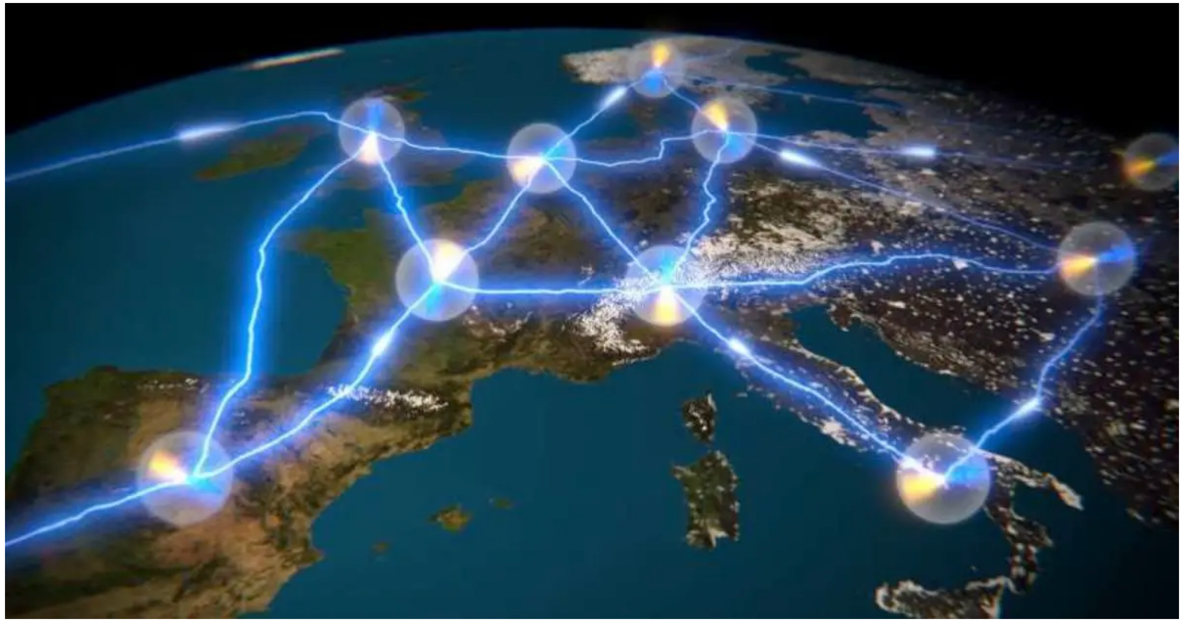
Verification of Continuous-Variable Quantum Memories

(and other devices)

Paolo Abiuso, CEQIP 2023

Some motivation



<u>Manipulation</u>

- Preparations
- Gates
- Measurements
- .....

vs

<u>Distribution</u>

- Storing
- Sending
- Interfacing

- Memory

$$t \longrightarrow \tau$$
$$\rho \longrightarrow \mathcal{M}[\rho]$$

- Transmission Line

$$x \longrightarrow y$$
$$\rho \longrightarrow \mathcal{L}[\rho]$$

- Transducer

$$\omega \longrightarrow \Omega$$
$$\rho \longrightarrow \mathcal{T}[\rho]$$

"Preserve information as well as possible"

What should a memory do?

- Channel should be as close as possible to the identity $\mathcal{M}[\rho] \approx \rho$
- Or should it? $\mathcal{M}[\rho] = U\rho U^\dagger$ is “equally” good

(also, isometries cannot be resolved without full trust in the devices)

- Fundamental property of a quantum memory:

being non Entanglement-Breaking (nEB)

$$\mathcal{N}^{EB} \otimes \mathbb{1}[\psi^+] = \rho^{\text{sep}}$$

$$\mathcal{N}^{EB}[\rho] = \sum_i \mathbf{Tr}[M^{(i)}\rho]\, \rho^{(i)}$$

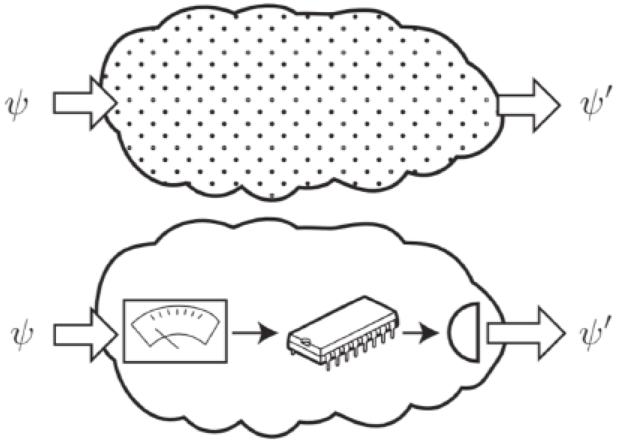
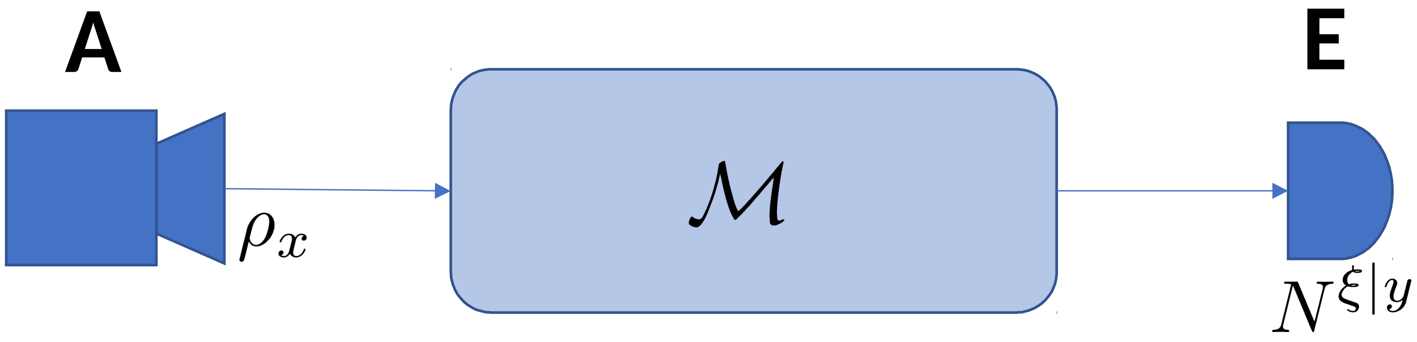


