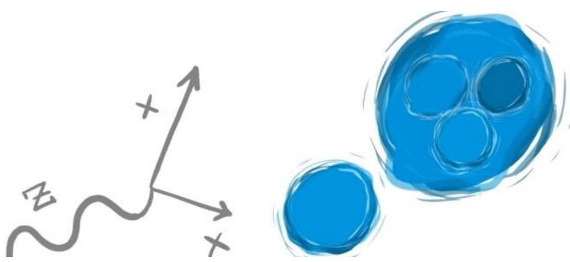
# Near-term quantum computers with linear optics

Saleh Rahimi-Keshari

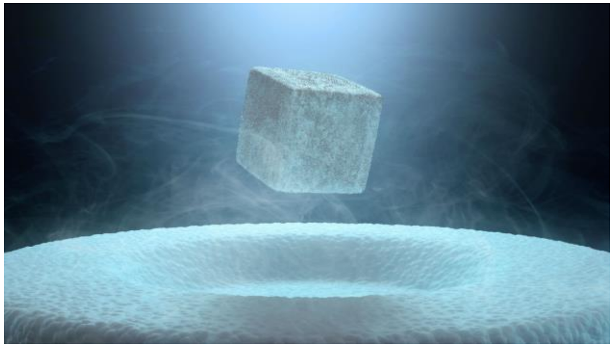
*Department of Physics, University of Tehran*
*School of Nano Science, IPM*

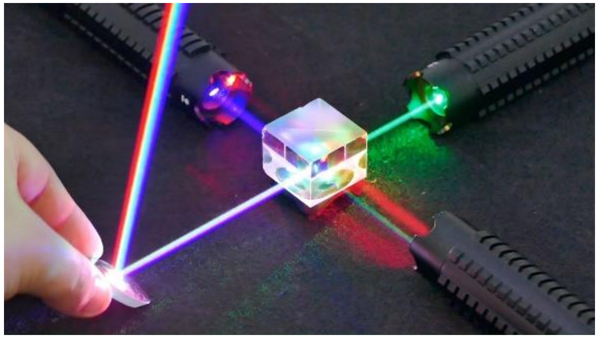
## Quantum mechanics is the greatest scientific achievement in the 20$^{th}$ century!

A fundamental theory that describes nature at the smallest scales.



Applications: semiconductors, superconducting materials, laser, …



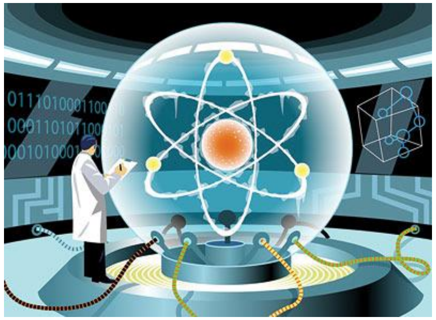
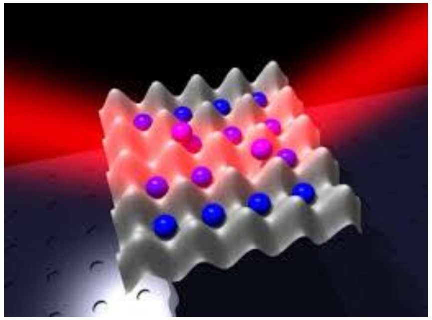


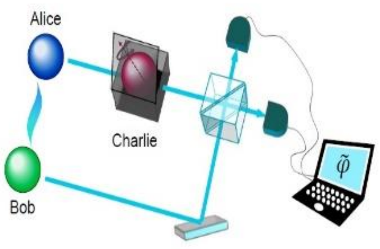
# Quantum information science is a new way of thinking!

John Preskill: “What are the scientific and technological implications of manipulating and controlling complex quantum systems?”

Theory: Quantum control theory, open quantum systems, entanglement theory, quantum computational complexity theory, …

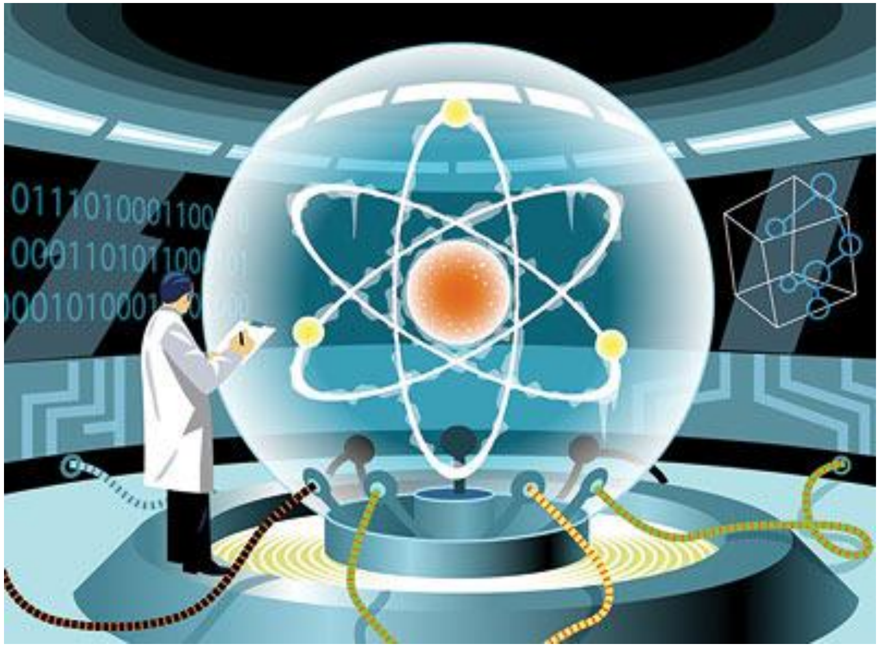
Applications: quantum computation, quantum simulation, quantum communication, quantum metrology, …



