Title: Entanglement-enhanced quantum sensing and quantum communication.

Date: Jan 10, 2018 04:00 PM

URL: http://pirsa.org/18010073

Abstract: (1) Entanglement-enhanced quantum sensing: parameter estimation and hypothesis testing.
(2) Security from entanglement: quantum key distribution.
(3) Entanglement enhanced communication: channel capacity and additivity issues.
(4) Some open problems.

rle MIT

Outline

- Entanglement-enhanced quantum sensing:
  Parameter estimation and hypothesis testing.
- Security from entanglement:
  Quantum key distribution.
- Entanglement enhanced communication:
  Channel capacity.
- Research proposals
  Resource theory, temperature estimation, quantum cryptography, quantum networks, quantum optics based computing

2

Quantum sensing

In collaboration with

Zheshen Zhang (now at U. of Arizona)

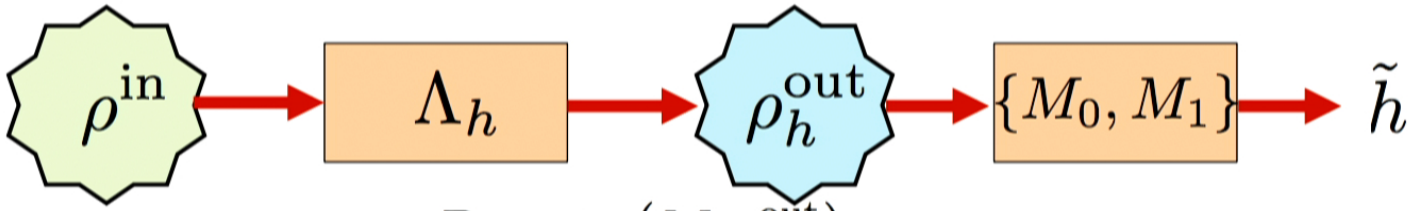
Jeffrey H. Shapiro

Zhuang *et al.*
Phys. Rev. Lett. **118**, 040801 (2017)
J. Opt. Soc. Am. B, **34**, 1567 (2017)
Phys. Rev. A **96**, 020302(R) (2017)
Phys. Rev. A **96**, 040304(R) (2017)
arXiv:1711.10459 [quant-ph] (2017)

rle MIT

Performance evaluation

- Hypothesis testing:

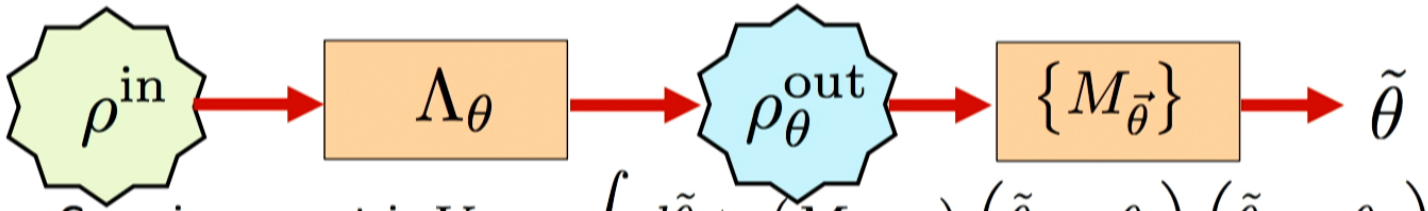


Detection prob.: $P_D = \text{tr}\left(M_1 \rho_1^{\text{out}}\right)$

False alarm prob.: $P_F = \text{tr}\left(M_1 \rho_0^{\text{out}}\right)$

Bayes: average error prob.: $P_E = P_1\left(1 - P_D\right) + P_0 P_F$

- Parameter estimation



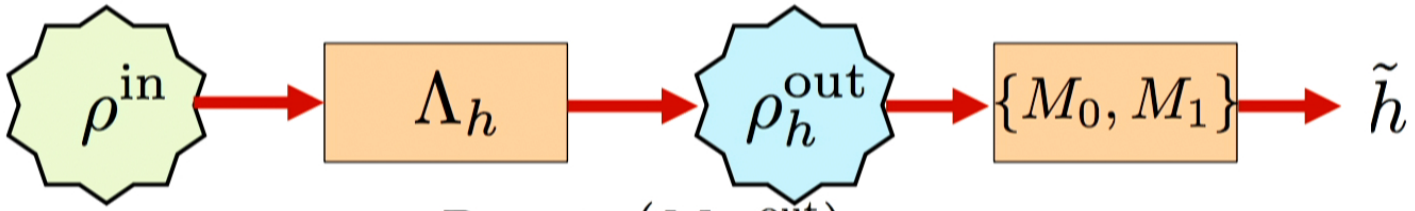
Covariance matrix: $V_{ij} = \int d\tilde{\theta}\ \text{tr}\left(M_{\tilde{\theta}}\ \rho_\theta\right)\left(\tilde{\theta}_i - \theta_i\right)\left(\tilde{\theta}_j - \theta_J\right)$

Penalty matrix: $G \geq 0$ Cost: $\text{tr}\left(GV\right)$

rle MIT

Performance evaluation

- Hypothesis testing:

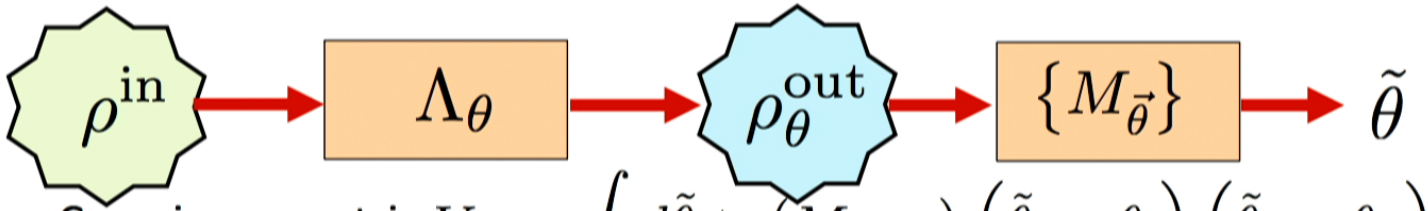


Detection prob.: $P_D = \text{tr}\left(M_1 \rho_1^{\text{out}}\right)$

False alarm prob.: $P_F = \text{tr}\left(M_1 \rho_0^{\text{out}}\right)$

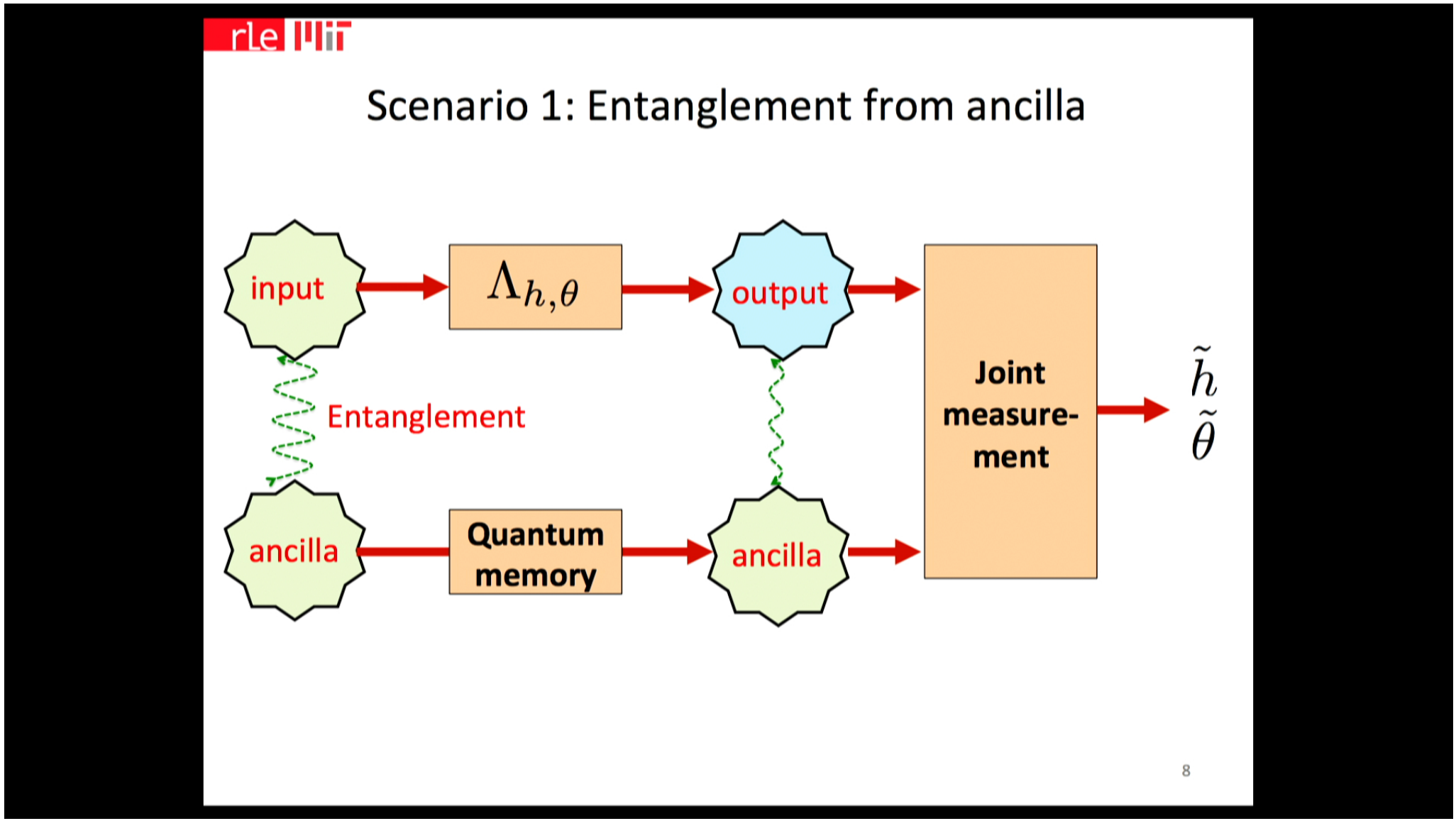
Bayes: average error prob.: $P_E = P_1\left(1 - P_D\right) + P_0 P_F$