Image from: Rosset et al. PRX 8, 021033

EB channels
=
Measure&Prepare

The true title of this talk…

Certifying non Entanglement-Breaking channels (nEB)



$$p(\xi|x,y) = \mathrm{Tr}\left\{N^{\xi|y}\mathcal{M}[\rho_x]\right\}$$

Journal of the Optical Society of America B
OPTICAL PHYSICS

Verifying the quantumness of a channel with an untrusted device

MATTHEW F. PUSEY
Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada (m@physics.org)

- A,E, both trusted: tomography
- A untrusted: trivial
- A trusted, E untrusted: “interesting”

Theorem 1. *A channel from a trusted Alice to an untrusted Bob can be shown not to be entanglement breaking if and only if the measurements Bob induces on the input to the channel are not jointly measurable.*

Measurement compatibility

- A set of measurements $N^{\xi|y}$ is compatible, or *jointly measurable*, if

$$N^{\xi|y} = \sum_a p(\xi|a,y) M^a$$

- EB channels break the incompatibility of any set of measurements

$$\mathrm{Tr}\left\{N'^{\xi|y}\mathcal{M}[\rho]\right\} = \sum_a \mathrm{Tr}\left\{N'^{\xi|y}\rho_a \mathrm{Tr}\left\{M^a\rho\right\}\right\} = \mathrm{Tr}\left\{N^{\xi|y}\rho\right\}$$

$$\left(p(\xi|a,y) = \mathrm{Tr}\{N'^{\xi|y}\rho_a\}\right)$$

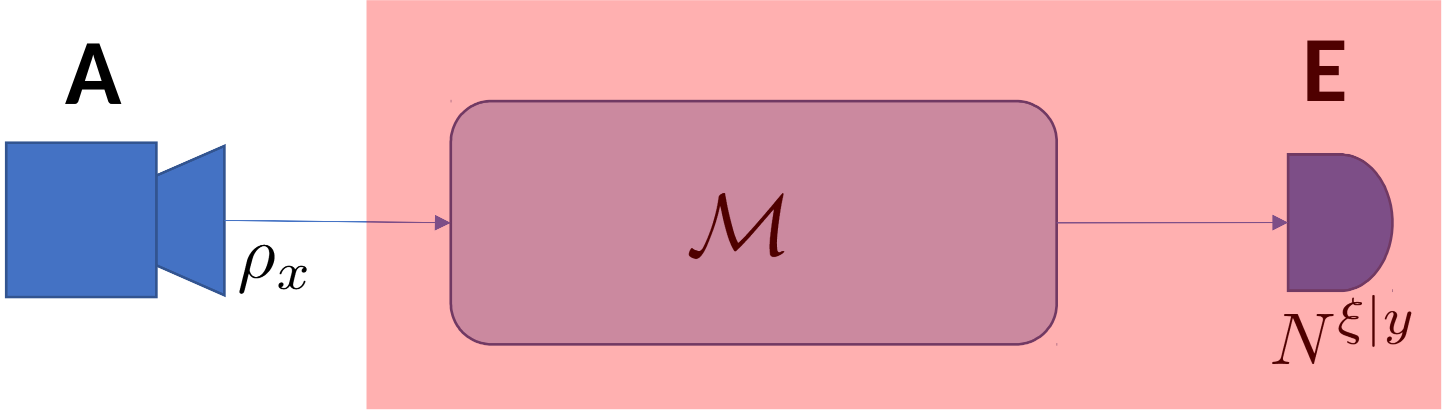
- EB channels IB channels

PAPER

Incompatibility breaking quantum channels

To cite this article: Teiko Heinosaari *et al* 2015 *J. Phys. A: Math. Theor.* **48** 435301

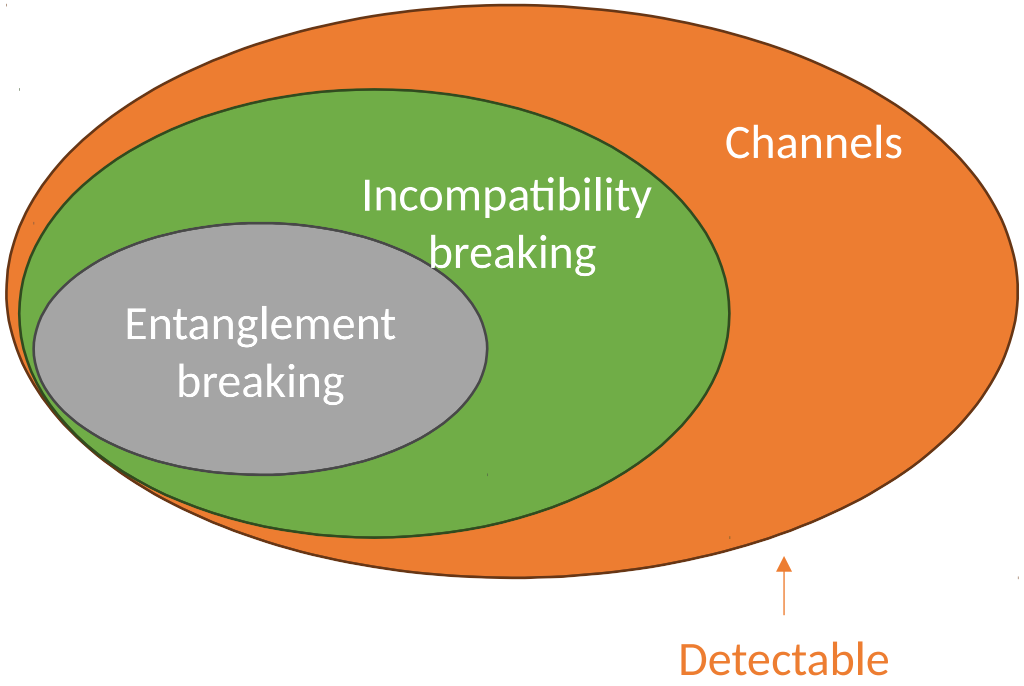
Pusey 1-mode *measurement-device-independent* scenario



