Institute for Quantum Computing

University of Waterloo

On the inefficacy of Gaussian regenerative amplifiers for quantum optical communication

Ryo Namiki, Oleg Gittsovich, Saikat Guha, Norbert Lütkenhaus

Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo,

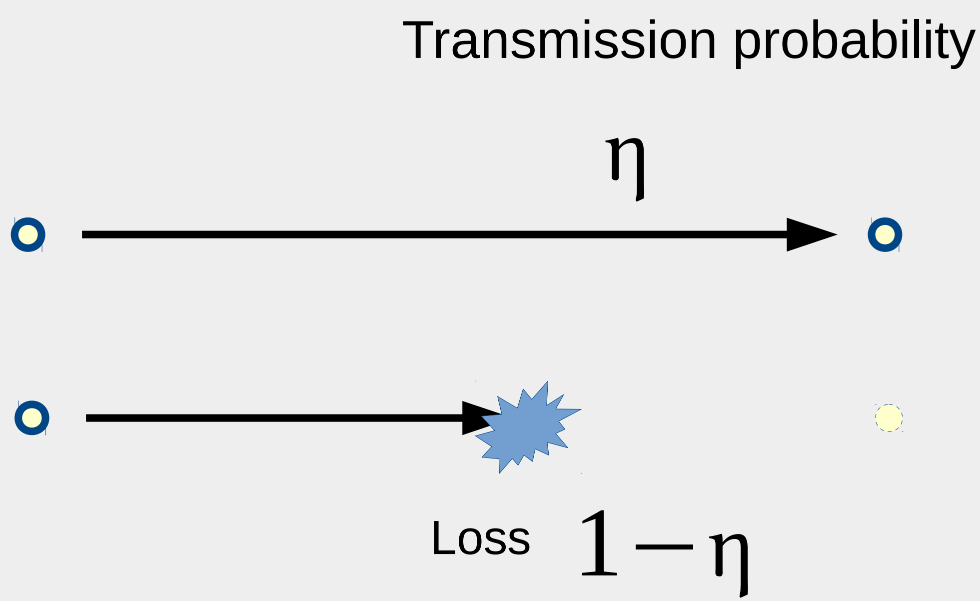
Institute for Theoretical Physics, University of Innsbruck,

Quantum Information Processing group, BBN Technologies

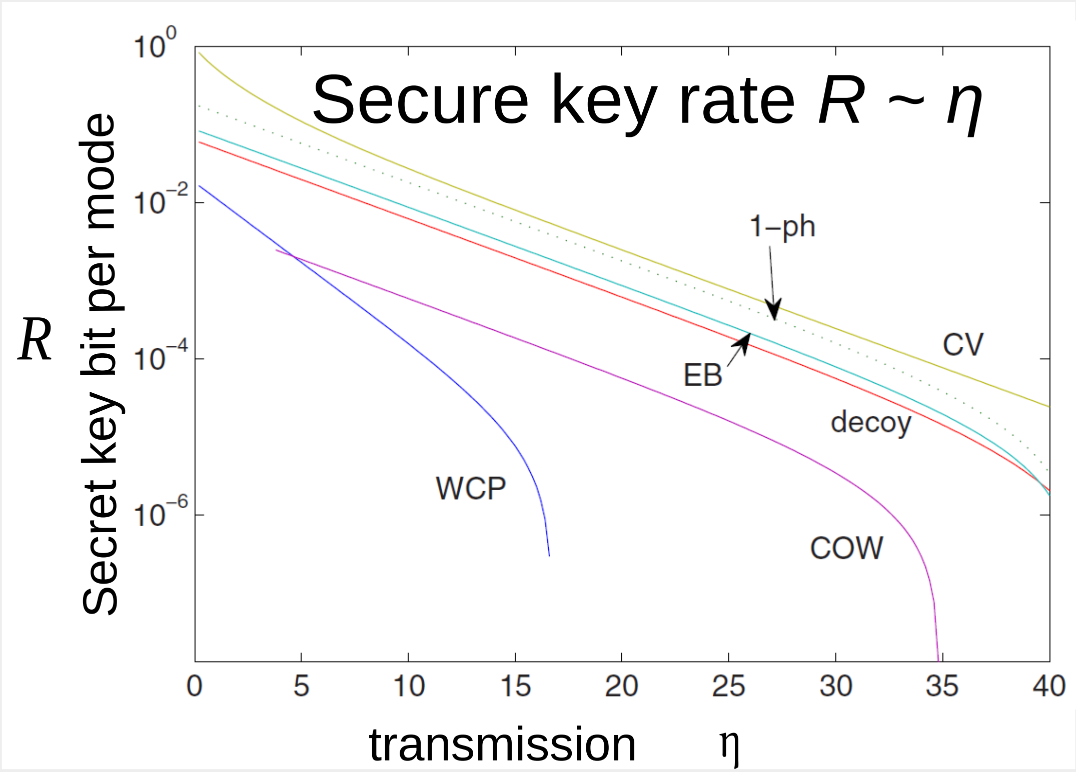
DARPA Quiness Program
Office of Naval Research

Introduction

- The photon loss limits long distance QKD.



Introduction



Scarani et al., Rev. Mod. Phys. 81, 1301 (2009)

- General unpper bound on the secure key rate $$R \leq \log_2\left(\frac{1+\eta}{1-\eta}\right) \sim 2.88\,\eta \quad (\eta \ll 1)$$
- Exponential decay with distance $$\eta = e^{-L_{tot}/L_0}$$

Takeoka, Guha, Wilde, arXiv:1310.0129; IEEE Trans. Inf. Theo. 60 4987 (2014).

Introduction

- Quantum Repeater

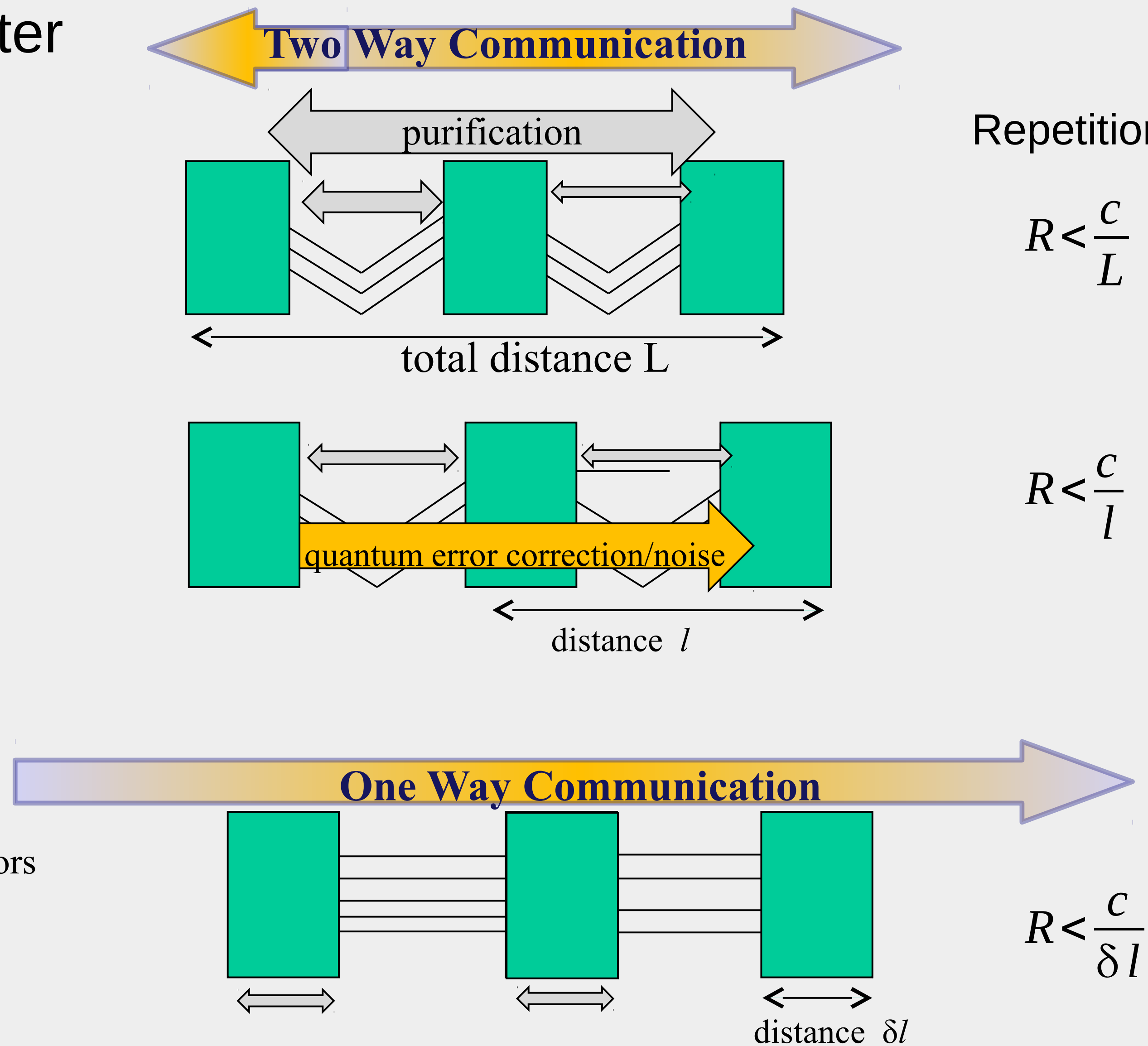
1st generation

2nd generation

3rd generation

QECC for operational errors

QECC for loss



Classical communication

Repetition rate

$$R < \frac{c}{L}$$

$$R < \frac{c}{l}$$

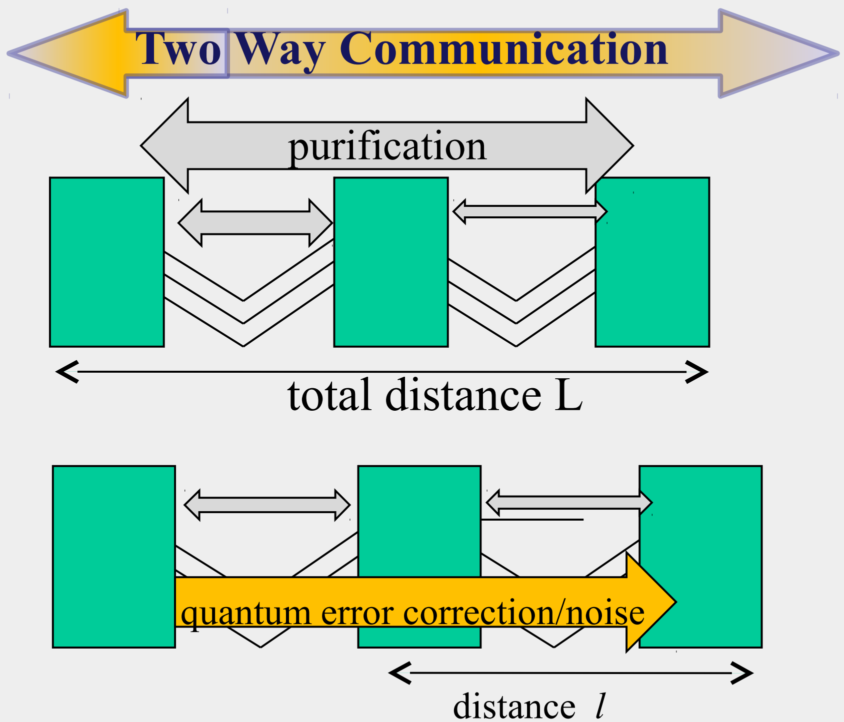
$$R < \frac{c}{\delta l}$$

Muralidharan, Kim, Lütkenhaus, Lukin, Jiang, PRL 112, 250501 (2014)