- Parameter estimation



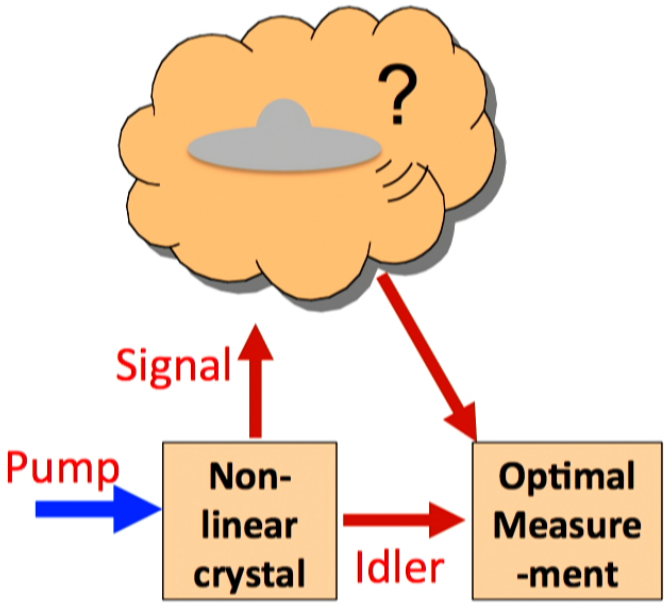
Covariance matrix: $V_{ij} = \int d\tilde{\theta}\ \text{tr}\left(M_{\tilde{\theta}}\ \rho_\theta\right)\left(\tilde{\theta}_i - \theta_i\right)\left(\tilde{\theta}_j - \theta_J\right)$

Penalty matrix: $G \geq 0$ Cost: $\text{tr}\left(GV\right)$

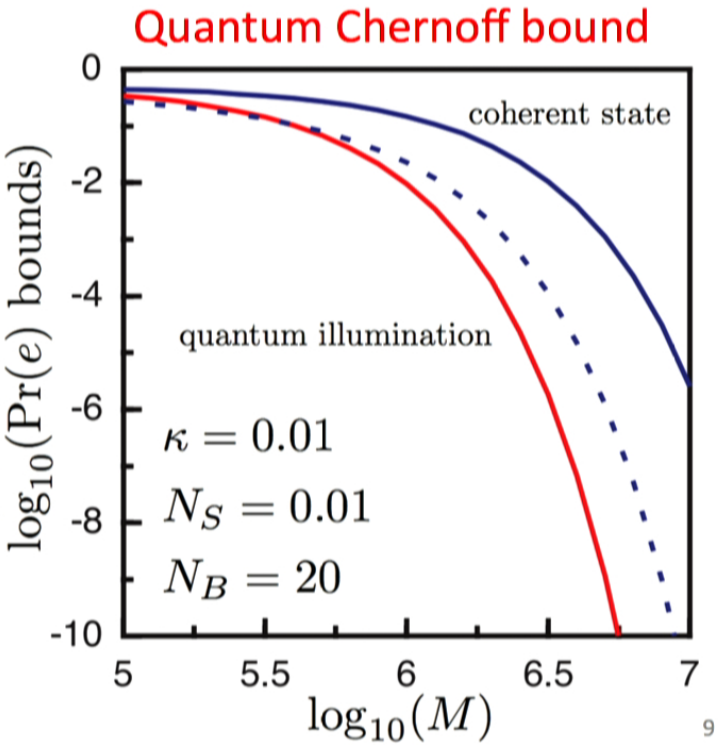

rle MIT
Scenario 1: Entanglement from ancilla
input
$\Lambda_{h,\theta}$
output
Joint measure-ment
$\tilde{h}$
$\tilde{\theta}$
Entanglement
ancilla
Quantum memory
ancilla
8

Example 1:quantum illumination (QI)

S. Lloyd, Science **321**, 1463 (2008)
Tan *et al.*, PRL **101**, 253601 (2008)

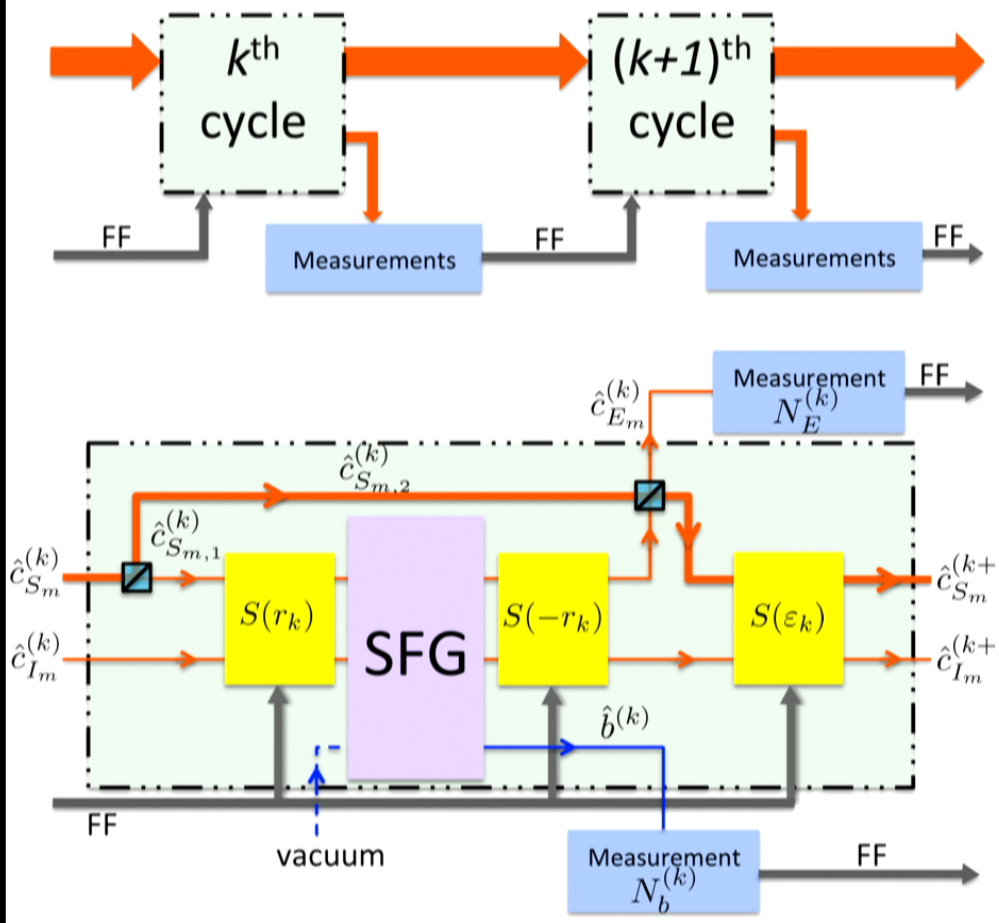


Assumption:
target reflectivity known,
phase known



Optimum receiver design for quantum illumination

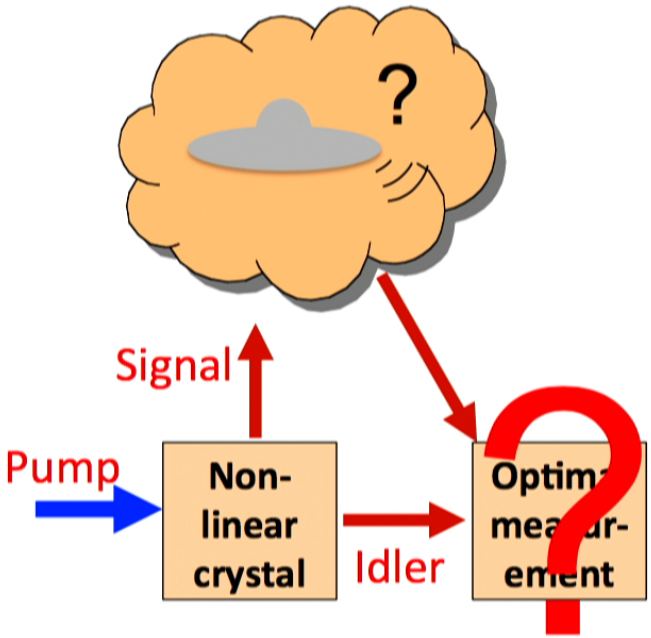
Zhuang *et al.* Phys. Rev. Lett. **118**, 040801 (2017)



