Photonic Quantum Information Processing
OPTI 647: Lecture 27

Christos Gagatsos
Saikat Guha

December 3, 2019
College of Optical Sciences
Meinel 501

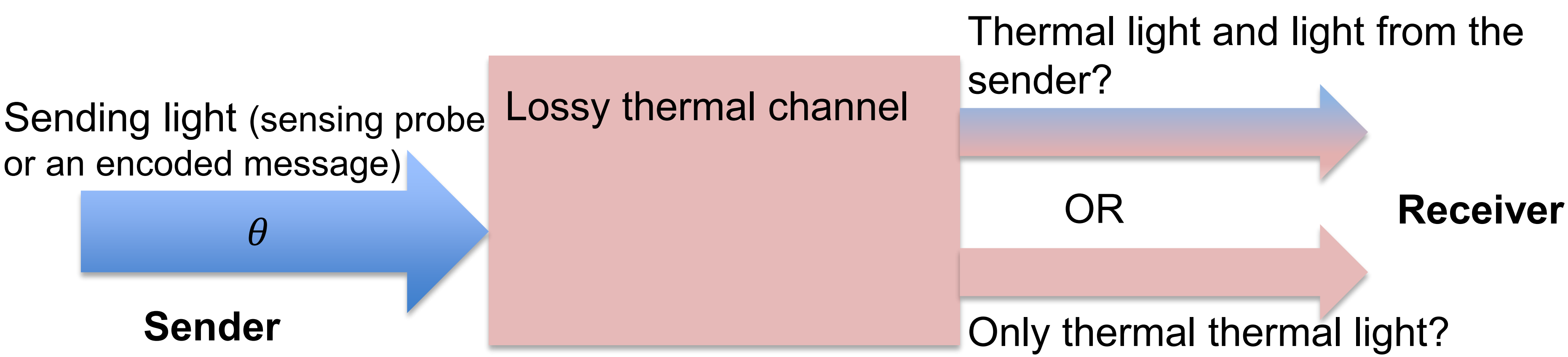
Plan for today

- The notion of *covertness*
- To get an idea of how the math on covert protocols work.
- Covert sensing:
  1. Brief overview of quantum sensing
  2. Covert quantum sensing
  3. Covert quantum sensing: Floodlight illumination

The idea of *covert*

Covert protocols are those where the task is to prevent an adversary (Willie) from detecting the protocols activity.

- Covert communications. Where the task is to transmit useful information while the adversary cannot detect the message.
- Covert sensing. Where the task is to sense a set of unknown parameters, while an adversary (who can be the target), is unaware of the sensing attempt.



Crucial ingredient: Thermal environment, as this will help to hide our probe light.

Quantum relative entropy (QRE)

QRE is one more measure of “closeness” of two density matrices.

$$D(\hat{\rho}|\hat{\sigma}) = \mathrm{tr}(\hat{\rho}\ln\hat{\rho} - \hat{\rho}\ln\hat{\sigma})$$

(Some) properties:

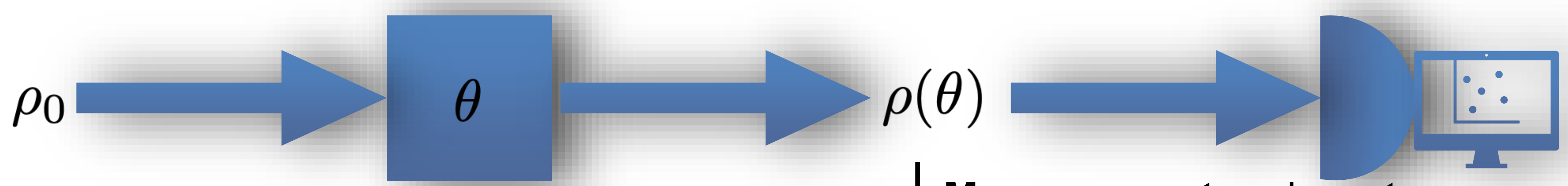
1. $D(\hat{\rho}|\hat{\sigma}) \geq 0.$
2. It can go infinity.
3. Not symmetric: $D(\hat{\rho}|\hat{\sigma}) \neq D(\hat{\sigma}|\hat{\rho})$, i.e., not a metric.
4. Jointly convex: $D(\lambda\hat{\rho}_1 + (1-\lambda)\hat{\rho}_2|\lambda\hat{\sigma}_1 + (1-\lambda)\hat{\sigma}_2) \leq \lambda D(\hat{\rho}_1|\hat{\sigma}_1) + (1-\lambda)D(\hat{\rho}_2|\hat{\sigma}_2)$
5. Decreasing under CPTP maps $\mathcal{E}$: $S(\mathcal{E}(\hat{\rho})|\mathcal{E}(\hat{\sigma})) \leq S(\hat{\rho}|\hat{\sigma})$
6. Additive: $D(\hat{\rho}|\hat{\sigma})$: $D\left(\hat{\rho}^{\otimes n}\middle|\hat{\sigma}^{\otimes n}\right) = n\,D(\hat{\rho}|\hat{\sigma})$.
7. Pinsker’s inequality: $\sqrt{2D(\hat{\rho}|\hat{\sigma})} \geq |\hat{\rho} - \hat{\sigma}|_1$ (lower bound on trace distance)