Journal of the Optical Society of America B
OPTICAL PHYSICS

Verifying the quantumness of a channel with an untrusted device

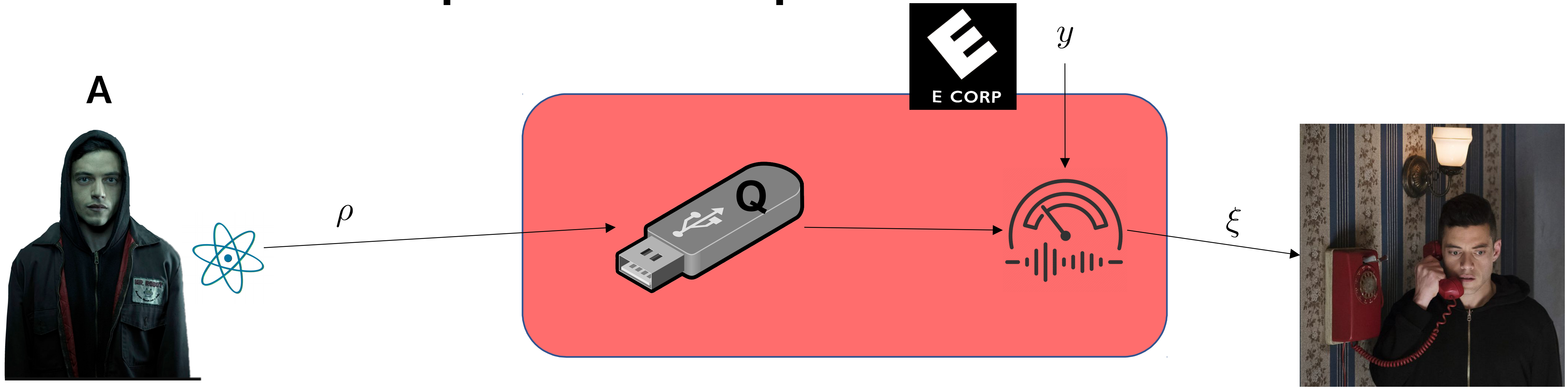
Matthew F. Pusey
Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada (m@physics.org)

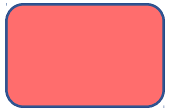


Theorem 1. *A channel from a trusted Alice to an untrusted Bob can be shown not to be entanglement breaking if and only if the measurements Bob induces on the input to the channel are not jointly measurable.*

Measurement-device-independent scenario:

Untrusted quantum providers



 $\equiv N^{\xi|y}$

MDI certification of nEB channel= Tomography of the induced measurement

However: how do we know the memory was used in the first place? (similarly for transmission lines, transducers)

no way to guarantee in general

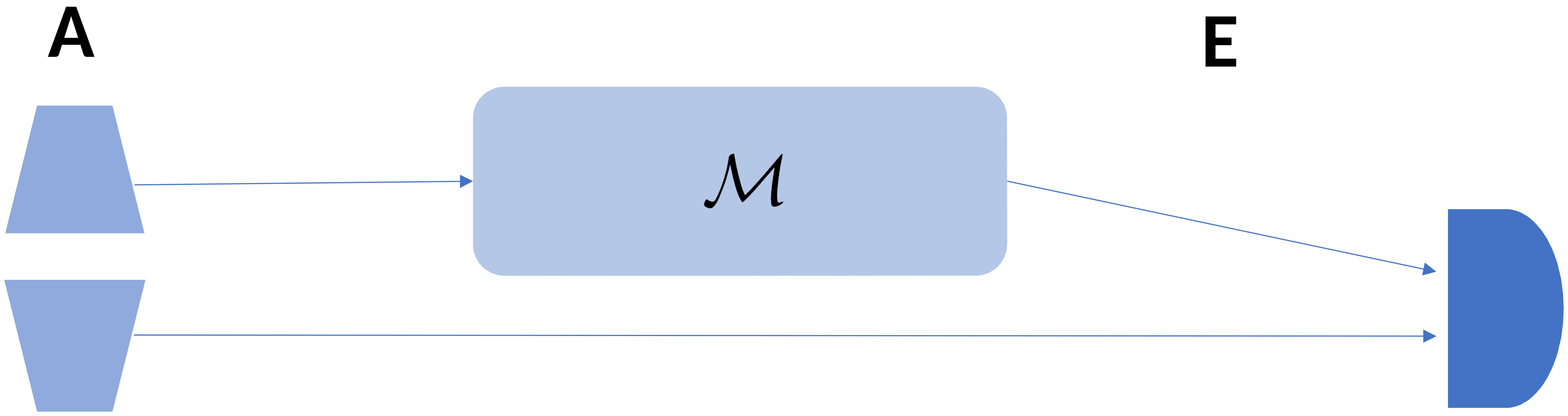
PHYSICAL REVIEW X **8**, 021033 (2018)

Resource Theory of Quantum Memories and Their Faithful Verification with Minimal Assumptions

Denis Rosset,[1,2,4,*] Francesco Buscemi,[3,†] and Yeong-Cherng Liang[1,‡]
[1]*Department of Physics, National Cheng Kung University, Tainan 701, Taiwan*
[2]*Group of Applied Physics, Université de Genève, 1211 Genève, Switzerland*
[3]*Department of Mathematical Informatics, Nagoya University, Chikusa-ku, Nagoya 464-8601, Japan*
[4]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, Canada N2L 2Y5*

Bipartite scenario

- A,E, both trusted: tomography
- A,E both untrusted? device-independent protocol, with no additional assumptions, is not possible
- An MDI protocol is "minimal" in this scenario, <u>can guarantee the use of the memory and can be constructed without using entangled sources</u>