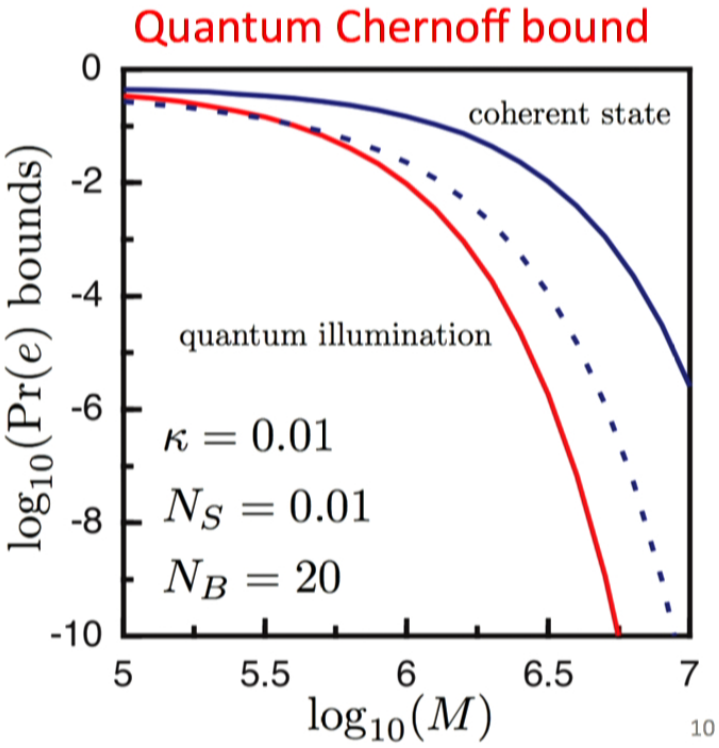
- Multiple cycle process enhanced by a Bayesian feed-forward scheme
- Key component: sum-frequency-generation process (SFG): convert correlation to displacement of the sum mode
- Analogy to Dolinar reciever for coherent state discrimination
- Monte-Carlo simulation confirms it's optimum

Example 1:quantum illumination (QI)

S. Lloyd, Science **321**, 1463 (2008)
Tan *et al.*, PRL **101**, 253601 (2008)

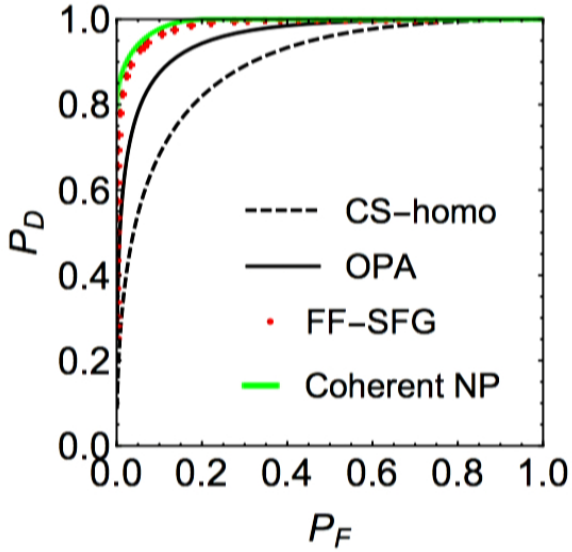


Assumption:
target reflectivity known,
phase known



Neyman-Pearson criterion

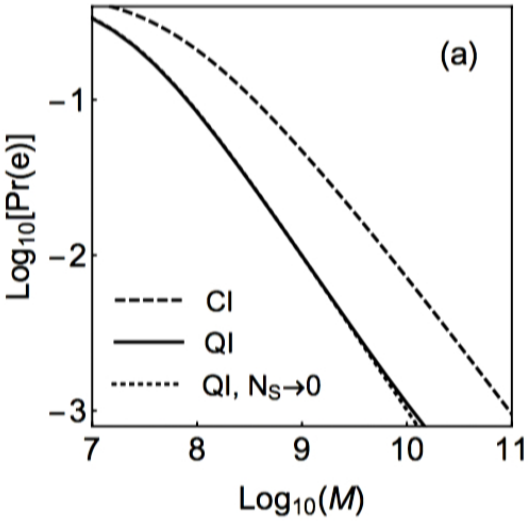
Beyond Bayesian point of view



Zhuang *et al.* J. Opt. Soc. Am. B, **34**, 1567 (2017)

Target fading

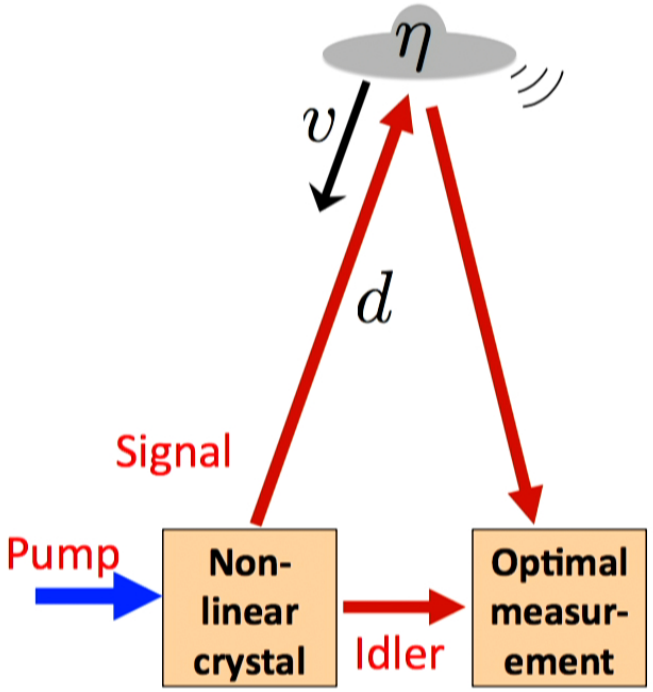
When target is present, reflectivity and return phase obey certain prior distribution



Zhuang *et al.* Phys. Rev. A **96**, 020302(R) (2017)

Example 2: simultaneous precise measurement of velocity and distance

Zhuang *et al.* Phys. Rev. A **96**, 040304(R) (2017)



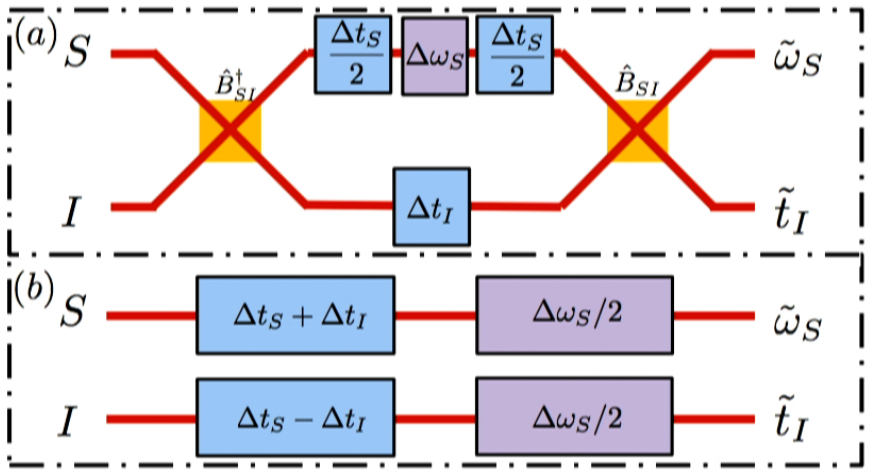
Doppler shift: $v \rightarrow \Delta\omega$

Time-delay: $d \rightarrow \Delta t$

Difficulty:
the generators of two parameters do not commute

Arthurs-Kelly uncertainty relation $\delta\omega\delta t \geq 1$

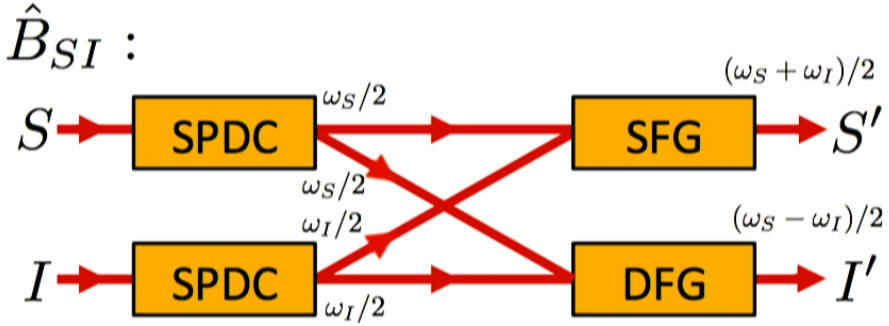
Example 2: simultaneous precise measurement of velocity and distance



