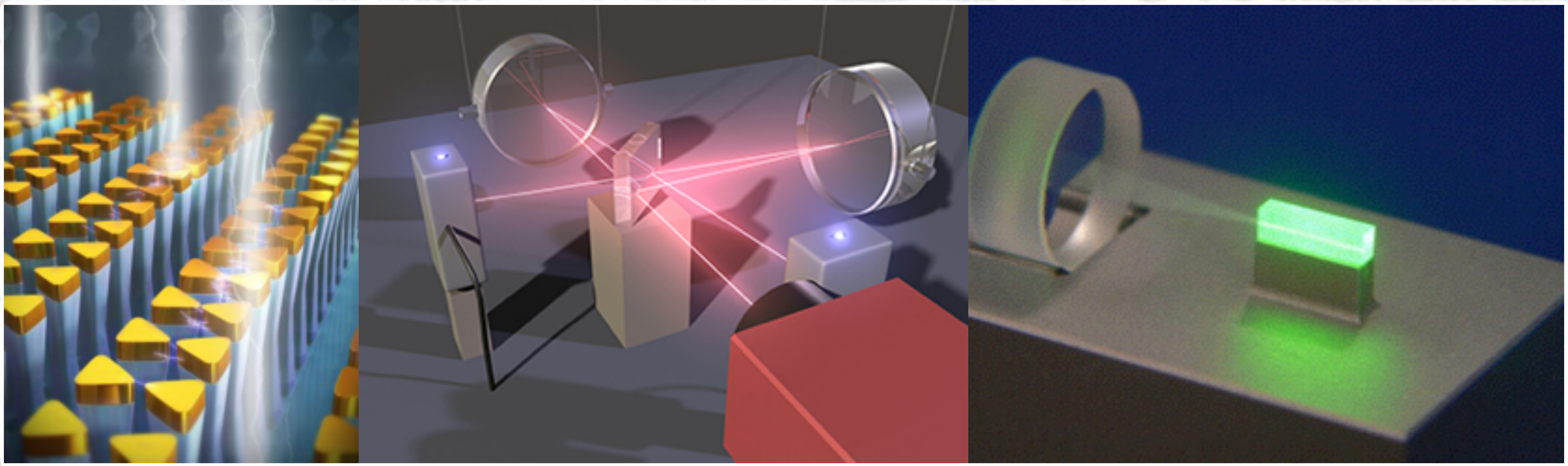
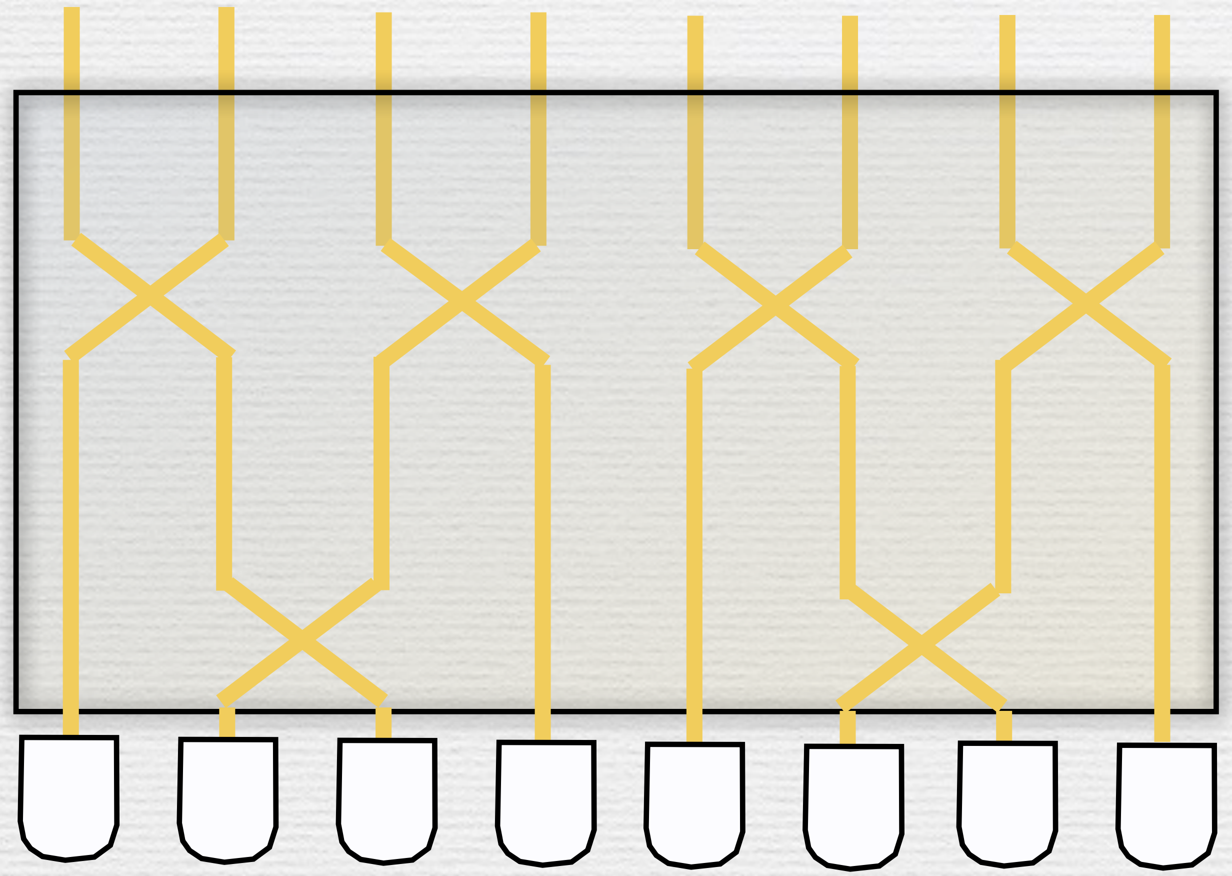
Certifying continuous-variable quantum systems



Jens Eisert, FU Berlin
Joint work with C. Gogolin, M. Kliesch, L. Aolita, P. Hyllus, A. Steffens

- Recent advances in continuous-variable quantum information

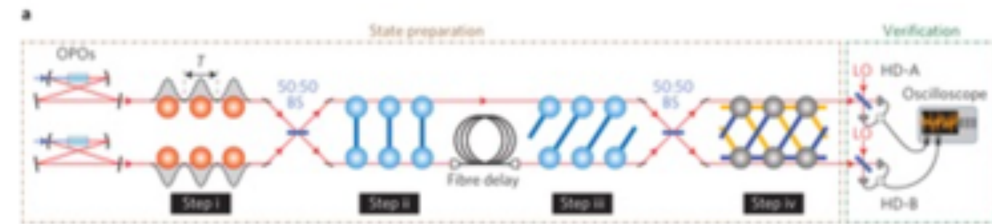
Continuous (and discrete) variable quantum devices



- Recent advances in continuous-variable quantum information
- Theoretical and mathematical advances (why we are here)

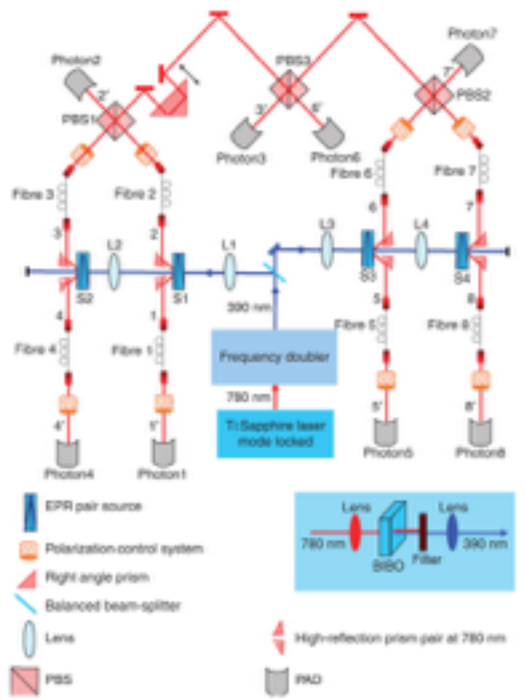
Continuous (and discrete) variable quantum devices

- **Multi-mode squeezed Gaussian states**



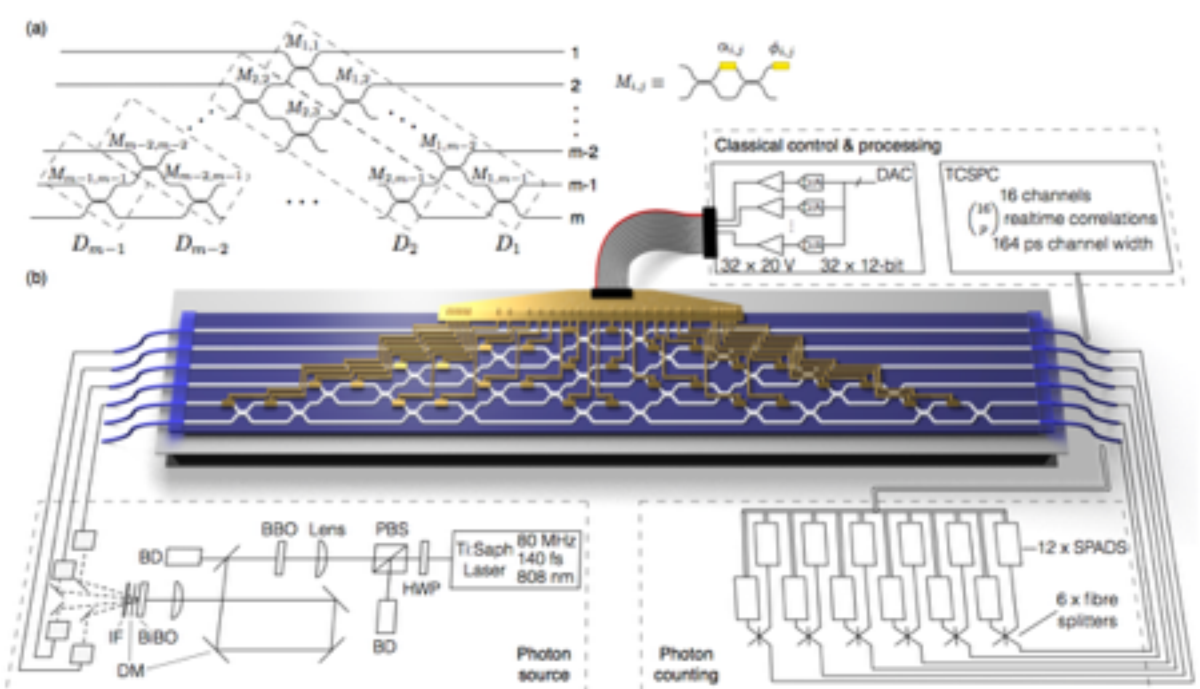
Pfister, Schnabel, Furusawa, Trebs, etc

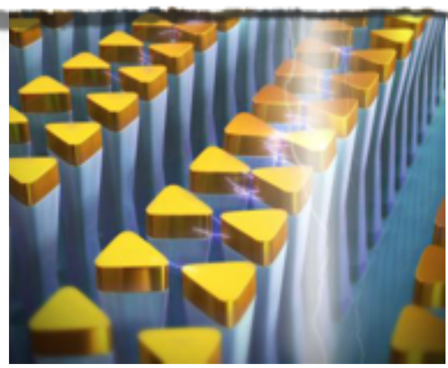
- **Photonic multi-qubit entangled states**



Weinfurter, Pan, Guo, Walther, Walborn, etc

- **On-chip integrated photonic devices**

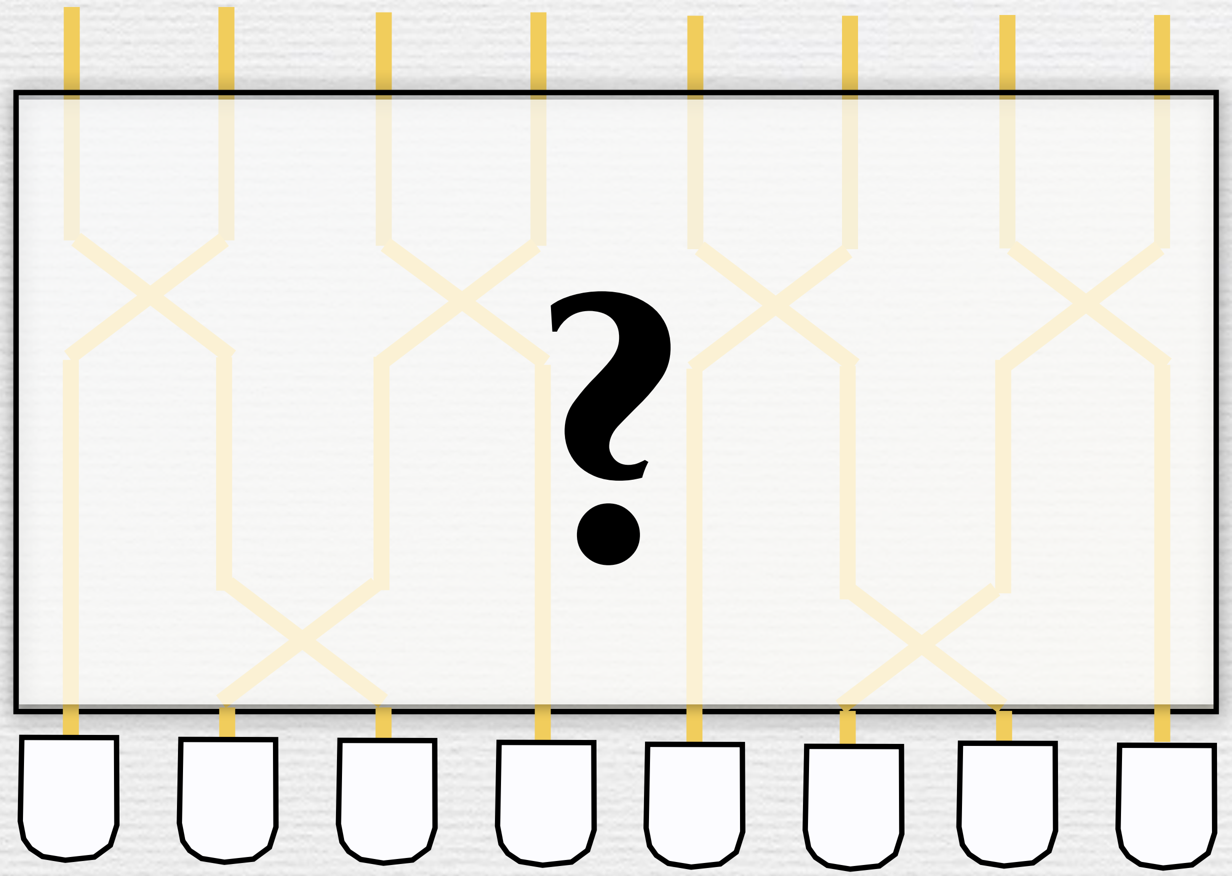




Aspelmeyer, Painter

- Recent advances in continuous-variable quantum information
- Theoretical and mathematical advances (why we are here)

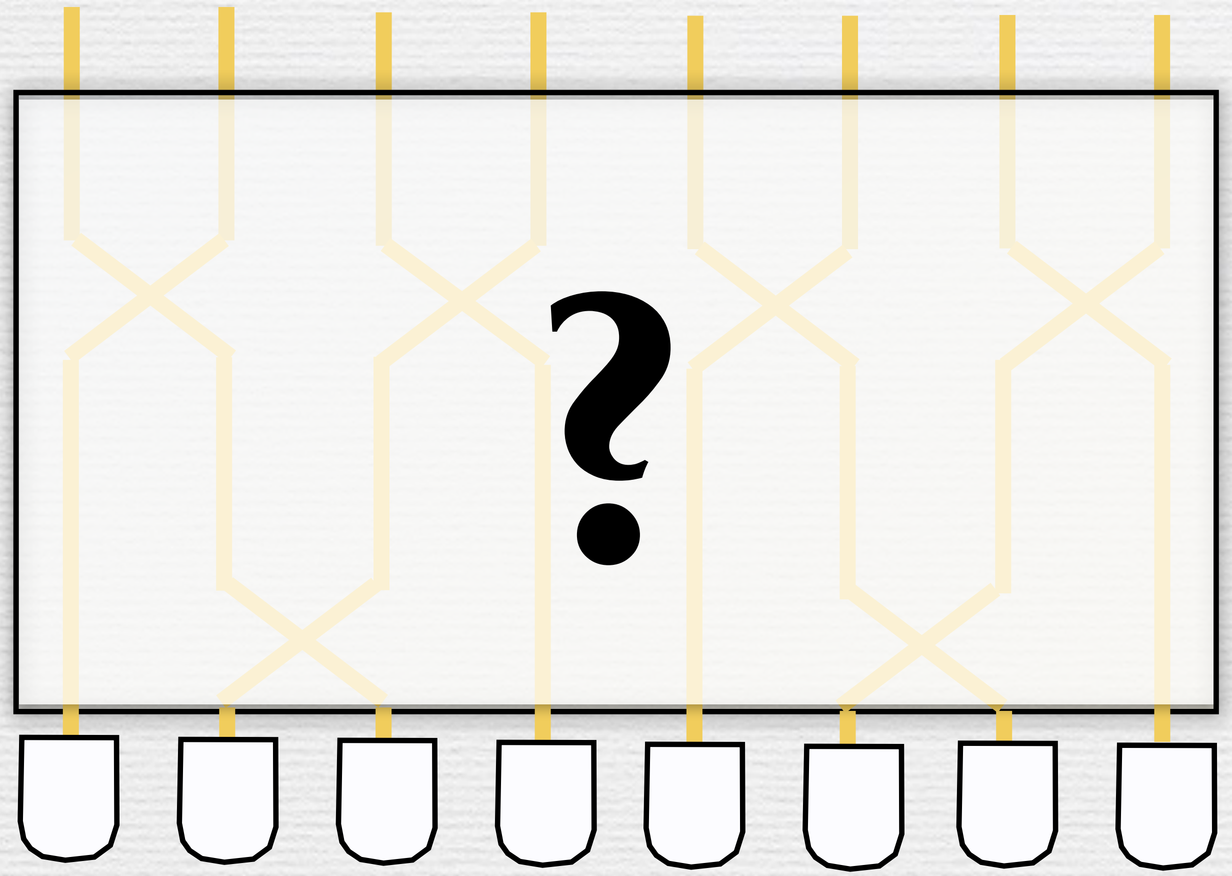
Continuous (and discrete) variable quantum devices



- How do we know the devices work?

- Recent advances in continuous-variable quantum information
- Theoretical and mathematical advances (why we are here)

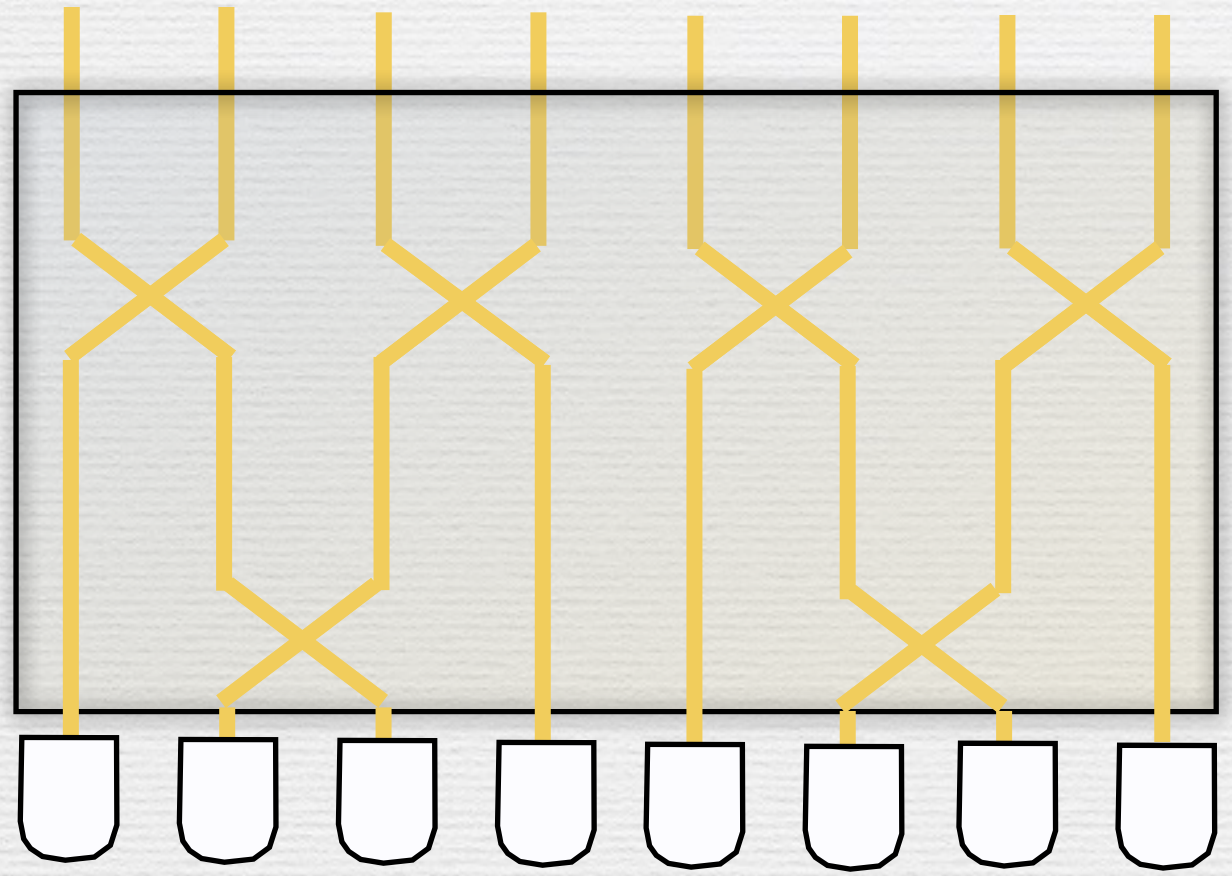
Continuous (and discrete) variable quantum devices



- How can properties such as entanglement be reliably estimated?