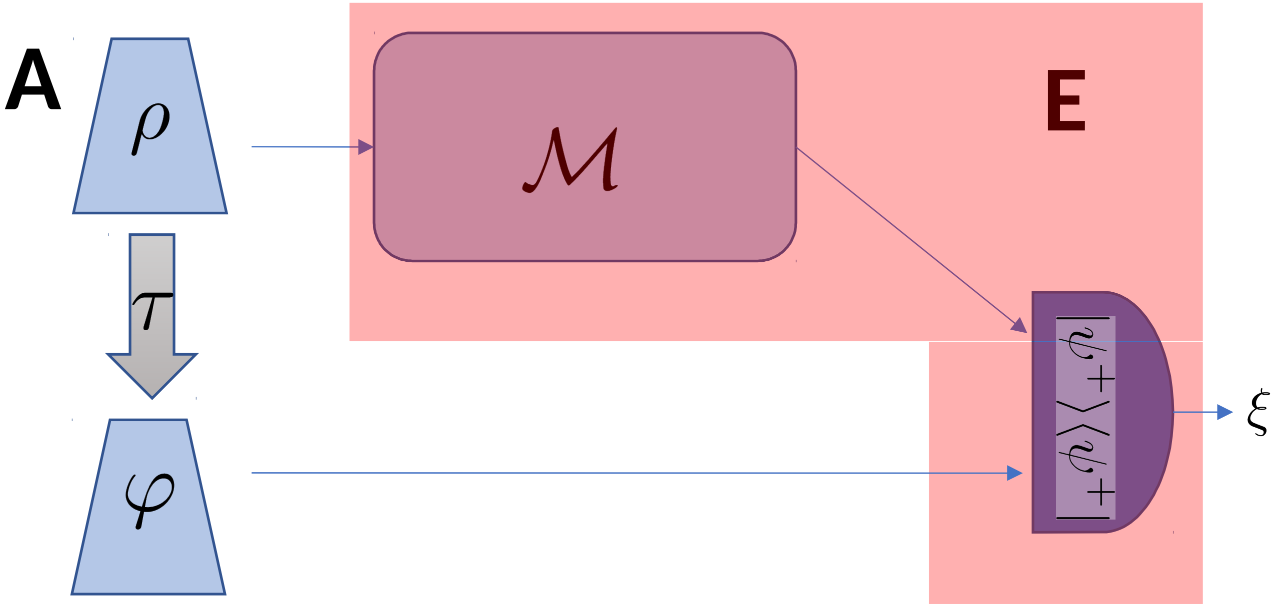
Protocol by Rosset et al., PRX 8

- Send ρ
- Wait memory time τ
- Send φ
- Eve's measurement:

- Send
- Wait memory time
- Send
- Eve's measurement:

$N^{\xi=0} = |\psi^+\rangle\langle\psi^+|\,,\ N^{\xi=1} = \mathbb{1} - |\psi^+\rangle\langle\psi^+|$

$$|\psi^+\rangle = \frac{1}{\sqrt{d}}\sum_i |ii\rangle$$



$$P(\xi = 0|\rho,\varphi) = \frac{1}{d}\mathrm{Tr}[\varphi^T \mathcal{M}[\rho]]$$

$$\mathrm{Tr}[W(\mathbf{1}\otimes\mathcal{M})[\psi^+]] > 0$$

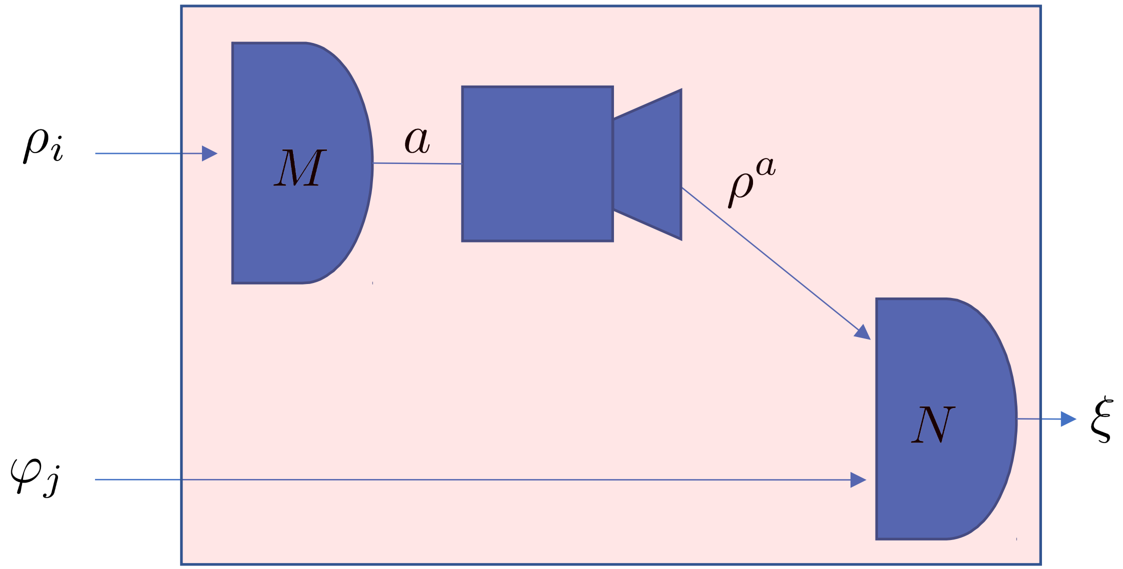
$$\mathrm{Tr}[W\rho^{\mathrm{sep}}] \leq 0$$

$$W = \sum_{ij} c_{ij}\rho_i^T \otimes \varphi_j^T$$

$$\sum_{ij} c_{ij} P(\xi = 0|\rho_i,\varphi_j) \propto \mathrm{Tr}[W(\mathbf{1}\otimes\mathcal{M})[\psi^+]] > 0$$

WITNESS of nEB

In case the memory is entanglement breaking



$$P(\xi = 0|\rho_i, \varphi_j) = \sum_a \mathrm{Tr}[N^\xi \rho^a \otimes \varphi_j]\mathrm{Tr}[M^a \rho_i]$$

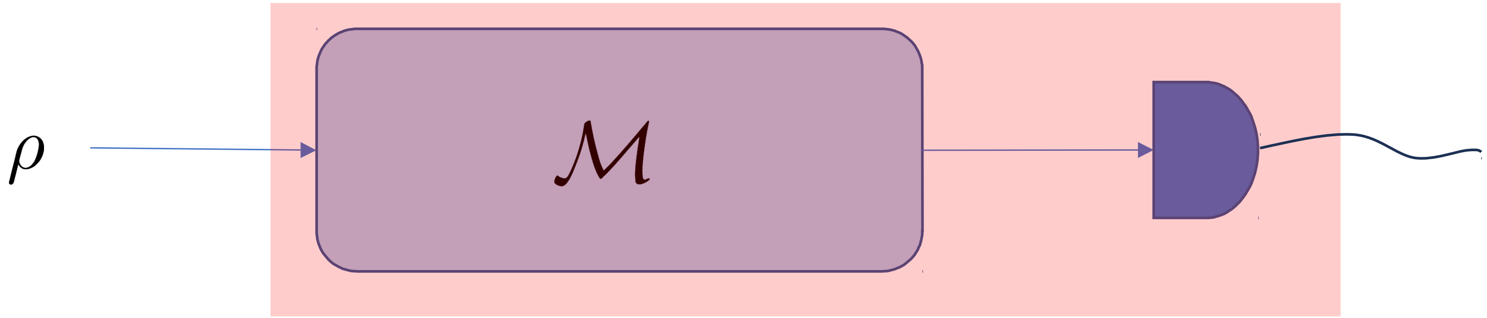
$$= \sum_a \mathrm{Tr}[(M^a \otimes N^{\xi=0|a})\rho_i \otimes \varphi_j]$$

