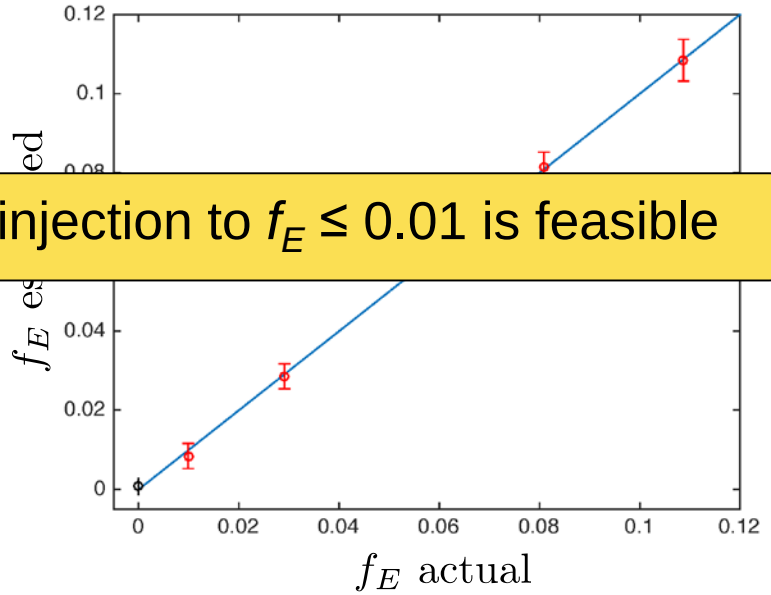
- Estimating f_E from these rates

$$\Delta C_{IA} = C_{IA} - S_I S_A T_g$$

$$\Delta C_{IB} = C_{IB} - S_I S_B T_g$$

T_g = coincidence gate (sec)

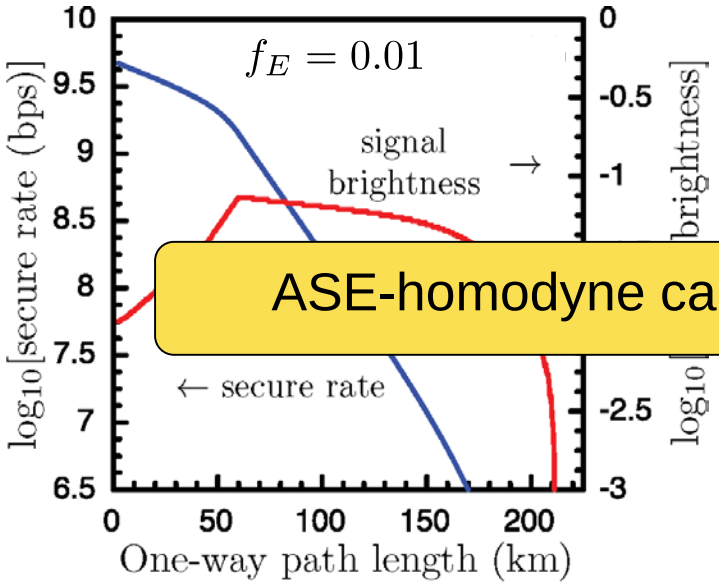
- Preliminary experiment



Channel monitoring to limit Eve's injection to $f_E \leq 0.01$ is feasible

ASE-Homodyne Quantum Key Distribution: Secure Rate versus a Collective Active Attack

- Secure rate and optimum source brightness



- Eve's beam-splitter active attack
  - SPDC is her optimum state for low-brightness injection
  - because Alice and Bob must verify $f_E \leq 0.01$ to ensure security level