- Recent advances in continuous-variable quantum information
- Theoretical and mathematical advances (why we are here)

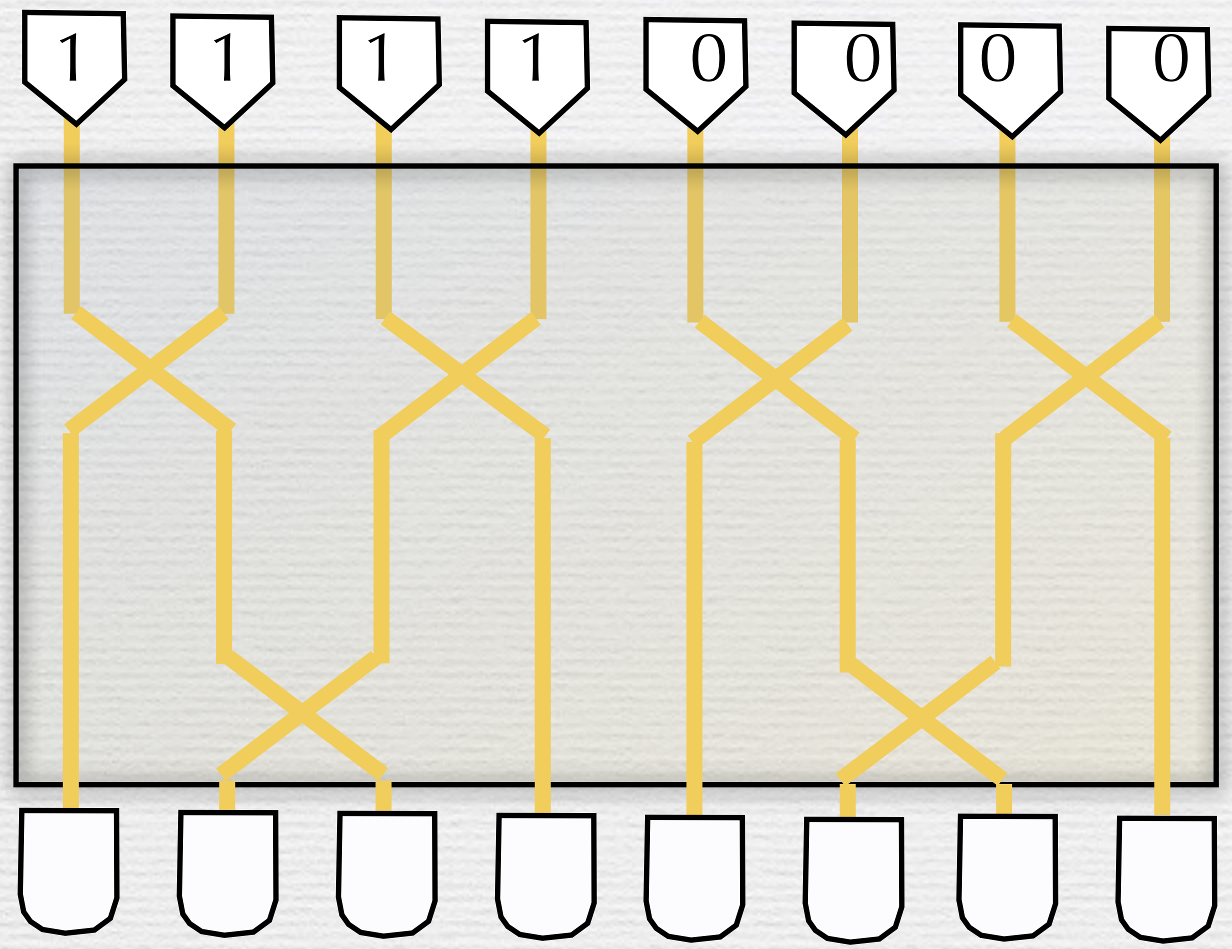
Continuous (and discrete) variable quantum devices



- Quantum **communication**, channels, cryptography
- **Sensing** and metrology
- **Q-computation** with significant resources: KLM, (CV) graph states, feedforward

Knill, Laflamme, Milburn, Nature 409, 46 (2001)
Browne, Rudolph, Phys Rev Lett 95, 010501 (2005)
Eisert, Phys Rev Lett 95, 040502 (2005)
Kok, Munro, Nemoto, Ralph, Dowling, Milburn, Rev Mod Phys 79, 135 (2007)

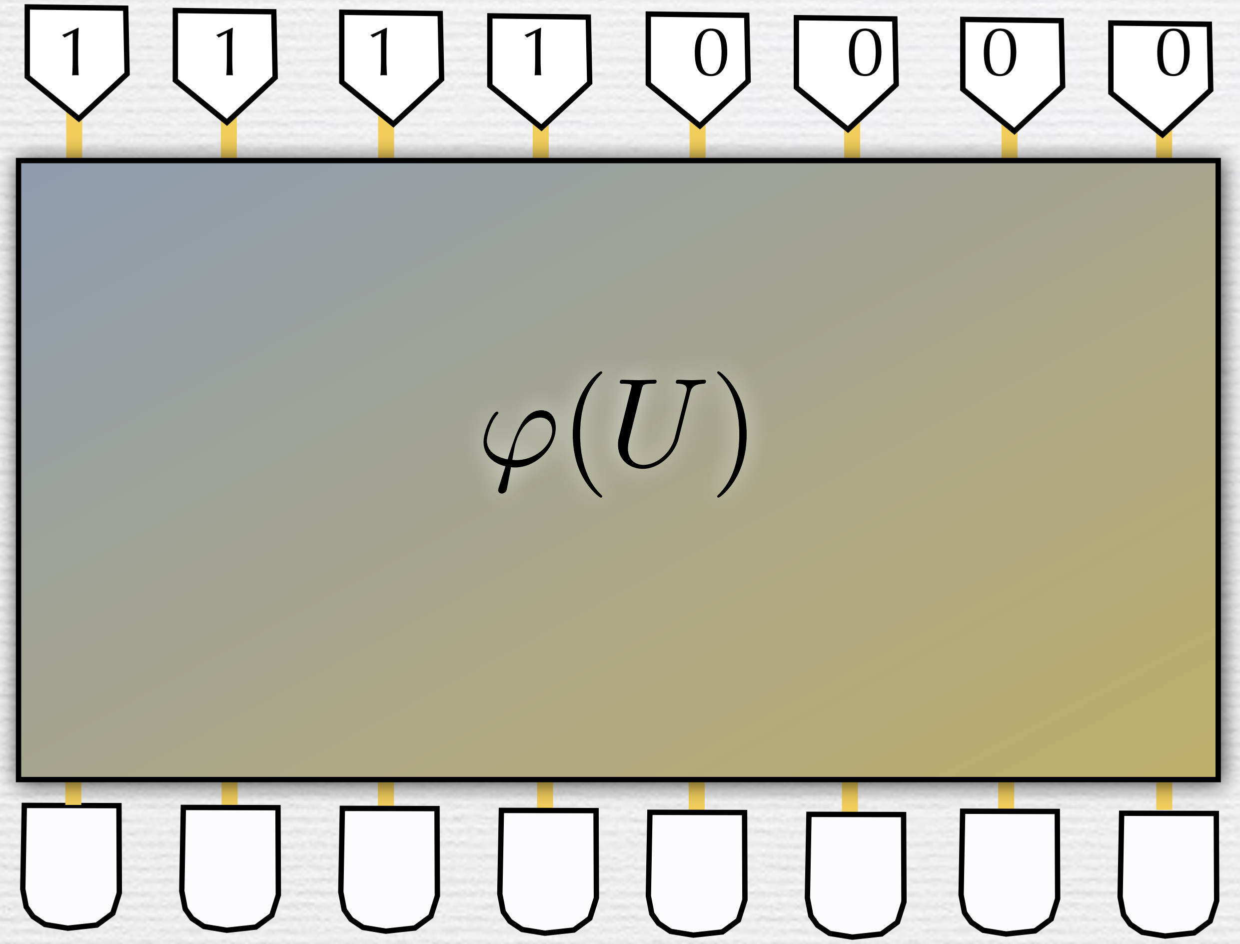
“Quantum supremacy”



- Think of **some quantum device** presumably outperforming classical computers
- Achieve "quantum supremacy" in John Preskill's words
- **Boson sampling:** Contested candidate

Preskill, Quantum supremacy now?, blog entry on July 22, 2012, in Quantum Frontiers

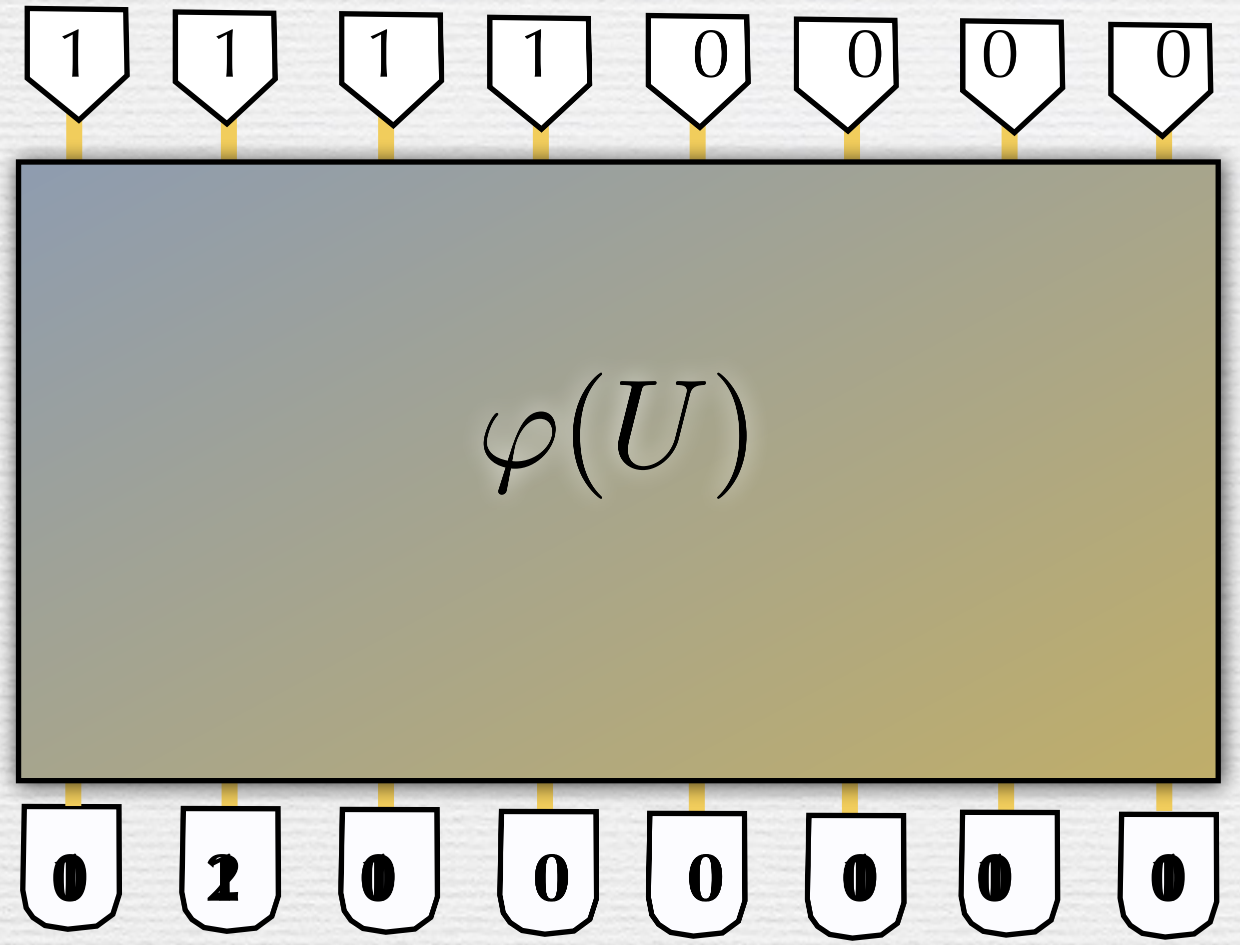
Boson sampling: A special purpose quantum algorithm



Variation 1: Boson sampling

Aaronson, Arkhipov, Proceedings of ACM Symposium on the Theory of Computing, STOC (2011)
Gogolin, Kliesch, Aolita, Eisert, arXiv:1306.3995

Boson sampling: A special purpose quantum algorithm



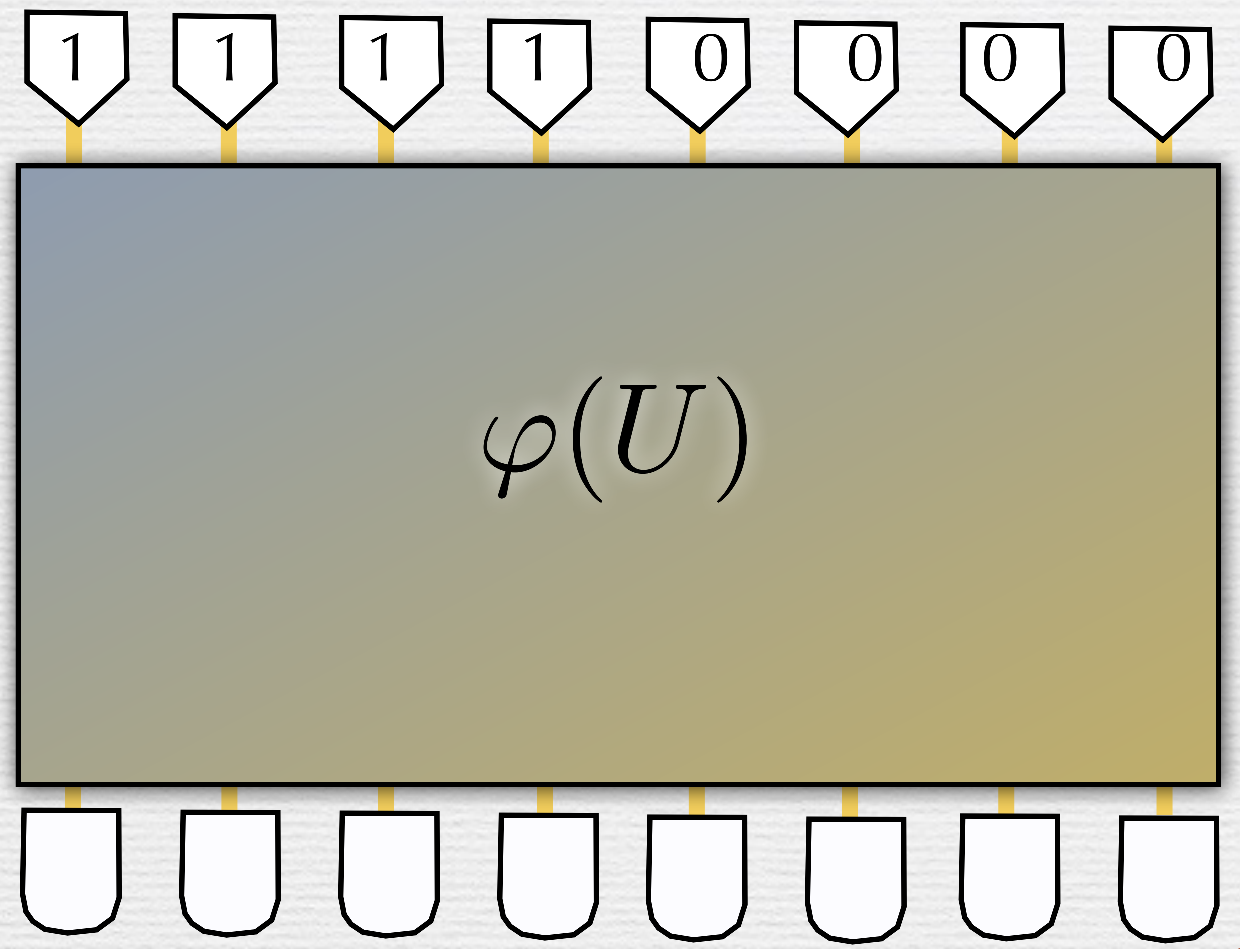
- **Input state vector** $|\psi\rangle = |1_n\rangle := |(1,\ldots,1,0,\ldots,0)\rangle$, n bosons in $m > n$ modes
- **Linear optical network**, transforming bosonic modes $b = (b_1,\ldots,b_m)^T$ as

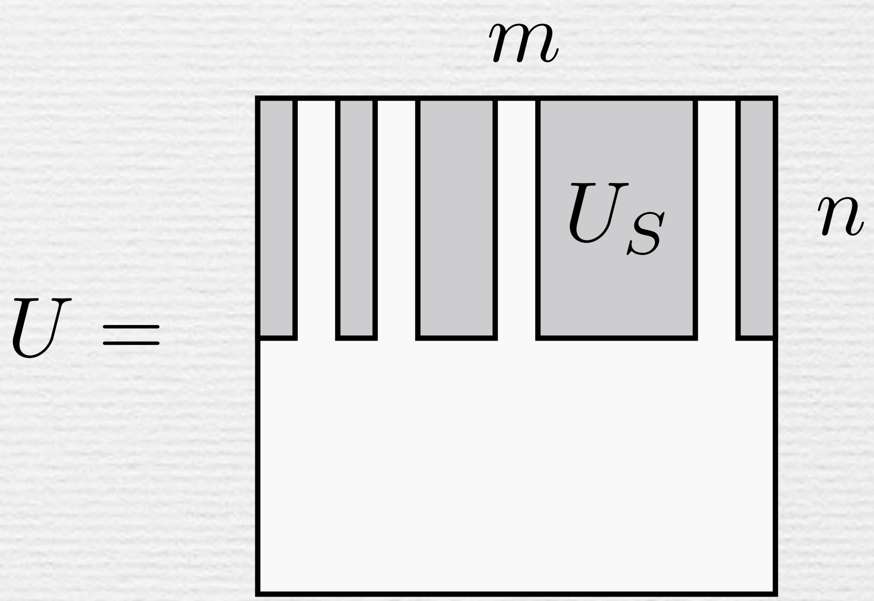
$$b \mapsto Ub$$

Hilbert space representation $\varphi(U)$, $U \in U(m)$

- **Single photon detection**, output pattern S

Boson sampling: A special purpose quantum algorithm





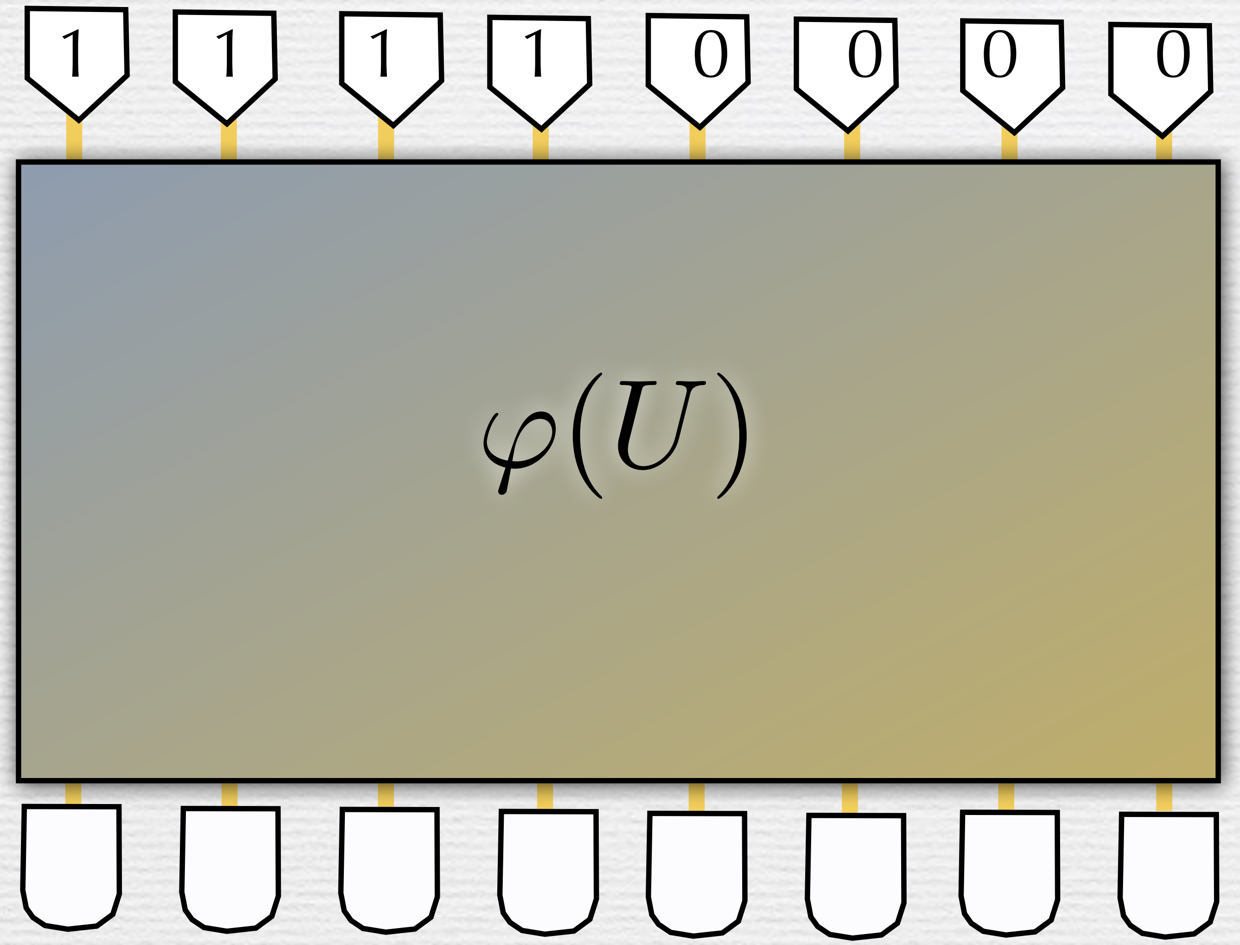
- **Probability** $\Pr_{\mathcal{D}_U}[S] := |\langle\psi|\varphi(U)|S\rangle|^2 = \frac{|\mathrm{Perm}(U_S)|^2}{\prod_{j=1}^{m}(s_j!)}$