$$W = \sum_{ij} c_{ij} \rho_i^T \otimes \varphi_j^T$$

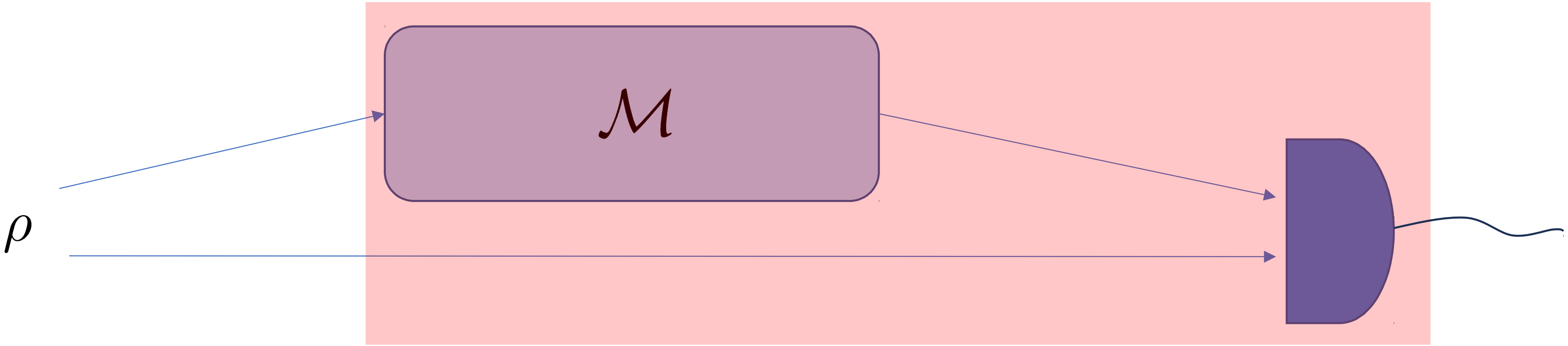
$$\sum_{ij} c_{ij} P(\xi = 0|\rho_i, \varphi_j) \propto \mathrm{Tr}[W \rho^{\mathrm{sep}}] \leq 0$$

A look at MDI protocols vs nEB channels, from the point of view of induced measurements

- Pusey scenario: compatible vs incompatible measurements



- Rosset scenario: All bipartite measurements vs 1-LOCC measurements



Some experiments

PHYSICAL REVIEW LETTERS **124**, 010503 (2020)

Measurement-Device-Independent Verification of Quantum Channels

Francesco Graffitti,[1,*] Alexander Pickston,[1] Peter Barrow,[1] Massimiliano Proietti,[1] Dmytro Kundys,[1]
Denis Rosset,[2] Martin Ringbauer,[3] and Alessandro Fedrizzi[1]

[1]*Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*
[2]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, Canada N2L 2Y5*
[3]*Institut für Experimentalphysik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria*

PHYSICAL REVIEW LETTERS **124**, 010502 (2020)

Experimentally Verified Approach to Nonentanglement-Breaking Channel Certification

Yingqiu Mao,[1,2,§] Yi-Zheng Zhen,[3,1,§] Hui Liu,[1,2] Mi Zou,[1,2] Qi-Jie Tang,[1,2] Si-Jie Zhang,[1,2] Jian Wang,[1,2]
Hao Liang,[1,2] Weijun Zhang,[4] Hao Li,[4] Lixing You,[4] Zhen Wang,[4] Li Li,[1,2] Nai-Le Liu,[1,2] Kai Chen,[1,2,*]
Teng-Yun Chen,[1,2,†] and Jian-Wei Pan[1,2,‡]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*
[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*
[3]*Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, Guangdong 518055, People's Republic of China*
[4]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, People's Republic of China*

Measurement-Device-Independent Verification of a Quantum Memory

Yong Yu, Peng-Fei Sun, Yu-Zhe Zhang, Bing Bai, Yu-Qiang Fang, Xi-Yu Luo, Zi-Ye An, Jun Li, Jun Zhang, Feihu Xu, Xiao-Hui Bao, and Jian-Wei Pan

Phys. Rev. Lett. **127**, 160502 – Published 14 October 2021

MDI witnessing of all nEB channels!

However:

- Only for finite-dimensional memories
- One needs to know the specific witness $\mathcal{W}$