# Quantum supremacy

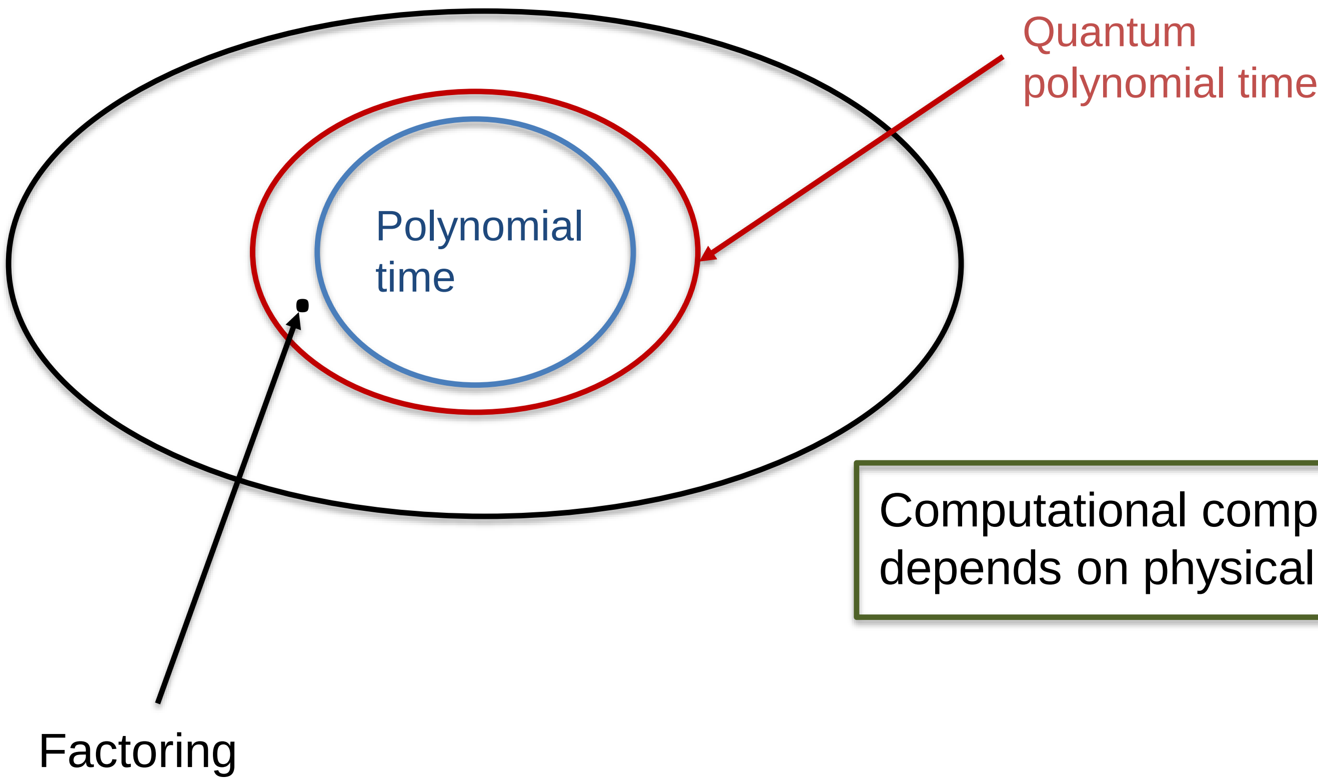
Based on computational complexity arguments, it is strongly believed that quantum computers can perform certain tasks beyond the power of  classical computers.



How can we demonstrate this without a universal quantum computer?

# Computational complexity theory

Hard = not solvable in polynomial-time in the size of the problem (not efficient)




Computational complexity depends on physical law.

# Shor's algorithm (1994)

Given N, find its prime factors: N=p x q

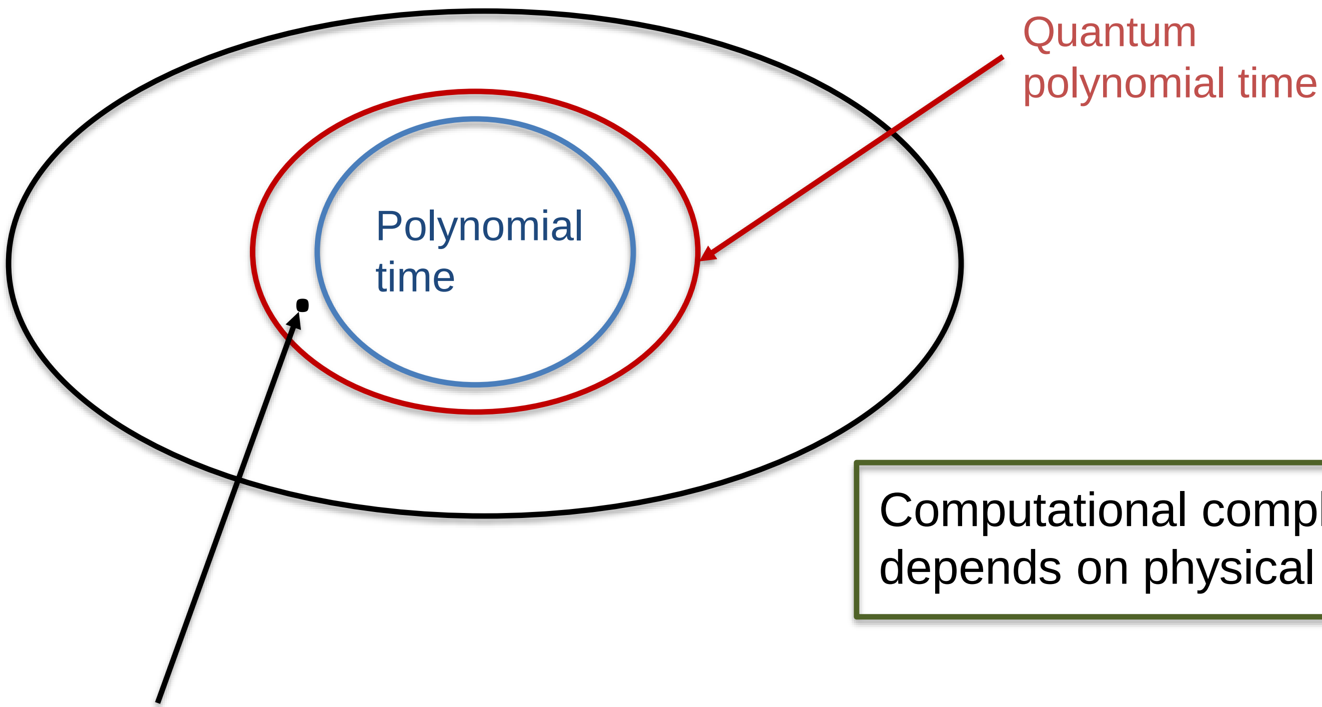
Important for public-key cryptography!

| Classical Computer | Quantum Computer |
|---|---|
| 193 digits in 30 CPU years (2.2 GHz) | 193 digits in 0.1 second |
| 500 digits in $10^{12}$ CPU years | 500 digits in 2 seconds |

John Preskill's presentation at CSSQI 2012

# Computational complexity theory

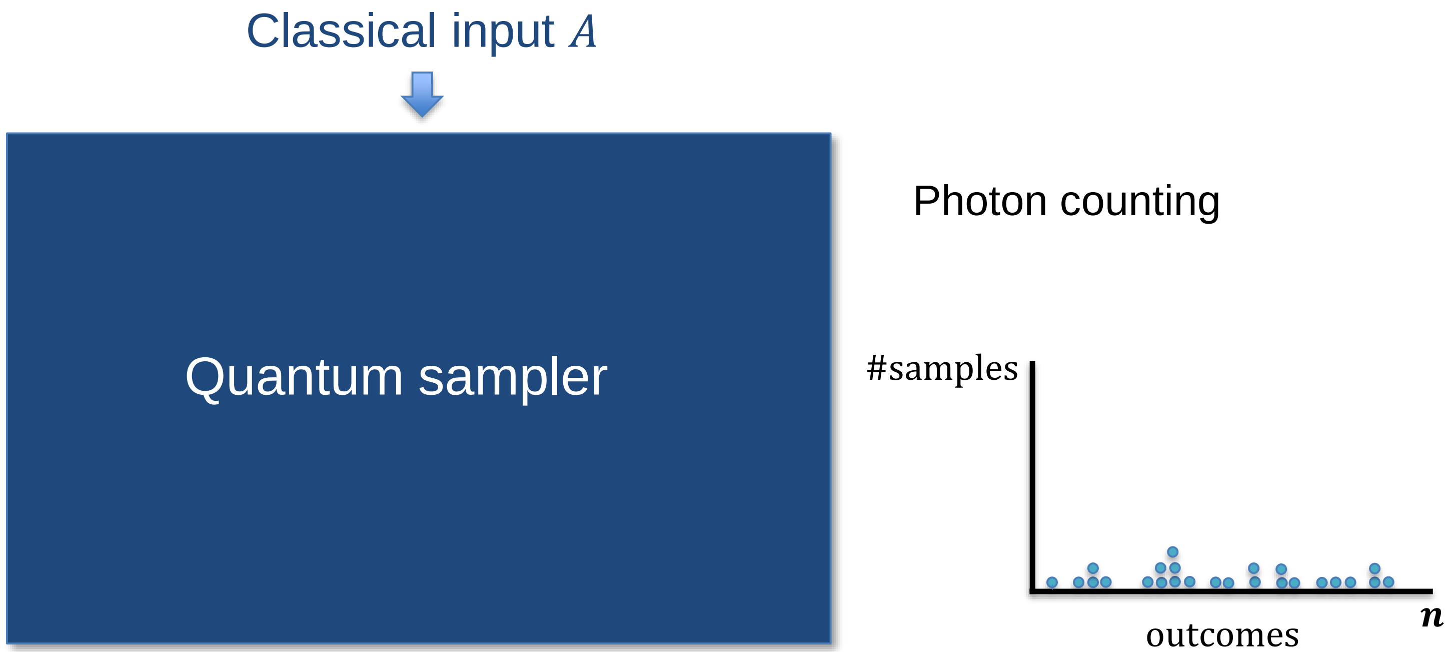
Hard = not solvable in polynomial-time in the size of the problem (not efficient)