Introduction

Classical communication

- Quantum Repeater
  1st generation



Repetition rate

$$R < \frac{c}{L}$$

2nd generation

$$R < \frac{c}{l}$$

3rd generation

QECC for operational errors

QECC for loss

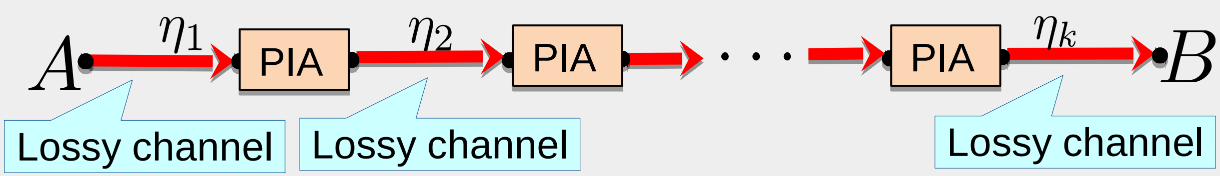
$$R < \frac{c}{\delta l}$$

Chain of lossy channels and black boxes

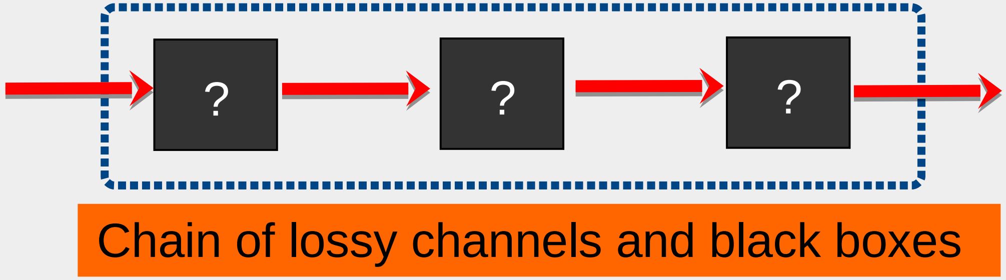
Muralidharan, Kim, Lütkenhaus, Lukin, Jiang, PRL 112, 250501 (2014)

Introduction

- Classical Communication
  Phase insensitive amplifier (PIA) extends transmission distance



- Quantum Communication:
  3rd generation quantum repeater



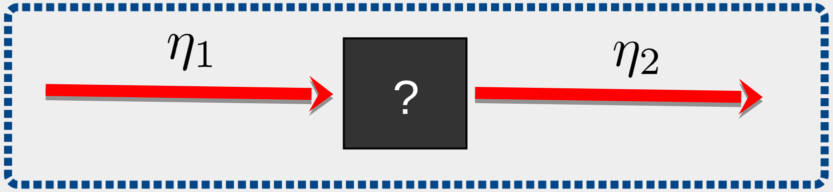
What could those black boxes be?

Single center station between lossy channel

How does a center station modify the total channel?

- Simplest tool box: Gaussian operations

- Could phase insensitive amplifiers (PIA) or generally Gaussian quantum channels work as a quantum repeater?



Chain of lossy channels and black boxes

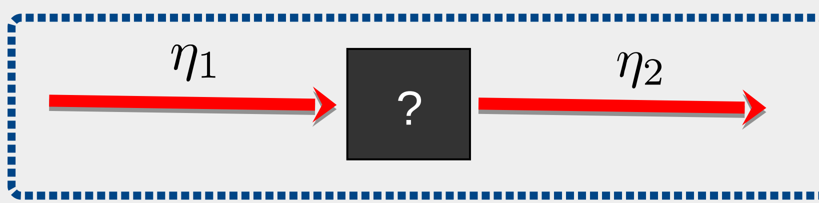
Single center station between lossy channel

How does a center station modify the total channel?

- Simplest tool box: Gaussian operations

- Could phase insensitive amplifiers (PIA) or generally Gaussian quantum channels work as a quantum repeater?

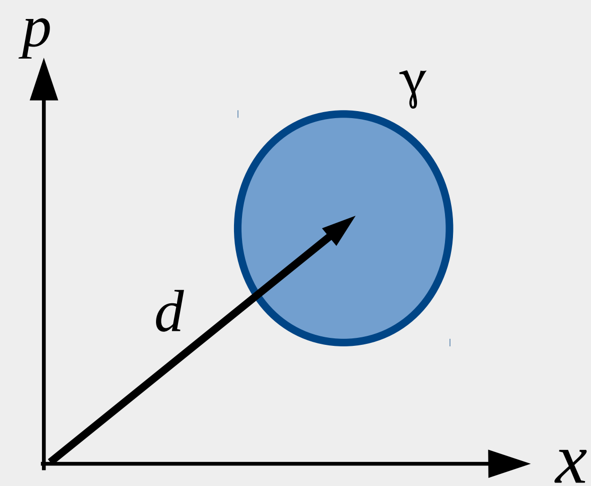
No!



Chain of lossy channels and black boxes

Gaussian states

Quantum states of Light: harmonic oscillators



n-mode bosonic field

- Displacement vector

$$d = \left.\begin{bmatrix} \square \\ \square \\ \square \\ \square \end{bmatrix}\right\} 2n$$

- Covariance matrix

$$\gamma = \begin{bmatrix} \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{bmatrix} \quad 2n \times 2n$$

$$\Delta x \Delta p \geq 1/2$$

canonical uncertainty relation

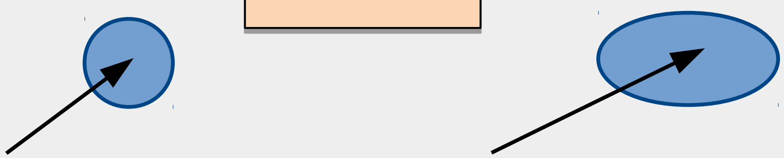
$$\gamma \geq \frac{i}{2}\sigma, \qquad \sigma := \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$$

Identity matrix: I_n

Gaussian channels

Def. Transform Gaussian states to Gaussian states

$$(\gamma, d) \longrightarrow \boxed{(K, \alpha)} \longrightarrow (\gamma', d')$$



(K, α) = (Gain, Noise)

$$\begin{cases} d' = K^T d, \\ \gamma' = K^T \gamma K + \alpha \end{cases}$$

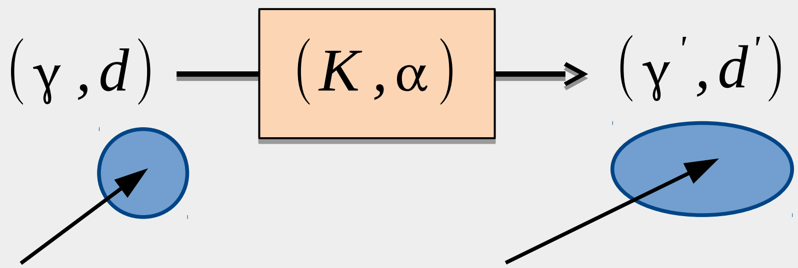
$$K = \begin{bmatrix} \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{bmatrix} \qquad \alpha = \begin{bmatrix} \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{bmatrix} \qquad 2n \times 2n$$

canonical uncertainty relation

$$\begin{cases} \gamma \geq \frac{i}{2}\sigma, \qquad \sigma := \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \\ \text{Identity matrix: } I_n \end{cases}$$

Gaussian channels

Def. Transform Gaussian states to Gaussian states



(K, α) = (Gain, Noise)

$$\begin{cases} d' = K^T d, \\ \gamma' = K^T \gamma K + \alpha \end{cases}$$

$$K = \begin{bmatrix} \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{bmatrix} \qquad \alpha = \begin{bmatrix} \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{bmatrix} \qquad 2n \times 2n$$

canonical uncertainty relation

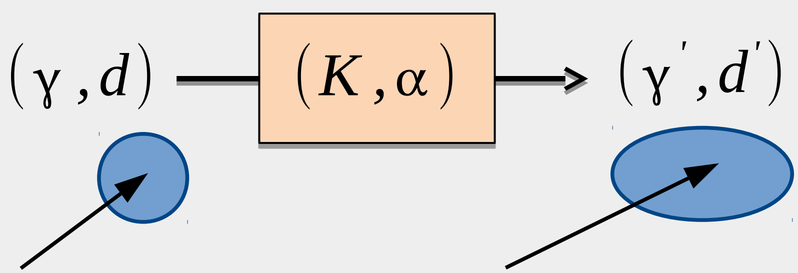
$$\begin{cases} \gamma \geq \frac{i}{2} \sigma, \qquad \sigma := \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \\ \text{Identity matrix: } I_n \end{cases}$$

Physical Condition for channels

$$\alpha \geq \frac{i}{2} (\sigma - K^T \sigma K)$$

Gaussian channels

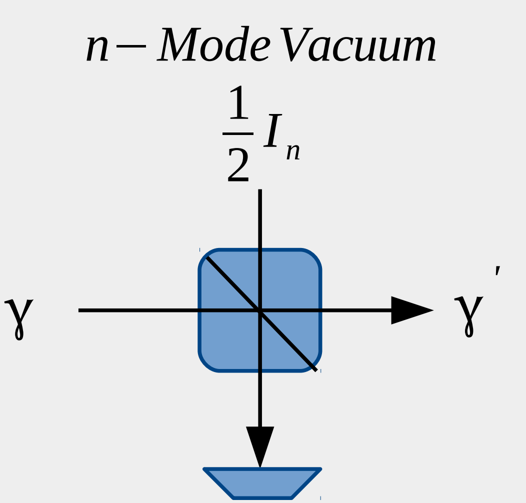
Def. Transform Gaussian states to Gaussian states