A proposal for continuous-variable systems

arXiv 2305.07513

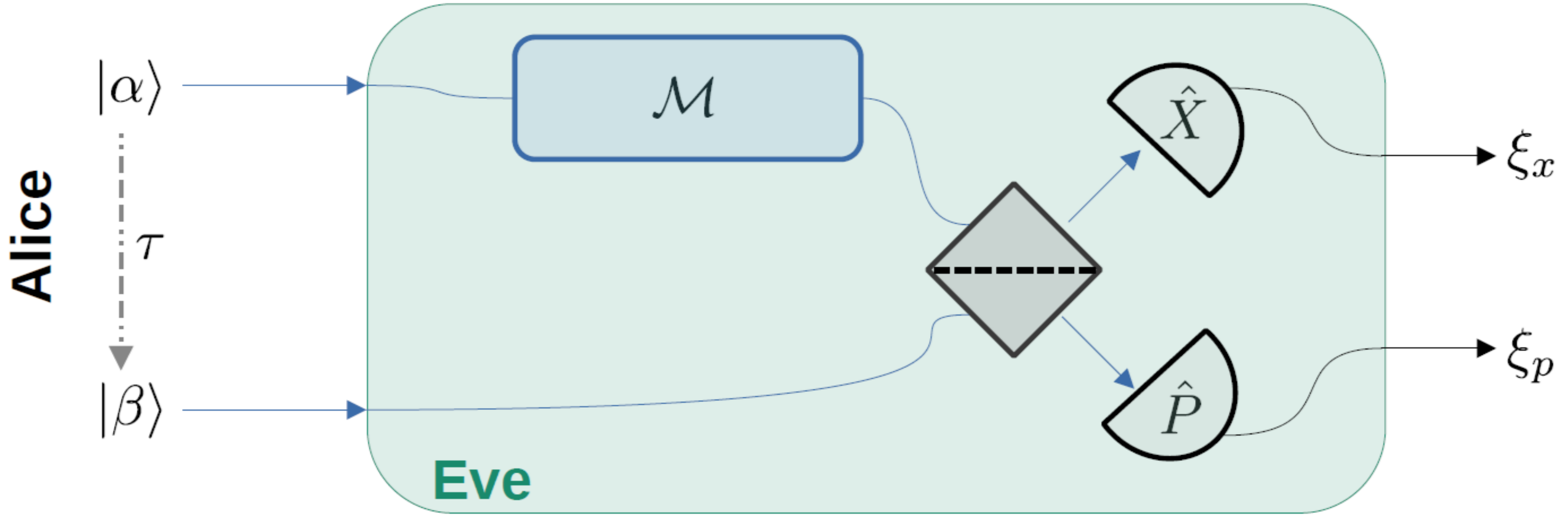
$$|\alpha\rangle = e^{\alpha \hat{a}^\dagger - \alpha^* \hat{a}}|0\rangle$$

$$\alpha = \alpha_x + i\alpha_p$$

$$\hat{X} = \frac{a + a^\dagger}{\sqrt{2}} \qquad \hat{P} = \frac{a - a^\dagger}{i\sqrt{2}}$$

$$\langle \hat{X} \rangle_\alpha = \sqrt{2}\alpha_x \quad \langle \Delta \hat{X}^2 \rangle_\alpha = \frac{1}{2}$$

$$\langle \hat{P} \rangle_\alpha = \sqrt{2}\alpha_p \quad \langle \Delta \hat{P}^2 \rangle_\alpha = \frac{1}{2}$$



$$\mathcal{W} := \left\langle \left(\xi_x - (\alpha_x + \beta_x)\right)^2 + \left(\xi_p - (\alpha_p - \beta_p)\right)^2 \right\rangle$$

$$\mathcal{M} \equiv \mathbb{1}$$

$$\hat{X}_E := \frac{\hat{x}_\alpha + \hat{x}_\beta}{\sqrt{2}} = \alpha_x + \beta_x + \hat{V}$$

$$\hat{P}_E := \frac{\hat{p}_\alpha - \hat{p}_\beta}{\sqrt{2}} = \alpha_p - \beta_p + \hat{V}$$

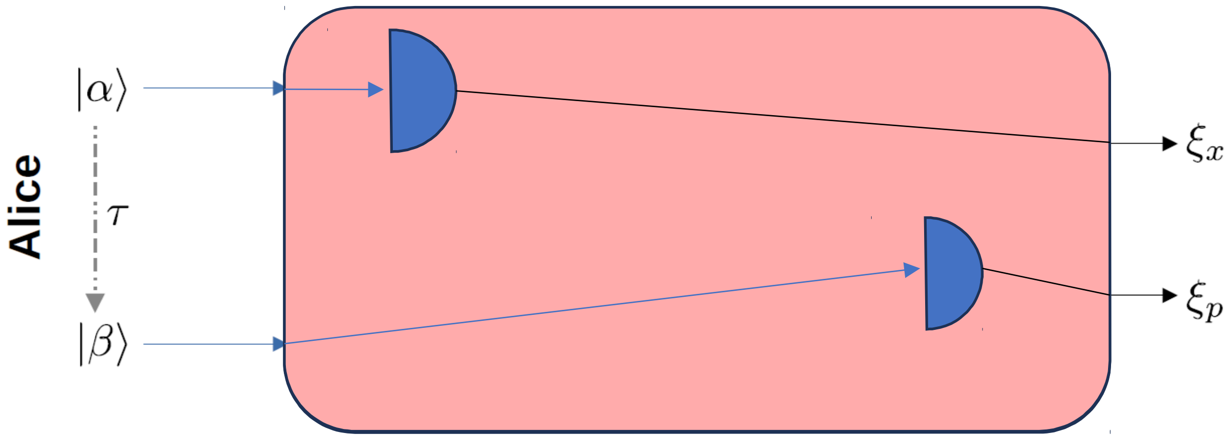
$$\to \mathcal{W} = 1$$

Main result

If $\mathcal{M}$ is EB $\Rightarrow \mathcal{W} \geq\sim 2$

Idea of the proof

$$\mathcal{W} := \left\langle (\xi_x - (\alpha_x + \beta_x))^2 + (\xi_p - (\alpha_p - \beta_p))^2 \right\rangle$$



Estimating $\alpha_x + \beta_x$ and $\alpha_p - \beta_p$

with minimum error

Memory is EB ~ measuring $|\alpha\rangle$ separately

$$\frac{\hat{x}_\alpha + \hat{x}_0}{\sqrt{2}} = \alpha_x + \hat{V} \qquad \frac{\hat{p}_\alpha + \hat{x}_0}{\sqrt{2}} = \alpha_p + \hat{V} \qquad \frac{\hat{x}_\beta + \hat{x}_0}{\sqrt{2}} = \beta_x + \hat{V} \qquad \frac{\hat{p}_\beta + \hat{x}_0}{\sqrt{2}} = \beta_p + \hat{V}$$

What channels can we witness this way?

- That is, for what class of channels can one achieve $1 \leq \mathcal{W} \leq 2$?