Computational complexity depends on physical law.

Can we find a problem for demonstration of quantum supremacy with simple physical systems and algorithms? In principle, yes!

# Quantum sampling problems for demonstrating quantum supremacy



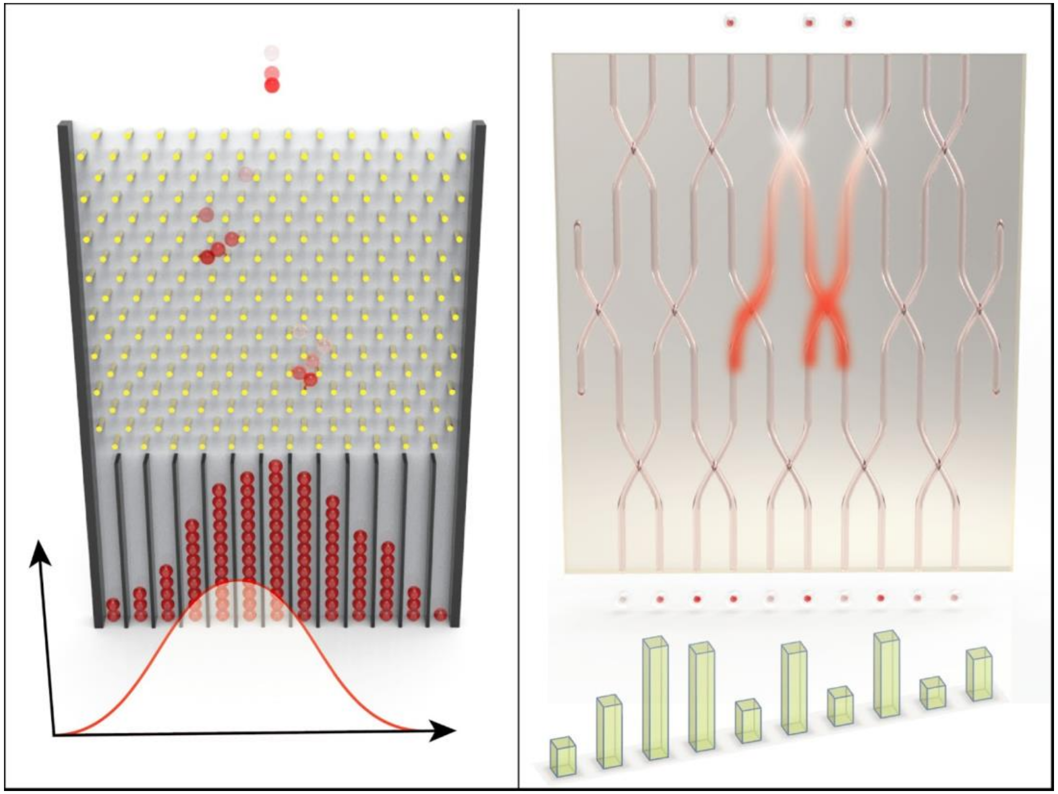

- Hard to simulate classically
- Simple physical realizations

## Outline:

I. Boson sampling: How quantum physics is different than classical physics, and how it can be used to demonstrate quantum supremacy.

II. Randomized boson sampling, and the power of entanglement in secret characterization of linear-optical networks.

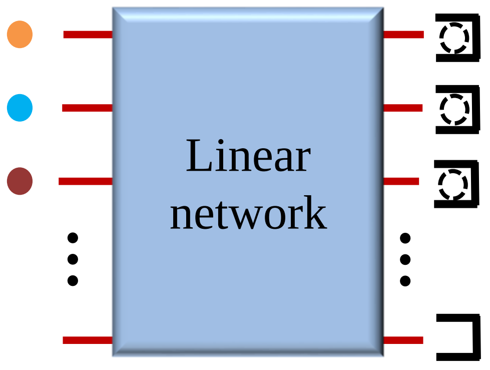
# What is boson sampling? Why is it classically hard to simulate?



http://www.2physics.com/2013/03/experimental-boson-sampling.html

Classical vs boson sampling

# Classical sampling




Example:

$$A_{11}A_{22}A_{33} + A_{11}A_{23}A_{32} + A_{12}A_{21}A_{33}$$
$$+ A_{12}A_{23}A_{31} + A_{13}A_{22}A_{31} + A_{13}A_{21}A_{32}$$
$$= \sum_{\sigma \in S_3} \prod_{i=1}^{3} A_{i,\sigma(i)} = \mathrm{Per}\left([A]_{3\times 3}\right)$$

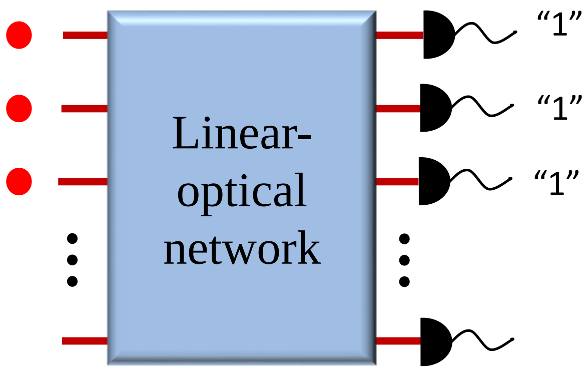
$$A = \begin{pmatrix} A_{11} & A_{12} & A_{13} & . & . & A_{1M} \\ A_{21} & A_{22} & A_{23} & . & . & . \\ A_{31} & A_{32} & A_{33} & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ A_{M1} & . & . & . & . & A_{MM} \end{pmatrix}$$

$$\boxed{0 \le A_{ij} \le 1}$$

Computing permanents is very difficult (#P-hard in complexity theory) [Valiant 1979].

$$\mathrm{Per}(B) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} B_{i,\sigma(i)}$$

# Boson sampling [Aaronson & Arkhipov 2010]




Example:

$$p = \left| U_{11}U_{22}U_{33} + U_{11}U_{23}U_{32} + U_{12}U_{21}U_{33} + U_{12}U_{23}U_{31} + U_{13}U_{22}U_{31} + U_{13}U_{21}U_{32} \right|^2$$

$$= \left| \sum_{\sigma \in S_3} \prod_{i=1}^{3} A_{i,\sigma(i)} \right|^2 = \left| \mathrm{Per}\left( [U]_{3\times 3} \right) \right|^2$$