- Permanent of "submatrix" U_S of U

- **Permanent is #P hard**... , but then, one merely **samples** from it

Scheel, quant-ph/0406127

Complexity claim on sampling under Haar random unitaries

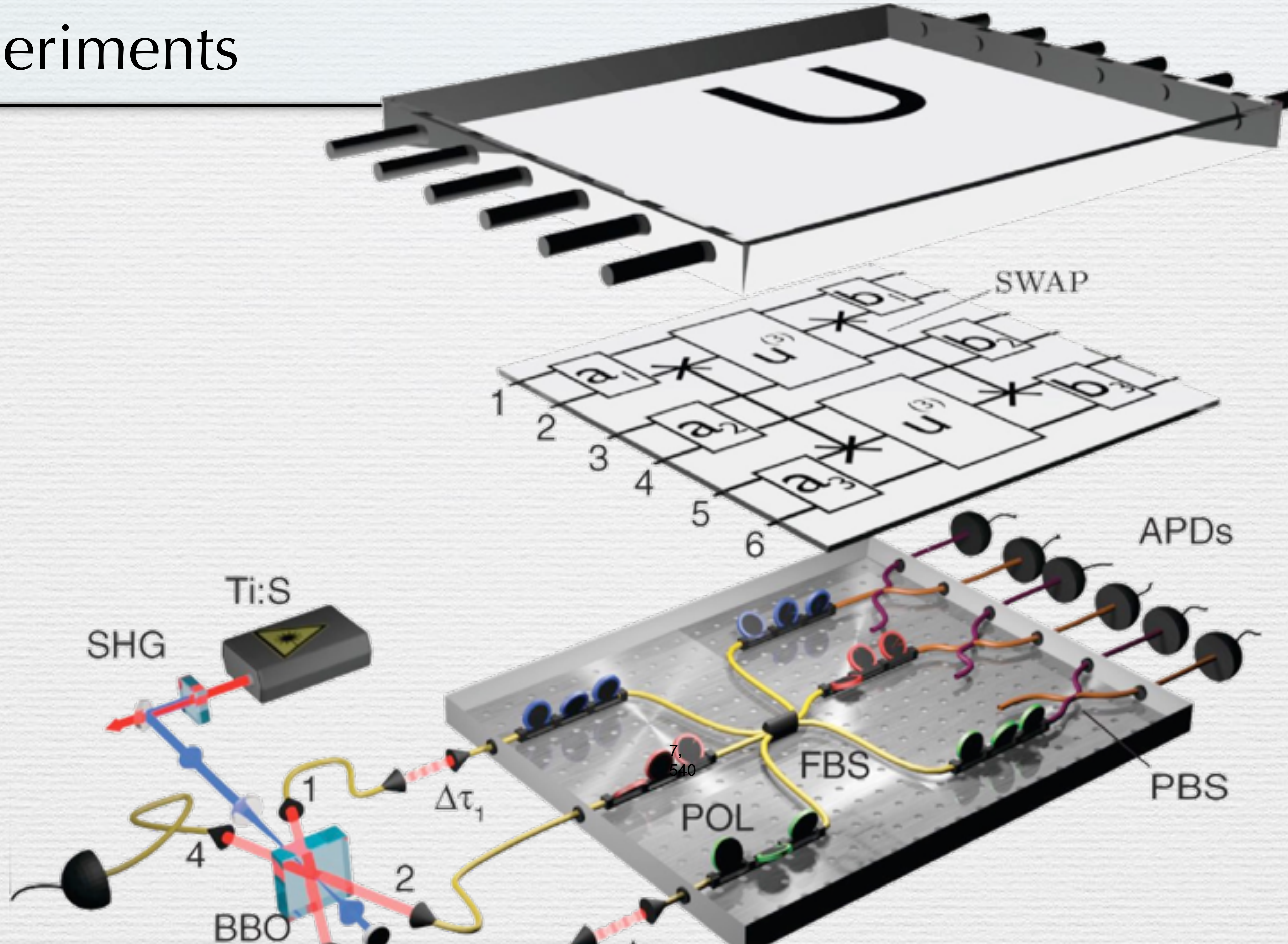


- **Non-technical statement:**

  Sampling from a distribution that is close in **1-norm** to boson sampling distribution, is "computationally hard" with high probability if the unitary U is chosen from Haar measure and m increases sufficiently fast with n $(m \in \Omega(n^5))$

Aaronson, Arkhipov, Proceedings of ACM Symposium on the Theory of Computing, STOC (2011)
Compare also Bremner, Jozsa, Shepherd, arXiv:1005.1407

Photonic experiments



NATURE PHOTONICS | LETTER

日本語要約

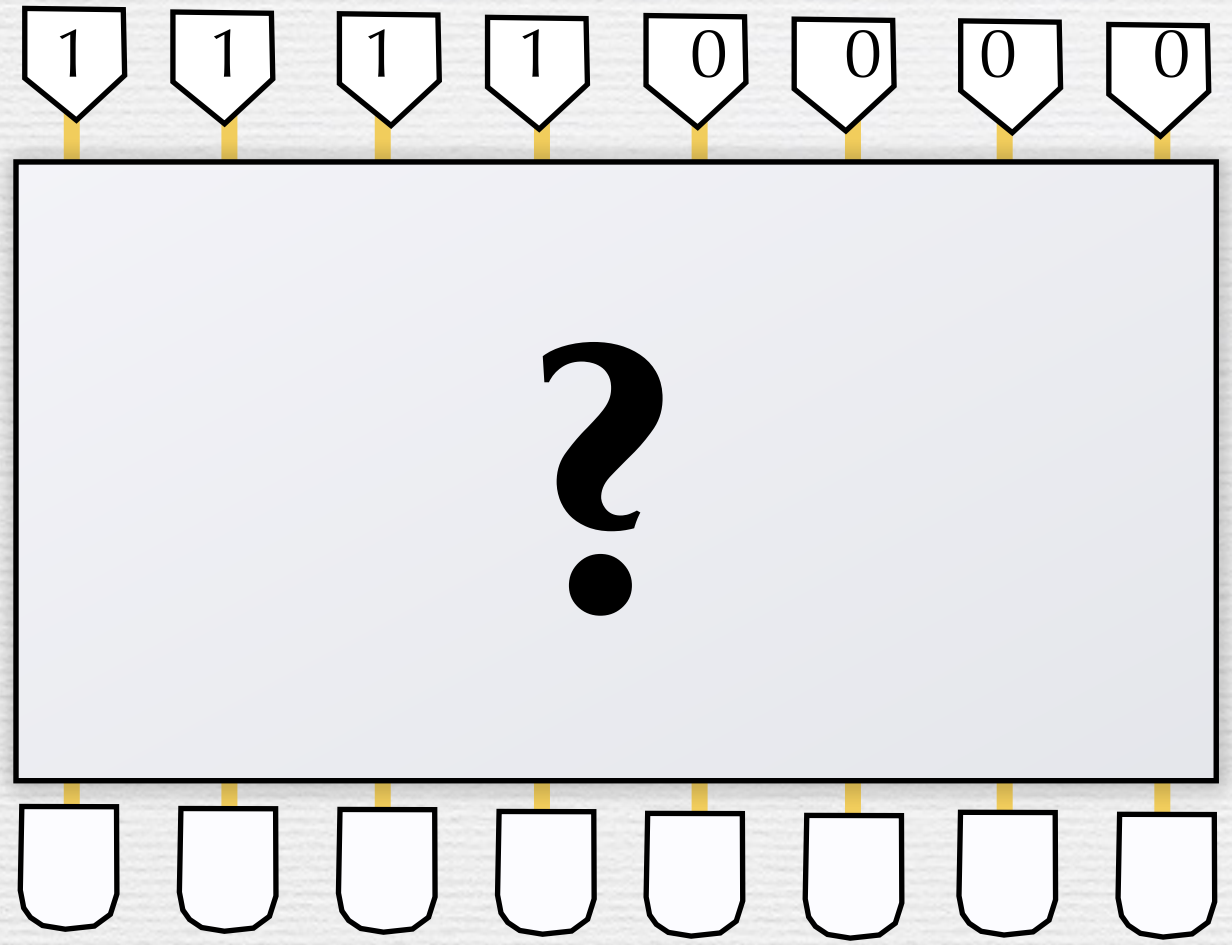
Integrated multimode interferometers with arbitrary designs for photonic boson sampling

Andrea Crespi, Roberto Osellame, Roberta Ramponi, Daniel J. Brod, Ernesto F. Galvão, Nicolò Spagnolo, Chiara Vitelli, Enrico Maiorino, Paolo Mataloni & Fabio Sciarrino

Affiliations | Contributions | Corresponding authors

Broome et al, Science 339, 794 (2012)
Spring et al, Science 339, 798 (2012)
Tillmann et al, Nature Photonics 7, 540 (2013)
Crespi et al, Nature Photonics 7, 545 (2013)

Crucial question of certification

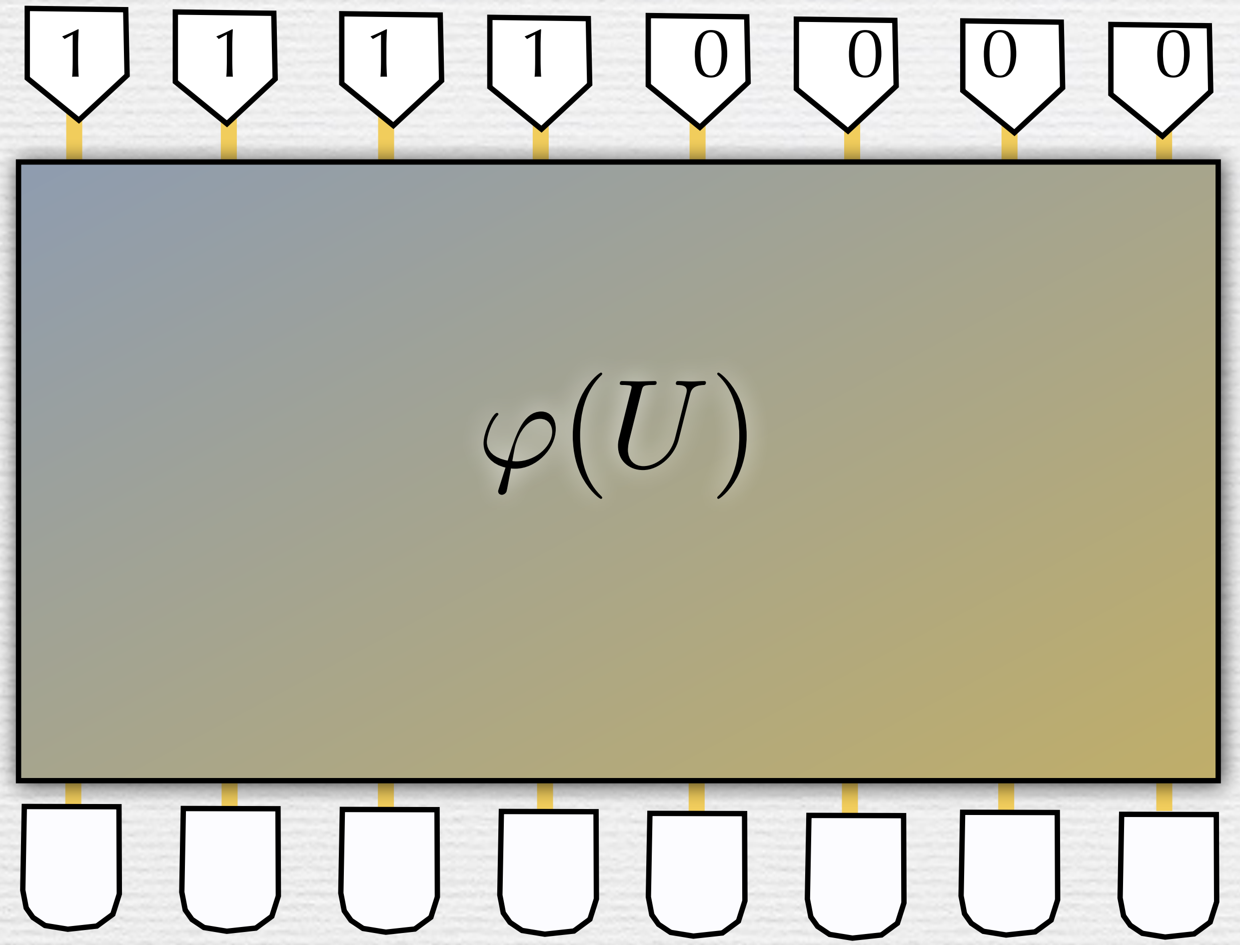


- **But, eh, how would we know whether we are correct?**

- Experiments **sample**, deliver lists of numbers

Gogolin, Kliesch, Aolita, Eisert, arXiv:1306.3995

Crucial question of certification



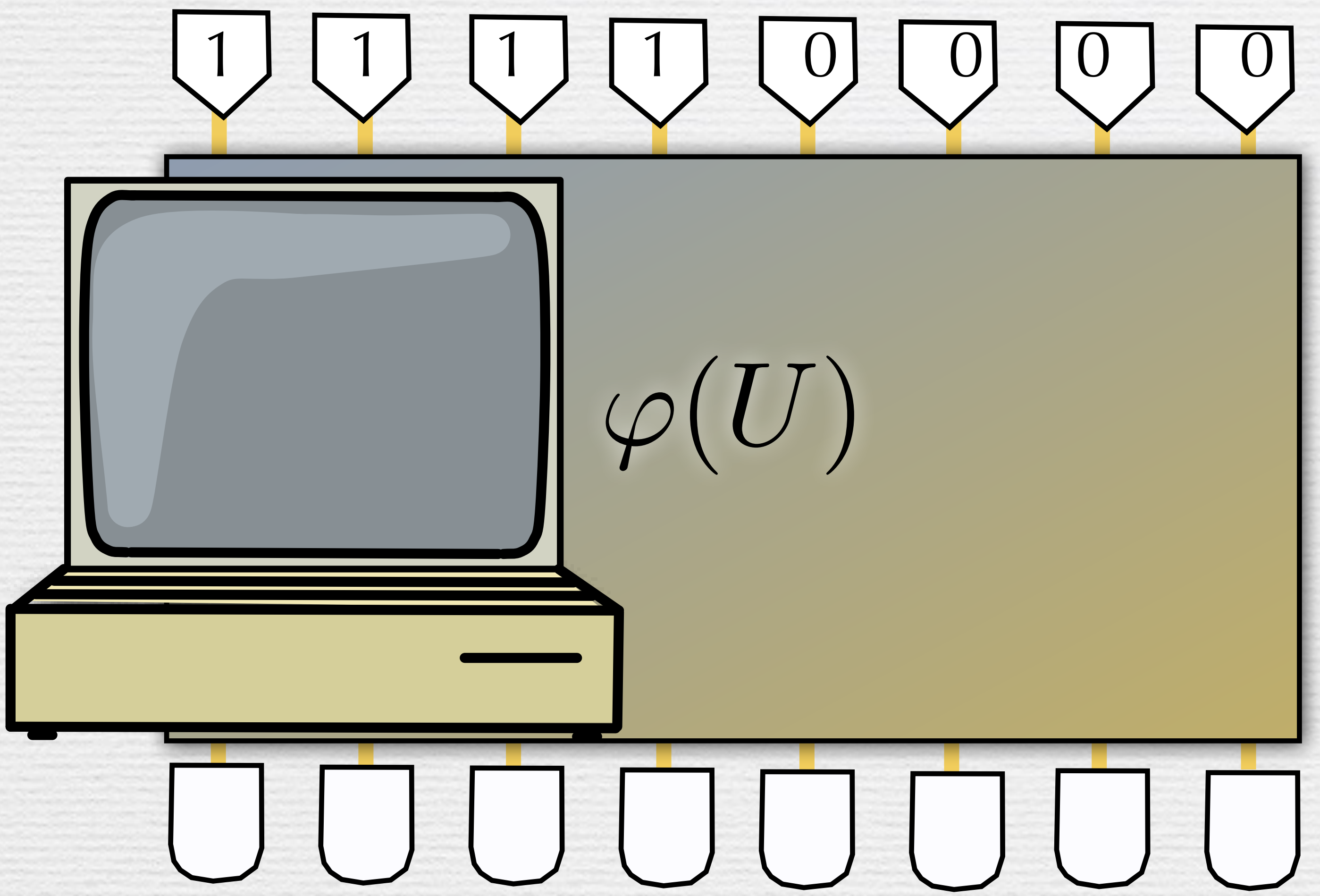
Methods:

- Large deviation bounds
- Random matrix theory

- Let $m \geq n^{5.1}$ and let $U \in U(m)$ be Haar random. Then with probability at least $1-\delta$, for every T and every $\epsilon > 0$, there exists a circuit of size $T\text{poly}(n, 1/\epsilon, 1/\delta)$ that samples a distribution that is ϵ- indistinguishable from (the collision-free part of) the boson sampling distribution by circuits of size at most T