ASE-homodyne capable of 2 Gbps QKD at 50 km

N_S = Alice's ASE signal brightness, chosen for maximum secure rate

W = Alice's ASE bandwidth = 2 THz

κ_S = one-way channel transmissivity for 0.2 dB/km fiber

G_B = Bob's amplifier gain = 10^4

N_B = Bob's ASE output-noise brightness = 10^4

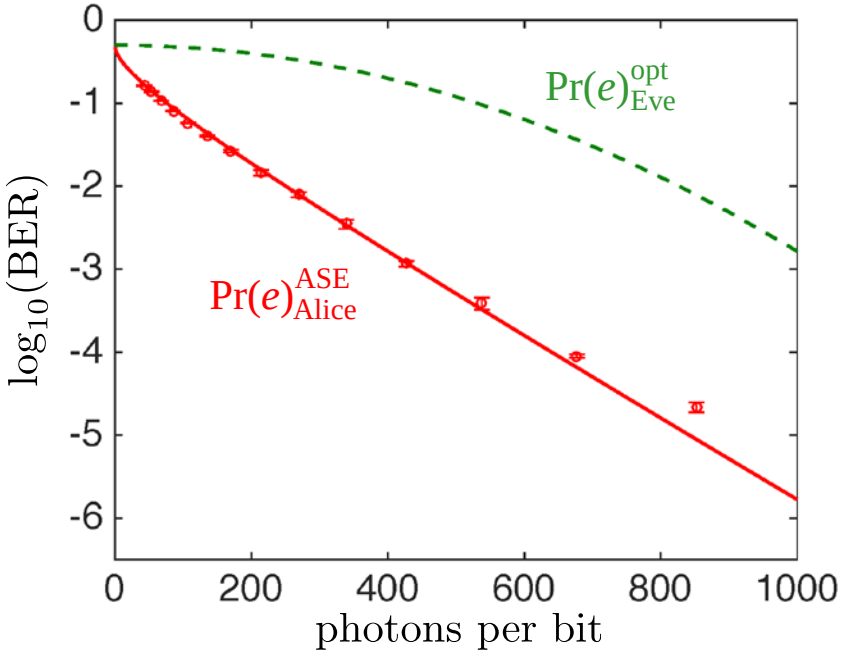
R = Bob's BPSK bit rate $\leq$ 10 Gbps, chosen for maximum secure rate with $\Pr(e)^{\text{ASE}}_{\text{Alice}} \leq 0.1$

β = ASE-homodyne's reconciliation efficiency = 0.94

Zhuang, Zhang, Dove, Wong, and Shapiro, arXiv:1508.01471 [quant-ph]

ASE Quantum-Secured Communication: Preliminary Experimental Result

- Preliminary experiment
  - passive individual attack



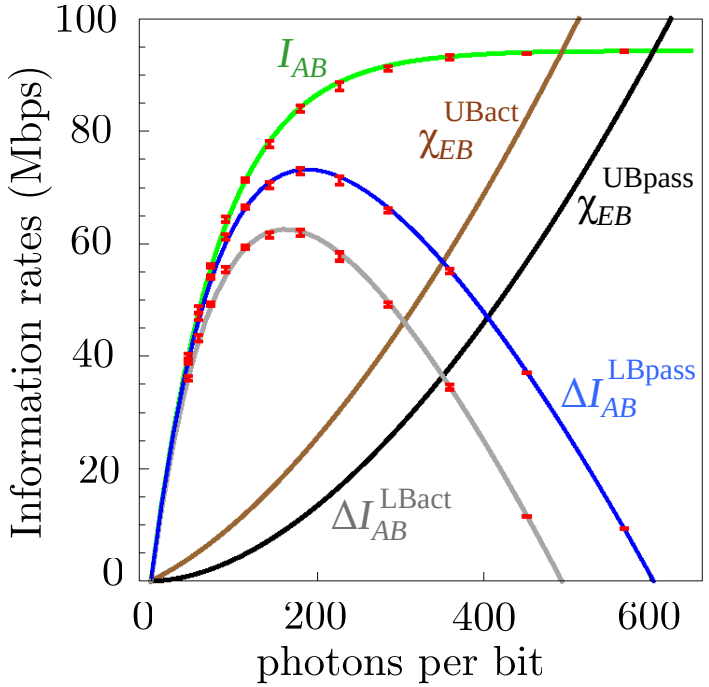
$W = 2\,\text{THz},\ \kappa_S = 0.1,\ R = 100\,\text{Mbps},$

$G_B \sim 10^4,\ N_B \sim 10^4,\ \text{estimated}\ f_E = 0.003$

$\text{Signal brightness} = 10^{-2}\ \text{at}\ 200\,\text{photons/bit}$

$\kappa_S = 0.1 \longleftrightarrow 50\,\text{km of fiber}$

- Predicted secure rates
  - passive or active collective attacks



- Passive attack
  - direct communication or QKD
- Active attack
  - QKD only

Conclusions

- Quantum-secured communication
  - low-brightness source provides security via no-cloning theorem
  - many modes/bit provides high rate via many photons/bit
- A
  - Alice's high-brightness reference for homodyne detection
  - Bo
  - Bo
- Passive attack
  - ASE-homodyne protocol can do direct communication and QKD
- Active attack
  - SPDC injection is optimal beam-splitter attack at low brightness
  - ASE-homodyne can only do QKD… *unless* Bob has quantum memory

ASE-homodyne capable of 3.5 Gbps at 50 km:
direct communication or QKD against passive eavesdropping

ASE-homodyne capable of 2 Gbps QKD at 50 km
against active eavesdropping

No new technology is needed to implement the ASE-homodyne protocol