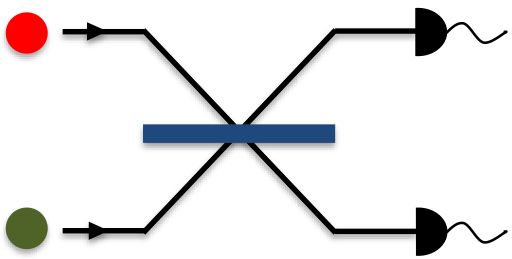
$$U = \begin{pmatrix} U_{11} & U_{12} & U_{13} & . & . & U_{1M} \\ U_{21} & U_{22} & U_{23} & . & . & . \\ U_{31} & U_{32} & U_{33} & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ U_{M1} & . & . & . & . & U_{MM} \end{pmatrix}$$

The transfer matrix

Multiplicative approximation of permanents of complex matrices is also very difficult (#P-hard) [Aaronson & Arkhipov 2013]

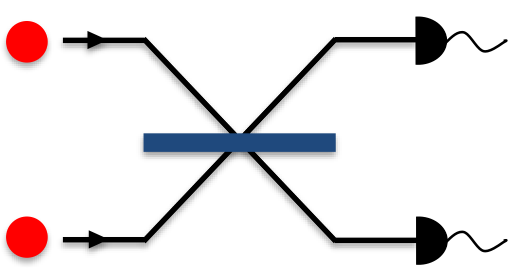
$$|p - \tilde{p}| \le \epsilon p$$

## Example: Hong-Ou-Mandel effect [PRL 1987]



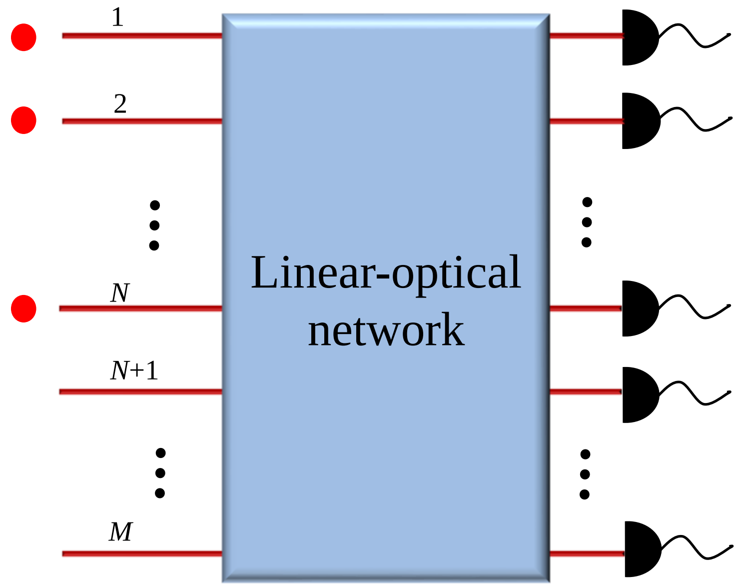

$$P_{\mathrm{dis}}(1,1) = \left(\frac{1}{2} \times \frac{1}{2}\right) + \left(\frac{1}{2} \times \frac{1}{2}\right) = \frac{1}{2}$$

$$U = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}$$ 50:50 beam splitter




$$P_{\mathrm{indis}}(1,1) = \left|\frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}}\right|^2 = 0$$

Boson Sampling: Sampling from a probability distribution of photon-counting events at the output of an $M$-mode linear-optical network for $N$ input single photons ($N \ll M$) [Aaronson & Arkhipov 2010].




**Theorem**: Modulo two conjectures, sampling from probability distributions that are close approximations of the output probability distribution is classically hard, unless the polynomial hierarchy collapses to the third level that is highly unlikely.

15 FEBRUARY 2013 VOL 339 SCIENCE

## Photonic Boson Sampling in a Tunable Circuit

Matthew A. Broome,[1,2]* Alessandro Fedrizzi,[1,2] Saleh Rahimi-Kesh
Scott Aaronson,[3] Timothy C. Ralph,[2] Andrew G. White[1,2]

NATURE PHOTONICS | VOL 7 | JULY 2013

## Experimental boson sampling

Max Tillmann[1,2]*, Borivoje Dakić[1], René Heilmann[3], Stefan Nolte[3], Alexander Szameit[3]
and Philip Walther[1,2]*

15 FEBRUARY 2013 VOL 339 SCIENCE

## Boson Sampling on a Photonic Chip

Justin B. Spring,[1]* Benjamin J. Metcalf,[1] Peter C. Humphreys,[1] W. Steven Kolthammer,[1]
Xian-Min Jin,[1,2] Marco Barbieri,[1] Animesh Datta,[1] Nicholas Thomas-Peter,[1] Nathan K. Langford,[1,3]
Dmytro Kundys,[4] James C. Gates,[4] Brian J. Smith,[1] Peter G. R. Smith,[4] Ian A. Walms

SCIENCE 14 AUGUST 2015 • VOL 349 ISSUE 6249 711

## Universal linear optics

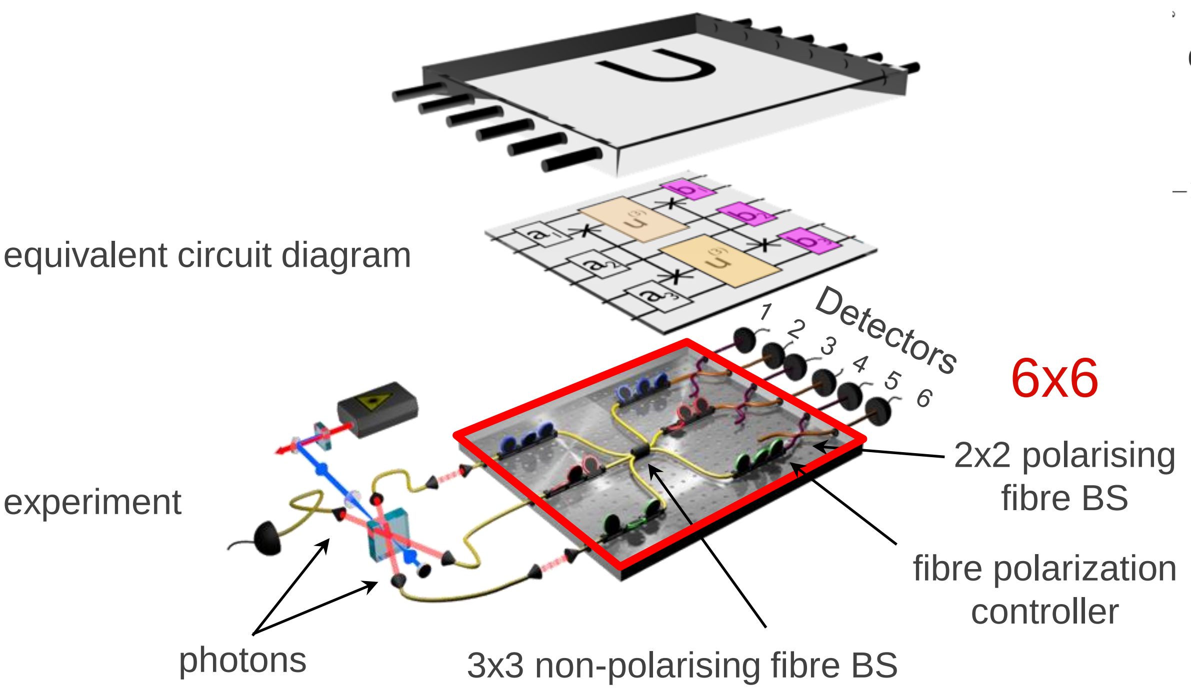
Jacques Carolan,[1] Christopher Harrold,[1] Chris Sparrow,[1,2] Enrique Martín-López,[3]
Nicholas J. Russell,[1] Joshua W. Silverstone,[1] Peter J. Shadbolt,[2] Nobuyuki Matsuda,[4]
Manabu Oguma,[5] Mikitaka Itoh,[5] Graham D. Marshall,[1] Mark G. Thompson,[1]
Jonathan C. F. Matthews,[1] Toshikazu Hashimoto,[5] Jeremy L. O'Brien,[1] Anthony Laing[1]*