Pinsker’s inequality is useful to calculate the average probability of error P_e when discriminating between two density matrices:

$$P_e = \frac{1}{2}\left(1 - \frac{1}{2}|\hat{\rho} - \hat{\sigma}|_1\right) \geq \frac{1}{2}\left(1 - \frac{1}{2}\sqrt{2D(\hat{\rho}|\hat{\sigma})}\right)$$

Quantum sensing (single parameter)

THE UNIVERSITY OF ARIZONA



An **input probe state** picks up an **unknown parameter** (e.g. single or many phases, loss rate, etc.) when is injected into a **quantum channel**

Fidelity: $\mathcal{F}\left(\rho(\theta), \rho(\theta+\epsilon)\right) = \mathrm{tr}\left[\left(\rho(\theta)^{1/2}\rho(\theta+\epsilon)\rho(\theta)^{1/2}\right)^{1/2}\right]$

Quantum Fisher Information (QFI):

$$F = -4\frac{d^2\mathcal{F}\left(\rho(\theta), \rho(\theta+\epsilon)\right)}{d\epsilon^2}\Big|_{\epsilon=0}$$

Captures the distance between two states.

Measurement and **post processing** are applied on the **final state**

Estimator $\hat{\theta}_n$ consists of two things: a measurement and data processing.

From these, the covariance of the estimator is constructed: $\langle(\theta-\hat{\theta})^2\rangle$

Unbiased estimator: $\langle\hat{\theta}\rangle = \theta$

Cramér-Rao bound: $\langle(\theta-\hat{\theta}_n)^2\rangle \geq 1/(nF)$

Gives the best performance of any unbiased estimator.

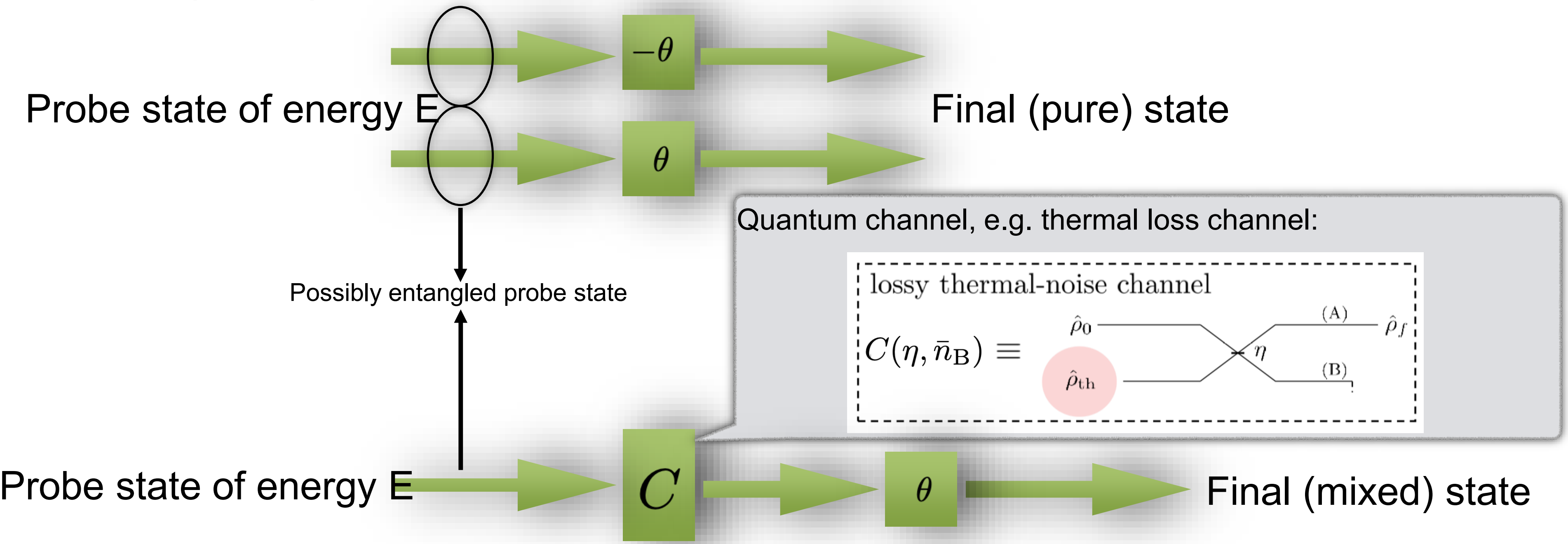
$\hat{\theta}_n$:unbiased estimator, repeated n times.