(K, α) = (Gain, Noise)

$$\begin{cases} d' = K^T d, \\ \gamma' = K^T \gamma K + \alpha \end{cases}$$

- Multi-mode Pure lossy channels; transmission *η*

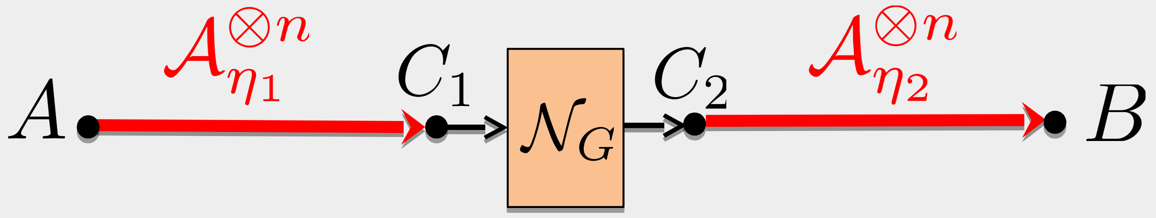


$$K = \sqrt{\eta}\, I_{2n}, \quad \alpha = \frac{1-\eta}{2} I_{2n}.$$

$$\begin{cases} d' = \sqrt{\eta}\, d, \\ \gamma' = \frac{1-\eta}{2} I_{2n} + \eta\, \gamma \end{cases}$$