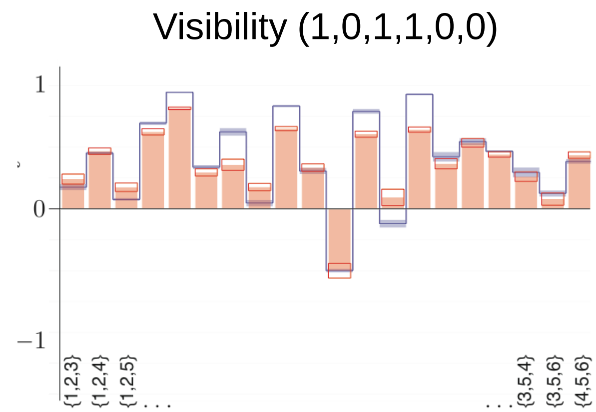
NATURE PHOTONICS | VOL 7 | JULY 2013

## Integrated multimode interferom arbitrary designs for photonic bo

Andrea Crespi[1,2], Roberto Osellame[1,2]*, Roberta Ramponi[1,2], Daniel J. Brod[3], Ernesto F. Galvão[3]*,
Nicolò Spagnolo[4], Chiara Vitelli[4,5], Enrico Maiorino[4], Paolo Mataloni[4] and Fabio Sciarrino[4]*

# First small-scale experimental demonstration

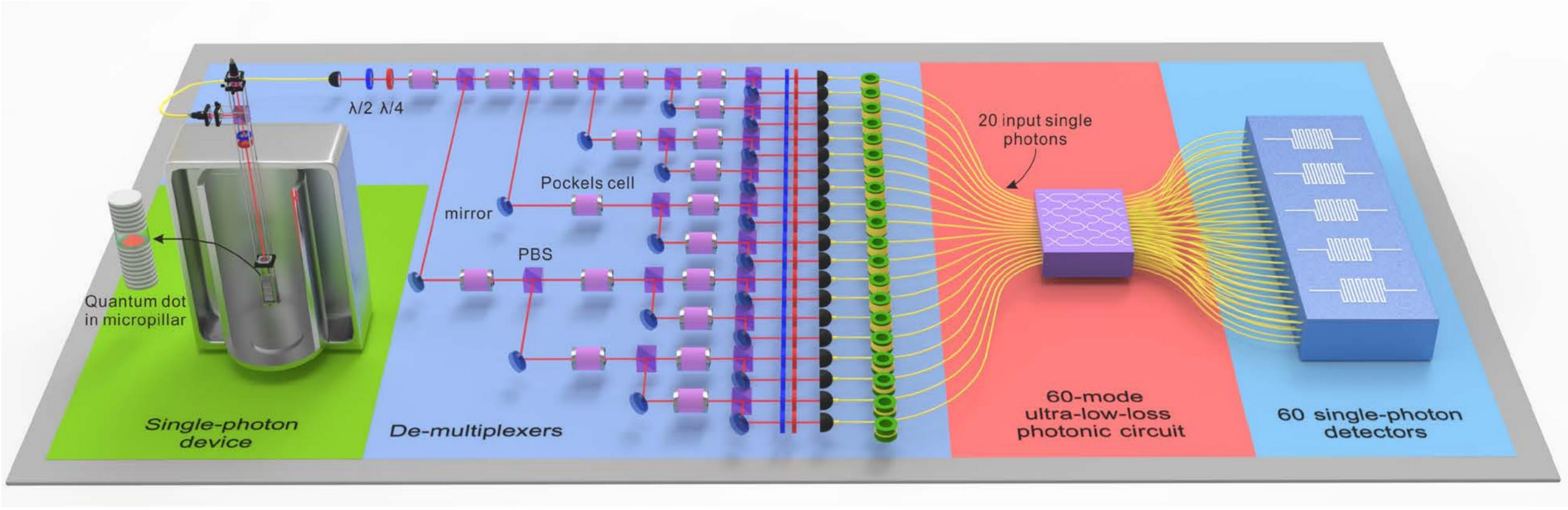



$$\text{Visibility} = \frac{P_{\text{dis}} - P_{\text{indis}}}{P_{\text{dis}}}$$

M. Broome, A. Fedrizzi, S. Rahimi-Keshari., J. Dove, S. Aaronson, T. Ralph, and A. White, *Science* **339**, 6121 (2013).

# The latest boson sampling experiment

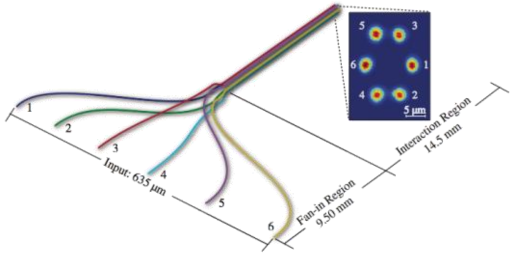


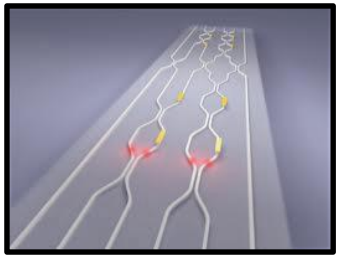

H. Wang, et al., Physical Review Letters 123, 250503 (2019).

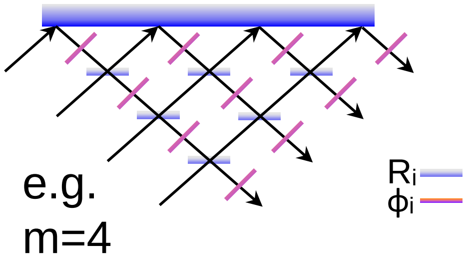
## Why boson sampling?

- In general, simulation of quantum systems is classically hard. Boson sampling is one of few cases that we have strong arguments about the classical hardness of the problem, through the connection between matrix permanents and probabilities, and we can learn a lot from it!

- Simple physical implementations: linear-optical networks are readily available, and in principle, it can demonstrate quantum supremacy using 50 photons.