Analog to continuous-variable superdense-coding

Reduce number of signal photons

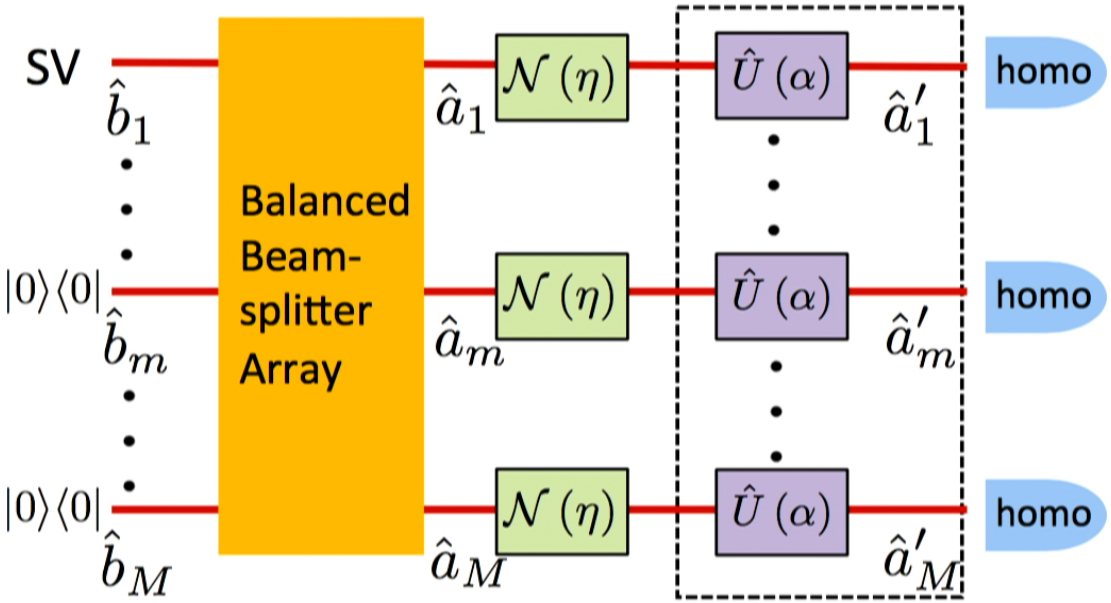
$$2/\eta \rightarrow 1/\eta$$



Zhuang *et al.* Phys. Rev. A **96**, 040304(R) (2017)

Example: Distributed Quantum Sensing Using Continuous-Variable Multipartite Entanglement

Zhuang *et al.* arXiv:1711.10459 [quant-ph] (2017)



Heisenberg scaling measurement of quadrature displacement
with only basic components in linear optics!

16

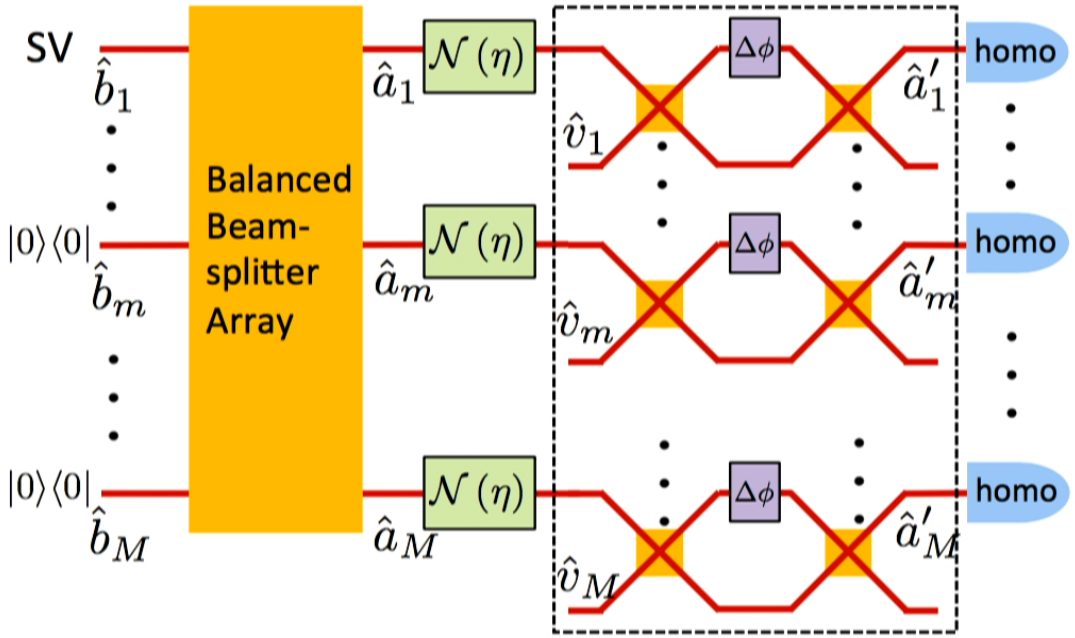
Example: Distributed Quantum Sensing Using Continuous-Variable Multipartite Entanglement

Zhuang *et al.* arXiv:1711.10459 [quant-ph] (2017)

Applications: joint calibration of CV-QKD Grosshans *et al.* Phys. Rev. Lett. 88,057902 (2002).

spin angular momentum measurement in cold-atom systems Eckert *et al.* Nat. Phys. 4, 50 (2008)

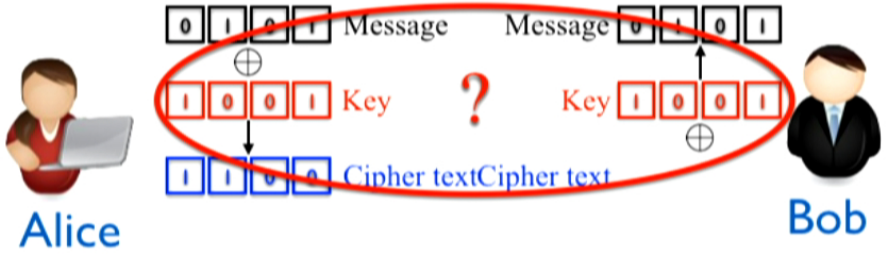
Interferometric phase sensing (LIGO) Demkowicz-Dobrzański *et al.*, Phys. Rev. A 88, 041802 (2013)



17

Quantum key distribution (QKD)

- Aim: to share secret-key for future use in one-time-pad encryption.



One-time pad allows unconditional security
but how do Alice and Bob share a long key?

- Quantum key distribution solves the issue, e.g. BB84 GG02

Bennetta and Brassard, 1984
Grosshans and Grangier, PRL **88,** 057902 (2002)

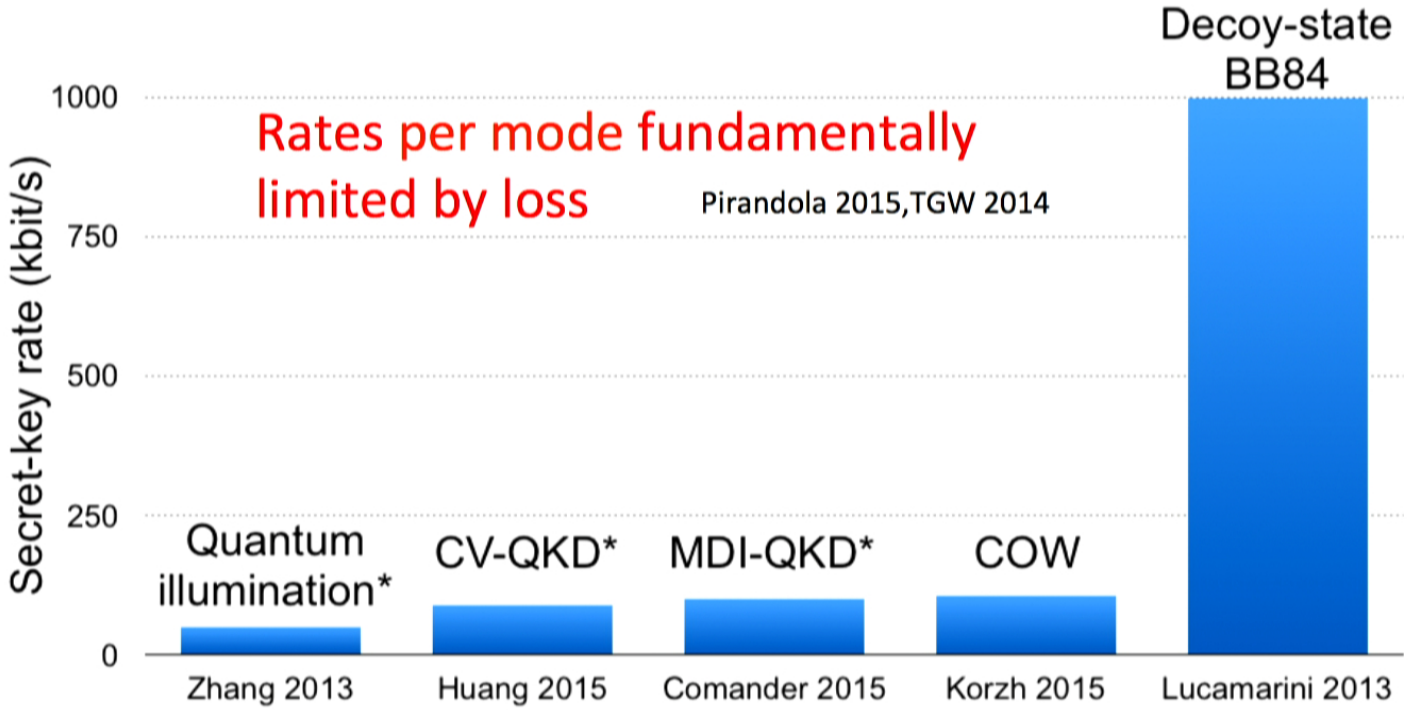
Quantum key distribution (QKD)

- Figure of merit: secret key rate (asymptotic)

$$r = R \max\left[\xi I_{AB} - I_E, 0\right]$$ Devetak and Winter, 2004

  - I_{AB} : Alice and Bob's mutual information
  - I_E : Eve's information gain
  - ξ : Error correction efficiency
  - R : modulation rate
- Important task: obtain upper bounds on I_E