Quantum sensing (single parameter)

THE UNIVERSITY OF ARIZONA

The task is to find the maximum possible QFI and an estimator which achieves that.

For example, in phase estimation: $\hat{U}(\theta) = \exp(i\theta\hat{n})$



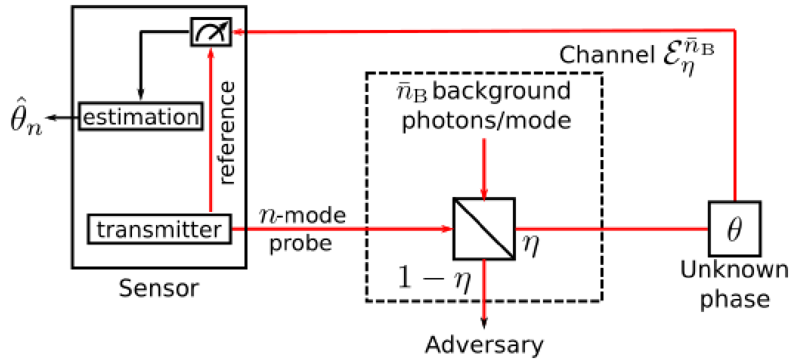
Depending on the probe state, different results have been obtained in the extensive literature and in class, on how to obtain the optimal precision and what estimator achieves it.

$$\langle(\theta - \hat{\theta}_n)^2\rangle \geq 1/(nF)$$

QFI $F \propto E^2$ (Heisenberg limit: better precision)

QFI $F \propto E$ (Classical limit)

Covert quantum sensing (CQS)



CQS: We ask if it is possible to optically probe and estimate an unknown phase while a fully quantum-equipped adversary is not able to credibly decide if such a sensing attempt took place or not.

The adversary performs a **binary test:** detection (0)/ no detection (1).

Photon number detected by the adversary

Threshold chosen By the adversary

If $X_{tot} \geq S$ the adversary declares that the sensor Interrogates.

Performance of the hypothesis test: detection error probability: false alarm (FA) and missed detection (MD).

$$P_e^{\text{det}} = \frac{P_{\text{FA}} + P_{\text{MD}}}{2}$$

Covertness condition:

$$P_e^{\text{det}} \geq \frac{1}{2} - \varepsilon, \;\; \varepsilon > 0$$

Arbitrarily close to random choice.

CQS conditions

THE UNIVERSITY OF ARIZONA

Adversary chooses a detected photons threshold S.

$P_{\mathrm{FA}} = P(\text{d.c.} + \text{th.ph.} \geq S)$

$P_{\mathrm{MD}} = P(\text{probe} + \text{d.c.} + \text{th.ph.} < S)$

Adversary chooses a detected photons threshold S.

High detection probability if

$$\langle N_{\mathrm{S}} \rangle = \omega(\sqrt{n})$$

Mean (total) photon number lower bounded by the sqrt of the number of modes (or uses).