Second main result

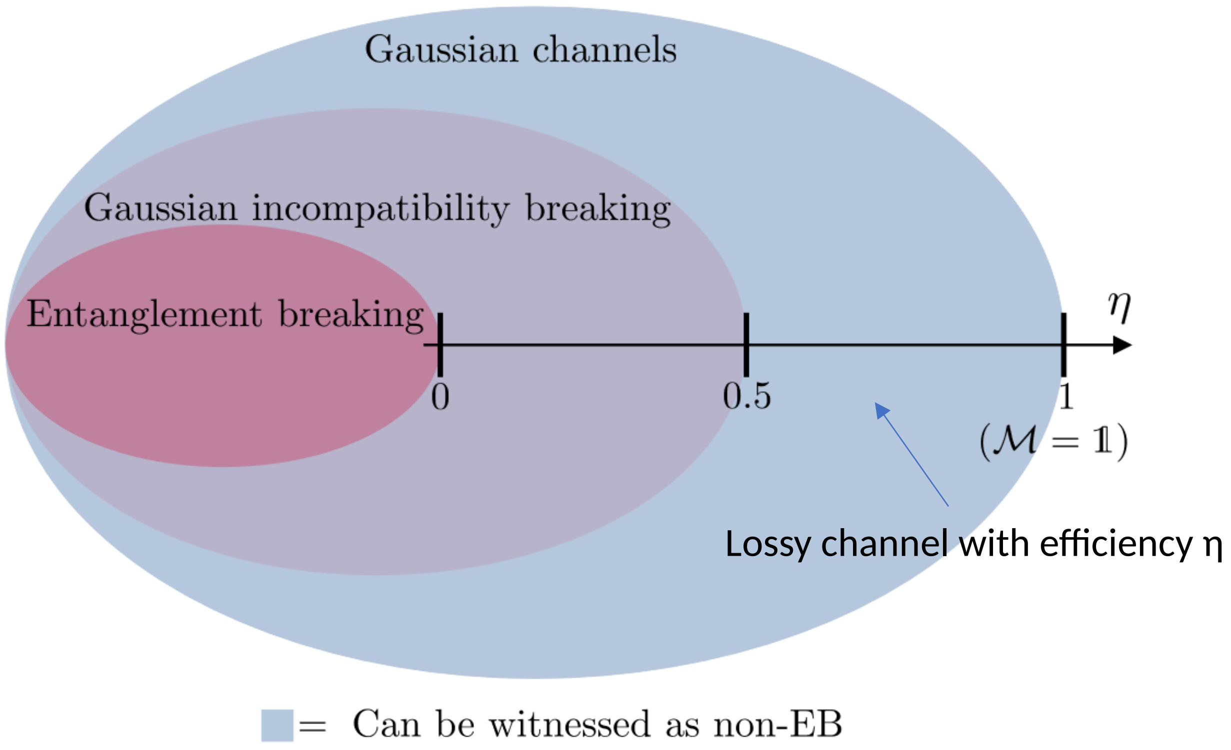
=Gaussian non Incompatibility-Breaking channels

i.e. those such that

$$\mathcal{C}^\dagger[N^{\xi|y}] = \sum_a p(\xi|a,y) M^a$$

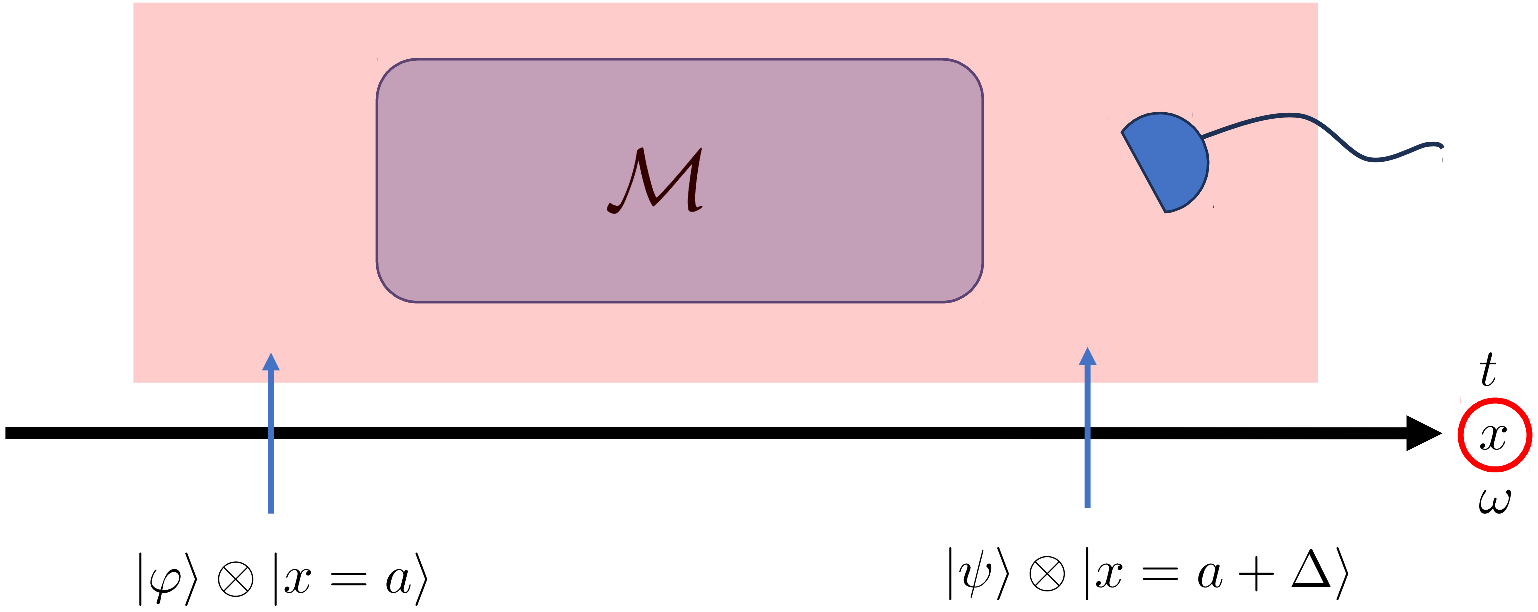
For all Gaussian measurements

ALL WITH THE SAME WITNESS
+ simple attenuations/amplifications



Other devices?