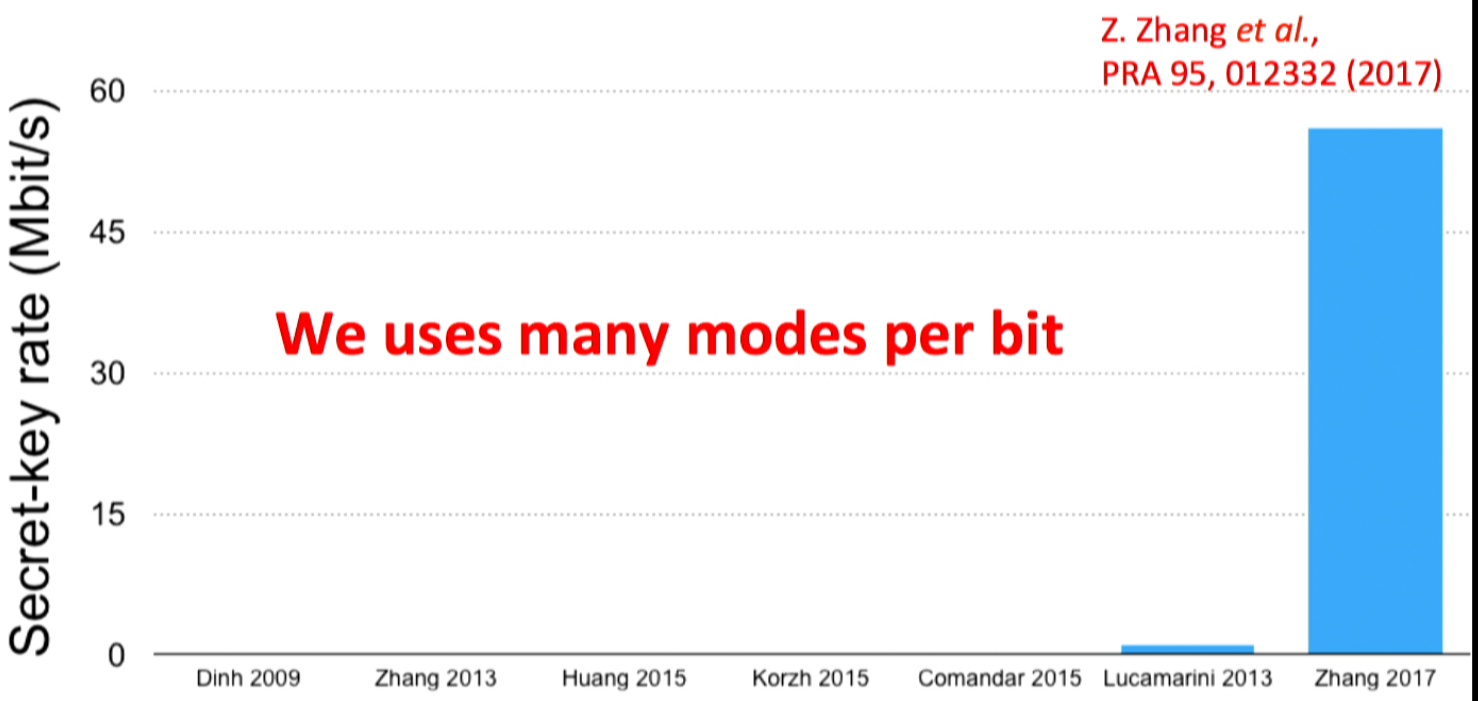
QKD secret-key rates for 10 dB propagation loss



1. Z. Zhang *et al.*, Phys. Rev. Lett. **111**, 010501 (2013)
2. D. Huang *et al.*, Opt. Express **23**, 17511 (2015)
3. L.C. Comandar *et al.*, Nature Photon. **10**, 312 (2016)
4. B. Korzh *et al.*, Nature Photon. **9**, 163 (2015)
5. M. Lucamarini *et al.*, Opt. Express **21**, 24550 (2013)

* rates scaled to 10 dB loss

QKD secret-key rates for 10 dB propagation loss



1. Z. Zhang *et al.*, Phys. Rev. Lett. **111**, 010501 (2013)
2. D. Huang *et al.*, Opt. Express **23**, 17511 (2015)
3. L.C. Comandar *et al.*, Nature Photon. **10**, 312 (2016)
4. B. Korzh *et al.*, Nature Photon. **9**, 163 (2015)
5. M. Lucamarini *et al.*, Opt. Express **21**, 24550 (2013)

Floodlight QKD

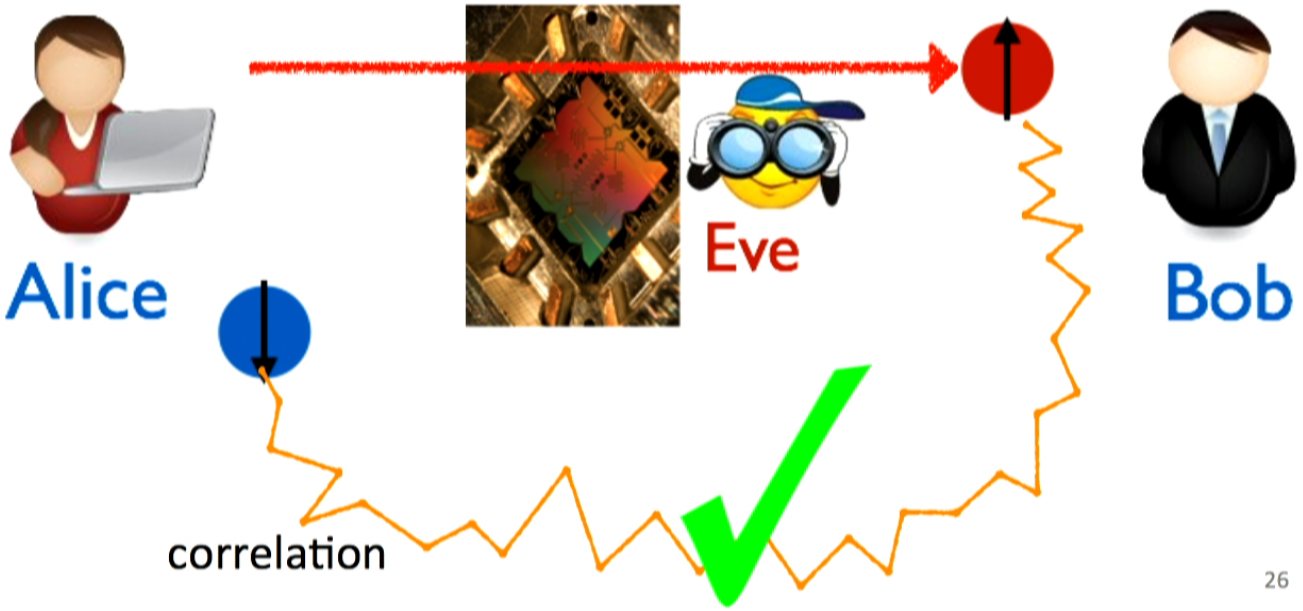
- Typical two-way protocols:

e.g. ping-pong Bostroem *et.al.*, PRL **89**, 187902 (2002)
two-way CV Pirandola *et.al.*, Nat. Phys. **4**, 726 (2008)
Floodlight-QKD Zhuang *et.al.*, PRA **94**, 012322 (2016)

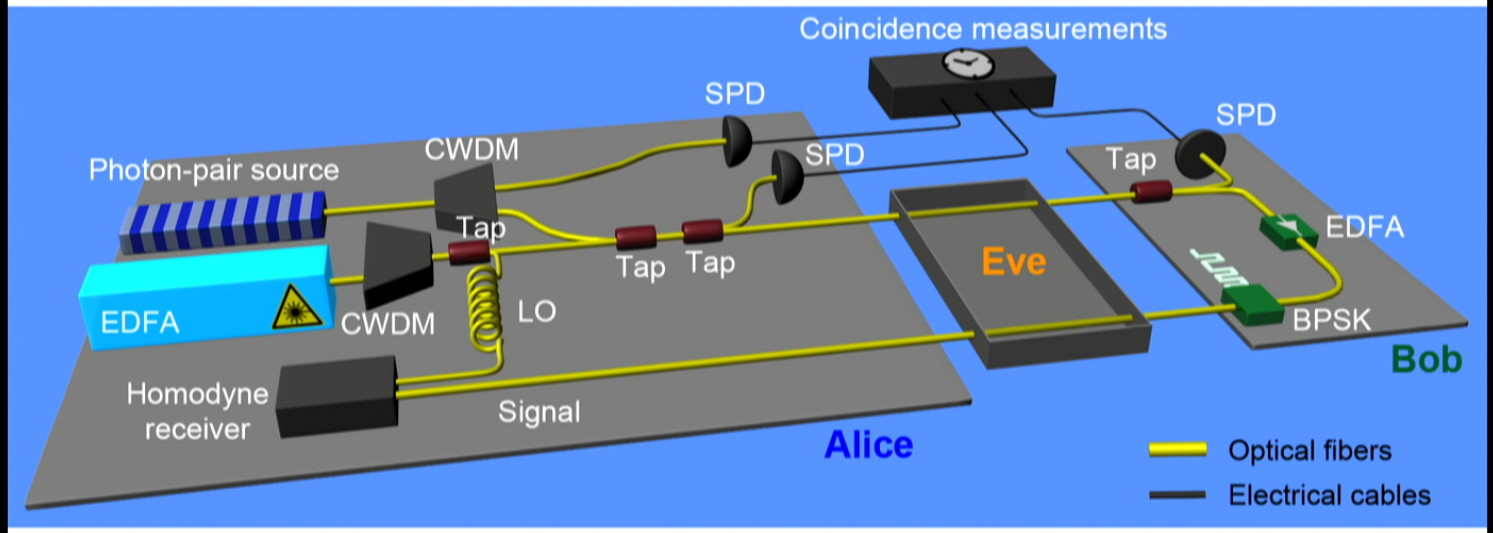
Floodlight QKD

- Typical two-way protocols:

e.g. ping-pong Bostroem *et.al.*, PRL **89**, 187902 (2002)
two-way CV Pirandola *et.al.*, Nat. Phys. **4**, 726 (2008)
Floodlight-QKD Zhuang *et.al.*, PRA **94**, 012322 (2016)