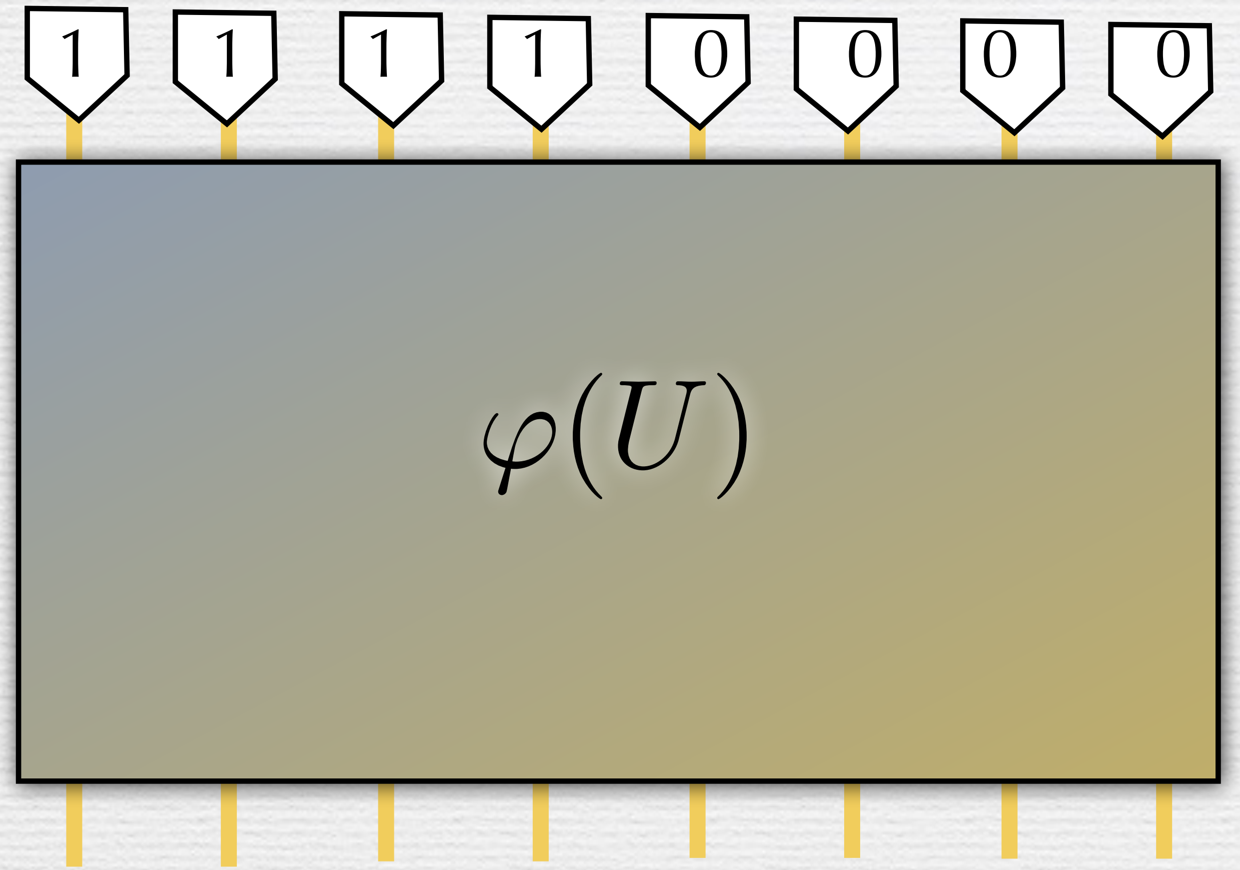
Trevisan, Tulsiani, Vadhan, Proc IEEE Conf Comp Complex, 126 (2009)
Gogolin, Kliesch, Aolita, Eisert, arXiv:1306.3995
Aaronson, Arkhipov, arXiv:1309.7460
Brandao, private communication

Crucial question of certification



- **Lesson:** Evidence that boson sampling is hard, but also that boson sampling cannot be efficiently distinguished from classical efficient device

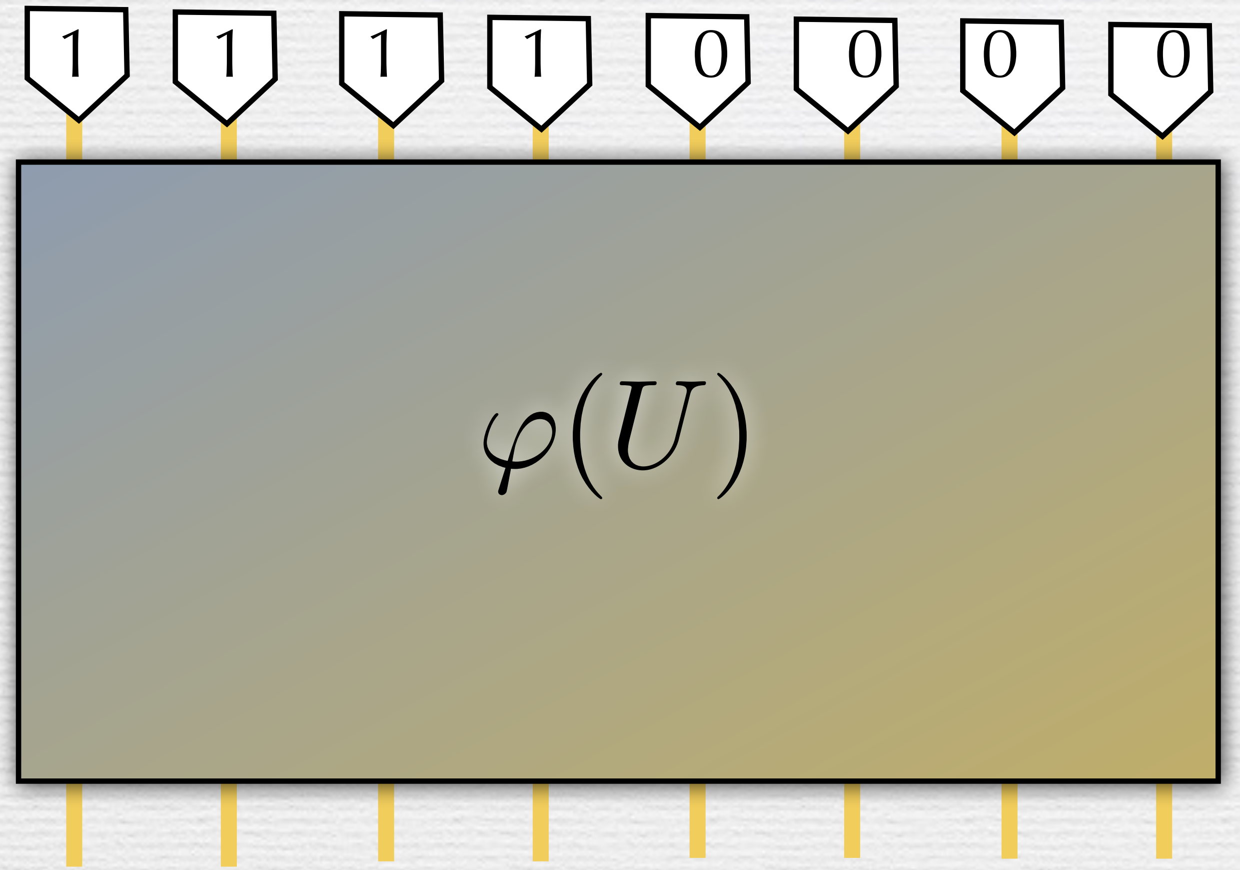
Reliable quantum certification



Variation 2: Reliable quantum certification

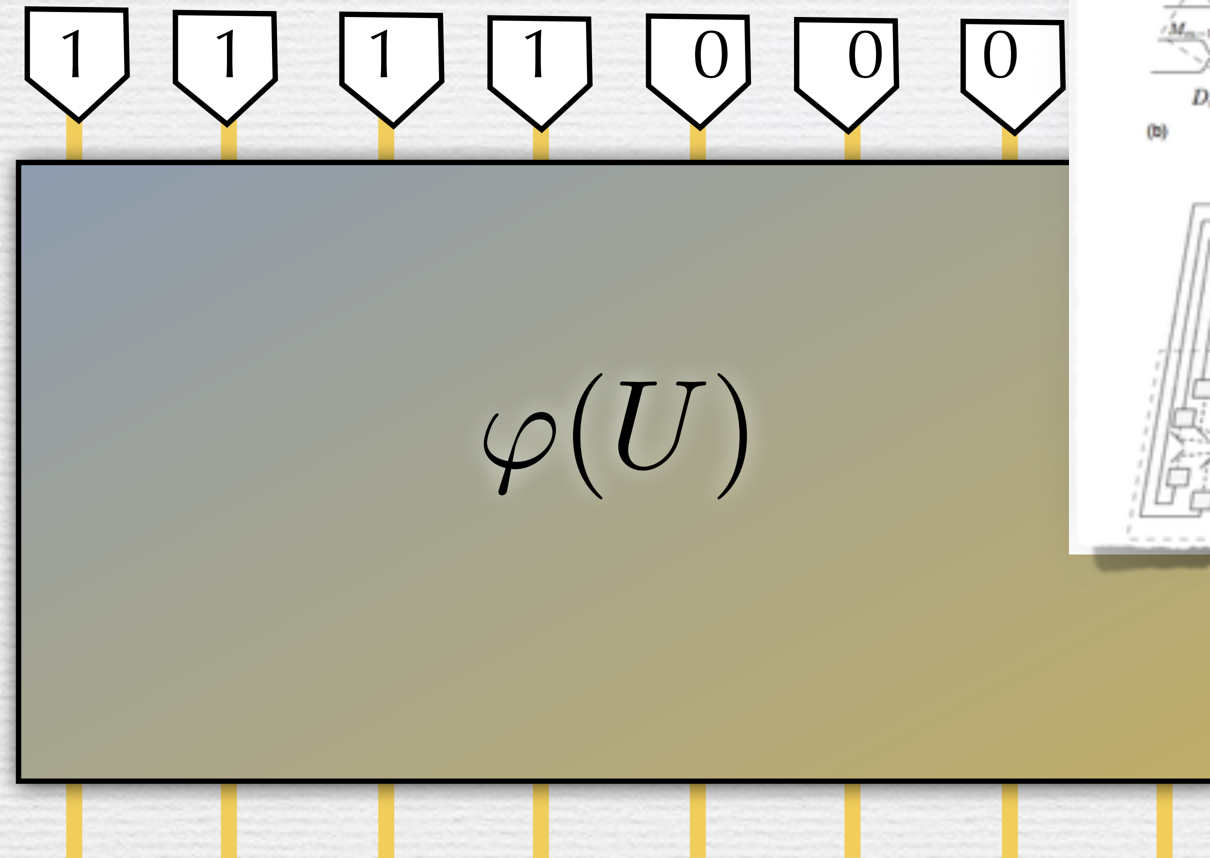
Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

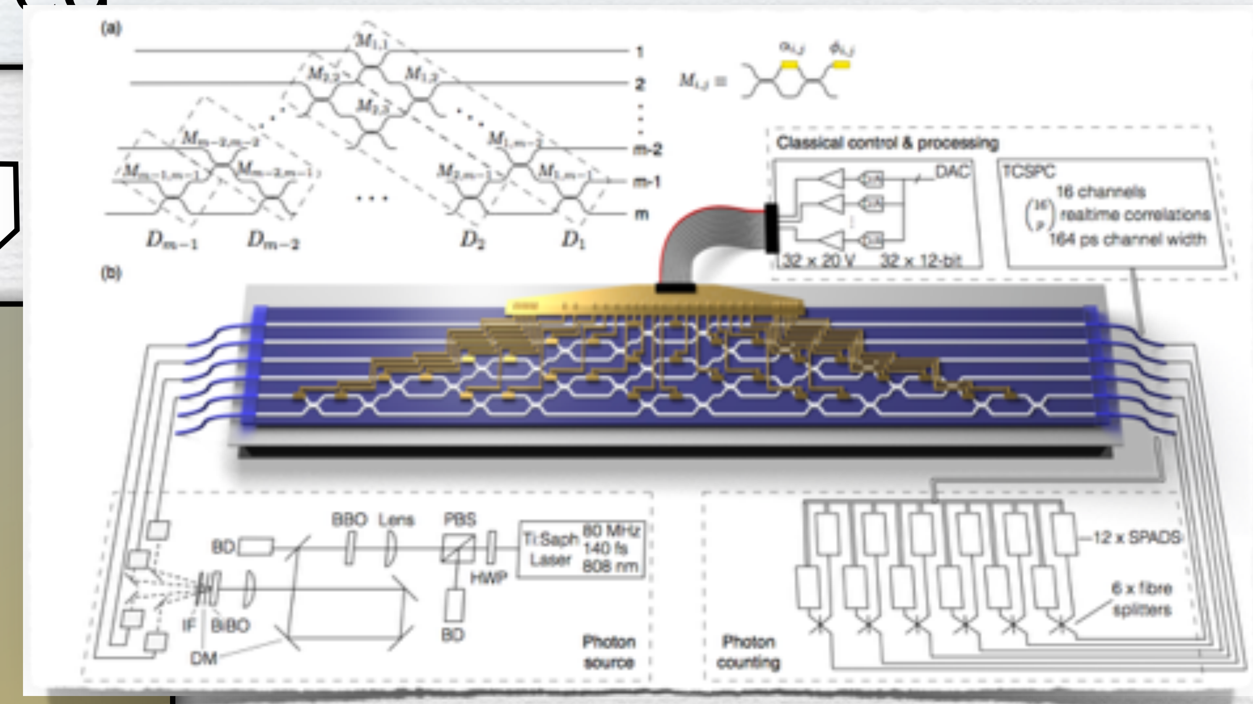
Reliable quantum certification



- **Can one efficiently certify quantum circuits as such with local measurements?**

State preparation settings considered



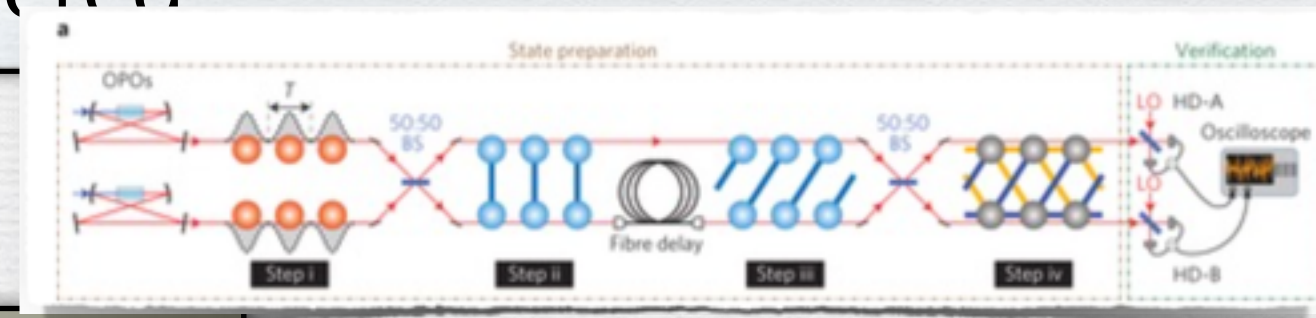


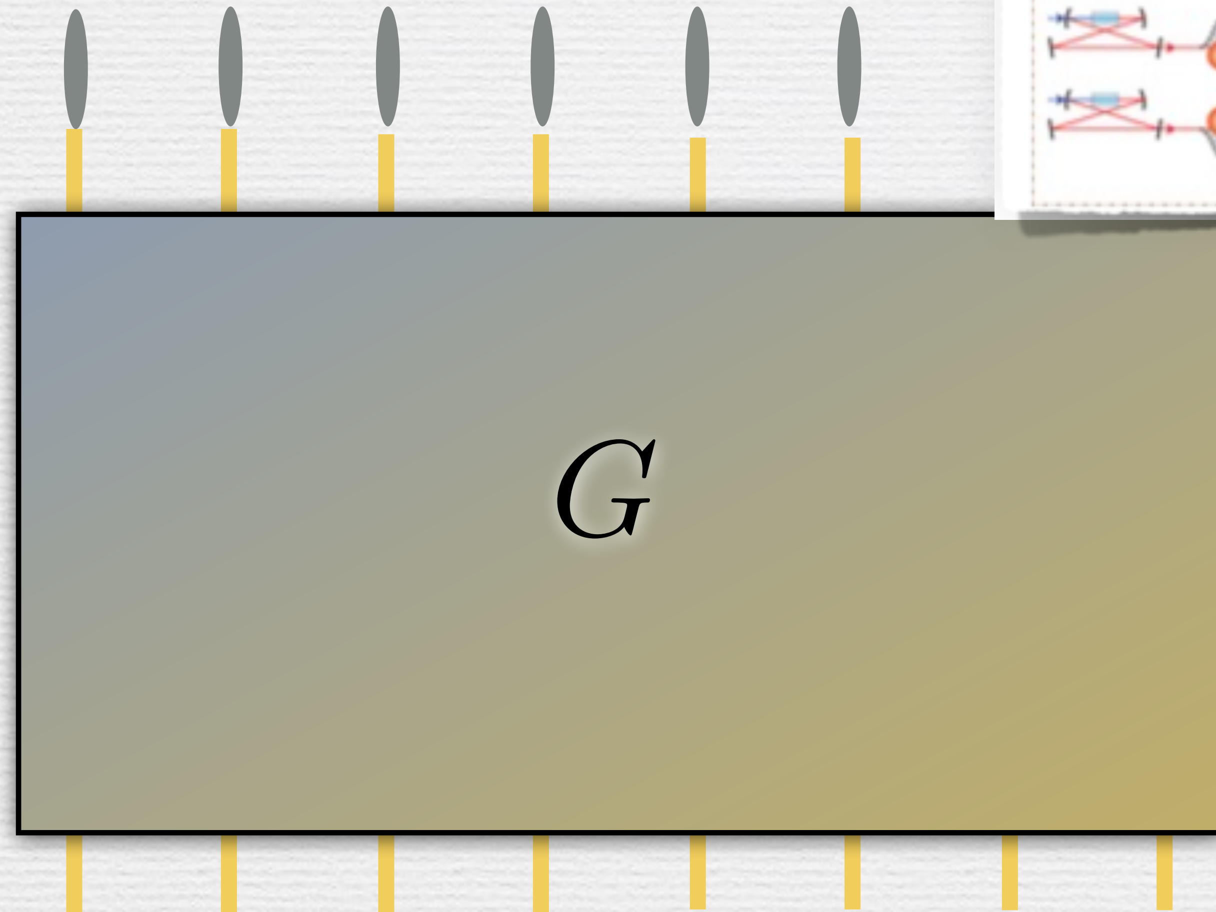
- **Linear optical setting** (single photons + passive optics)

$$\mathcal{S}_{\mathrm{LO}} = \{U|1_n\rangle\langle 1_n|U^\dagger : U \text{ passive unitary}\}$$

Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

State preparation settings considered



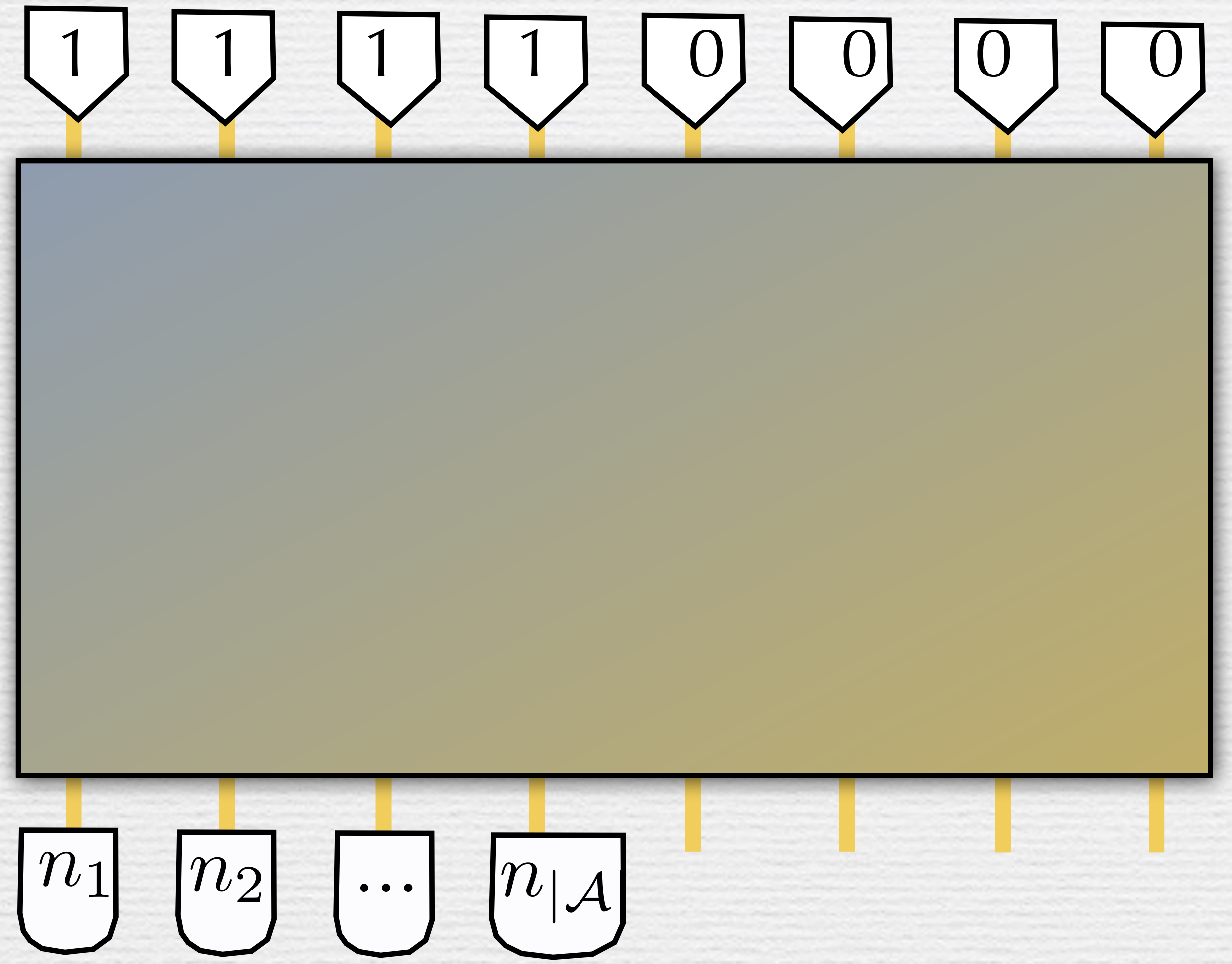


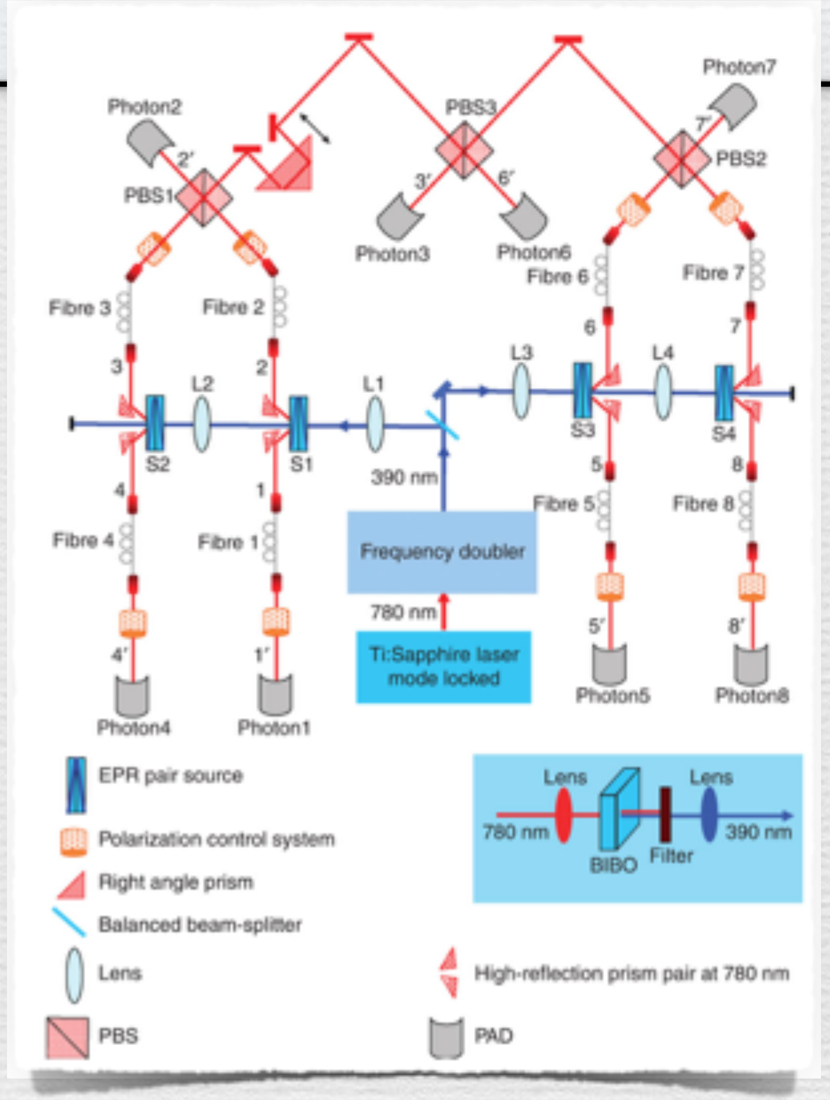
- **Linear optical setting** (single photons + passive optics)
- **Continuous-variable setting** (Gaussian states + active Gaussian unitaries)

$$\mathcal{S}_{\mathrm{G}} = \{U|0\rangle\langle 0|U^\dagger : U \text{ Gaussian unitary}\}$$

Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

State preparation settings considered



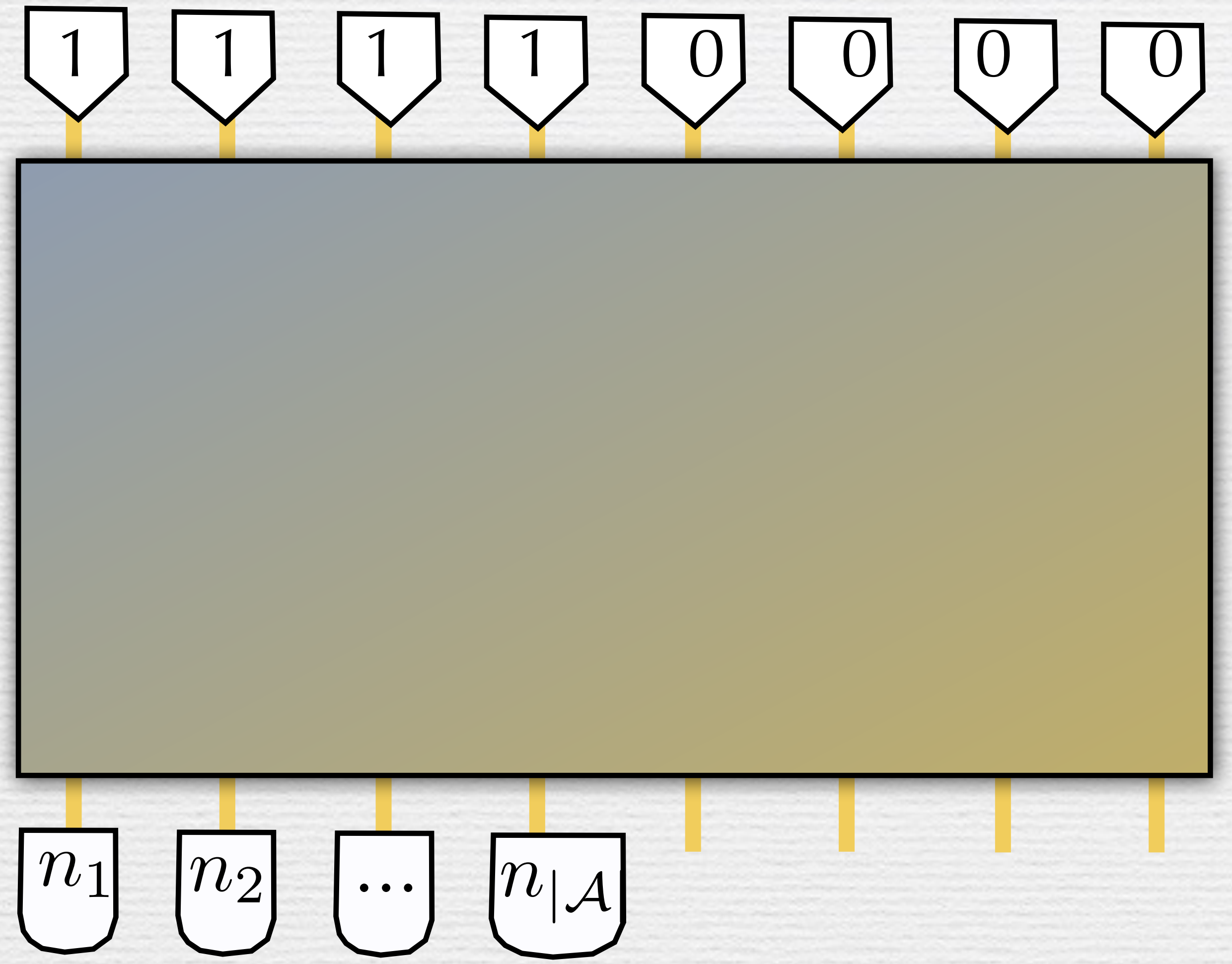


- **Linear optical setting** (single photons + passive optics)
- **Continuous-variable setting** (Gaussian states + active Gaussian unitaries)
- **Post-selected instances**, in both settings (e.g., KLM-type quantum gates)

$$\mathcal{S}_{\mathrm{LPS}} = \left\{ \frac{\langle \mathbf{n}_{\mathcal{A}} | \rho_t | \mathbf{n}_{\mathcal{A}} \rangle}{p(\mathbf{n}_{\mathcal{A}} | \rho_t)} : \rho_t \in \mathcal{S}_{\mathrm{LO}} \right\}$$

Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

State preparation settings considered

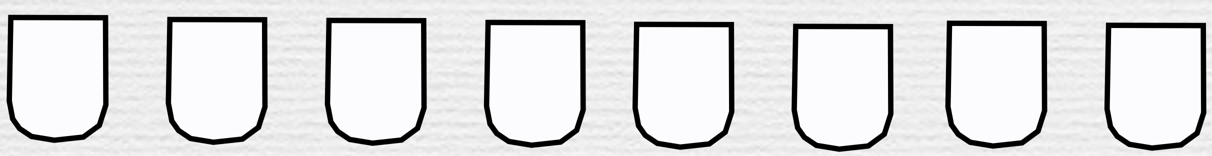


- **Linear optical setting** (single photons + passive optics)
- **Continuous-variable setting** (Gaussian states + active Gaussian unitaries)
- **Post-selected instances**, in both settings (e.g., KLM-type quantum gates)
- Includes most multi-photon state preparations

Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

Certification mindset

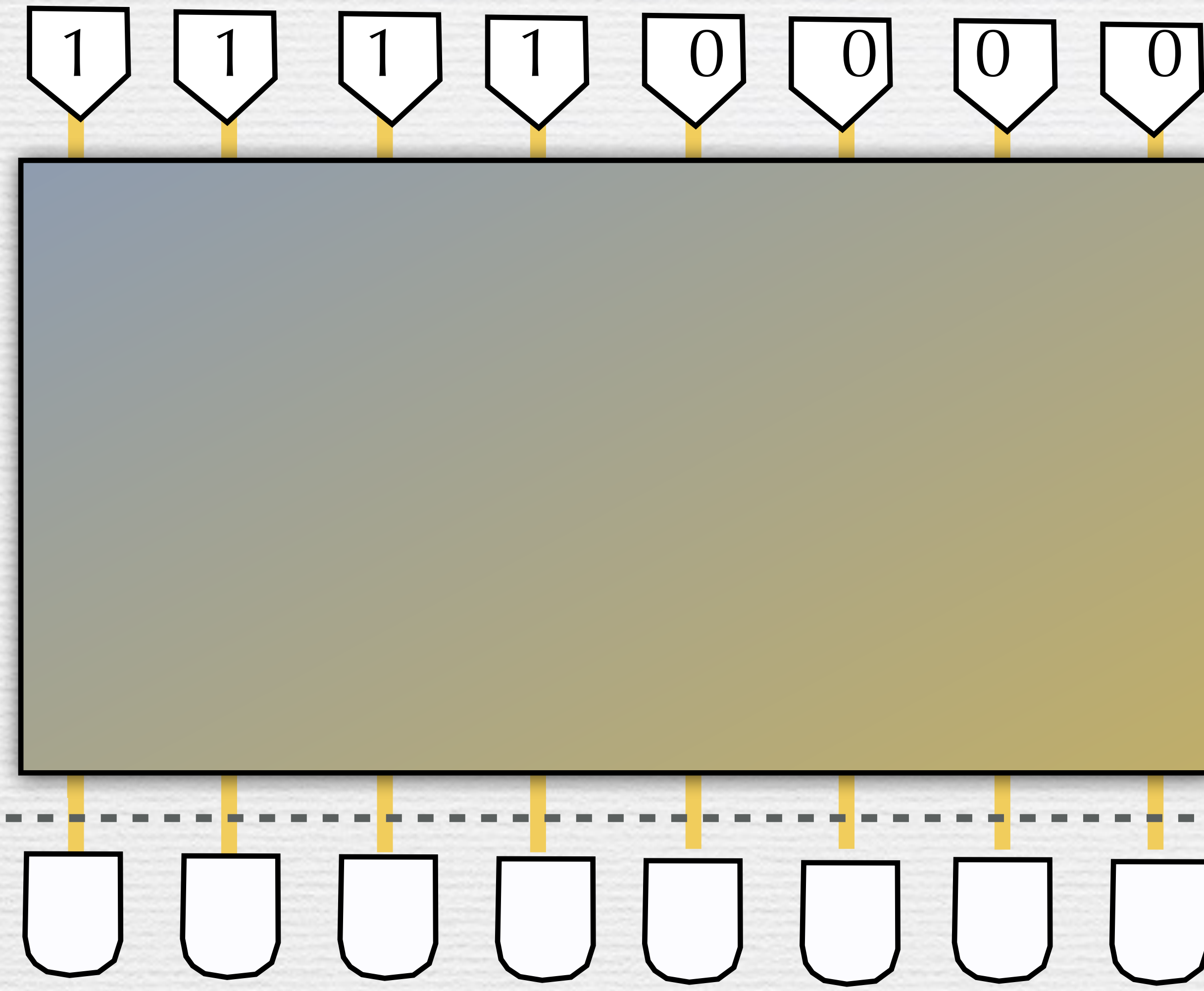
- Similar to **interactive proofs**



Sceptic certifier, **Arthur**, with limited quantum capabilities (single mode measurements, almost classical), who wishes to ascertain...

Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

Certification mindset



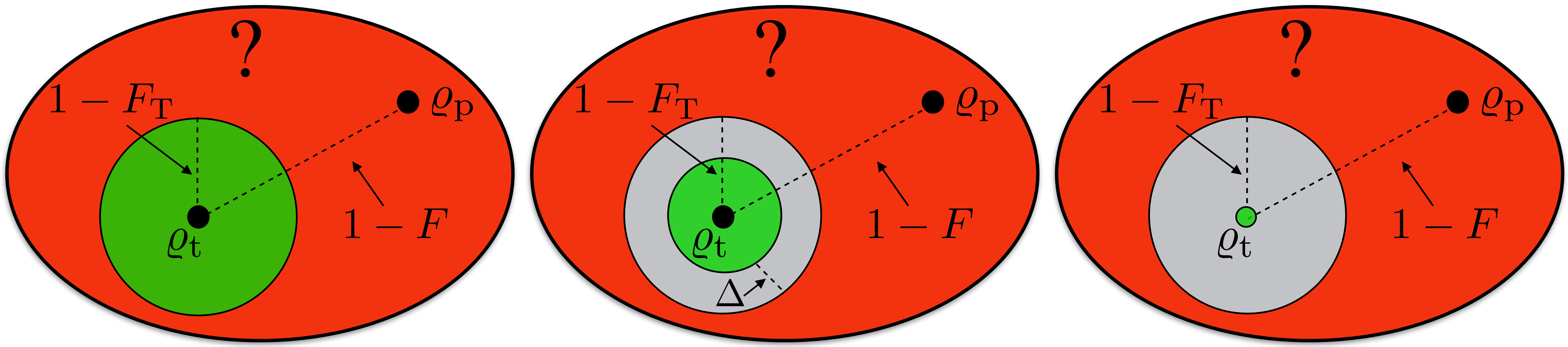
...whether an **untrusted quantum prover**, **Merlin**, presumably with more quantum capabilites, can indeed prepare certain quantum states up to target fidelity

$$F := F(\rho_t, \rho_p) \geq F_{\mathrm{T}} \,?$$

Sceptic certifier, **Arthur**, with limited quantum capabilities (single mode measurements, almost classical), who wishes to ascertain...

Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

Certification mindset



- Naive approach
- Robust certification
- Not robust, but can be practical

$\alpha > 0$ *maximum failure probability*

Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

Extremality-based fidelity lower bound

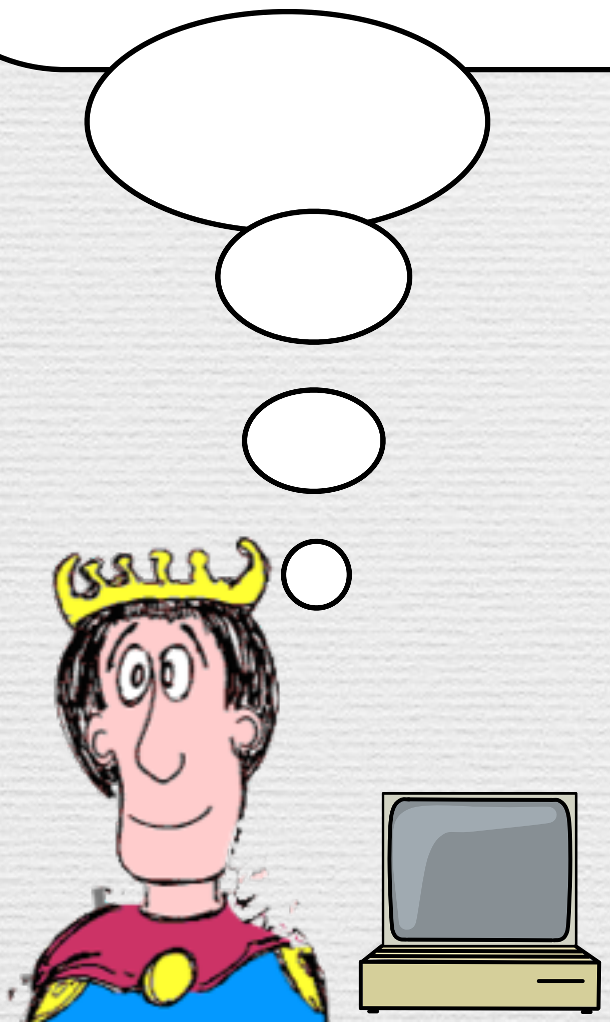
Methods:

- Fidelity lower bounds

$$\forall \rho_t \in \mathcal{S}_{\mathrm{G}} \wedge \mathcal{S}_{\mathrm{LO}} : F \geq F_n := 1 - \langle (\hat{n} - n) \prod_{j=1}^{n} \hat{n}_j \rangle_{U^\dagger \rho_p U} \forall \rho_p$$

($\hat{n} := \sum_{j=1}^{m} \hat{\hat{n}}_j$ total photon number)

- Extremality of Gaussian operations

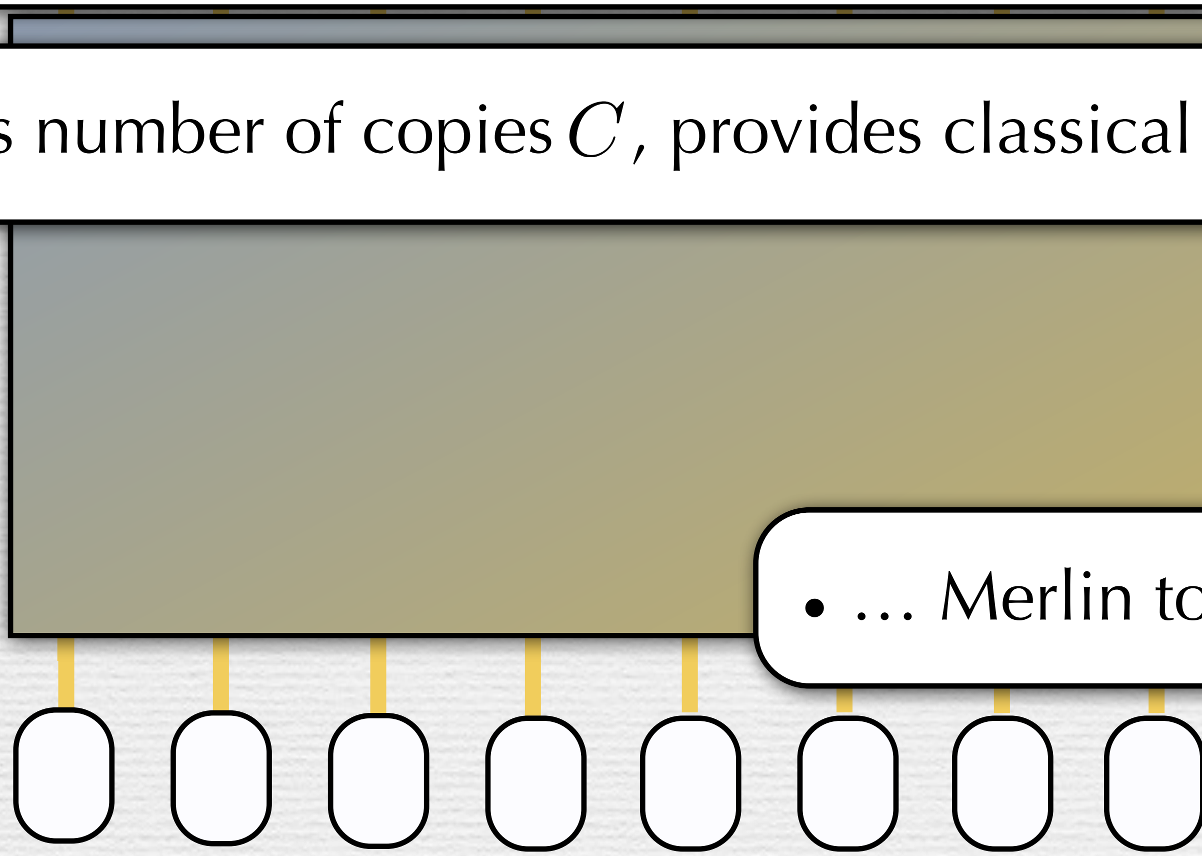


Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

Quantum state certification

- Choose fidelity F_T, max failure probability α and estimation error $\epsilon \leq \dfrac{1 - F_{\mathrm{T}}}{2}$