- Time, position, frequency.....
- Time is different ✉ irreversibility allows 1-way certification

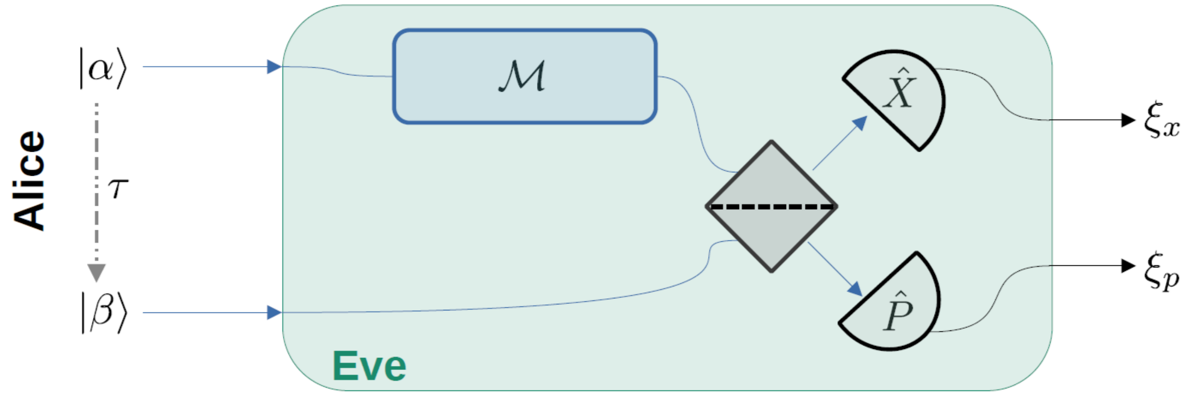


…and that's a wrap!

- Good quantum memories (lines, transducers…) are non Entanglement-Breaking
- Certification of nEB channels makes sense (mostly) in the MDI scenario
- Constructive protocol for discrete-variable memories
- Simple protocol for CV memories
- Outlook: other devices, MDI certifications in networks, practical protocols for honest users with untrusted providers…

- Papers:

Pusey, 2015; *JOSA B*, *32*(4),
Rosset, Buscemi, Liang, 2018; *PRX*, *8*(2).
Abiuso; 2305.07513

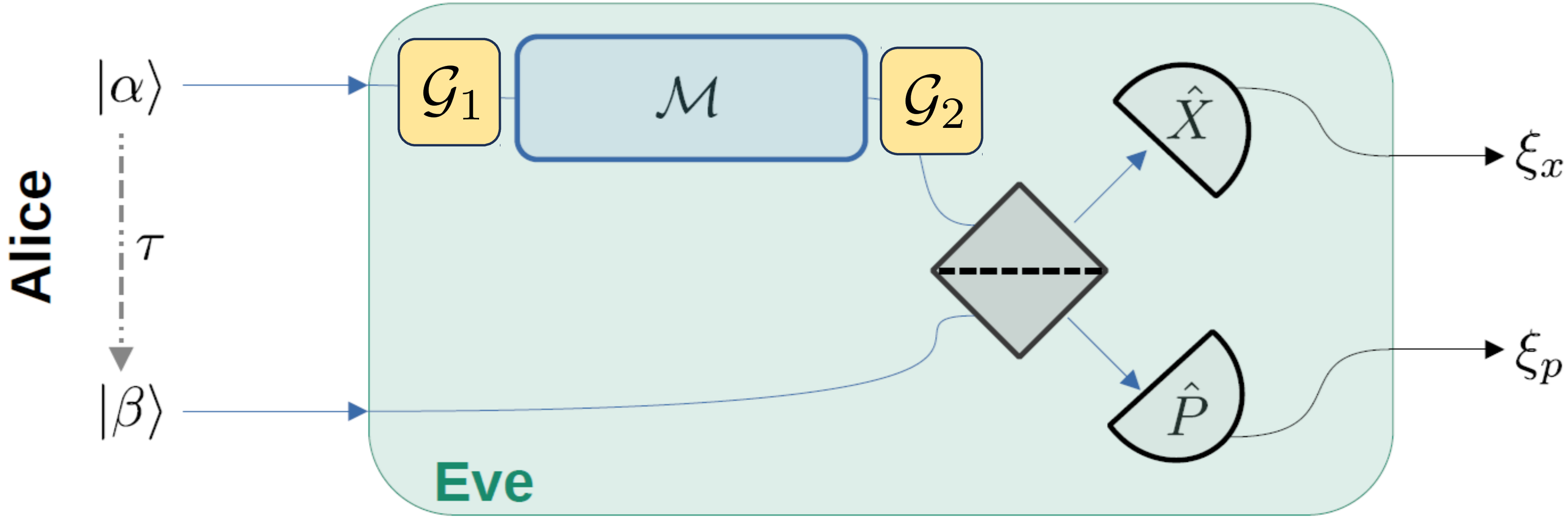


$$\mathcal{W} := \left\langle (\xi_x - (\alpha_x + \beta_x))^2 + (\xi_p - (\alpha_p - \beta_p))^2 \right\rangle$$

Result 1 *Consider the above protocol in which uncorrelated random coherent states $|\alpha\rangle$,$|\beta\rangle$ are sent (with a delay between them) to Eve, which stores $|\alpha\rangle$ in their memory and is then able to perform any joint measurement on $\mathcal{M}[|\alpha\rangle\langle\alpha|] \otimes |\beta\rangle\langle\beta|$. If $\mathcal{M}$ is entanglement breaking, the minimum value of $\langle\mathcal{W}\rangle$ (10) is bounded by*

$$\langle\mathcal{W}\rangle \geq \frac{\sigma_\alpha^2}{1+\sigma_\alpha^2} + \frac{\sigma_\beta^2}{1+\sigma_\beta^2} \,. \tag{12}$$

Here $\sigma_{\alpha,\beta}$ correspond to the width of the distribution with which $\{\alpha, \beta\}$ are sampled, which we assume to be Gaussian for simplicity, i.e. $P(\alpha) = (\pi\sigma_\alpha^2)^{-1}\mathrm{Exp}[-|\alpha|^2/\sigma_\alpha^2]$



Result 2 *Any memory $\mathcal{M}$ consisting in a Gaussian channel that is not Gaussian incompatibility breaking (gIB) [18], can be used to obtain a score* (10) $\langle \mathcal{W} \rangle < 2$, *by appending Gaussian channels $\mathcal{G}_{1,2}$ to it and performing the above described protocol (cf. Fig. 1) with $\mathcal{M}' \equiv \mathcal{G}_2 \circ \mathcal{M} \circ \mathcal{G}_1$. By choosing $\sigma_{\alpha,\beta}$ large enough, this implies the violation of the bound* (12) *and certifies the memory $\mathcal{M}$ to be non-EB.*