Floodlight QKD-experiment



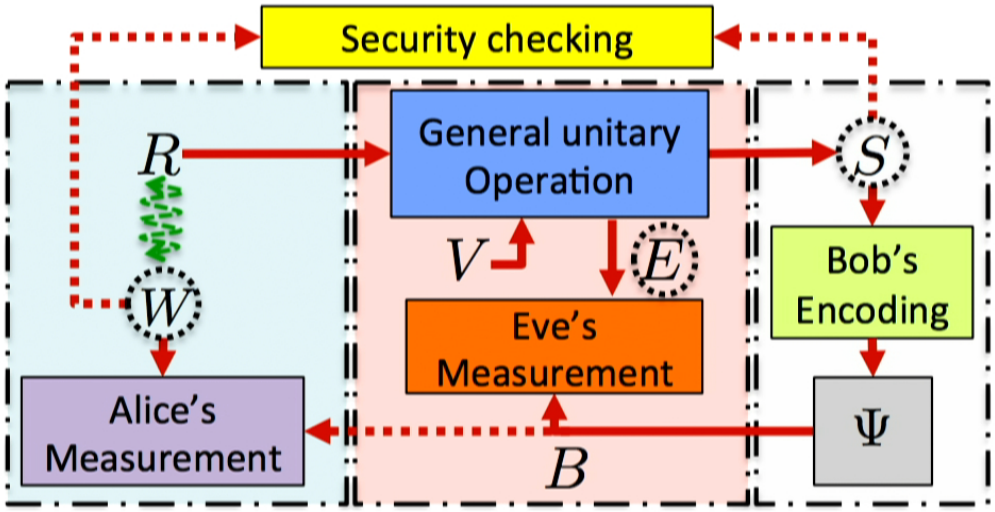
Zhang *et.al.*, Phys. Rev. A **95**, 012332 (2017).

Zhang *et.al.*, arXiv:1712.04973 (2017) posted last week

Gbps secret-key rate achieved at 10dB one-way loss!

29

Security proof of two-way QKD protocols from limited noisy entanglement assisted classical capacity



$$I_E \leq \chi_L$$

Zhuang *et al.*, PRL **118**, 200503 (2017)

Additivity of the capacity formula implies:

- Collective attack is most powerful for two-way QKD protocols.
- Gaussian protocol: collective Gaussian attack is most powerful.

Apply to various two-way QKD protocols.

Zhuang *et al.*, arXiv:1704.08169 (full paper in preparation)

Quantum key distribution

- Floodlight QKD protocol---Gbps secret rate at metropolitan distance
- Security framework for two-way protocols

Zhuang *et.al.*,
PRA **94**, 012322 (2016)
arXiv:1702.02424 (2017)
arXiv:1704.08169 (2017)

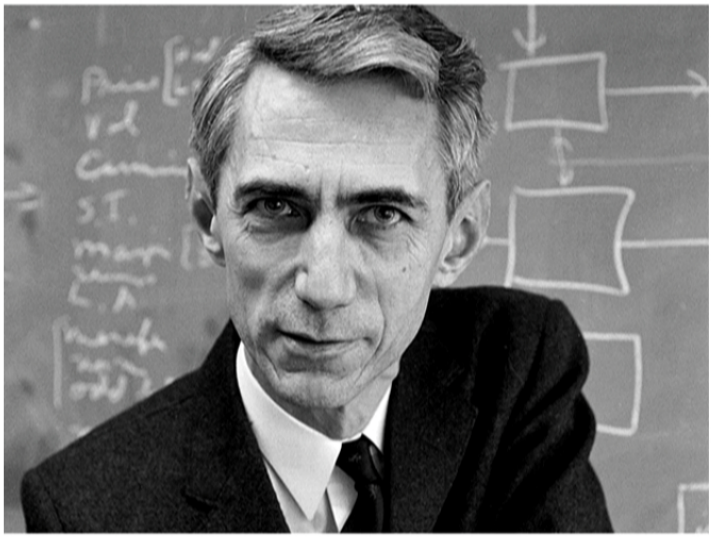
Zhang *et.al.*,
Phys. Rev. A 95, 012332 (2017)
arXiv:1712.04973 (2017)

Shannon, Claude E. "A mathematical theory of communication.", 1948

- Channel: model the information transmission media

$$X \rightarrow Y \qquad P_{Y|X}$$

- Robust classical communication is possible when there is noise and loss in the channel, but below the capacity



$$\chi = \max_{P_X} I(X:Y)$$

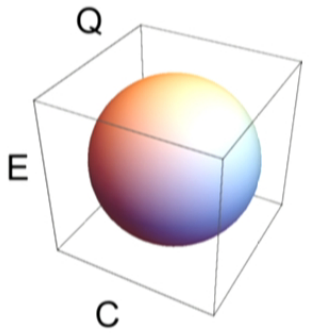
Capacities of quantum channels

- CQE capacity region

$$\mathcal{C}_{\mathrm{CQE}}(\mathcal{N}) = \overline{\bigcup_{k=1}^{\infty} \frac{1}{k} \mathcal{C}^{(1)}_{\mathrm{CQE}}(\mathcal{N}^{\otimes k})},$$

$$\mathcal{C}^{(1)}_{\mathrm{CQE}}(\mathcal{N}) \equiv \bigcup_{\sigma} \mathcal{C}^{(1)}_{\mathrm{CQE},\sigma}(\mathcal{N}).$$

Wilde and Hsieh, QIP **11** 1431 (2012)



$$C + 2Q \leq I(AX;B)_\sigma,$$
$$Q + E \leq I(A\rangle BX)_\sigma,$$
$$C + Q + E \leq I(X;B)_\sigma + I(A\rangle BX)_\sigma.$$
$$\sigma^{XAB} \equiv \sum_x p(x) |x\rangle\langle x|^X \otimes \mathcal{N}^{A'\to B}(\phi_x^{AA'}),$$

- Sub-regions
  - Classical capacity C ; $Q = E = 0$
  - Quantum capacity Q ; $C = E = 0$
  - (unlimited) Entanglement assisted classical capacity C_E ; $Q = 0$
  - Limited pure entanglement assisted classical capacity (C, E); $Q = 0$