The sensor doesn't interrogate

$$P_{\mathrm{FA}} = P(X_{\mathrm{tot}}^{(0)} \geq S) \leq \frac{\langle \Delta N_{\mathrm{N}}^2 \rangle}{(S - n\bar{n}_{\mathrm{N}})^2}$$

$$X_{\mathrm{tot}}^{(0)} = X_{\mathrm{D}} + X_{\mathrm{T}}$$

Mean thermal photons

Dark counts (Poisson statistics with rate λ)

Total noise photons per mode and variance: $\bar{n}_{\mathrm{N}} = \lambda + \eta \bar{n}_{\mathrm{B}}$

$$\langle \Delta N_{\mathrm{N}}^2 \rangle = n\lambda + n\eta^2(\bar{n}_{\mathrm{B}} + \bar{n}_{\mathrm{B}}^2)$$

The adversary sets threshold: $S = n\bar{n}_{\mathrm{N}} + \sqrt{\langle \Delta N_{\mathrm{N}}^2 \rangle / P_{\mathrm{FA}}^*}$

to obtain the desired P_{FA}^*

The sensor interrogates

$$P_{\mathrm{MD}} = P(X_{\mathrm{tot}}^{(1)} < S) \leq \frac{\langle \Delta N_{\mathrm{N}}^2 \rangle + (1-\eta)^2 \langle \Delta N_{\mathrm{S}}^2 \rangle}{((1-\eta)\langle N_{\mathrm{S}} \rangle - \sqrt{\langle \Delta N_{\mathrm{N}}^2 \rangle / P_{\mathrm{FA}}^*})^2}$$

$$X_{\mathrm{tot}}^{(1)} = X_{\mathrm{D}} + X_{\mathrm{T}} + X_u$$

Count from probe

$\langle \Delta N_{\mathrm{N}}^2 \rangle = \mathcal{O}(n)$ and assuming: $\langle \Delta N_{\mathrm{S}}^2 \rangle = \mathcal{O}(n)$

If $\langle N_{\mathrm{S}} \rangle = \omega(\sqrt{n}) \longrightarrow \lim_{n \to \infty} P_{\mathrm{MD}} = 0$

Thus, given large enough n, the adversary can detect the probes that have mean photon number $\langle N_{\mathrm{S}} \rangle = \omega(\sqrt{n})$ with arbitrary low error of detection probability.

Covertness conditions

$\langle N_{\mathrm{S}} \rangle = O(\sqrt{n})$ (for total photons) $\bar{n}_{\mathrm{S}} = O(1/\sqrt{n})$ (for photons per mode or per use)

CQS converse

1. The sensor must use an n-mode probe with photons $\langle N_{\mathrm{S}} \rangle = O(\sqrt{n})$ to avoid detection.
2. The Cramér-Rao bound and a further lower bound for the thermal loss channel:

$$\langle (\theta - \hat{\theta})^2 \rangle \geq F_{\mathrm{Q}}^{-1} \geq C_{\mathrm{Q}}^{-1} \qquad C_{\mathrm{Q}}^{-1} = O(\tfrac{1}{\sqrt{n}})$$

[CNG, B. Bash, S. Guha, A. Datta Phys. Rev. A **96**, 062306 (2017)]

Suppose the target is interrogated using an n-mode probe with a total of photons $\langle N_{\mathrm{S}} \rangle = n\bar{n}_{\mathrm{S}}$ and that the total photon number variance of the probe is $\langle \Delta N_{\mathrm{S}}^2 \rangle = \mathcal{O}(n)$

Then, the sensing attempt is either detected by the adversary with arbitrarily low detection error probability, or the estimator has mean squared error:

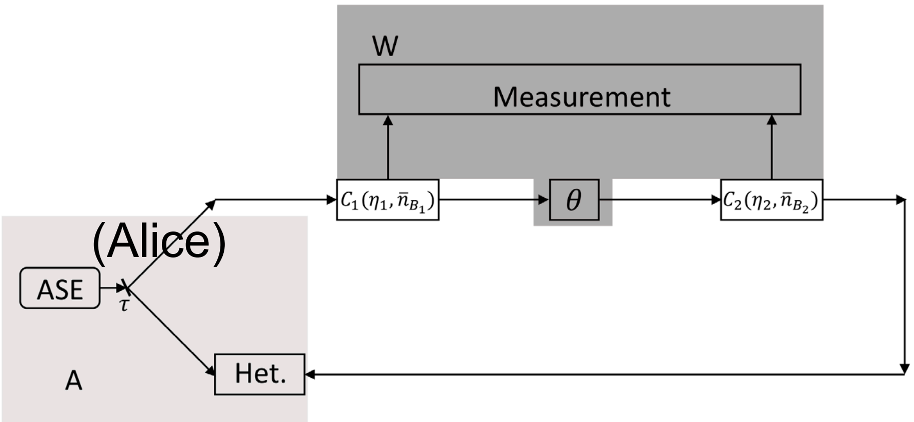
$$\langle (\theta - \hat{\theta}_n)^2 \rangle = \Omega\left(\frac{1}{\sqrt{n}}\right) \quad \text{(tight lower bound)}$$