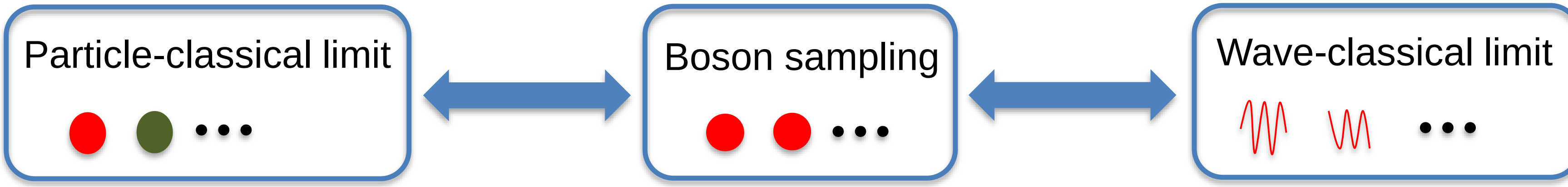

- Other applications have been recently proposed:

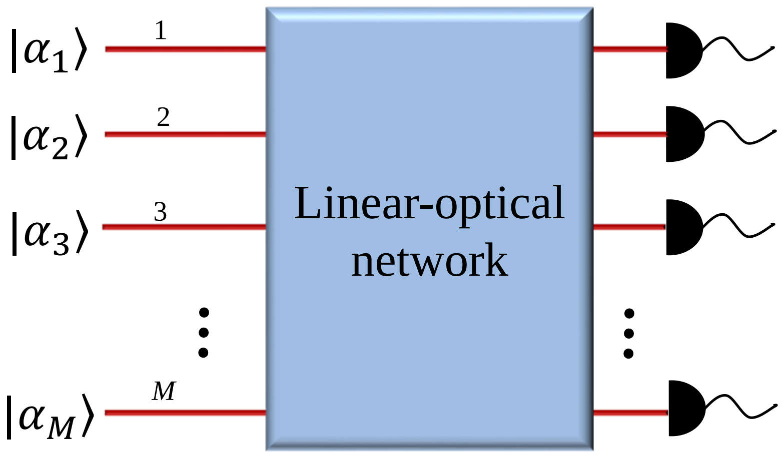
  - Cryptography [G. Nikolopoulos, arXiv:1907.01788 (2019)] [Z. Huang, et al., arXiv:1905.03013 (2019)]

  - Molecular computations [J. Huh, et al., *Nature Photonics* **9**, 615 (2015)]

  - Metrology [PRL **114**, 170802 (2015)]

# Wave-classical limit of boson sampling




Coherent state $|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$

$$(\beta_1\ \beta_2 \ldots\ \beta_M) = (\alpha_1\ \alpha_2 \ldots\ \alpha_M) \underbrace{\begin{pmatrix} U_{11} & U_{12} & \ldots \\ U_{21} & U_{22} & \ldots \\ \vdots & \vdots & \ddots \end{pmatrix}}_{\text{Transfer matrix}}$$

Coherent states can be used for characterization of linear-optical networks

[S. Rahimi-Keshari *et al*., Optics Express 2013]

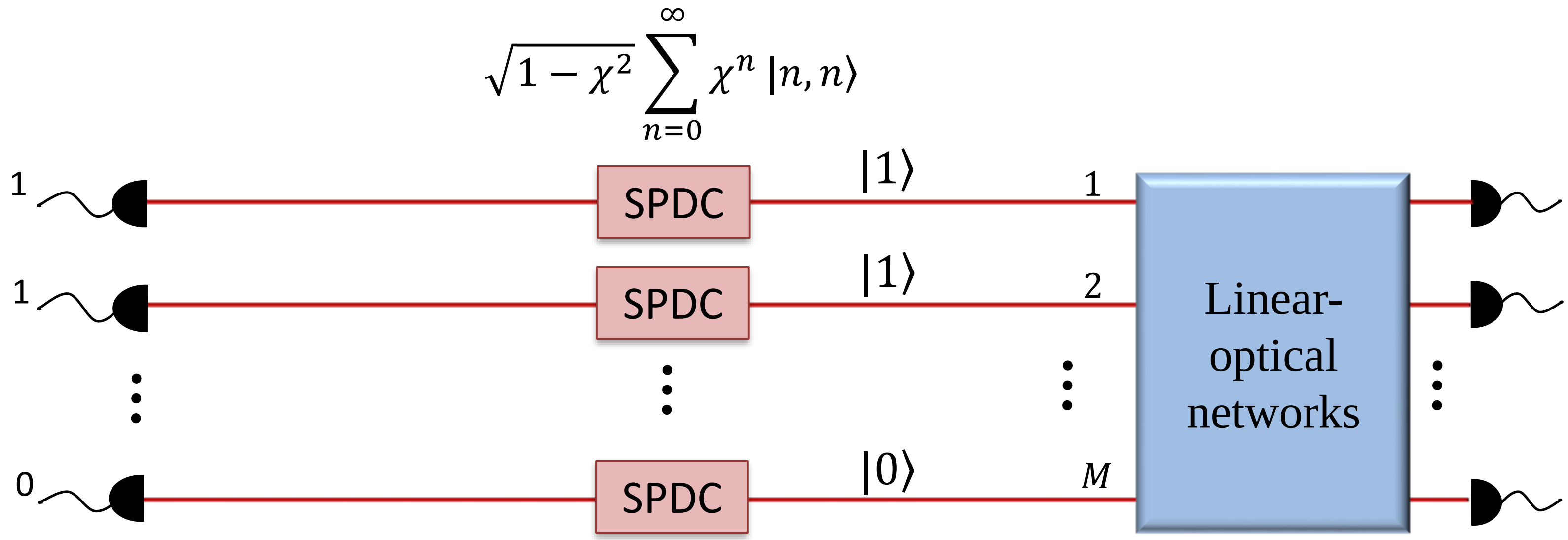
# Outline:

I. Boson sampling: How quantum physics is different than classical physics, and how it can be used to demonstrate quantum supremacy.