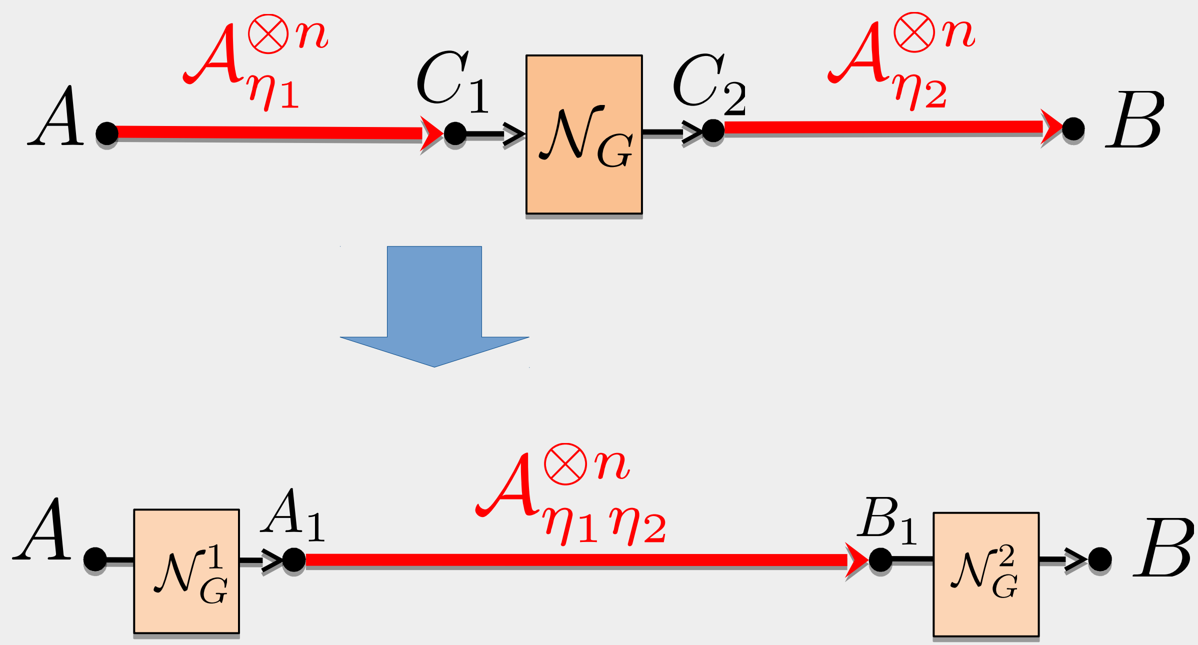
Setting

- Gaussian channel sandwiched between lossy channel segment



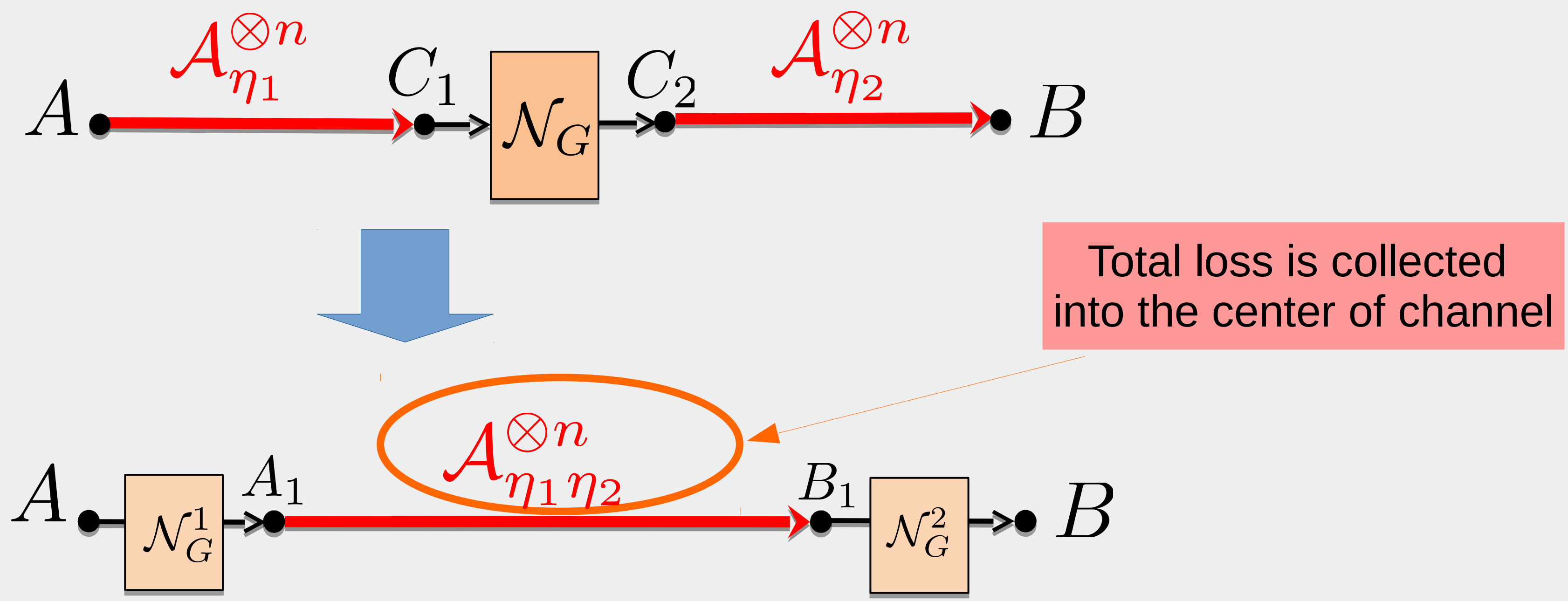
Main theorem

- Decomposition of Gaussian center station



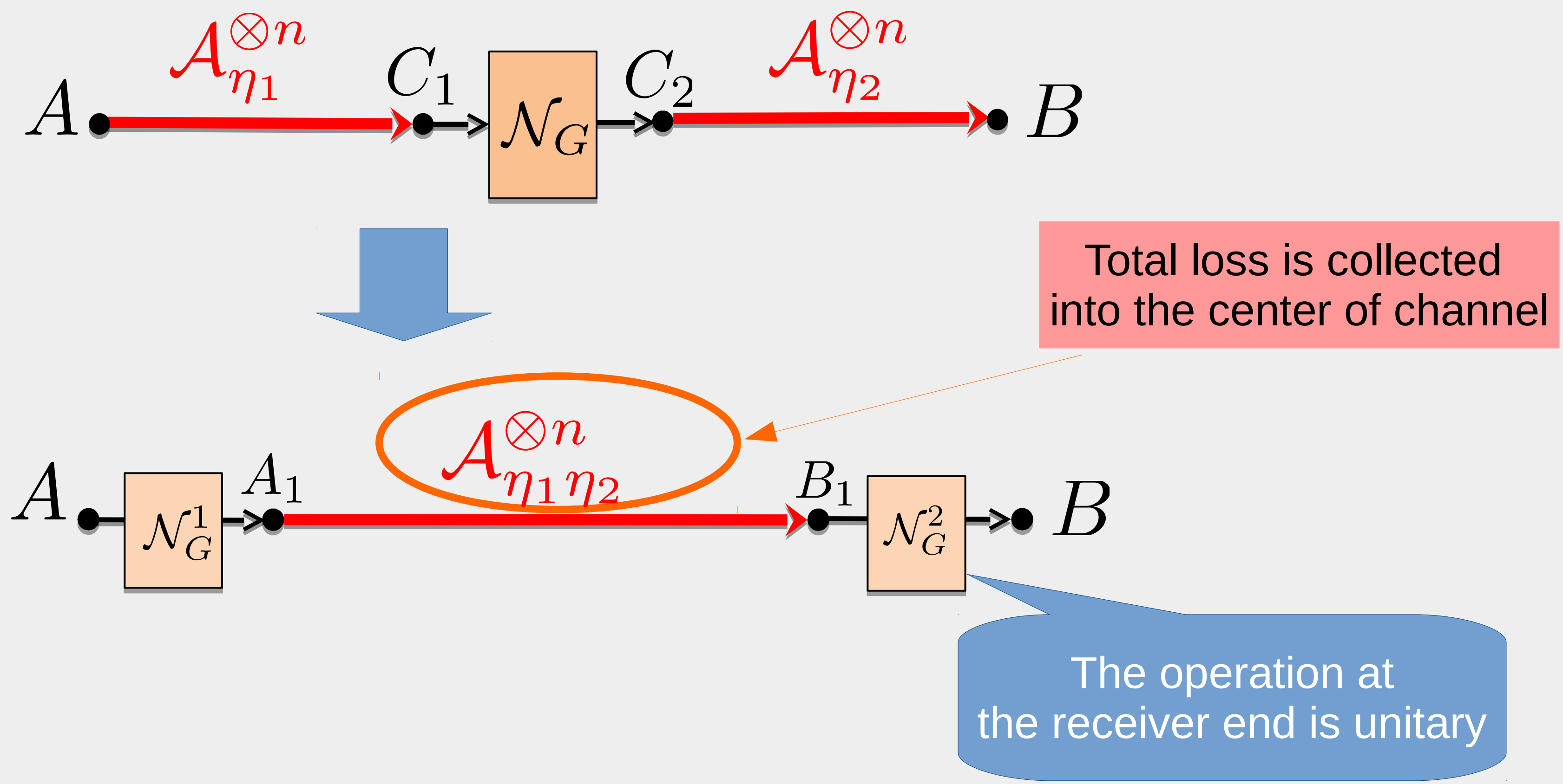
Main theorem

- Decomposition of Gaussian center station

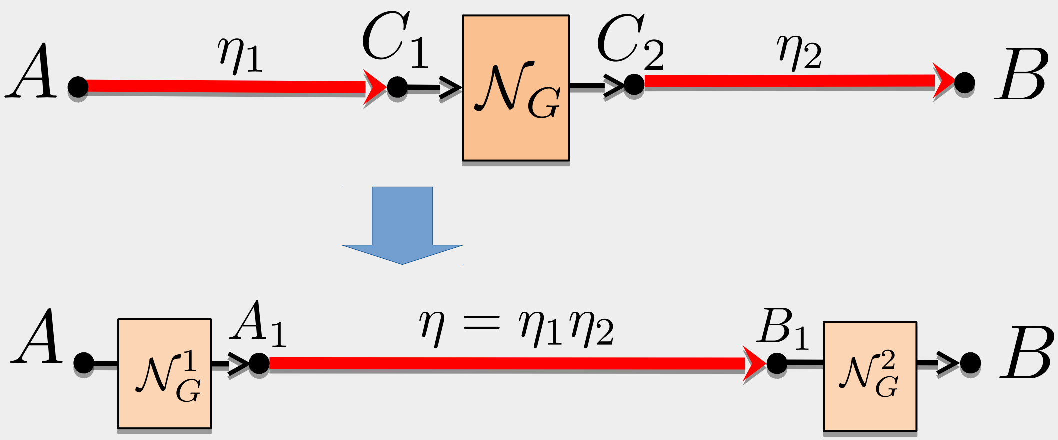


Main theorem

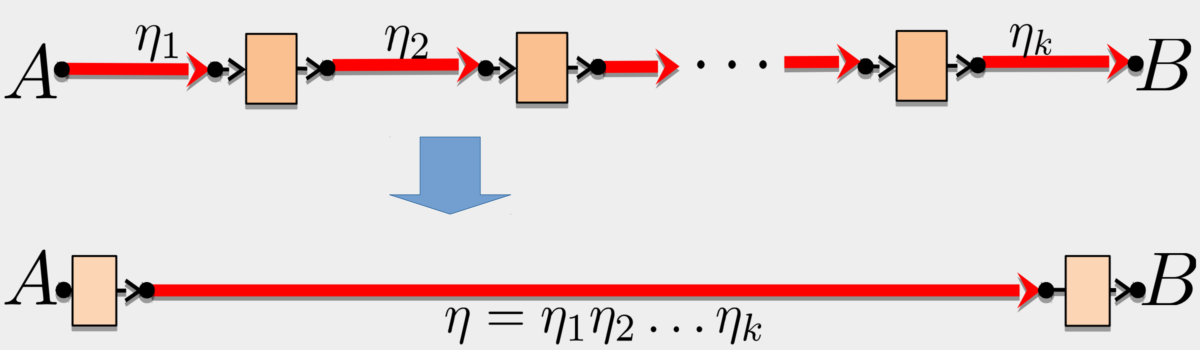
- Decomposition of Gaussian center station



Implication for many stations



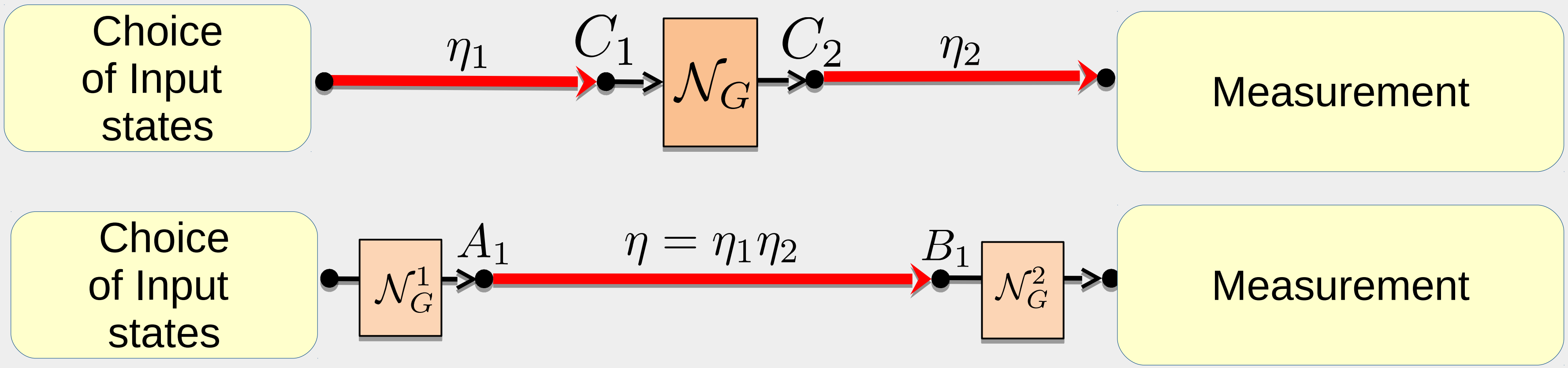
-Effect of loss cannot be reduced!
-Cannot be improved by Interspersing many stations!



★ No difference in Gaussian or Non-Gaussian input states

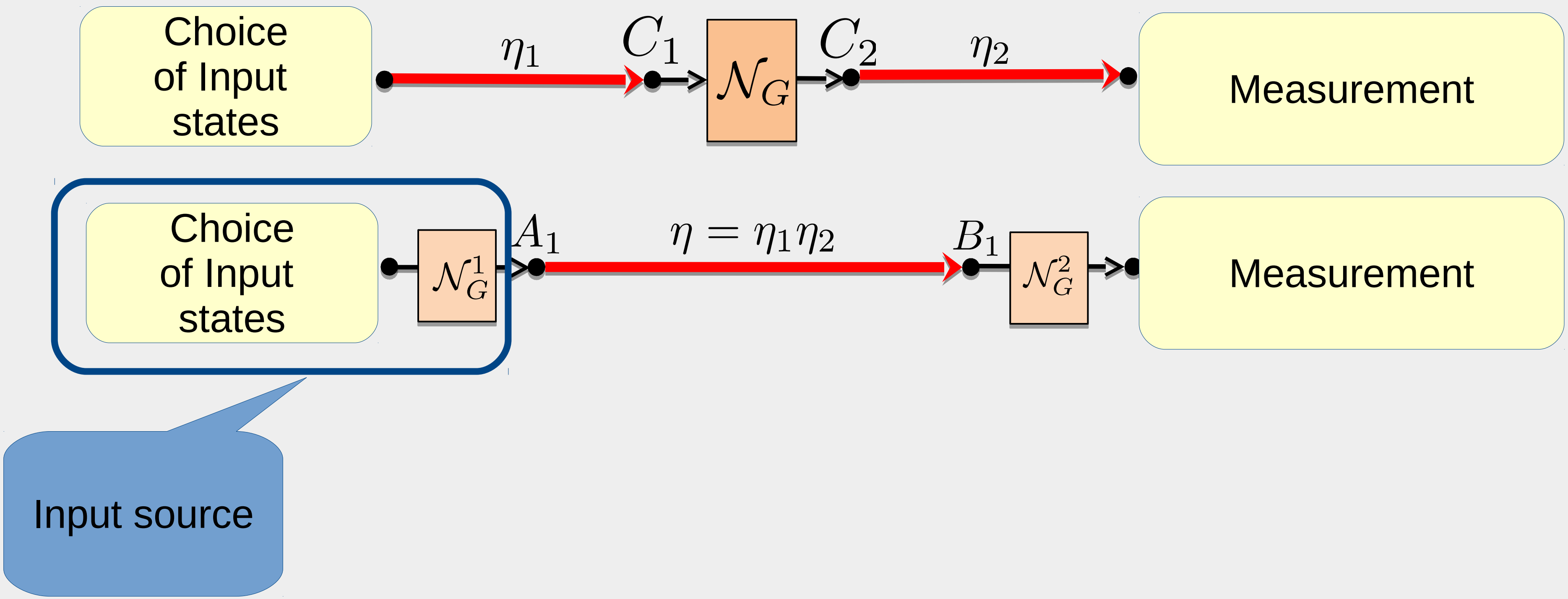
No-Go result for Gaussian repeater

- Center station → Modification of transmitter and receiver.



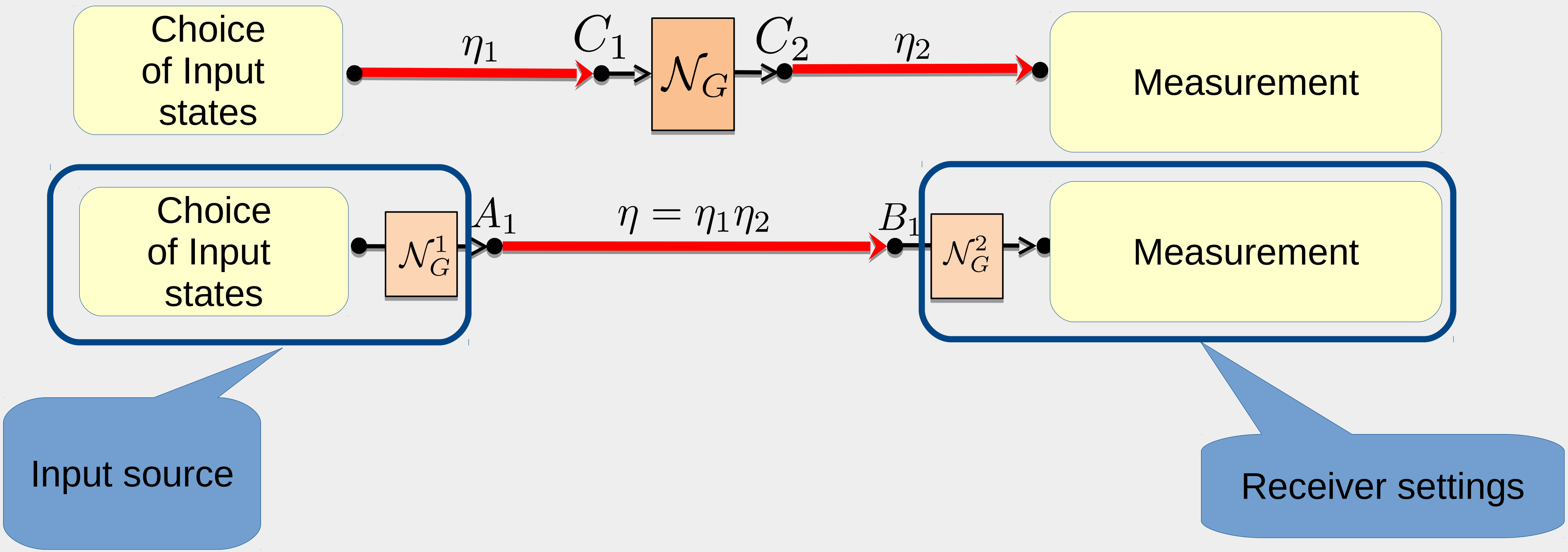
No-Go result for Gaussian repeater

- Center station → Modification of transmitter and receiver.