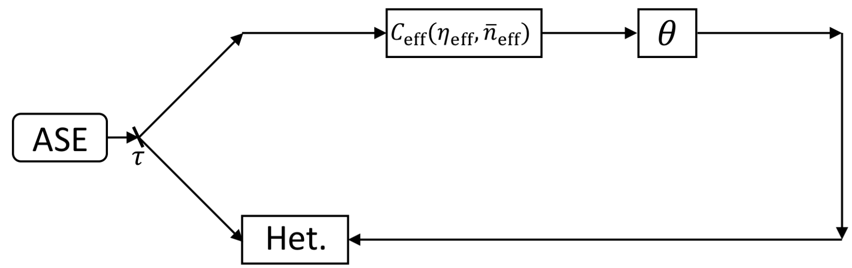
Fundamental limit: $\langle (\theta - \hat{\theta}_n)^2 \rangle = O\left(\frac{1}{\sqrt{n}}\right)$

The converse holds for any input state which satisfies this set of restrictions.

CQS achievability: Floodlight illumination

(Willie)





Equivalent to left scheme for sensor (Alice).

Floodlight illumination (~THz ASE source):
Thermal correlated light with zero mean and covariance matrix,

$$V_{\mathrm{ASE}} = \begin{pmatrix} A_{\mathrm{ASE}} & 0_{2\times 2} \\ 0_{2\times 2} & A_{\mathrm{ASE}} \end{pmatrix} \quad A_{\mathrm{ASE}} = \begin{pmatrix} \bar{n}_{\mathrm{S}} + \frac{1}{2} & \sqrt{\bar{n}_{\mathrm{S}}\bar{n}_{\mathrm{LO}}} \\ \sqrt{\bar{n}_{\mathrm{S}}\bar{n}_{\mathrm{LO}}} & \bar{n}_{\mathrm{LO}} + \frac{1}{2} \end{pmatrix}$$

CQS achievability: Floodlight illumination (continued)

Willie's task is to discriminate between two states:

$\hat{\rho}_1$ (Alice is sensing)

$\hat{\rho}_0$ (Alice is not sensing).

$$P_e^{\text{det}} \geq \frac{1}{2} - \sqrt{\frac{1}{8} D(\hat{\rho}_0^{\otimes n} \| \hat{\rho}_1^{\otimes n})}$$

$$D(\hat{\rho}_0 \| \hat{\rho}_1) = \operatorname{tr}(\hat{\rho}_0 \ln \hat{\rho}_0) - \operatorname{tr}(\hat{\rho}_0 \ln \hat{\rho}_1)$$

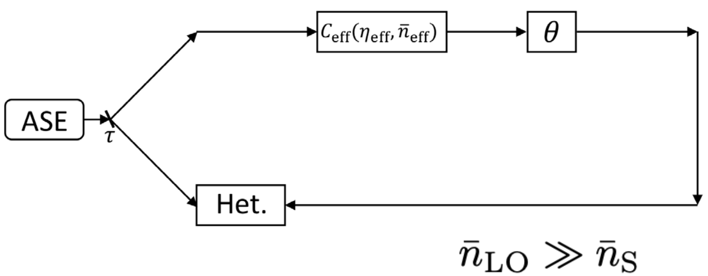
Quantum relative entropy (which is additive)