- Computes number of copies C, provides classical description, asks…

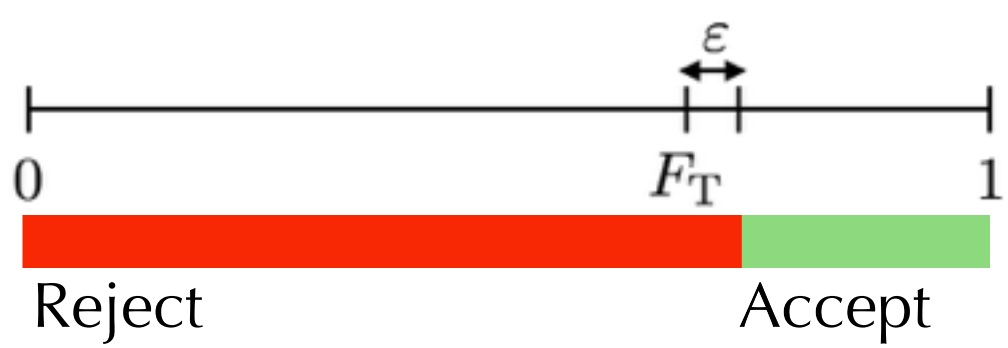


- … Merlin to prepare C copies of ρ_p

- Measures F_{T}, obtains estimate $F_{\mathrm{T}}^* \in [F_n - \epsilon, F_n + \epsilon]$

$$F = 1 \Rightarrow F_n = 1 \Rightarrow F_n^* \geq 1 - \epsilon \geq F_{\mathrm{T}} + \epsilon$$

$$F < F_{\mathrm{T}} \Rightarrow F_n < F_{\mathrm{T}} \Rightarrow F_n^* < F_{\mathrm{T}} + \epsilon$$



Efficient measurements

- How to measure F_n?
- **Non-Gaussian nullifiers**

$$F_n = 1 - \left\langle U r^2 U^\dagger - \frac{m+2n}{2} \prod_{j=1}^{n} \left(U q_j^2 U^\dagger + U p_j^\dagger U^\dagger - \frac{1}{2} \right) \right\rangle$$

- Requires single-mode **homodyning** only

- **Theorem:** For both $\mathcal{S}_{\rm LO}$ and $\mathcal{S}_{\rm G}$ the test can certify the states with

$$O\left(\frac{\mathrm{poly}(m)}{\log(1/(1-\alpha))} \right)$$

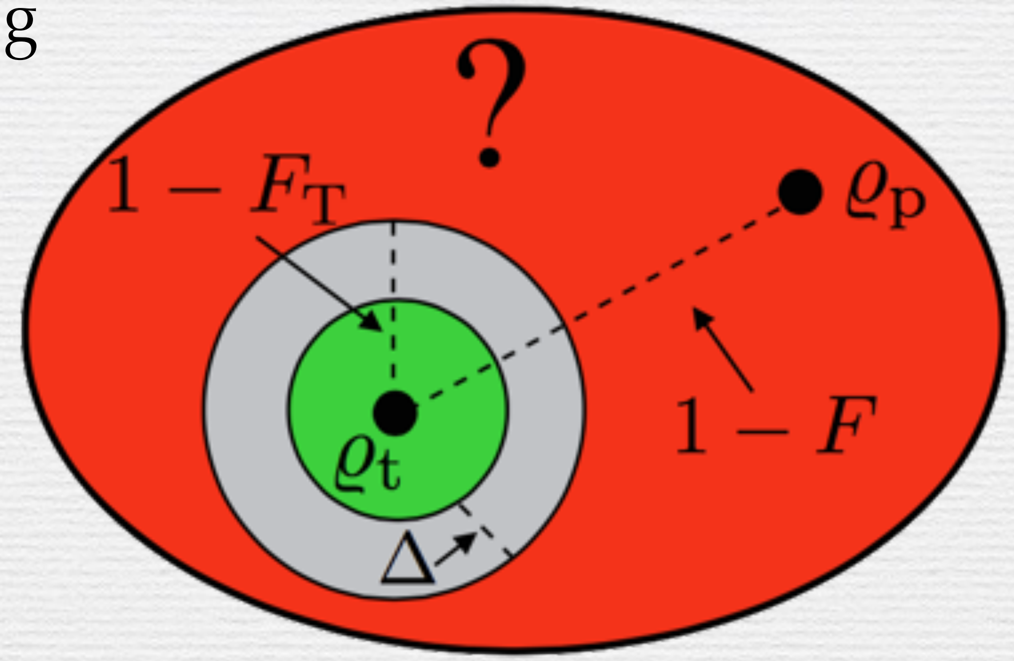
homodyne measurement settings, efficient in mode number (but not in the photon number)

- Works also for post-selection

Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

Robust state certification

- Same is true in robust setting



- **Theorem:** The test can certify the states with

$$O\left(\frac{\mathrm{poly}(m, 1/\Delta)}{\log(1/(1-\alpha))}\right)$$

homodyne measurement settings, efficient in mode number (but not in the photon number)

Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

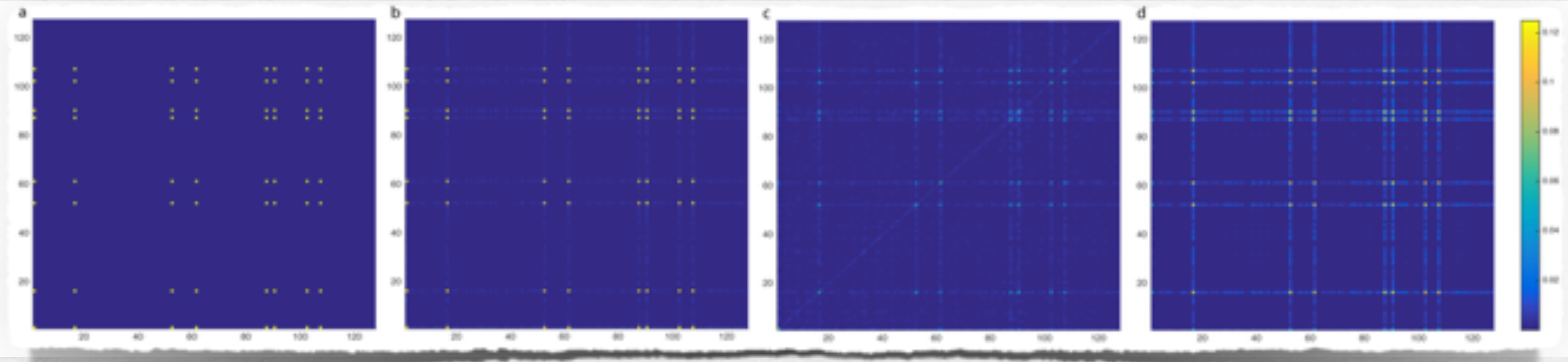
Lesson

- **Lesson:** Can efficiently certify state preparations, much more efficient than tomography, with feasible continuous-variable measurements

Aolita, Gogolin, Kliesch, Eisert, Nature Comm 6, 8498 (2015)

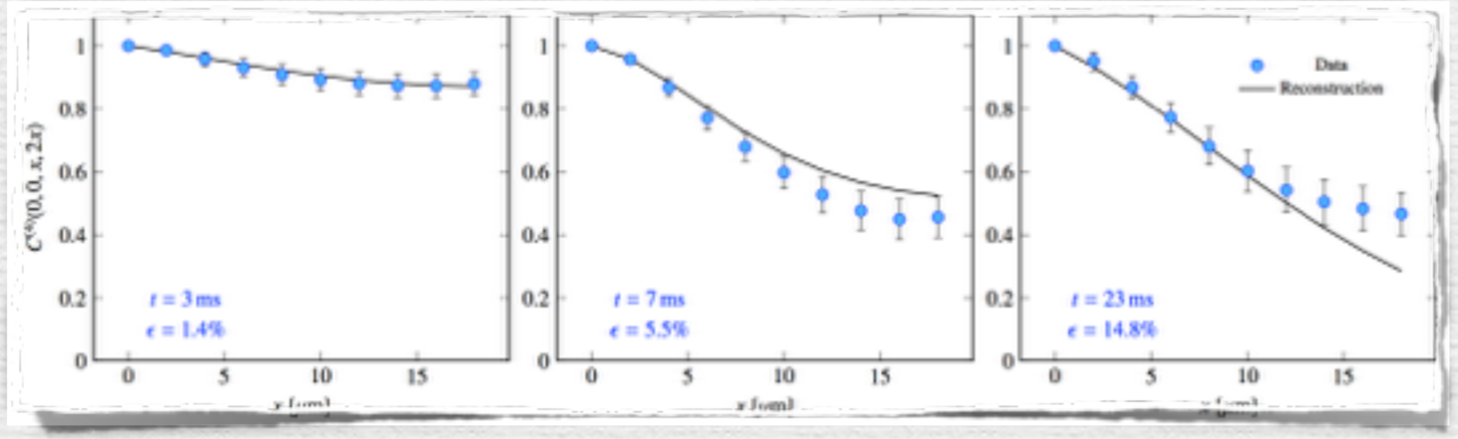
Other recent certification and tomography efforts

- Experimental compressed sensing tomography



Riofrio, Gross, Flammia, Monz, Roos, Blatt, Eisert, arXiv:1604.xxxxx
Gross, Liu, Flammia, Becker, Eisert, Phys Rev Lett 105, 150401 (2010)

- Quantum field tomography

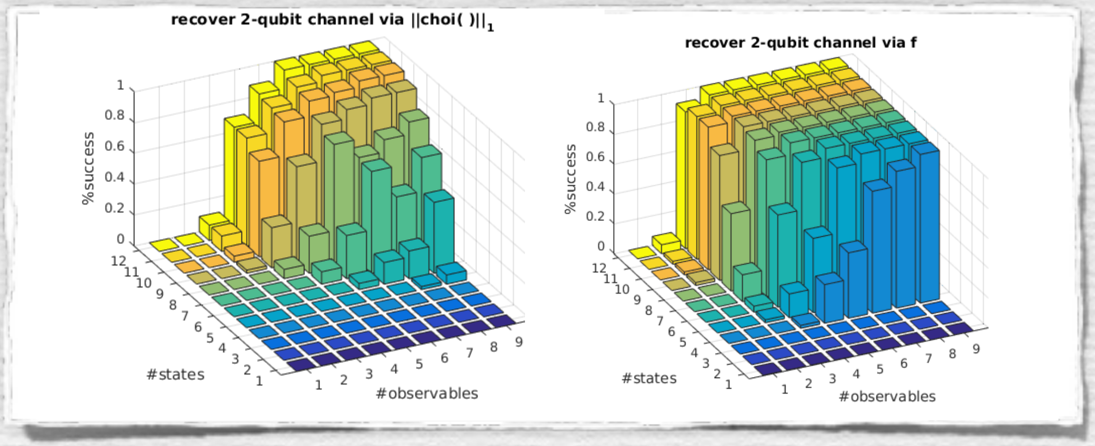


Steffens, Friesdorf, Langen, Rauer, Schweigler, Huebener, Schmiedmayer, Riofrio, Eisert, Nature Comm 6, 7663 (2015)

- Feasible channel super-activation

Schulze, Eisert, Schnabel, in preparation (2016)

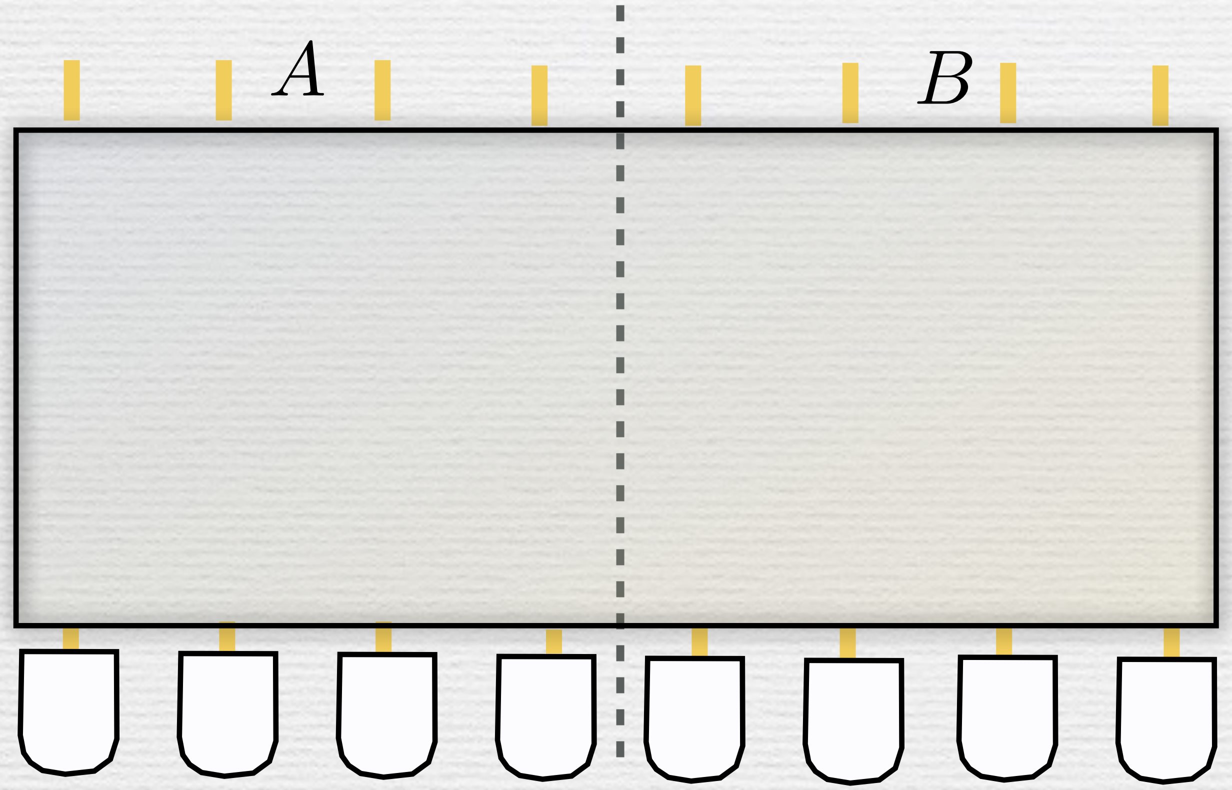
- Tensor completion and improved process tomography



Kliesch, Kueng, Eisert, Gross, arXiv:1511.01513

- Rigorous error bars

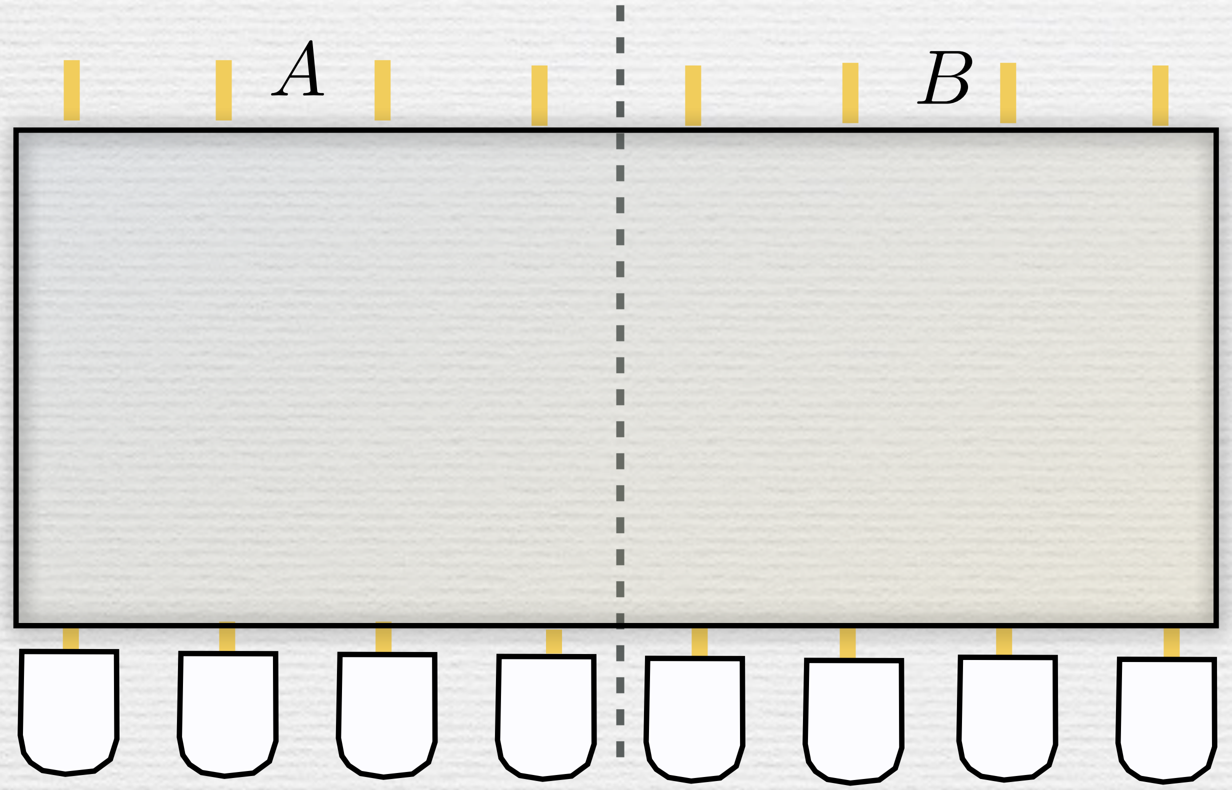
Carpentier, Eisert, Gross, Nickl, arXiv:1504.0323



Variation 3: Revisiting CV entanglement witnesses

Hyllus, Eisert, New J Phys 8, 51 (2006)
Hoelscher-Obermaier, Wieczorek, Hammerer, Steffens, Eisert, Aspelmeyer, in preparation (2016)

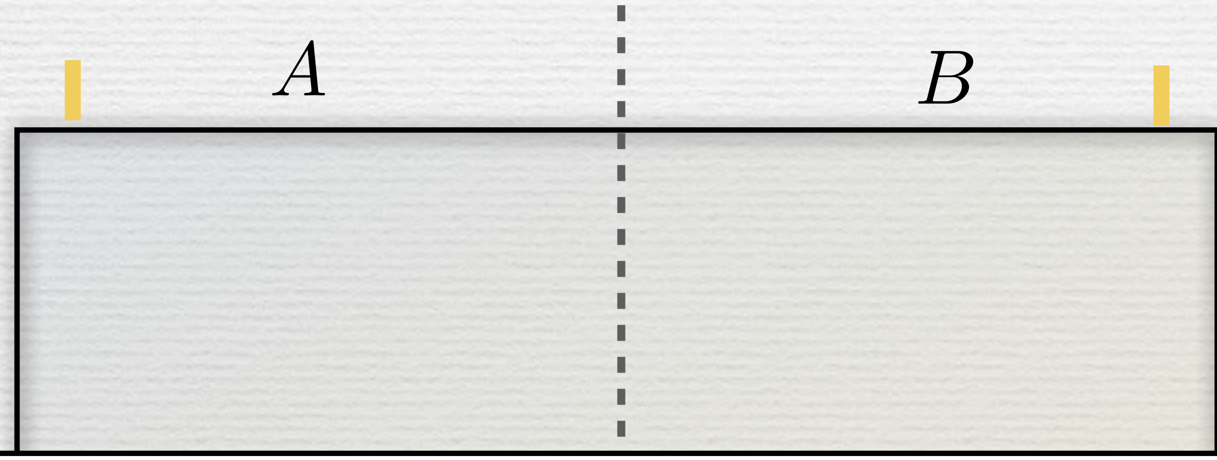
Detecting continuous-variable entanglement



- **How can optimal continuous variable entanglement witnesses be found?**

Detecting continuous-variable entanglement

- Famous **bi-partite criterion**



- **Theorem**: Bi-partite states with vanishing first moments satisfying

$$\frac{1}{2}\langle (x_1 + x_2)^2 \rangle + \frac{1}{2}\langle (p_1 - p_2)^2 \rangle < 1$$

are entangled

Duan, Giedke, Cirac, Zoller, Phys Rev Lett 84, 2722 (2000)