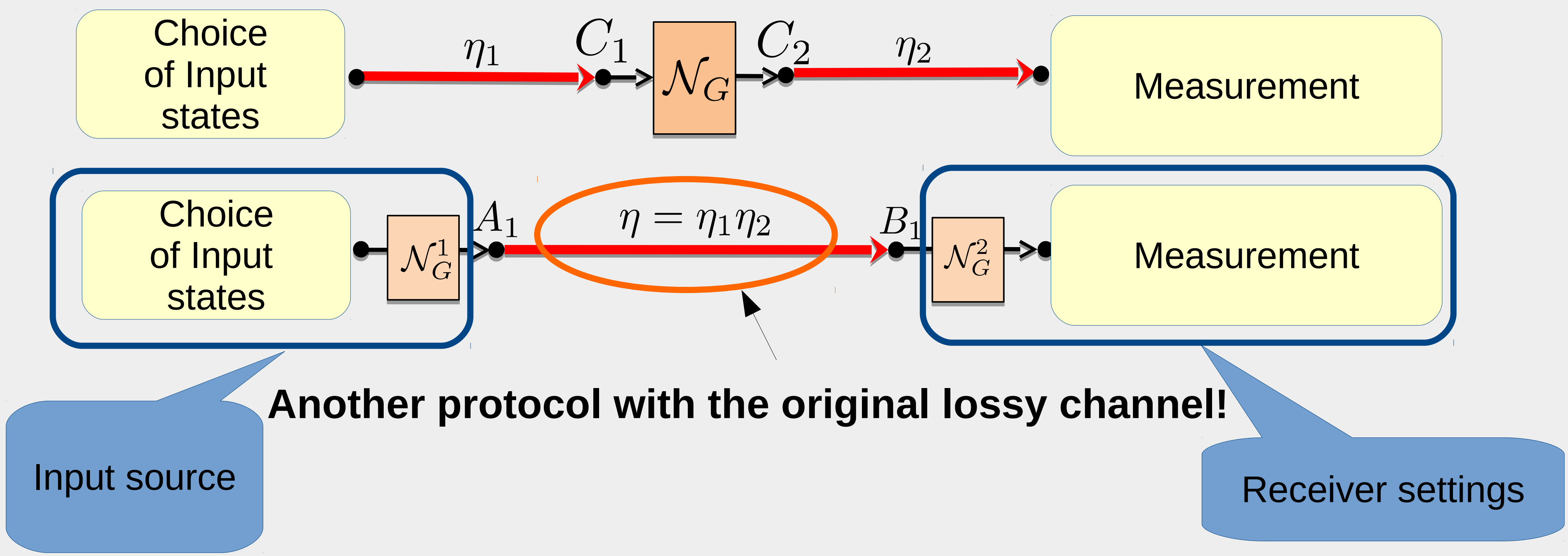
No-Go result for Gaussian repeater

- Center station → Modification of transmitter and receiver.



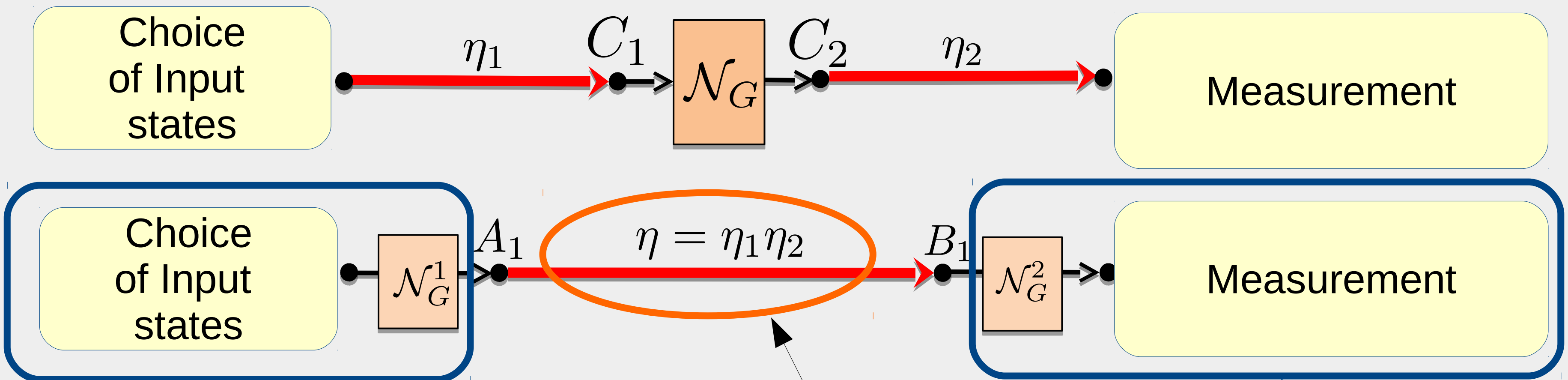
No-Go result for Gaussian repeater

- Center station → Modification of transmitter and receiver.



No-Go result for Gaussian repeater

- Center station → Modification of transmitter and receiver.



Another protocol with the original lossy channel!

Input source

Receiver settings

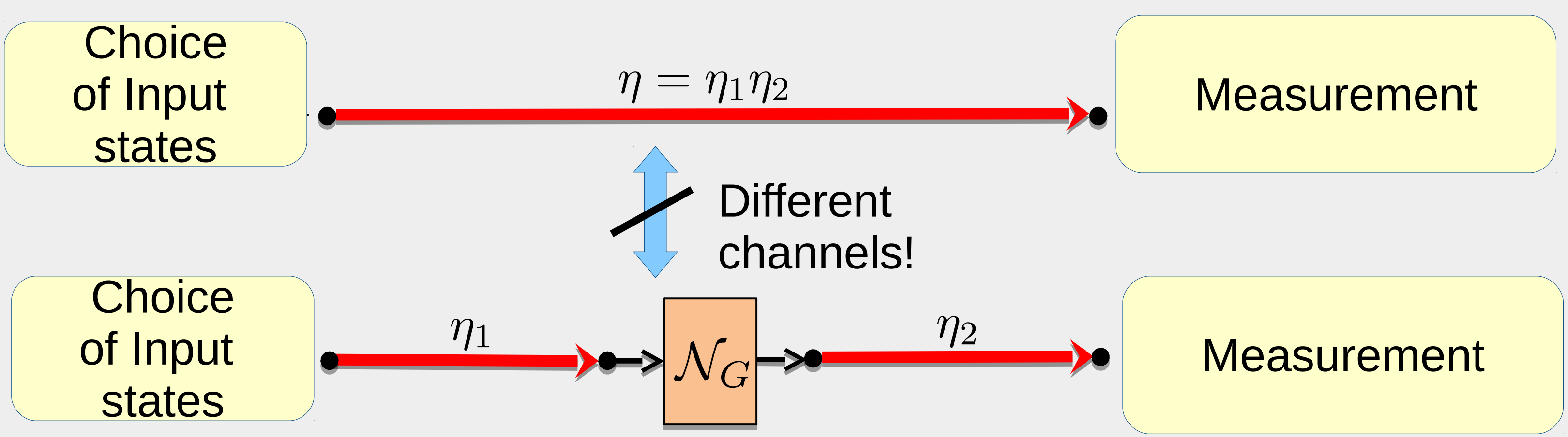
General bound of the secure key rate

$$R \leq \log_2\left(\frac{1+\eta}{1-\eta}\right) \sim 2.88\,\eta$$

can be applied.
[Takeoka, Guha, Wilde, arXiv:1310.0129]

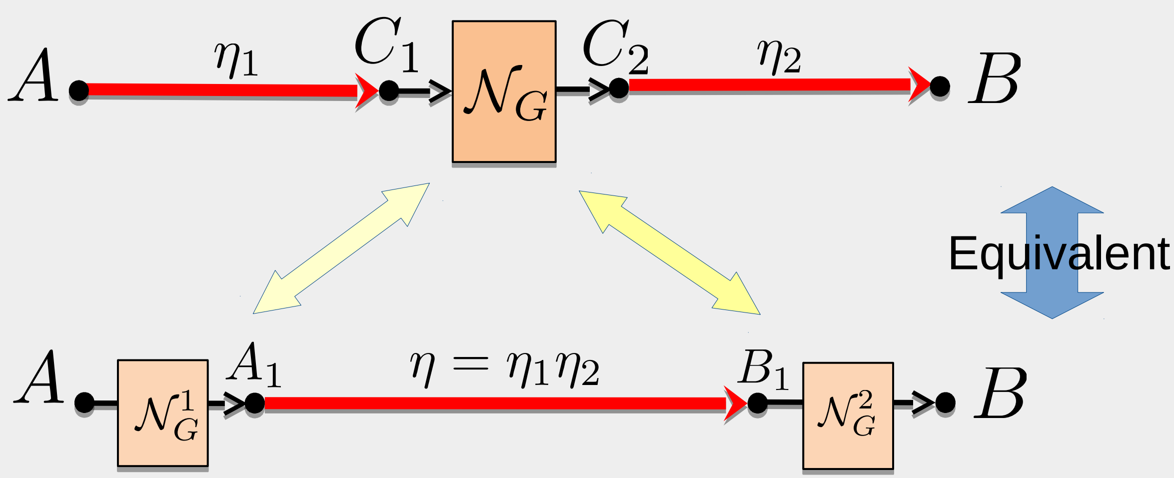
Remarks

- The performance may or may not improve
  if the transmitter and receiver are the same.



Remarks

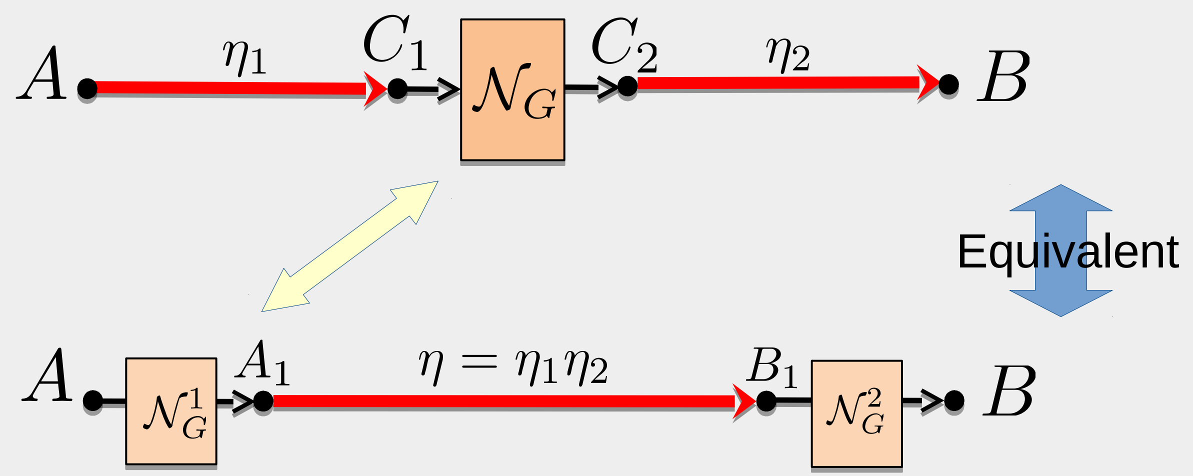
- The performance may or may not improve
  if the transmitter and receiver are the same.
- Mathematically equivalent, not technically or economically.