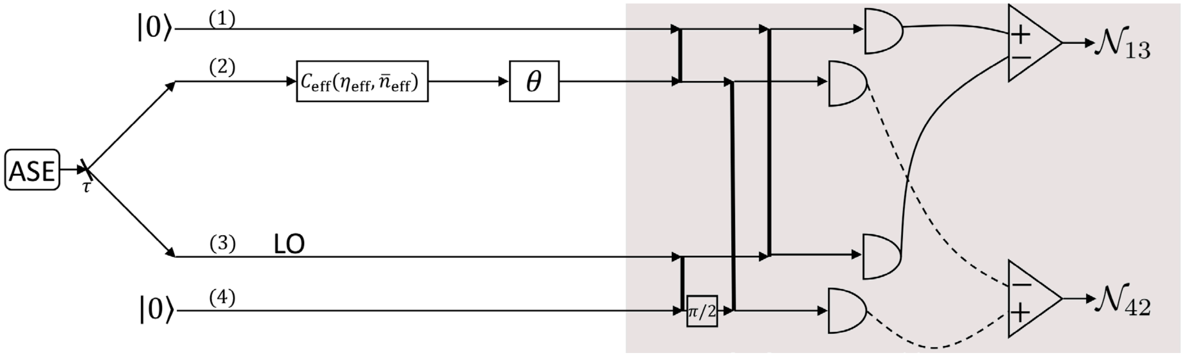
$$P_e^{\text{det}} \geq \frac{1}{2} - \frac{\sqrt{c_2}}{4} \sqrt{n}\, \bar{n}_S \qquad c_2 = f(\eta_1, \eta_2, \bar{n}_{B_1}, \bar{n}_{B_2}) > 0$$

Alice sets $\bar{n}_S = \frac{4\varepsilon}{\sqrt{c_2}} \frac{1}{\sqrt{n}}$ to ensure covertness:

$$P_e^{\text{det}} \geq \frac{1}{2} - \varepsilon, \; \varepsilon > 0$$

CQS achievability: Floodlight illumination





Can we attain the covert quantum limit?

Hetorodyne measurement (dual homodyne):

$$\langle(\theta - \hat{\theta}_{\mathrm{het},n})^2\rangle \approx \frac{\tilde{c}_{\mathrm{het}}}{\varepsilon\sqrt{n}} = \mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$$

$$\tilde{c}_{\mathrm{het}} = [1 + \bar{n}_{\mathrm{B_{eff}}}(1 - \eta_{\mathrm{eff}})]\sqrt{c_2}/(8\eta_{\mathrm{eff}})$$

QFI calculation for the ultimate quantum bound:

$$\langle(\theta - \hat{\theta}_n)^2\rangle \geq \frac{c_{\mathrm{ASE}}}{\varepsilon\sqrt{n}}$$

$$c_{\mathrm{ASE}} = [1 + 2\bar{n}_{\mathrm{B_{eff}}}(1 - \eta_{\mathrm{eff}})]\sqrt{c_2}/(16\eta_{\mathrm{eff}})$$

Heterodyne detection yields an MSE that is at most twice compared to what is attainable by the optimal quantum receiver (but it scales the same).

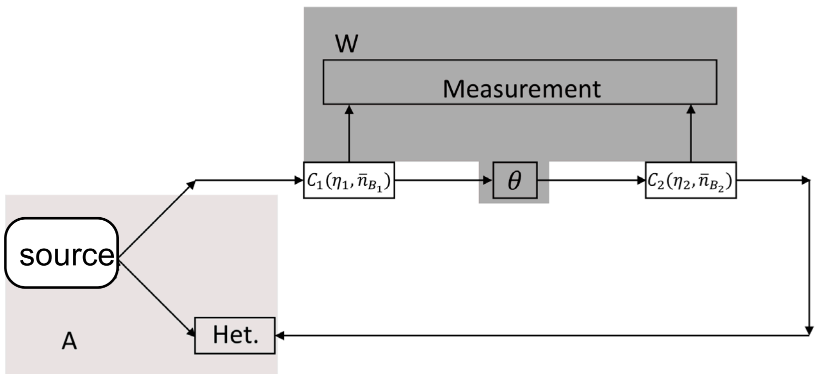
Comparison of sources

THE UNIVERSITY OF ARIZONA

Quantum limits: LASER (coherent state sources) v ASE

We compare the QFI's which correspond to the two sources.

$\mu = F_{\mathrm{A}}^{-1}/F_{\mathrm{coh}}^{-1}$ If $\mu < 1$, the ASE source outperforms the coherent probe.