Holevo 97, Schumacher, and Westmoreland 98

Lloyd 97, Shor 02, and Devetak 05

Bennett, Shor, Smolin and Thapliyal 99, 02

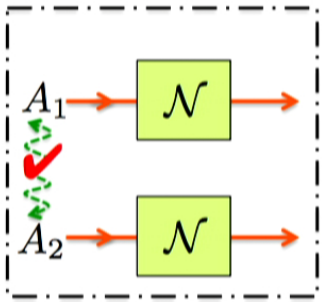
Shor, 2004

Devetak and Shor, 2004

Issue of additivity

(a) Superadditive

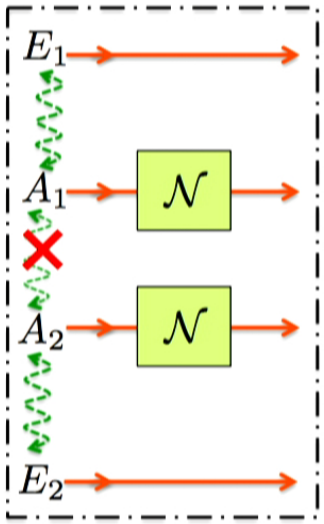
C can be superadditive



Hasting 09, Hayden 08, Shor 04

(b) Additive

C_E is always additive

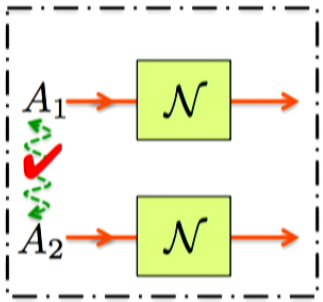


Bennett, Shor, Smolin and Thapliyal 99, 02
Adami and Cerf, 1997

Issue of additivity

(a) Superadditive

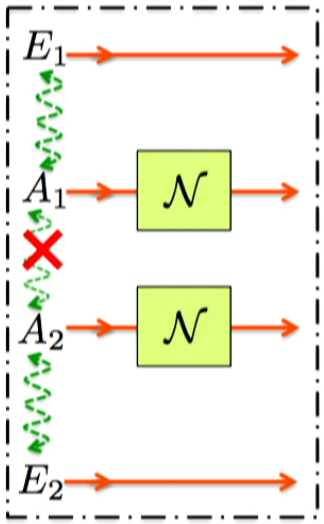
C can be superadditive



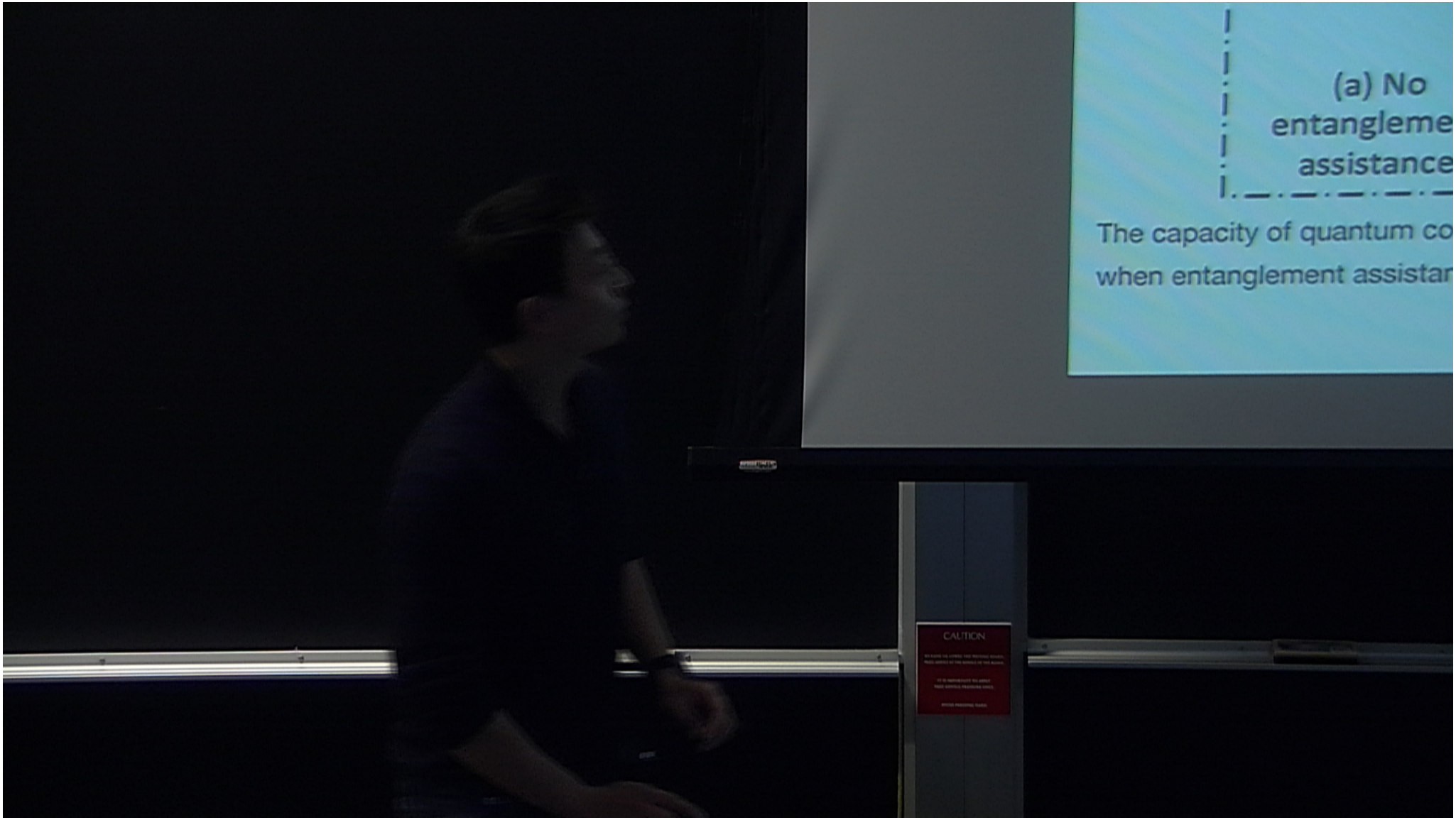
Hasting 09, Hayden 08, Shor 04

(b) Additive

C_E is always additive



Bennett, Shor, Smolin and Thapliyal 99, 02
Adami and Cerf, 1997


(a) No
entanglemen
assistance
The capacity of quantum co
when entanglement assistan
CAUTION

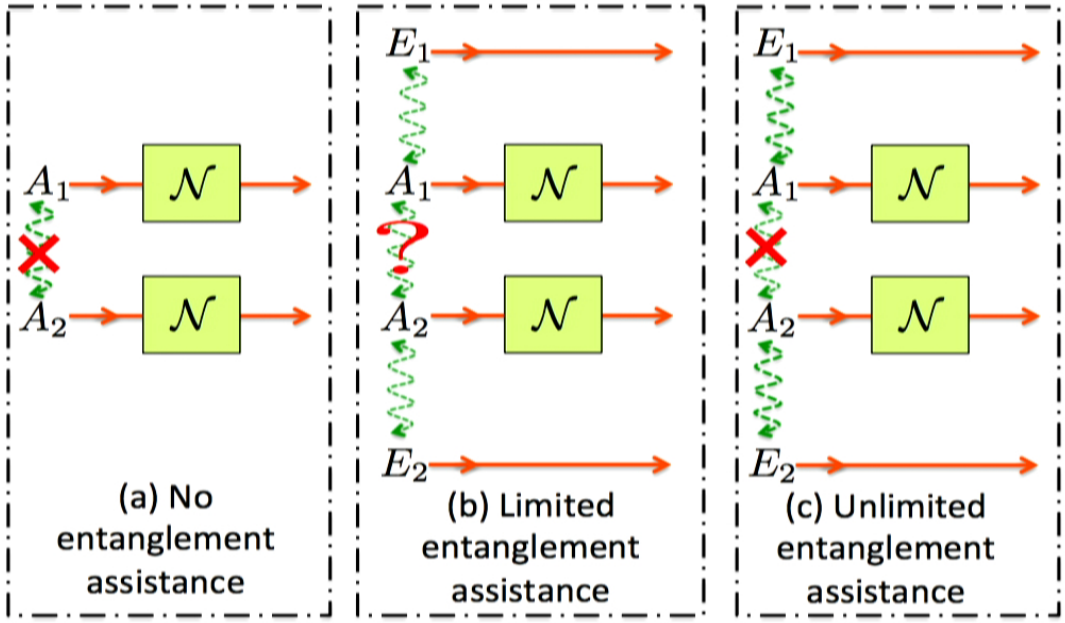
rle MIT

Editors' Suggestion

Superadditivity of the Classical Capacity with Limited Entanglement Assistance

Elton Yechao Zhu, Quntao Zhuang, and Peter W. Shor

Phys. Rev. Lett. **119**, 040503 (2017) – Published 27 July 2017



The capacity of quantum communication channels is predicted to switch from additive to superadditive when entanglement assistance is limited.

37

rle MIT

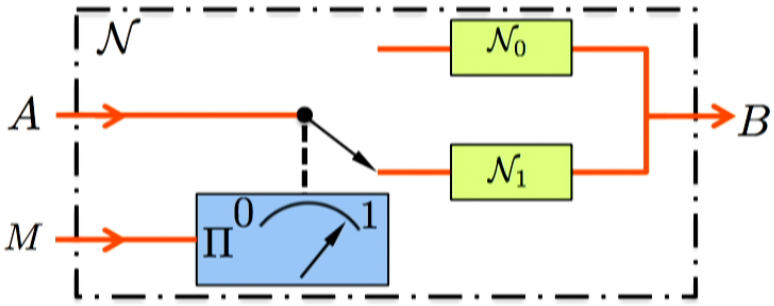
Editors' Suggestion

Superadditivity of the Classical Capacity with Limited Entanglement Assistance

Elton Yechao Zhu, Quntao Zhuang, and Peter W. Shor

Phys. Rev. Lett. **119**, 040503 (2017) – Published 27 July 2017

Construction: switch channel



- Channel $\mathcal{N}_0$ is a classical channel
- Channel $\mathcal{N}_1$ is a random unitary channel constructed by Hastings
- Extensions to other trade-offs: Zhu, Zhuang, Hsieh, and Shor, arXiv: 1708.04314 (2017)