Remarks

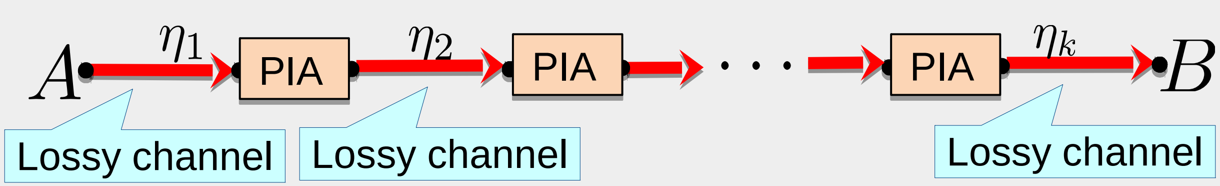
- The performance may or may not improve

  if the transmitter and receiver are the same.
- Mathematically equivalent, not technically or economically.



-Classical Communication

Phase insensitive amplifier (PIA) extends transmission distance



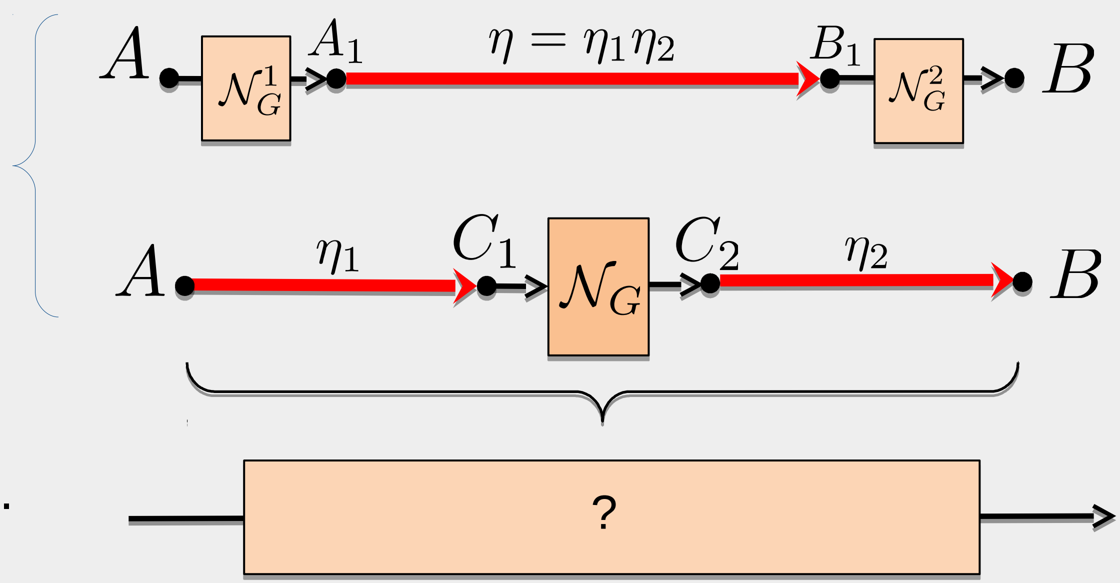
Single center station between lossy channels

- How does a center station modify the total channel?

-Single-mode Gaussian channels
-Entanglement breaking (EB) conditions

Equivalent decomposition

As a single module....



Single center station between lossy channels

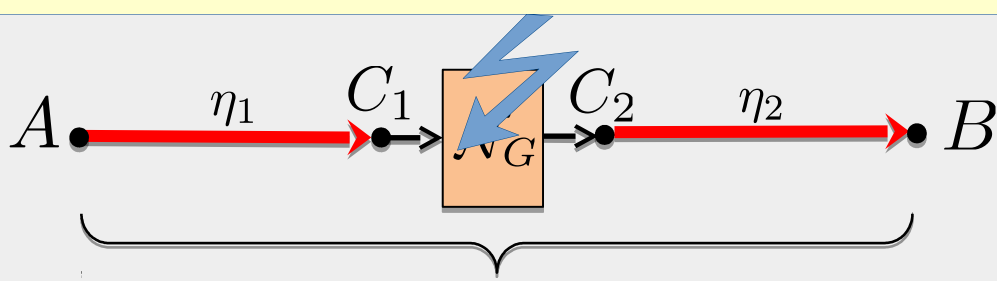
- How does a center station modify the total channel?

  -Single-mode Gaussian channels
  -Entanglement breaking (EB) conditions

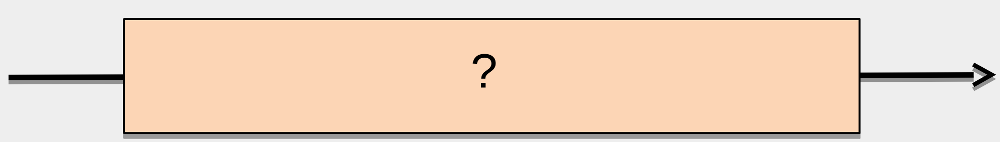
<u>Break any quantum correlation</u>

No entanglement / No secret key

Curty, Lewenstein & Lütkenhaus, Phys. Rev. Lett. 92, 217903 (2004).



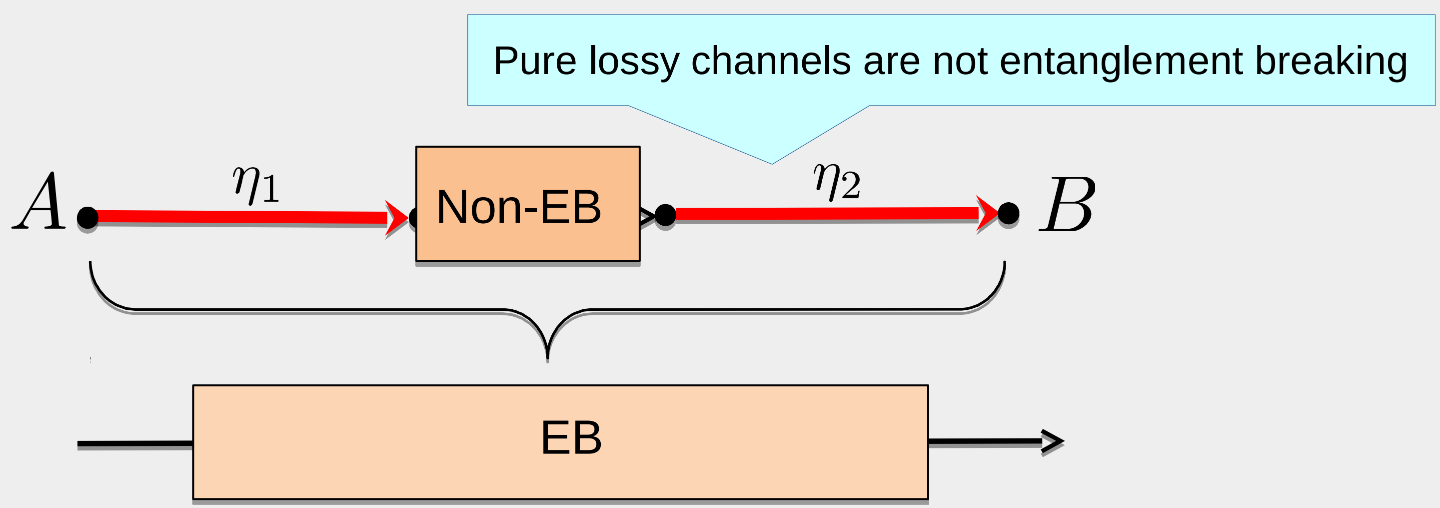
As a single module....



Single center station between lossy channels

- How does a center station modify the total channel?

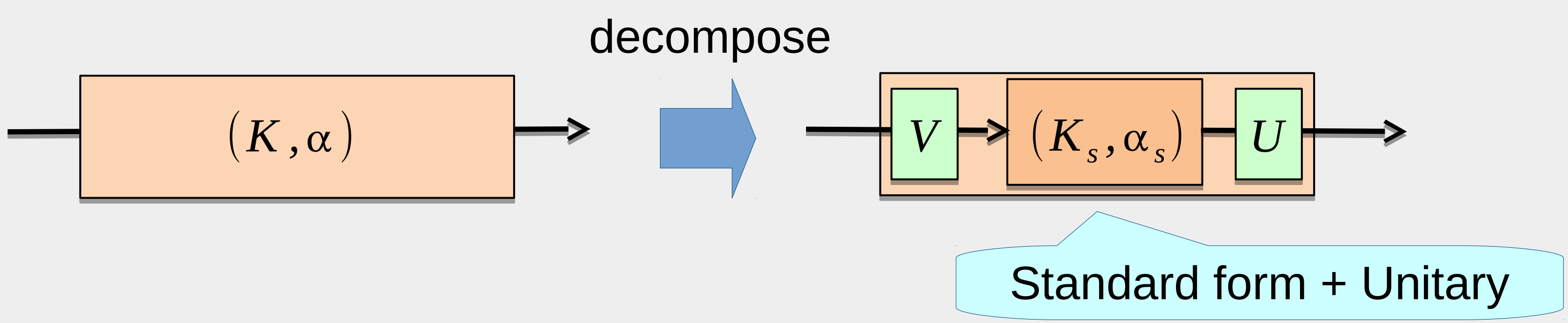
  -Single-mode Gaussian channels
  -Entanglement breaking (EB) conditions
  EB center station yields total EB channel.
  All we have to concern about is non-EB center stations!



As a single module....

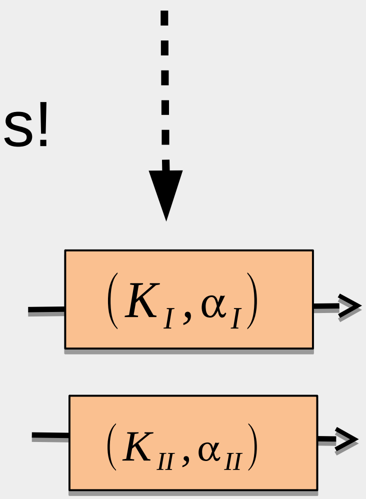
Single-mode Gaussian channels

- Unitary equivalent classification



Sufficient to consider two standard forms!