II. Randomized boson sampling, and the power of entanglement in secret characterization of linear-optical networks.

## Randomized boson sampling

uses spontaneous-parametric-down conversion (SPDC) sources



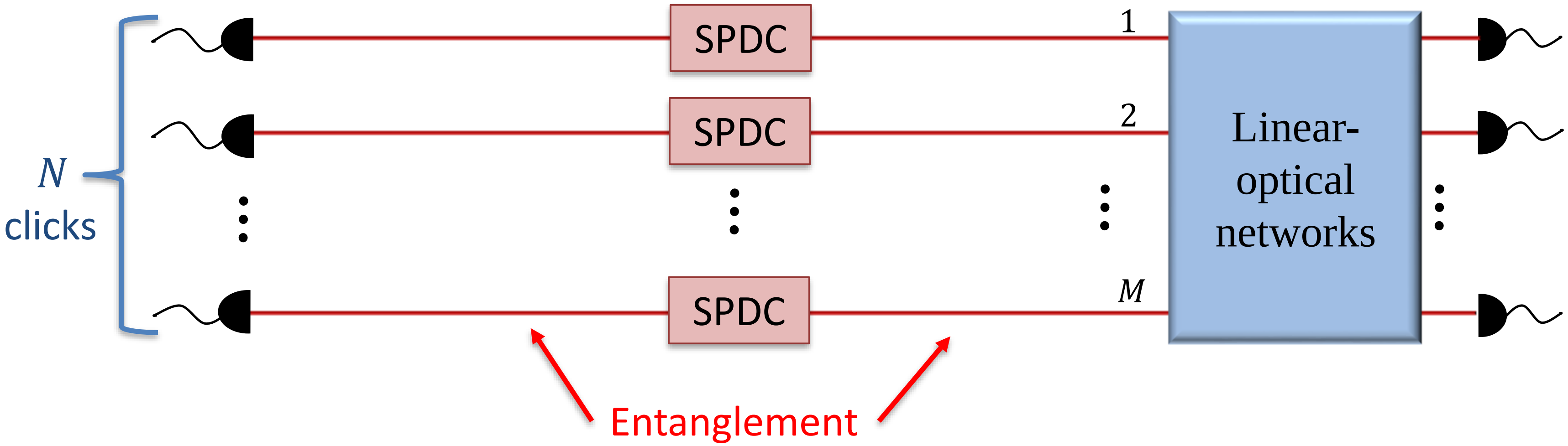

Probability of detecting $N$ single photons: $\left(1-\chi^2\right)^M\chi^{2N}$

A. Lund, A. Linag, S. Rahimi-Keshari, T. Rudolph, J. O'Brien, and T. Ralph, PRL **113**, 100502 (2014)

## Randomized boson sampling

uses spontaneous-parametric-down conversion (SPDC) sources

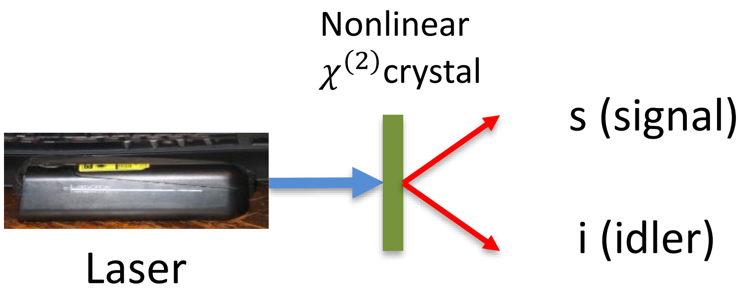
$$\sqrt{1-\chi^2}\sum_{n=0}^{\infty}\chi^n\,|n,n\rangle$$

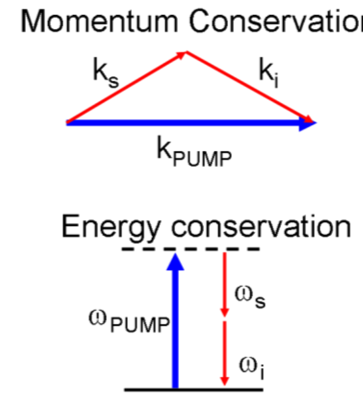



Probability of detecting $N$ random single photons: $\binom{M}{N}\left(1-\chi^2\right)^M\chi^{2N}\simeq\frac{1}{\sqrt{N}}$

A. Lund, A. Linag, S. Rahimi-Keshari, T. Rudolph, J. O'Brien, and T. Ralph, PRL **113**, 100502 (2014)

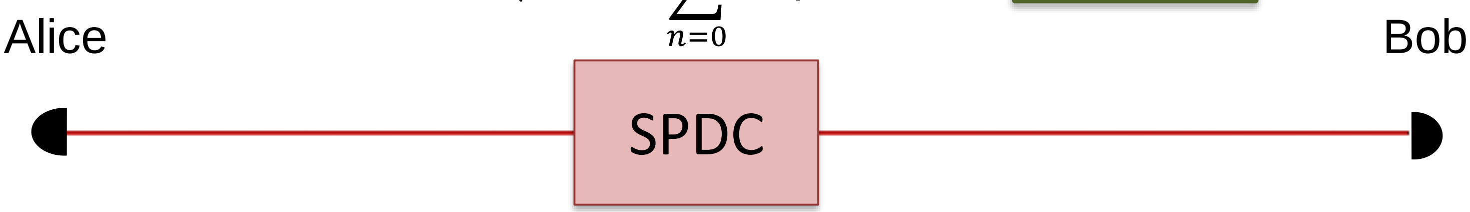
# Spontaneous-parametric-down conversion (SPDC) source




$$\sqrt{1-\chi^2}\sum_{n=0}^{\infty}\chi^n\,|n,n\rangle$$

$$\boxed{0<\chi<1}$$




Photodetector: $|n\rangle$

Number state: $|n\rangle$

Heterodyne: $|\alpha\rangle$

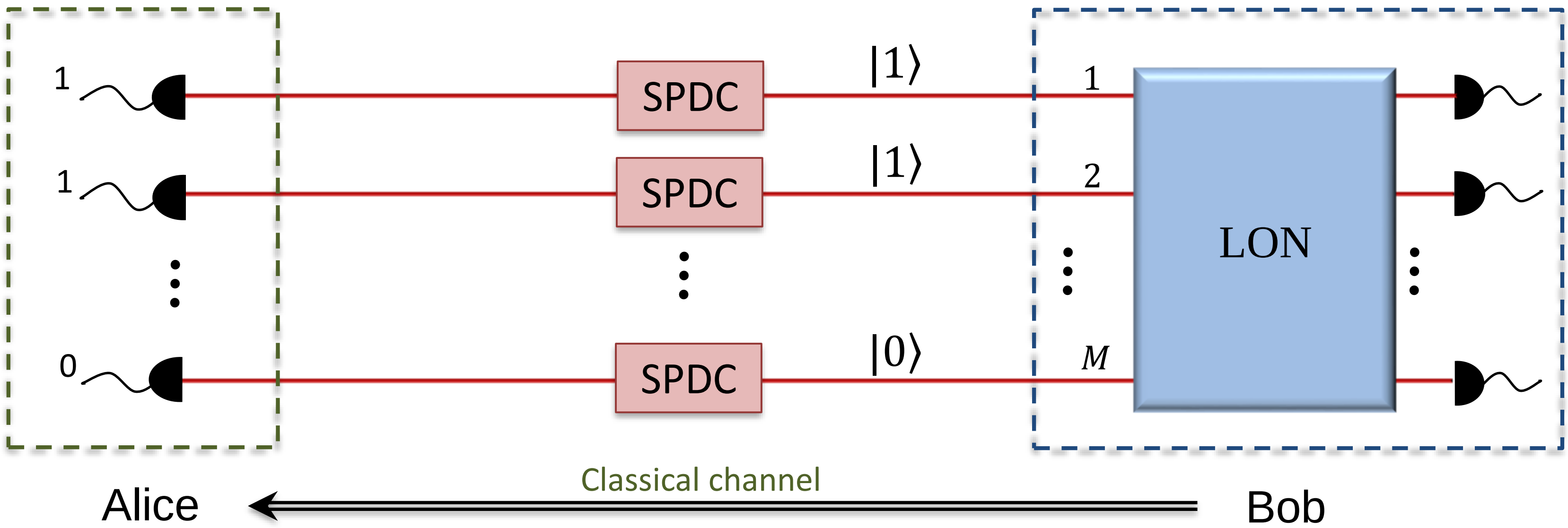
Coherent state: $|\chi\alpha^*\rangle$

If Alice doesn't tell anything, Bob's state: $\rho_B = (1-\chi^2)\sum_{n=0}^{\infty}\chi^{2n}\,|n\rangle\langle n|$

Thermal state!