For thermal equilibrium between the two stations

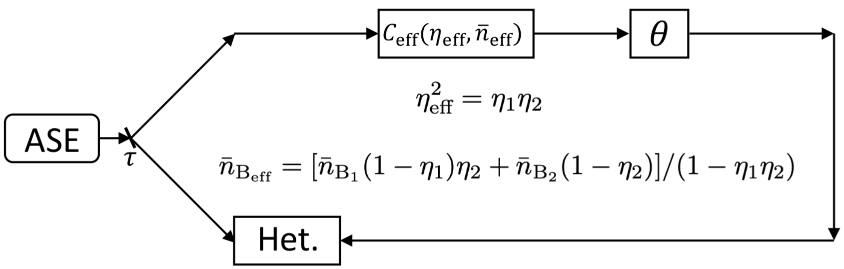
$\bar{n}_{\mathrm{B}_1} = \bar{n}_{\mathrm{B}_2}$

$n =$(optical bandwidth) × (fixed interrogation time)

$\mu = \sqrt{W_{\mathrm{coh}}/W_{\mathrm{ASE}}} < 1$ W: optical bandwidth

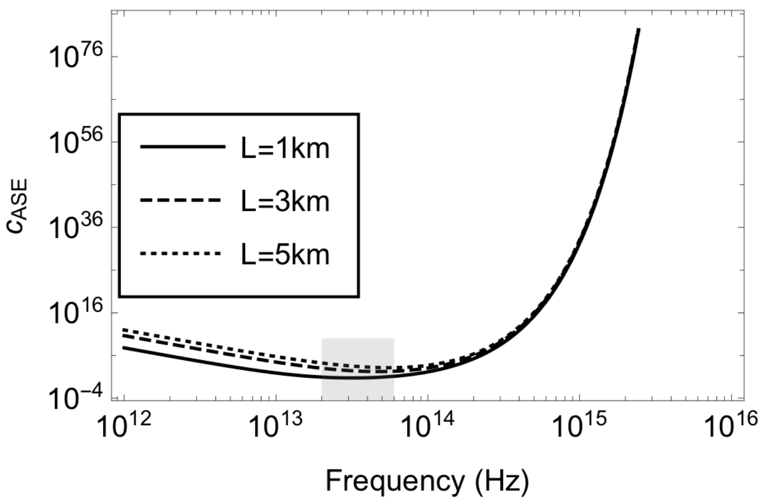
The ASE source would outperform a coherent state probe because of its larger bandwidth

Towards a realistic model



$$\langle(\theta - \hat{\theta}_n)^2\rangle \geq \frac{c_{\text{ASE}}}{\varepsilon\sqrt{n}}$$

$$c_{\text{ASE}} = [1 + 2\bar{n}_{\text{B}_{\text{eff}}}(1-\eta_{\text{eff}})]\sqrt{c_2}/(16\eta_{\text{eff}})$$



$$r_t = 4\text{cm} \; r_T = 10\text{cm}, \; T = 1s, \; \varepsilon = 10^{-3}$$

$$\eta_1 = \eta_2 = \eta = [1 + 2D - \sqrt{1+4D}]/(2D)$$

(e.g. monostatic sensor)

$$D = (A_t A_T)/(\lambda L)^2$$

A_t: Alice's transmitter apparatus exit area.

A_T: Effective area of target's cross section.

λ : Central wavelength.

L : Distance to target.

$$\bar{n}_{B_1} = \bar{n}_{B_2} = \bar{n}_B = [\exp(hc/(\lambda k_B T_0)) - 1]^{-1}$$

(thermal equilibrium) $T_0 = 300K$

Smaller frequencies have more thermal noise to hide the probe, which tends to make c_{ASE} smaller. On the other hand, smaller frequencies have more diffraction limited loss, giving more photons to Willie, which tends to make c_{ASE} higher.

Minimum in the mid to long wave infrared (ML- IR) region.

Conclusions

- Covert sensing *is* possible.
- Covertness condition: $\bar{n}_{\mathrm{S}} = O(1/\sqrt{n})$
- Fundamental limit: $\langle(\theta - \hat{\theta}_n)^2\rangle = O\left(\frac{1}{\sqrt{n}}\right)$
- Attempt to go beyond the fundamental limit leads to detection.
- ASE source and heterodyne detection appear to be efficient.

CNG, B. Bash, A. Datta, Z. Zhang, S. Guha, Phys. Rev. A **99**, 062321 (2019)

B. Bash, CNG, A. Datta, S. Guha, 2017 IEEE (ISIT 2017), 10.1109/ISIT.2017.8007122

Upcoming topics

- Covert sensing (continued)
- Covert communications
- Other topics…