(I) Phase insensitive channel (PIC)
(II) Additive noise channel (ANC)



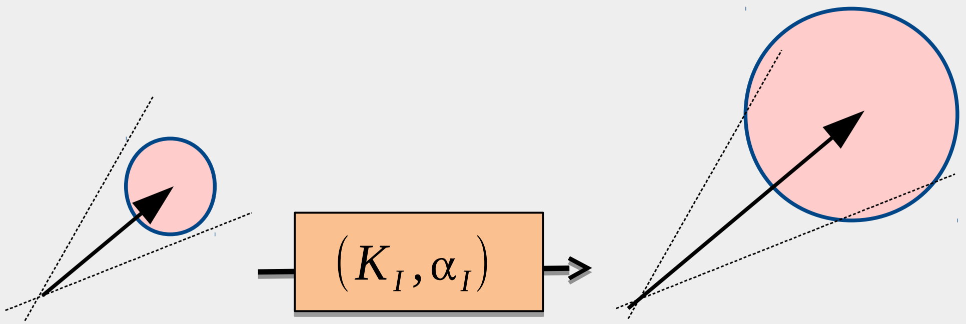
Holevo, Probl. Inf. Trans., 43, 1 (2007); Probl. Inf. Trans., 44, 171 (2008)

Non-entanglement breaking center stations

(I) Phase insensitive channel (PIC)

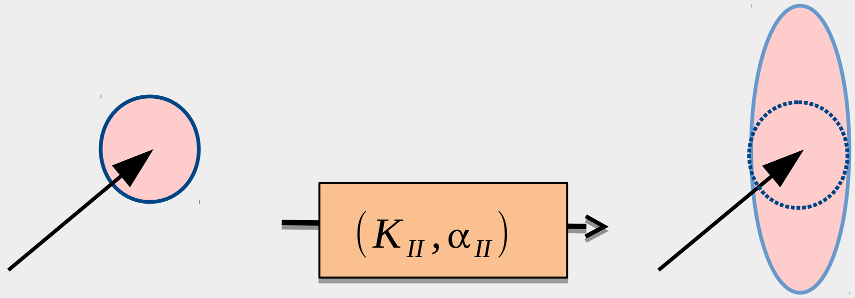
– Phase insensitive amplification/attenuation

Phase insensitive noise addition



(II) Additive noise channel (ANC)

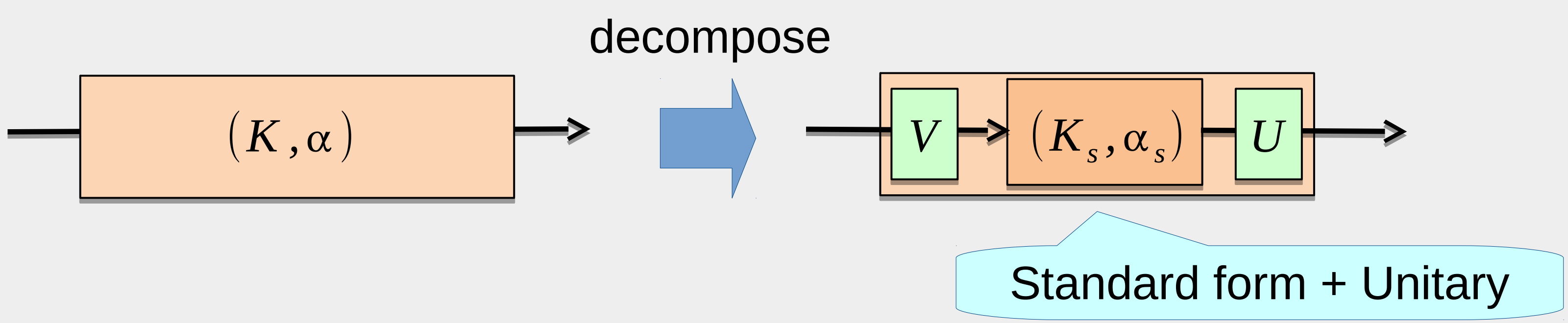
– Addition of a rank-1 noise



Holevo, Probl. Inf. Trans., 43, 1 (2007); Probl. Inf. Trans., 44, 171 (2008)

Single-mode Gaussian channels

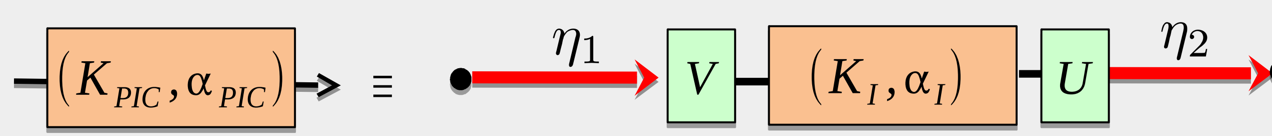
- Unitary equivalent classification



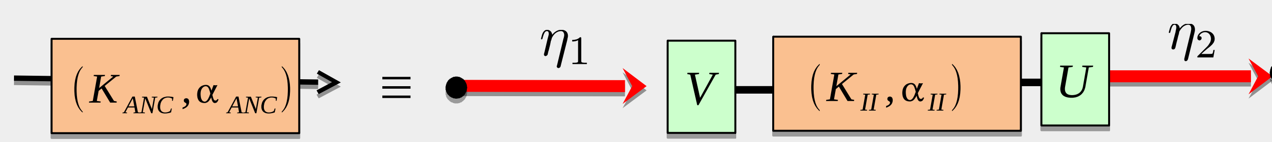
Sufficient to consider two standard forms!

- Entanglement breaking (EB) conditions:

$$\sqrt{det(\alpha_{PIC})} \geq \frac{1}{2}(1+g\,\eta_1\eta_2)$$



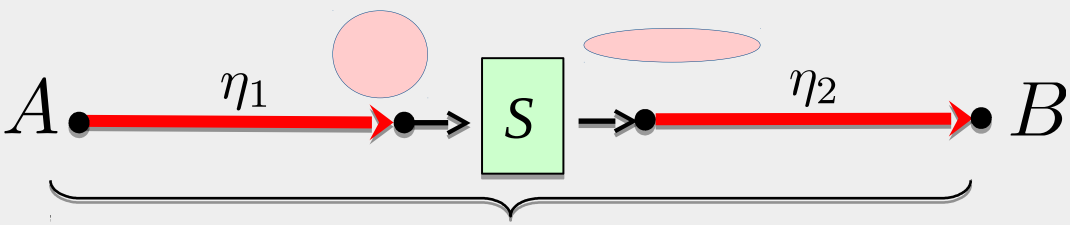
$$\sqrt{det(\alpha_{ANC})} \geq \frac{1}{2}(1+\eta_1\eta_2)$$



Holevo, Probl. Inf. Trans., 43, 1 (2007); Probl. Inf. Trans., 44, 171 (2008)

Examples: Quantum limited amplifiers

- Squeezer (Phase sensitive amplifier:PSA)



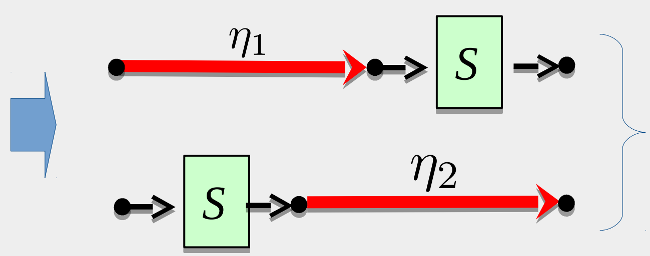
$$\frac{\Delta p^2}{\Delta x^2} = \left(\frac{\sqrt{G} - \sqrt{G-1}}{\sqrt{G} + \sqrt{G-1}} \right)^2, \; G \geq 1$$

$$K = Diag\left[\sqrt{G} + \sqrt{G-1}, \sqrt{G} - \sqrt{G-1}\right]$$

$$\alpha = 0$$

$\eta_2 = 1$

$\eta_1 = 1$

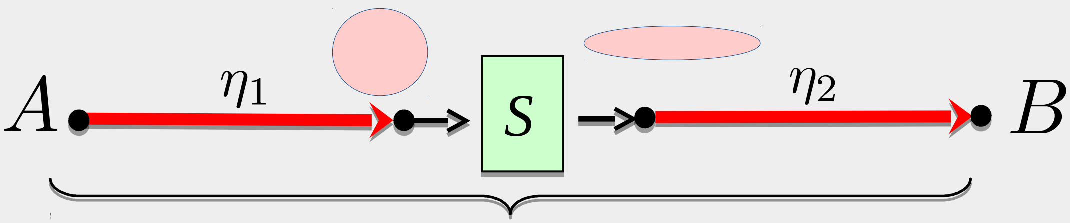


Unitary equivalent to a pure lossy channel

⇒ Not EB!

Examples: Quantum limited amplifiers

- Squeezer (Phase sensitive amplifier:PSA)



$$\frac{\Delta p^2}{\Delta x^2} = \left(\frac{\sqrt{G} - \sqrt{G-1}}{\sqrt{G} + \sqrt{G-1}} \right)^2, \; G \geq 1$$

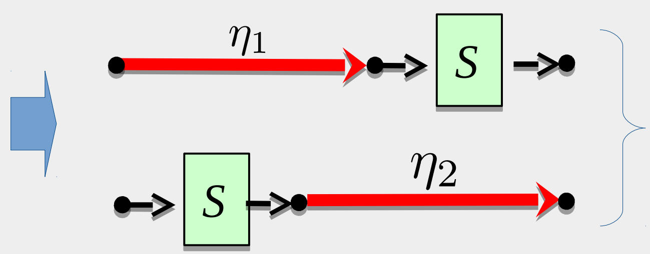
$$K = Diag\left[\sqrt{G} + \sqrt{G-1}, \sqrt{G} - \sqrt{G-1}\right]$$

$$\alpha = 0$$

EB if the gain fulfils $$G_{\mathrm{PSA}} \geq 1 + \frac{\eta_1}{(1-\eta_1)(1-\eta_2)}$$

$\eta_2 = 1$

$\eta_1 = 1$

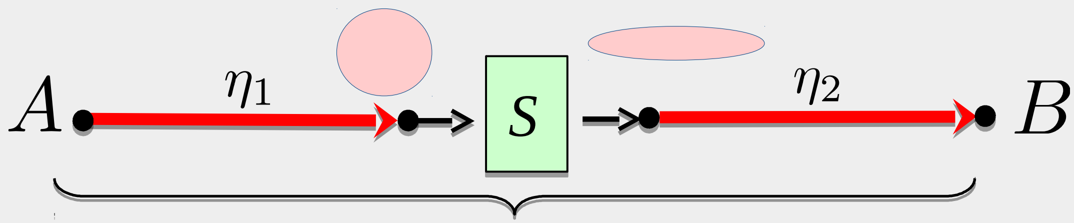


Unitary equivalent to a pure lossy channel
$\Rightarrow$ Not EB!

A middle unitary operation renders the channel entanglement breaking!