rle MIT

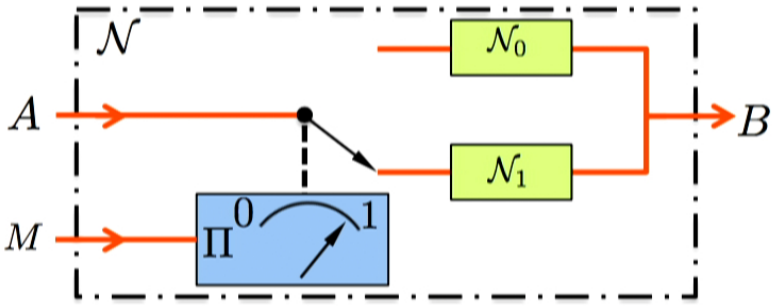
Editors' Suggestion

Superadditivity of the Classical Capacity with Limited Entanglement Assistance

Elton Yechao Zhu, Quntao Zhuang, and Peter W. Shor

Phys. Rev. Lett. **119**, 040503 (2017) – Published 27 July 2017

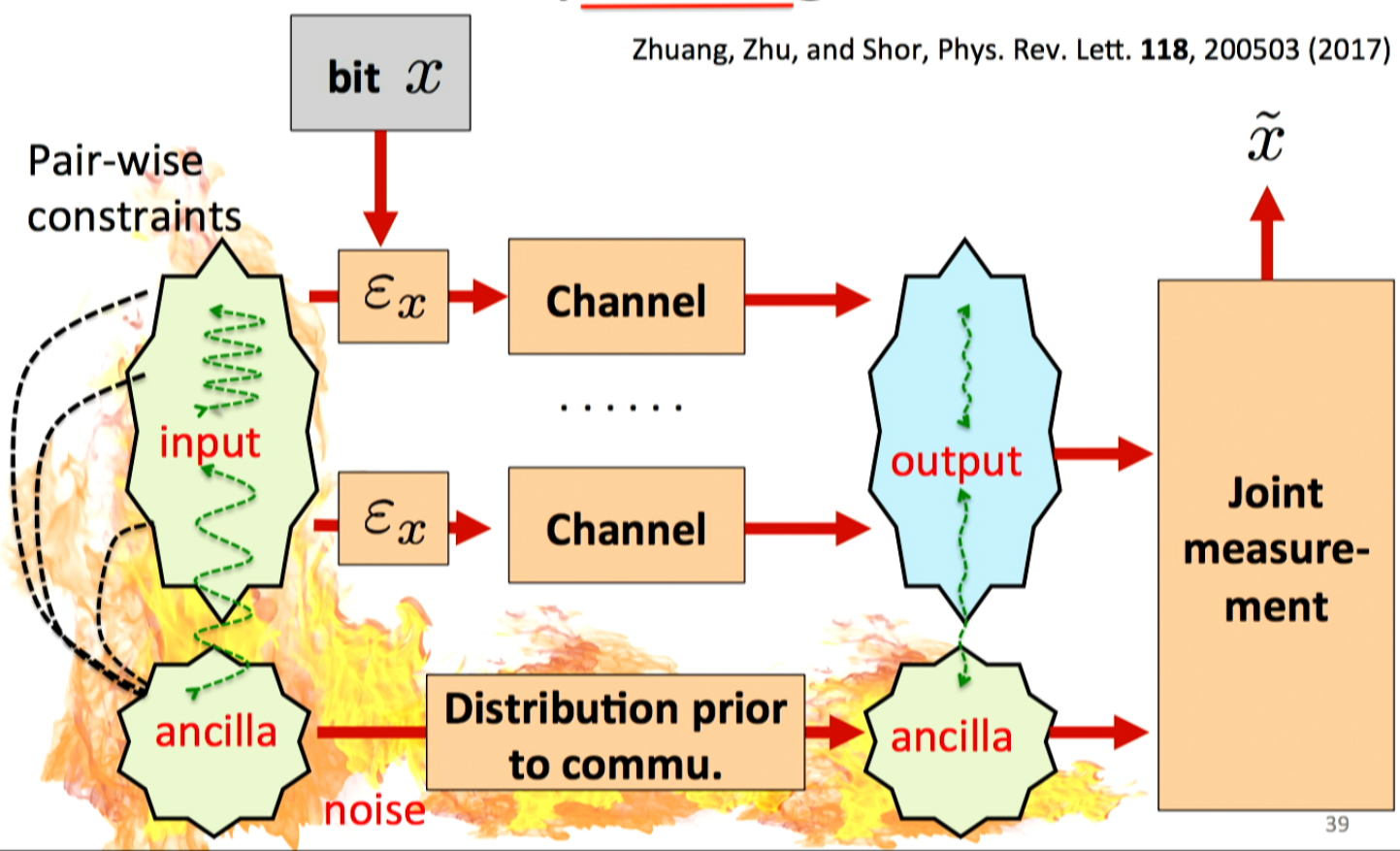
Construction: switch channel



- Channel $\mathcal{N}_0$ is a classical channel
- Channel $\mathcal{N}_1$ is a random unitary channel constructed by Hastings
- Extensions to other trade-offs: Zhu, Zhuang, Hsieh, and Shor, arXiv: 1708.04314 (2017)

An additive classical capacity assisted by noisy entanglement

Zhuang, Zhu, and Shor, Phys. Rev. Lett. **118**, 200503 (2017)



Information theory-entanglement enhanced communication

- Entanglement assists classical communication in a weird way---superadditivity

- Additive classical capacity assisted by noisy entanglement, with applications in quantum key distributions

Zhuang, Zhu, and Shor Phys. Rev. Lett. **118**, 200503 (2017)

Zhu, Zhuang, and Shor, Phys. Rev. Lett. **119**, 040503 (2017)

Zhu, Zhuang, Hsieh, and Shor, arXiv: 1708.04314 (2017)

Information theory-entanglement enhanced communication

- Entanglement assists classical communication in a weird way---superadditivity

- Additive classical capacity assisted by noisy entanglement, with applications in quantum key distributions

Zhuang, Zhu, and Shor Phys. Rev. Lett. **118**, 200503 (2017)

Zhu, Zhuang, and Shor, Phys. Rev. Lett. **119**, 040503 (2017)

Zhu, Zhuang, Hsieh, and Shor, arXiv: 1708.04314 (2017)

Quantum sensing in many-body systems

- Why interesting?
  - Nanoscale systems are being engineered, need to measure their properties precisely.
  - Important for quantum information processing, e.g. quantum simulation
- Example
  - Temperature estimation of a few-body systems in Gibbs state

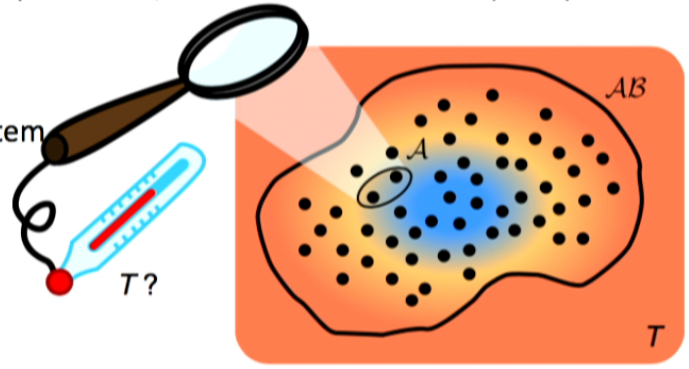
Global $\frac{\delta T}{T} \geq \frac{1}{\sqrt{C(T)}}$ Correa *et al.*, Phys. Rev. Lett. **114**, 220405 (2015)

Local thermal susceptibility:
Only measure part of the system

Pasquale *et al.*, Nat. Commun. **7** 12782 (2016)

LOCC thermal susceptibility:
Multiple local measurements on the system

Realization in NV centers?



Quantum cryptography

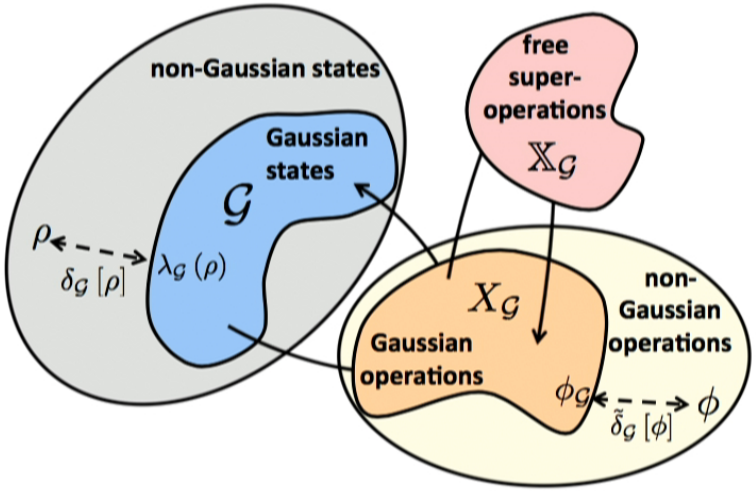
- Security proof and designing new protocols
  - Commercial fiber communication is at Gbps secret key rate, while mature QKD protocols at metropolitan distances has relatively low rate.
  - Floodlight QKD has Gbps rate, but for now only against collective attacks
- Composable security against coherent attack for two-way protocols
  - Parameter estimation?
  - One-way CV-QKD protocol examples:

Leverrier, Phys. Rev. Lett. 118, 200501 (2017)

Understanding non-Gaussianity

Zhuang, Shapiro, and Shor, in preparation

- Why interesting?
  - Linear optics implements Gaussian operations and uses Gaussian states
  - Gaussian states and operations are limited in power
    - Not universal for quantum computation
    - Cannot perform entanglement distillations, error corrections. Etc.
- How to understand non-Gaussianity
  - Resource theory point of view



- Free states: Gaussian states
- Free operations: Gaussian operations
- Monotone:
  non-Gaussianity generating power
- Resource state: non-Gaussian state
- Resource operation:
  non-Gaussian operation

Photonic based quantum computation

- Why photons?
  - Long room temperature coherence time, high transmission speed, high fidelity preparation schemes, efficient photon detectors.

- Different approaches
  - Linear optical quantum computing: post-selection enabled non-linearity. However, probabilistic. Knill *et al.*, Nature (London) **409**, 46 (2001).
  - $\chi^{(2)}$ interaction. Requires high efficiency interaction. Niu *et al.*, arXiv:1704.03431 (2017)
  - Time-delayed feedback: atom mediated photon interaction.

Pichler *et al.*, PNAS 201711003 (2017)