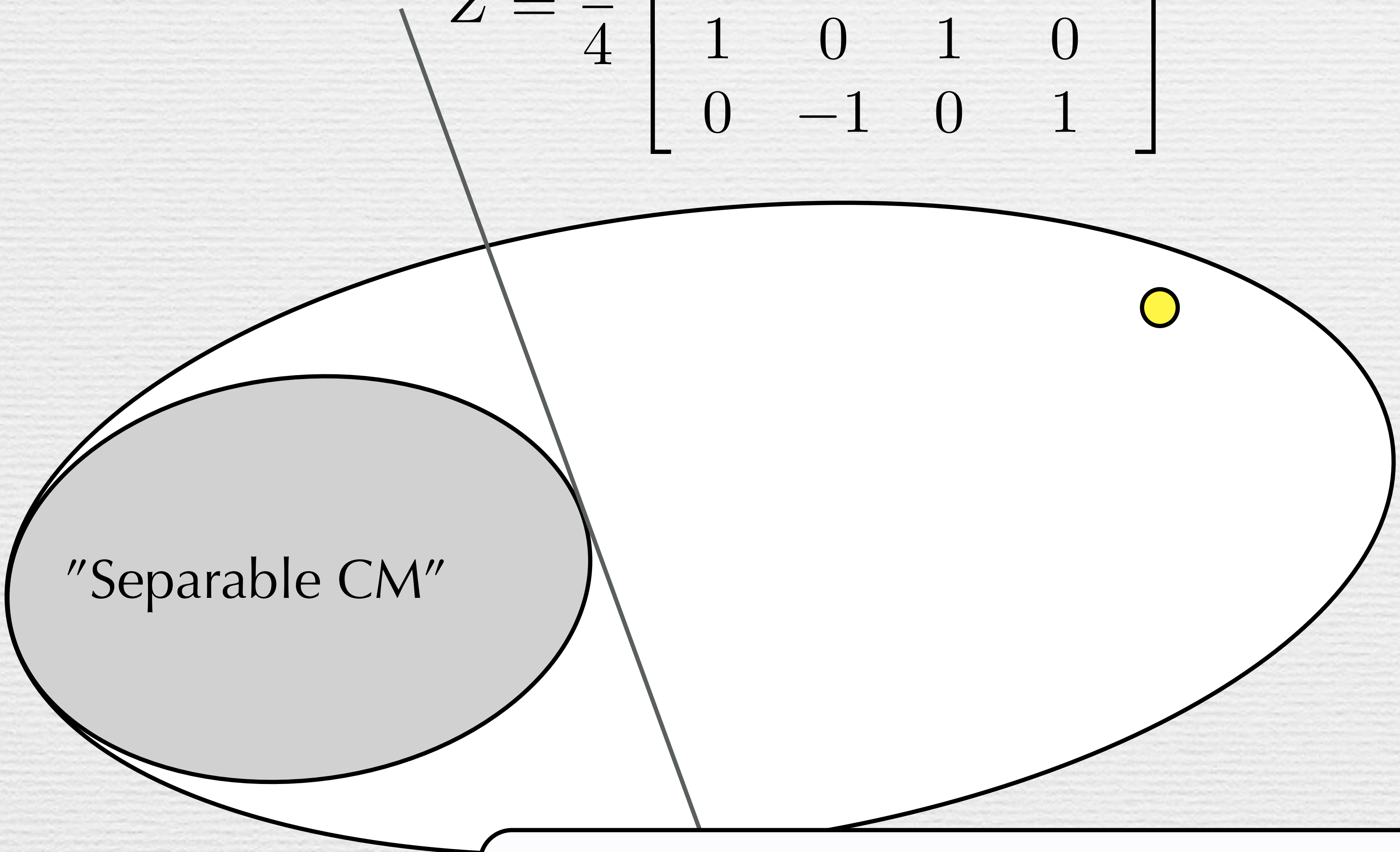
- **Multi-partite analogues**

van Loock, Furusawa, Phys Rev A 67, 052315 (2003)

Geometric picture of covariance matrix witnesses

- **Geometric picture:** $\mathrm{tr}(Z\gamma) < 1$ in terms of covariance matrices $\gamma = \gamma^T$

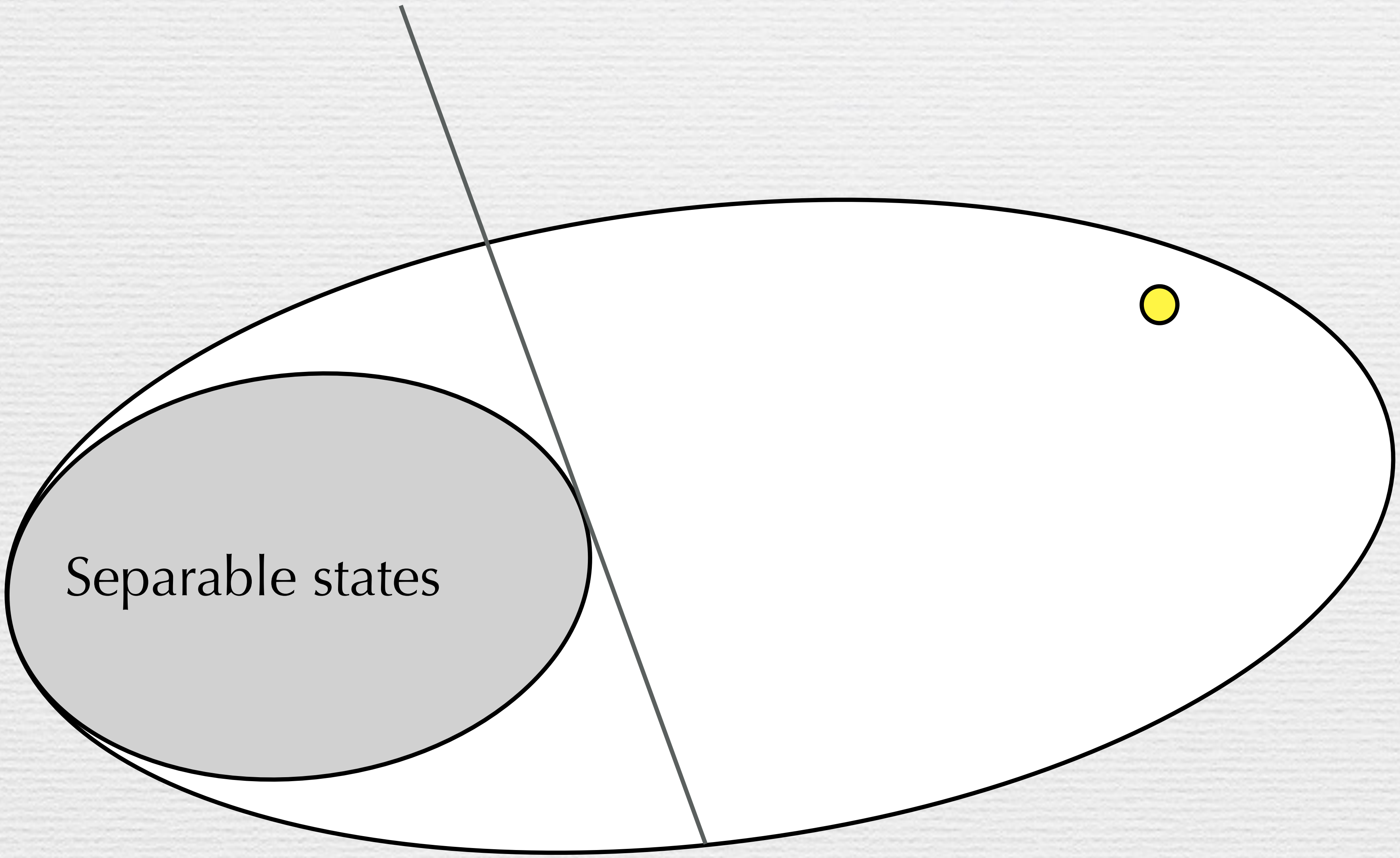
$$Z = \frac{1}{4}\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$$



- Can complete picture of valid tests Z be found?

Optimal witnesses

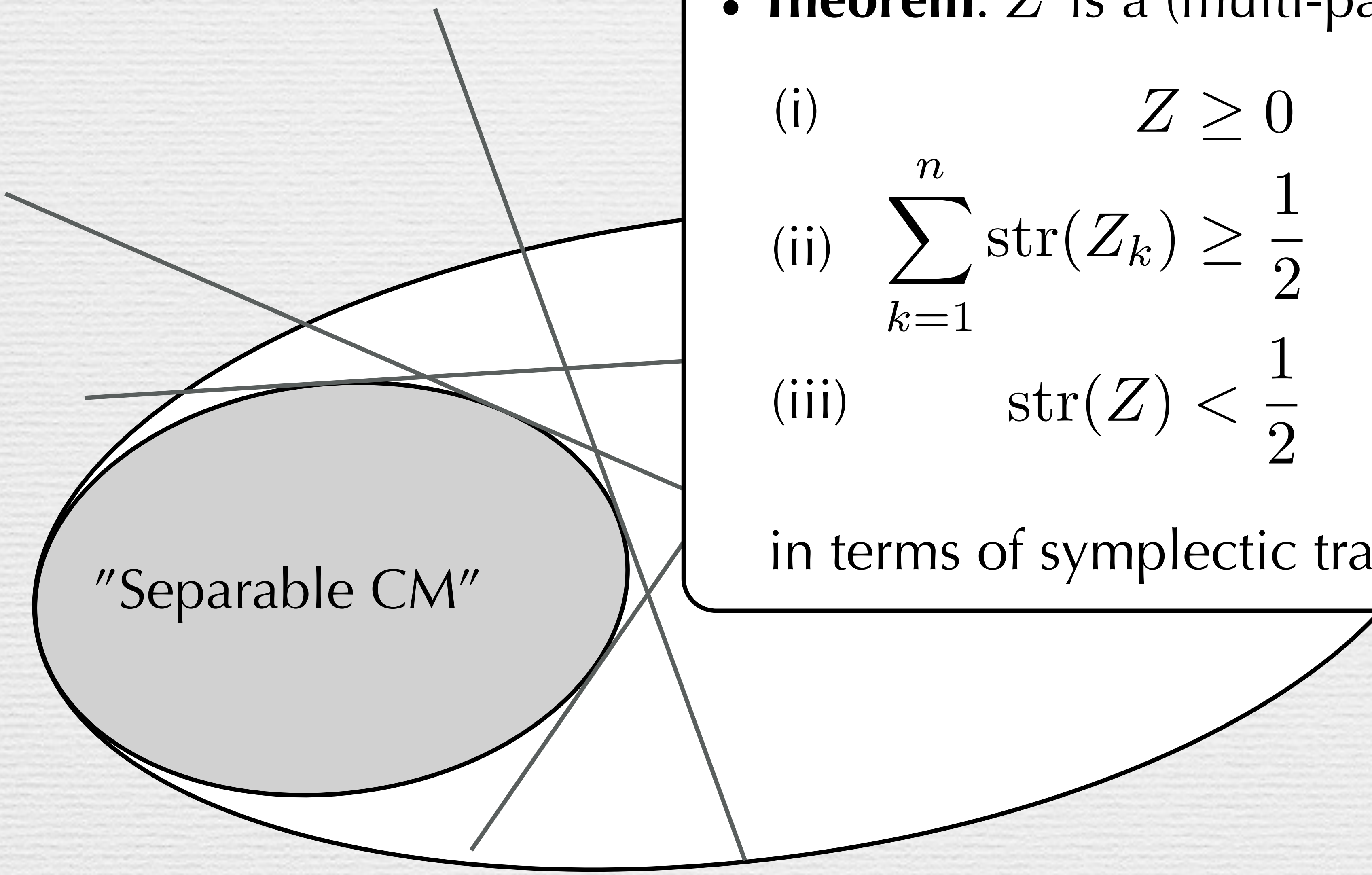
- **Entanglement witness problem** is "slightly harder" than separability problem (NP-hard)



Lewenstein, Kraus, Cirac, Horodecki, Phys Rev A 62, 052310 (2000)
Ioannou, Travaglione, Cheung, Ekert, Phys Rev A 70, 060403(R) (2004)

Optimal witnesses

- Here, **all tests** based on second moments can be classified



- **Theorem**: Z is a (multi-partite) entanglement test iff

(i) $$Z \geq 0$$

(ii) $$\sum_{k=1}^{n} \mathrm{str}(Z_k) \geq \frac{1}{2}$$

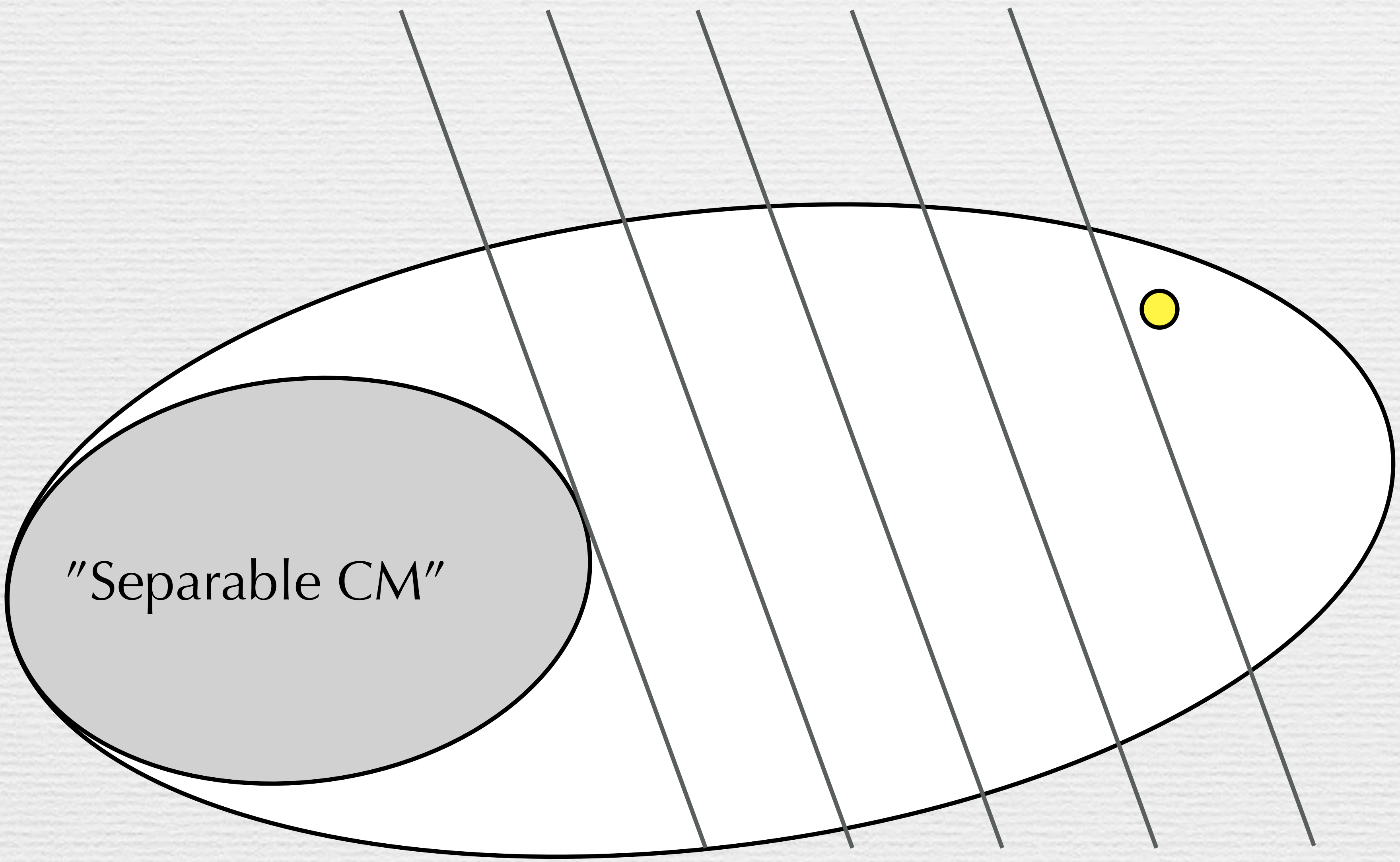
(iii) $$\mathrm{str}(Z) < \frac{1}{2}$$

in terms of symplectic traces

Hyllus, Eisert, New J Phys 8, 51 (2006)

Quantitative entanglement witnesses

- In bi-partite setting: **quantitative entanglement implications** (e.g., negativity)



Hyllus, Eisert, New J Phys 8, 51 (2006)

Optimal witnesses as semi-definite programmes

- Practically **finding optimal test** as solution to **semi-definite problem**

- **Theorem**: For a given covariance matrix γ , the optimal witness solves

$$
\begin{aligned}
\text{minimize}_{X_1, X_2} \quad & \mathrm{Tr}[\gamma X_1^{\mathrm{re}}] - 1 \\
\text{subject to} \quad & X_1^{\mathrm{bd,re}} = X_2^{\mathrm{bd,re}} \\
& X_1 \geq 0,\ X_2 \geq 0 \\
& \mathrm{Tr}[i\sigma X_2] = -1
\end{aligned}
$$

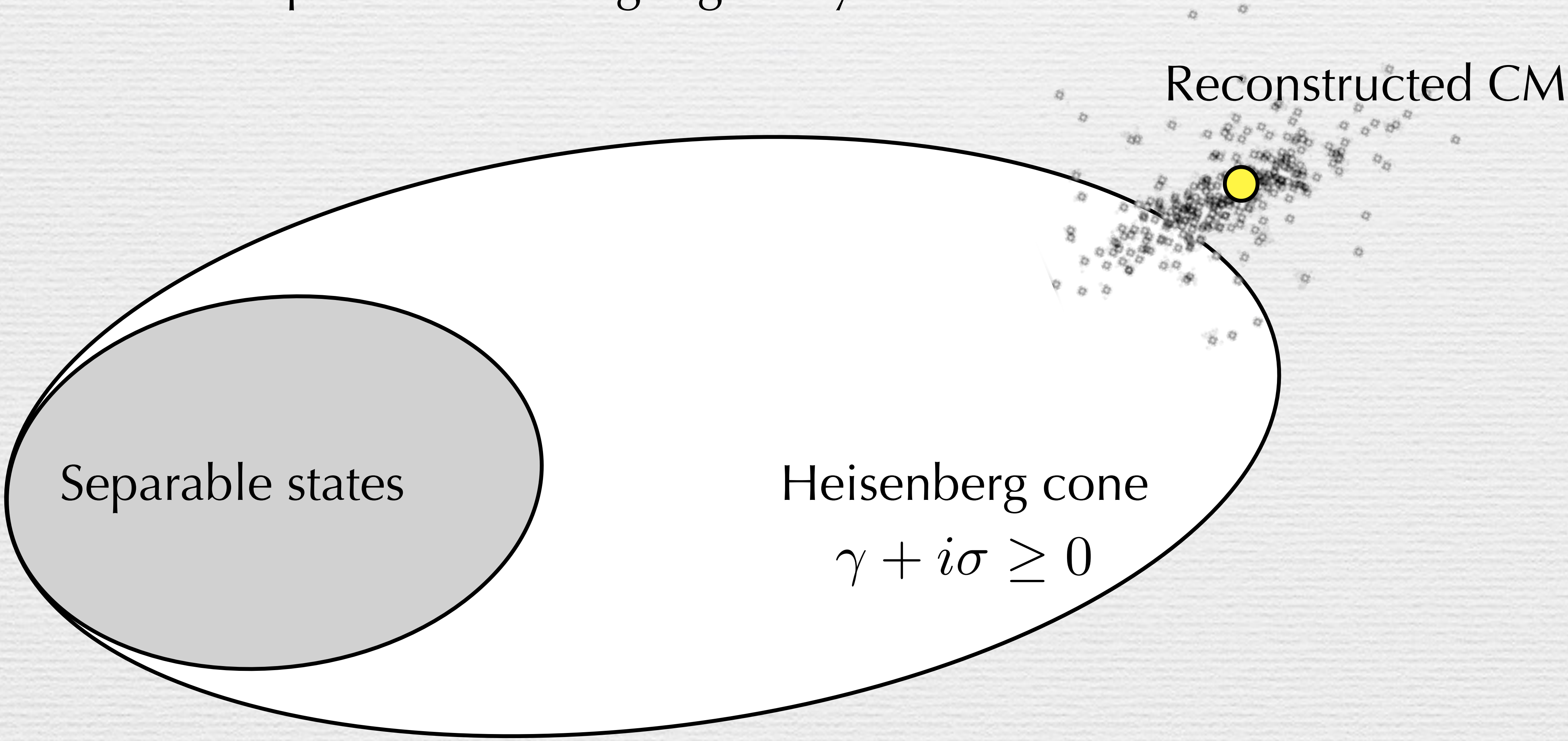
the Lagrange dual of

$$
\begin{aligned}
\text{minimize}_{\gamma_A, \gamma_B, x_e} \quad & (-x_e), \\
\text{subject to} \quad & \gamma - \gamma_A \oplus \gamma_B \geq 0 \\
& \gamma_A \oplus \gamma_B + (1 + x_e) i\sigma \geq 0
\end{aligned}
$$

Hyllus, Eisert, New J Phys 8, 51 (2006)