Examples: Quantum limited amplifiers

- Squeezer (Phase sensitive amplifier:PSA)

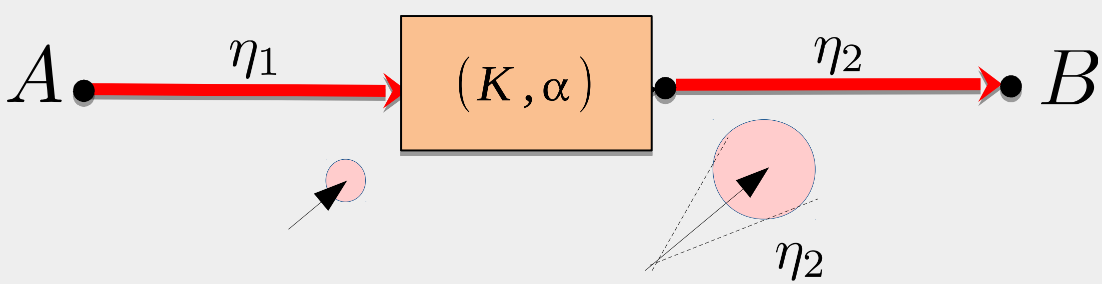


$$\frac{\Delta p^2}{\Delta x^2}=\left(\frac{\sqrt{G}-\sqrt{G-1}}{\sqrt{G}+\sqrt{G-1}}\right)^2,\ G\geq 1$$

$$K=Diag\left[\sqrt{G}+\sqrt{G-1},\sqrt{G}-\sqrt{G-1}\right]$$
$$\alpha=0$$

EB if the gain fulfils
$$G_{\mathrm{PSA}}\geq 1+\frac{\eta_1}{(1-\eta_1)(1-\eta_2)}$$

- Quantum-limited phase insensitive amplifier (PIA)

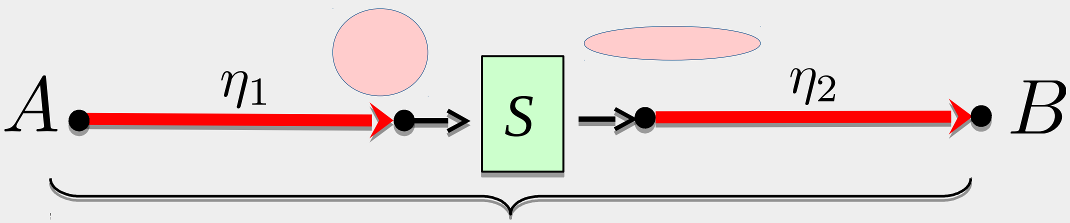


$$\frac{X_{output}}{X_{input}}=\sqrt{G}$$

$$K=\sqrt{G}\,I_2$$
$$\alpha=|1-G|\,I_2/2$$

Examples: Quantum limited amplifiers

- Squeezer (Phase sensitive amplifier:PSA)

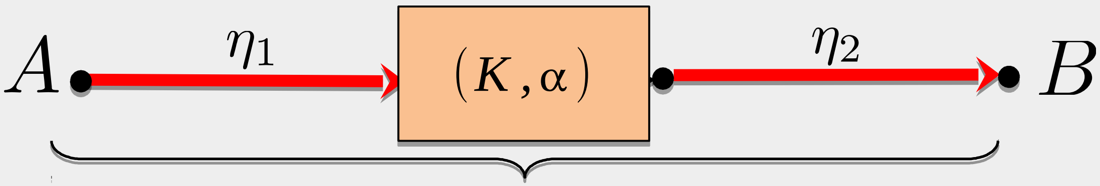


$$\frac{\Delta p^2}{\Delta x^2} = \left(\frac{\sqrt{G}-\sqrt{G-1}}{\sqrt{G}+\sqrt{G-1}}\right)^2, \; G \geq 1$$

$$K = Diag[\sqrt{G}+\sqrt{G-1}, \sqrt{G}-\sqrt{G-1}]$$
$$\alpha = 0$$

EB if the gain fulfils $$G_{\mathrm{PSA}} \geq 1 + \frac{\eta_1}{(1-\eta_1)(1-\eta_2)}$$

- Quantum-limited phase insensitive amplifier (PIA)



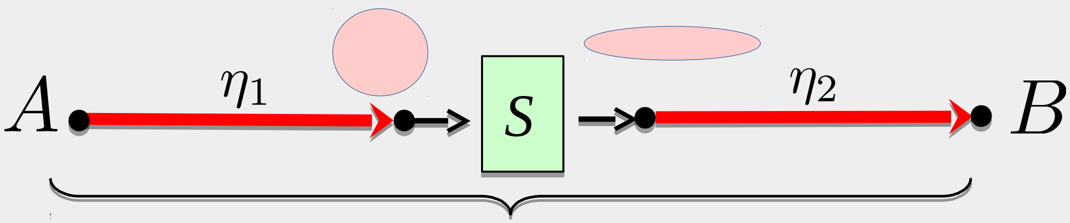
$$\frac{X_{output}}{X_{input}} = \sqrt{G}$$

$$K = \sqrt{G}\, I_2$$
$$\alpha = |1-G|\, I_2/2$$

EB if the gain fulfils $$G_{\mathrm{PIA}} \geq \frac{1}{1-\eta_1}$$

Examples: Quantum limited amplifiers

- Squeezer (Phase sensitive amplifier:PSA)



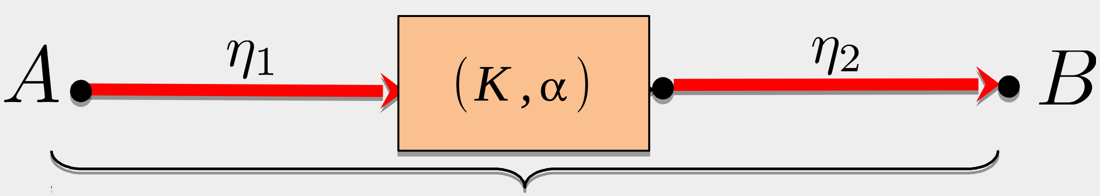
$$\frac{\Delta p^2}{\Delta x^2} = \left(\frac{\sqrt{G} - \sqrt{G-1}}{\sqrt{G} + \sqrt{G-1}} \right)^2, \; G \geq 1$$

$$K = Diag\left[\sqrt{G} + \sqrt{G-1}, \sqrt{G} - \sqrt{G-1}\right]$$

$$\alpha = 0$$

EB if the gain fulfils $G_{\mathrm{PSA}} \geq 1 + \frac{\eta_1}{(1-\eta_1)(1-\eta_2)}$

- Quantum-limited phase insensitive amplifier (PIA)



$$\frac{X_{output}}{X_{input}} = \sqrt{G}$$

$$K = \sqrt{G} I_2$$

$$\alpha = |1-G| I_2 / 2$$

EB if the gain fulfils $G_{\mathrm{PIA}} \geq \frac{1}{1-\eta_1}$

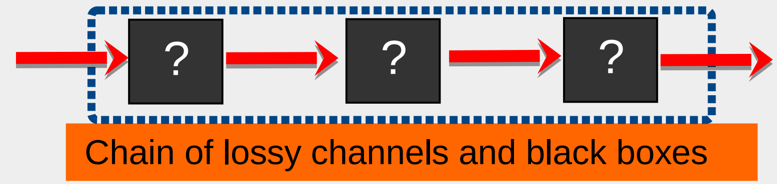
For a long distance $\eta_1, \eta_2 \ll 1 \rightarrow G \gtrsim 1$

– a small gain amplification renders the channel entanglement breaking!

Conclusion

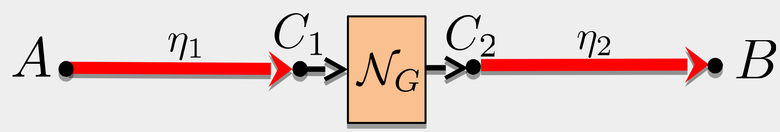
- Useful black boxes do exist!

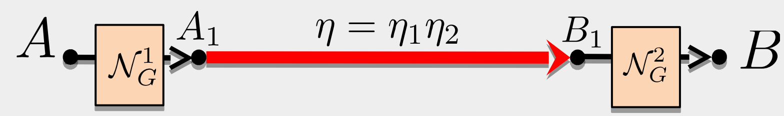
  Break the linear scaling R ~ η



- No-go result for Gaussian center stations

  General multi-mode Gaussian channels

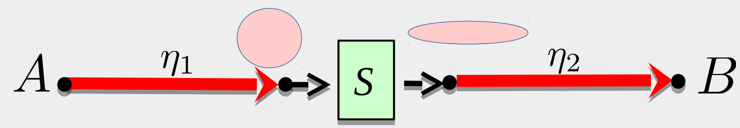




- Conditions that a single-mode Gaussian station make whole channel entanglement breaking (EB)

  Special cases: quantum limited amplifier

  – A small amplification could make the channel entanglement breaking Better off using amplifiers as repeater stations



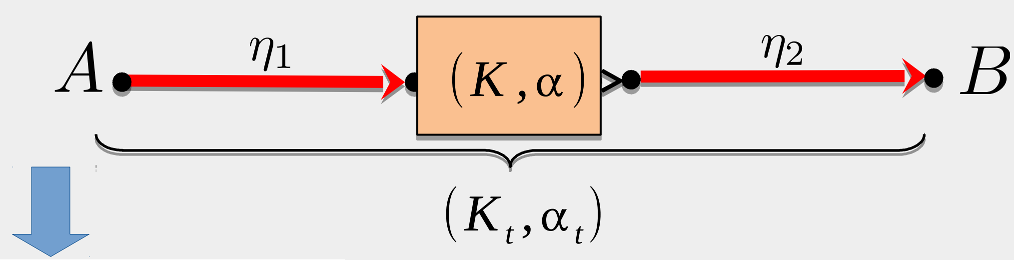
Construction

Sketch of Proof

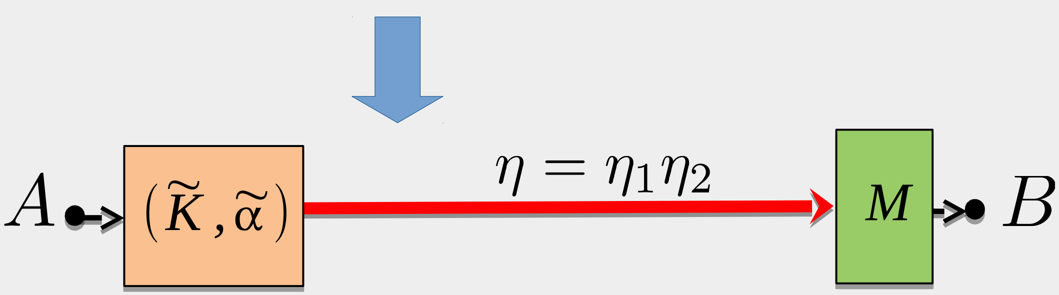
I. The total channel action

II. Existence of a noise term and a unitary matrix

III. Choose a gain term



$$\gamma' := \frac{\alpha_t - \eta_1 \eta_2 \alpha}{1 - \eta_1 \eta_2}, \quad M^T \gamma' M \geq \frac{1}{2} I_{2n}$$



$$\tilde{K} = \frac{1}{\sqrt{\eta_1 \eta_2}} K M$$

$$\tilde{\alpha} := \frac{1}{\eta_1 \eta_2} \left(M^T \alpha_t M - \frac{1 - \eta_1 \eta_2}{2} I_{2n} \right)$$