Revisiting this for extremely noisy opto-mechanical experiments

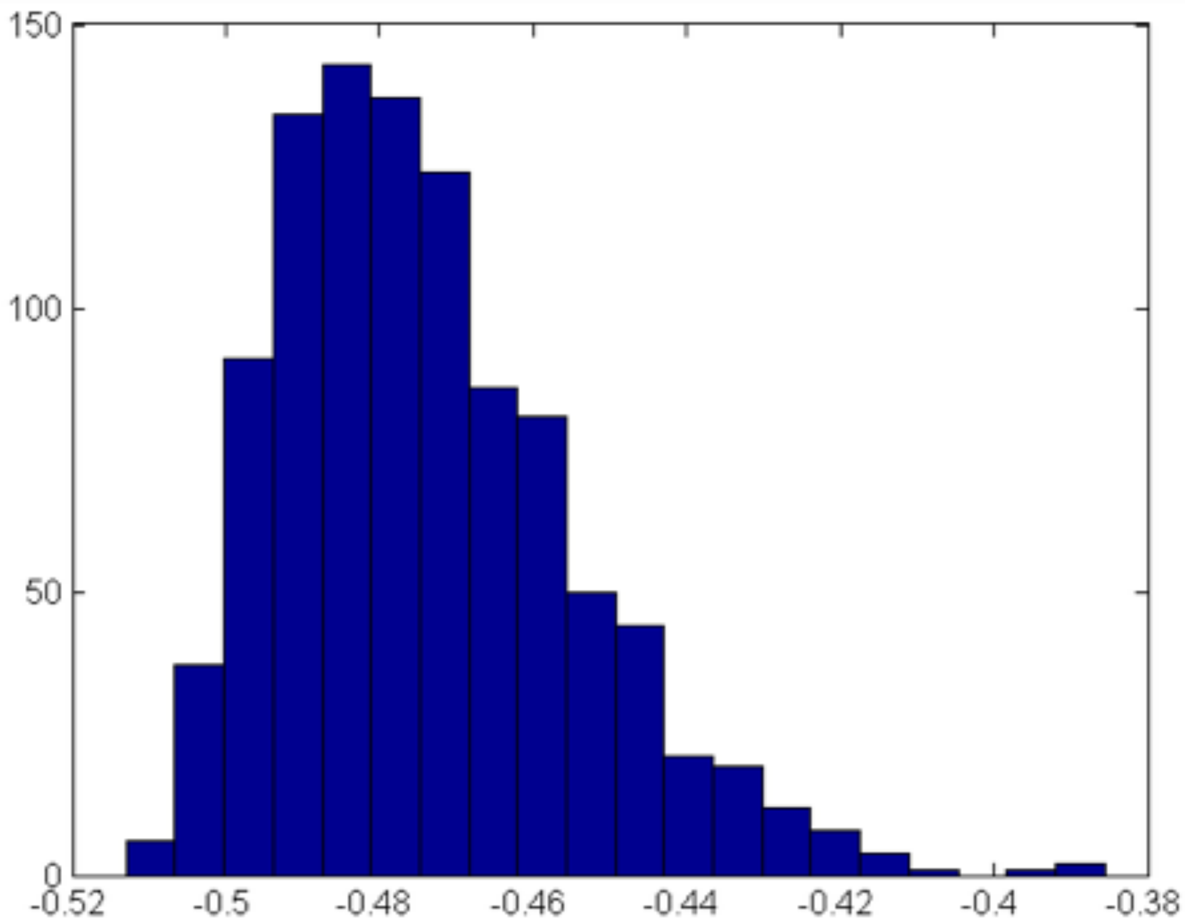
- In reality, approximately **low-rank state and CM** and **noisy data**
- Projection onto positive cone fiercly unreliable: **Use quantitative tests**
- Tool in first experiment entangling many **mechanical oscillators**

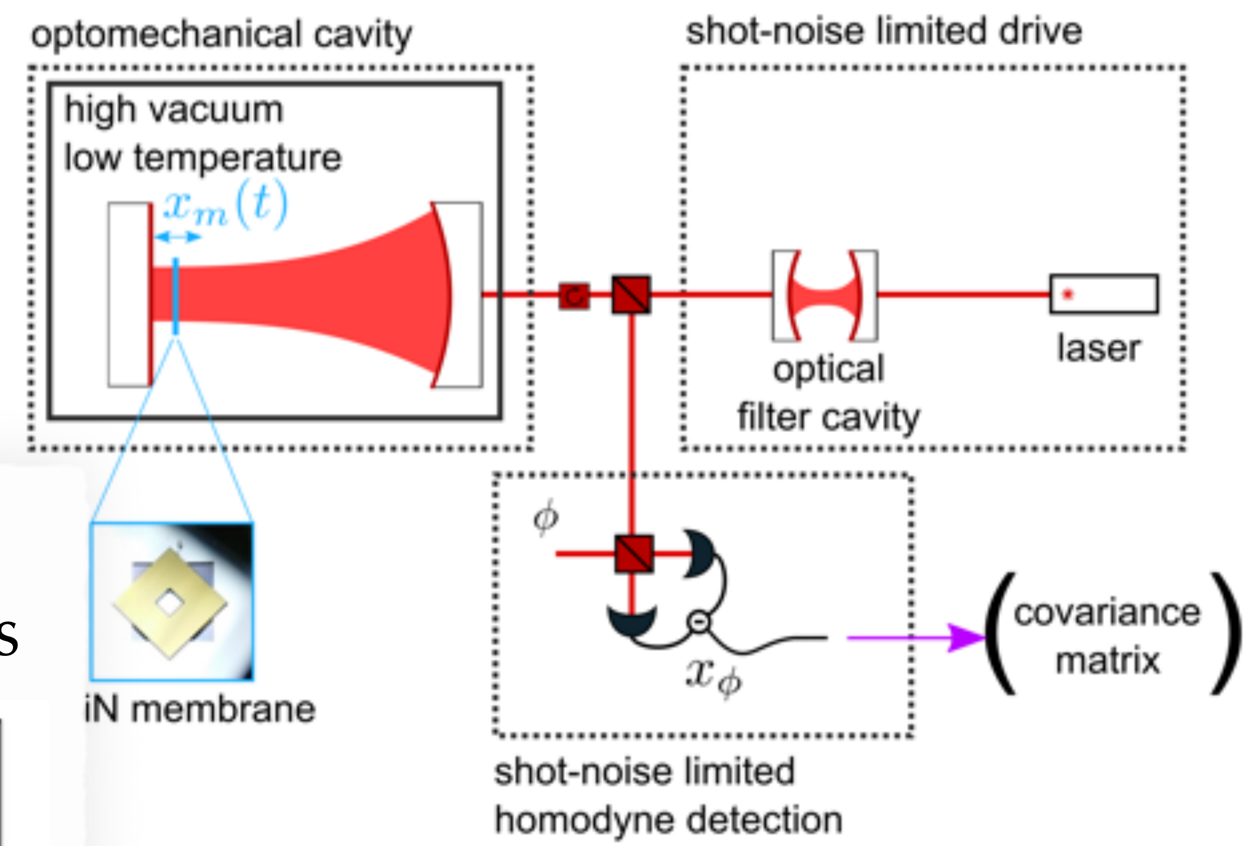


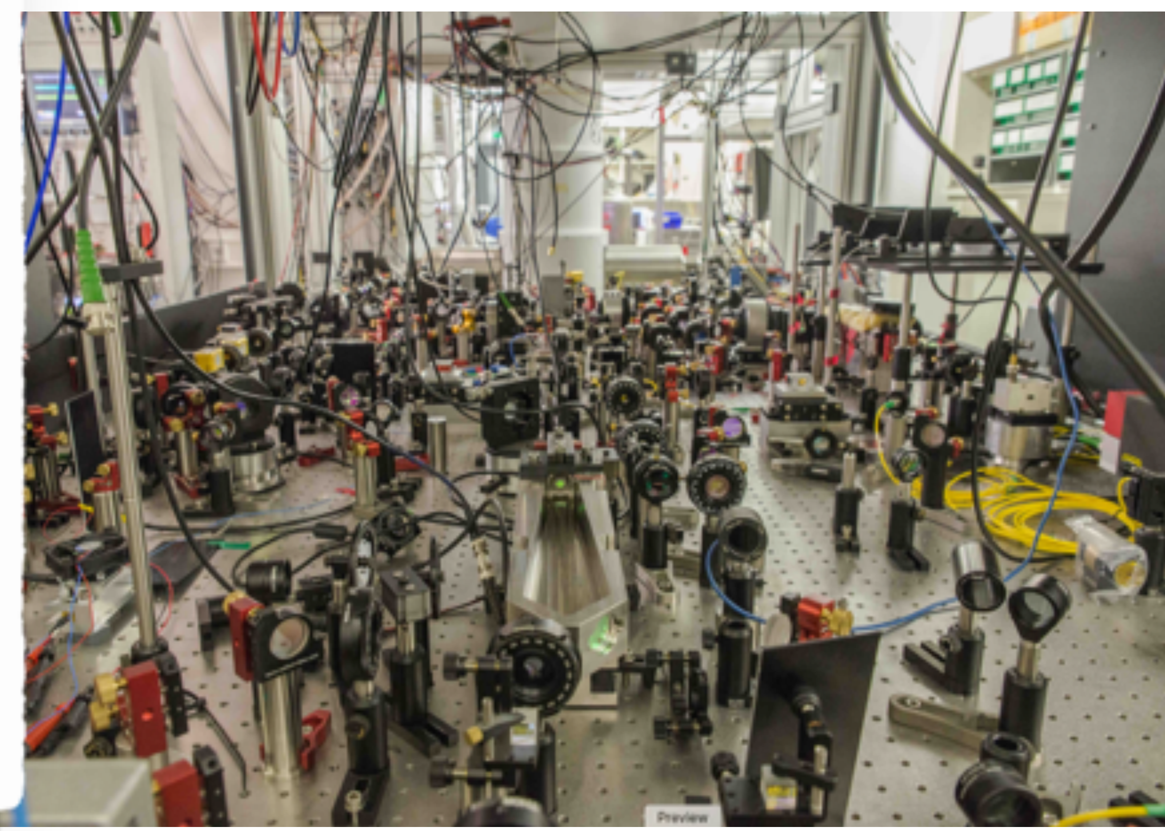
Hyllus, Eisert, New J Phys 8, 51 (2006)

Revisiting this for extremely noi

- In reality, approximately **low-rank state**
- Projection onto positive cone unreliabl
- Violation of entanglement test in 10-10 split for 20 mechanical modes



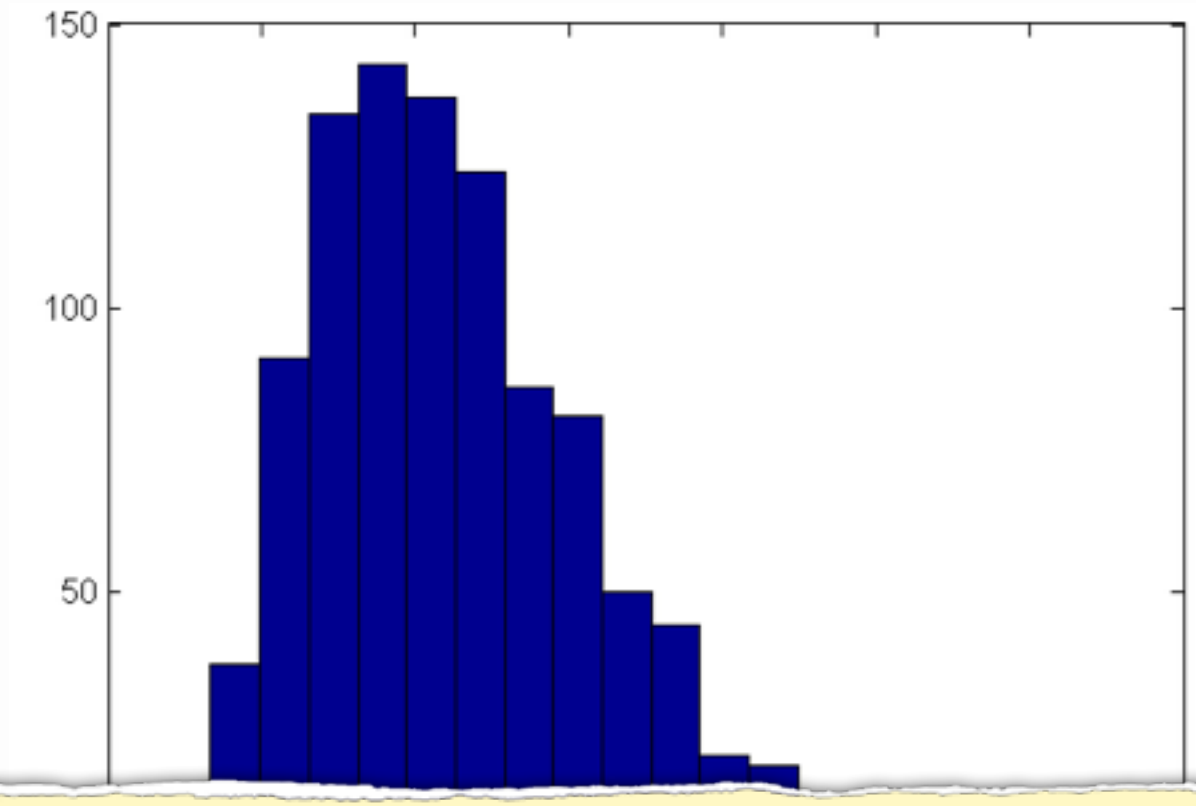




Hoelscher-Obermaier, Wieczorek, Hammerer, Steffens, Eisert, Aspelmeyer, in preparation (2016)

Revisiting this for extremely noisy opto-mechanical experiments

Violation of entanglement test in
10-10 split for 20 mechanical modes

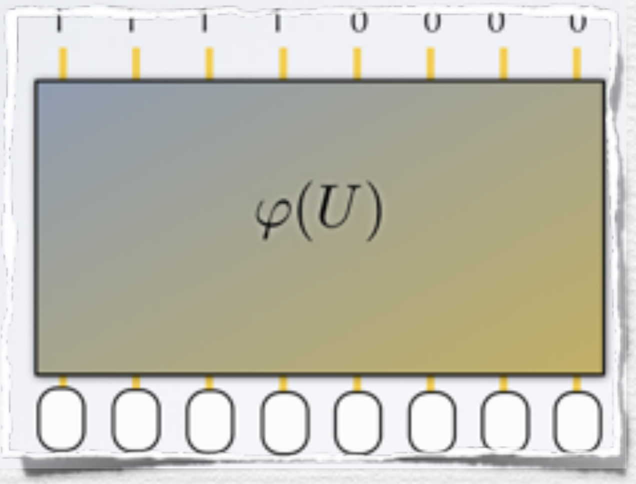


- **Lesson:** Continuous-variable entanglement tests provide powerful tools to detect entanglement specifically for noisy data

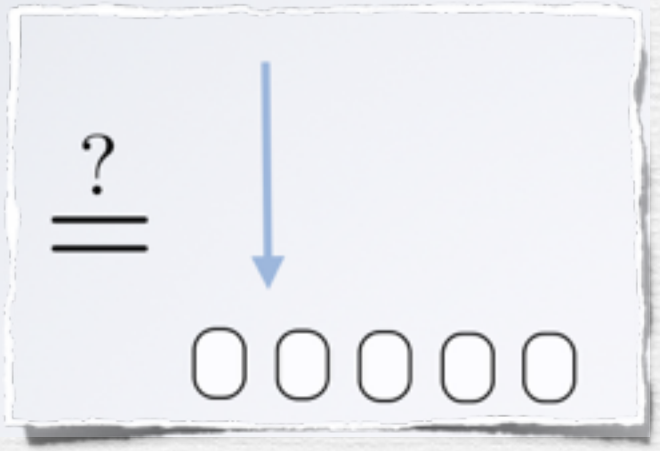
Hoelscher-Obermaier, Wieczorek, Hammerer, Steffens, Eisert, Aspelmeyer, in preparation (2016)

Summary: Certifying quantum systems

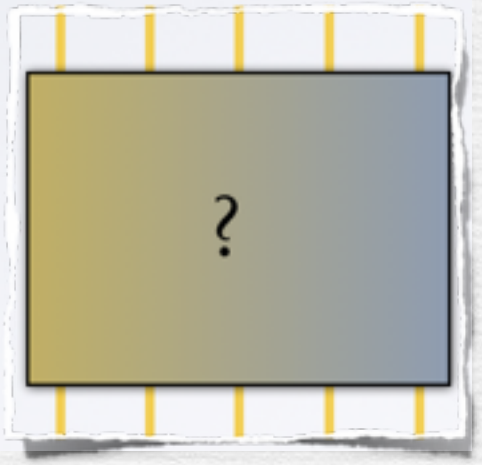
- Themes of classical and quantum certification



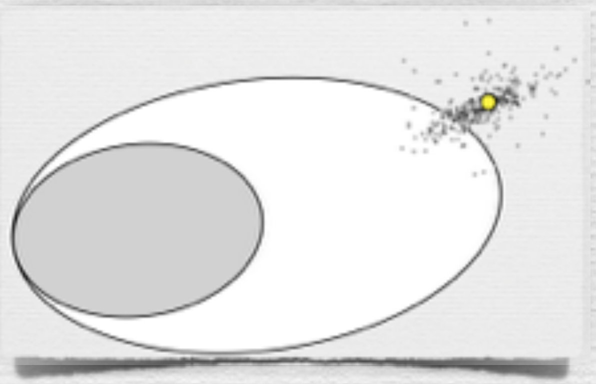
Boson sampling



Classical certification?



Quantum certification

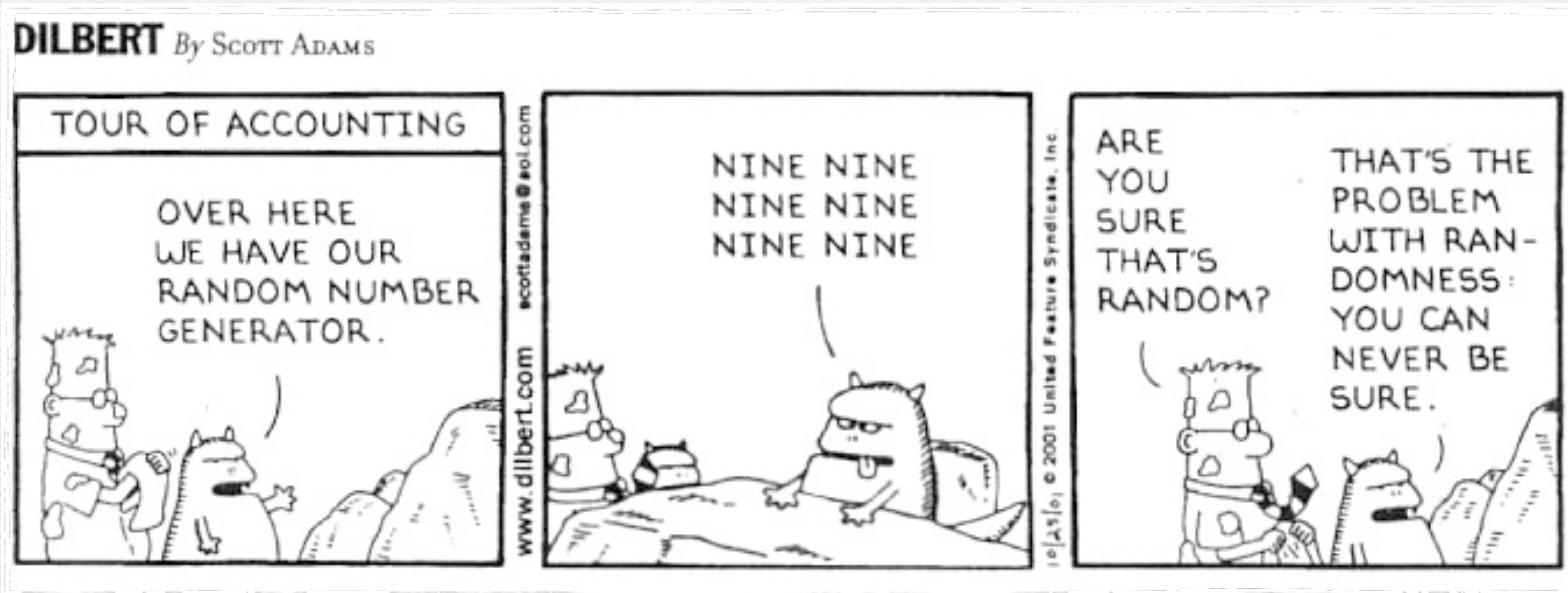


Optimal CV witnesses

- Quantum simulations and intermediate problems are not in NP, does it mean that whenever a quantum simulation is "hard", it can not efficiently be classically certified?

No

Summary: Certifying quantum systems



Thanks for your attention!