# In situ and secret characterization of linear-optical

Randomized boson sampling as a distributed task between two parties:



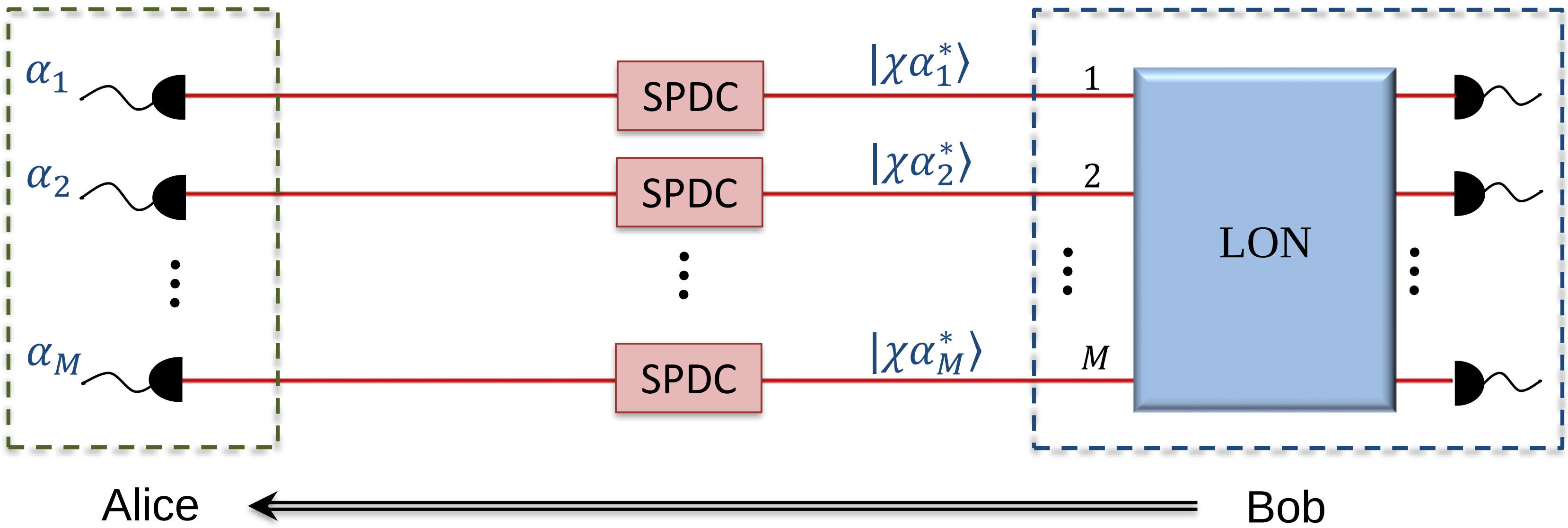

**Computational Runs:** Alice uses photon-counting measurements and samples from a classically hard joint probability distribution

$$P_{\mathrm{RBS}}(\boldsymbol{n}_A, \boldsymbol{n}_B) = P(\boldsymbol{n}_A)|\langle \boldsymbol{n}_B|\mathcal{U}_{\mathrm{LON}}|\boldsymbol{n}_A\rangle|^2$$

S. Rahimi-Keshari, S. Baghbanzadeh, and C. M. Caves, arXiv:1909.00827 (2019).

# In situ and secret characterization of linear-optical

Randomized boson sampling as a distributed task between two parties:



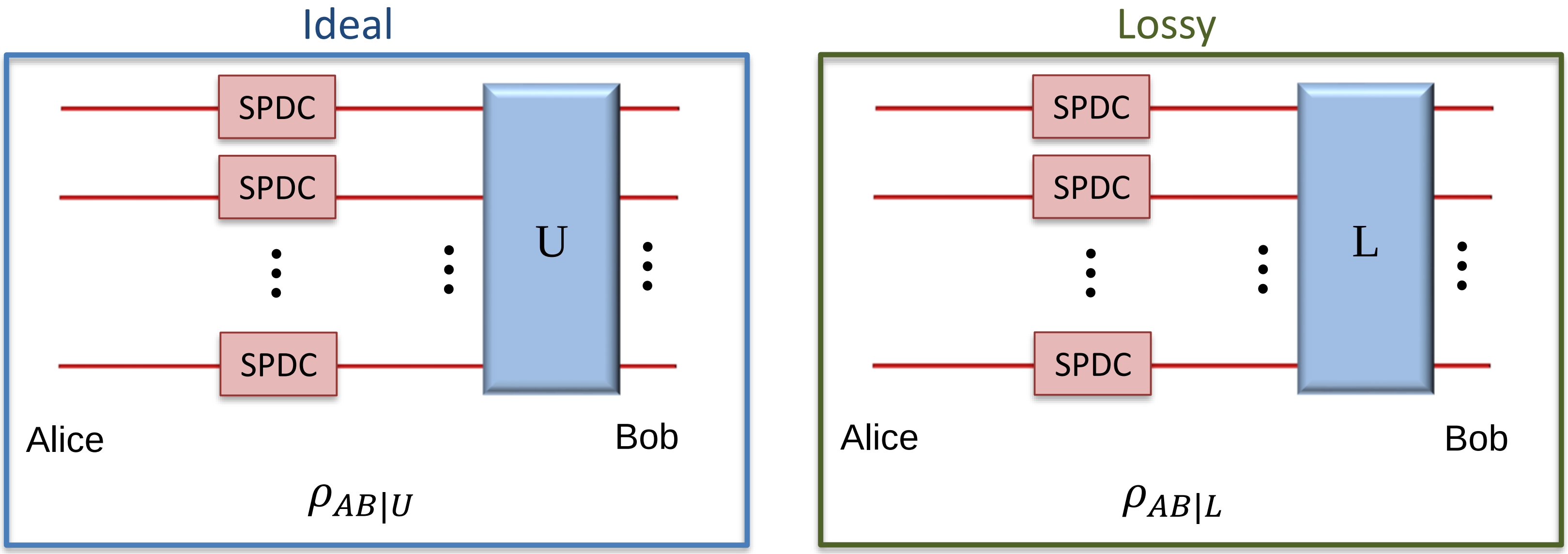

**Characterization Runs:** Alice uses heterodyne measurements and by sampling from

$$P_{\mathrm{C}}(\boldsymbol{\alpha}, \boldsymbol{n}_B) = P(\boldsymbol{\alpha})|\langle \boldsymbol{n}_B|\mathcal{U}_{\mathrm{LON}}|\boldsymbol{\alpha}\rangle|^2 = P(\boldsymbol{\alpha})|\langle \boldsymbol{n}_B|\boldsymbol{\alpha}\,\boldsymbol{U}\rangle|^2$$

she converts the experiment to a problem to a classically simulable problem that enables the characterization of the LON on the fly without Bob's knowing!

S. Rahimi-Keshari, S. Baghbanzadeh, and C. M. Caves, arXiv:1909.00827 (2019).

## Having characterized Bob's LON, Alice can assess the validity of the experiment!



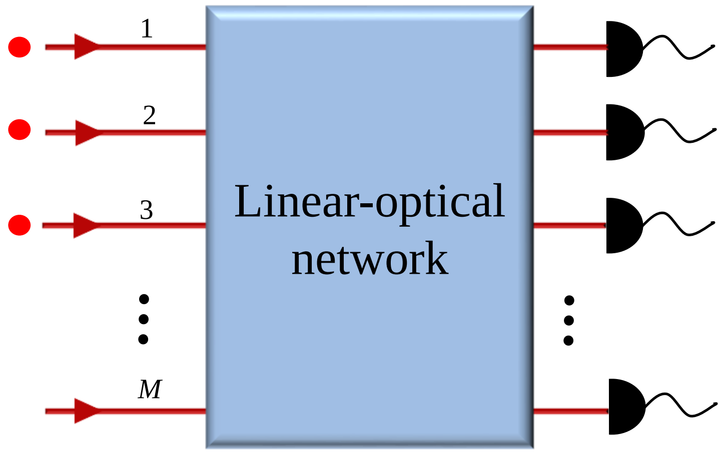

$$F\left(\rho_{AB|U}, \rho_{AB|L}\right) = \frac{\left(1-\chi^2\right)^M}{|\det(I - \chi^2 L U^\dagger)|}$$

Alice can determine whether samples are drawn from a probability distribution close enough to the desired, ideal distribution!

$$\frac{1}{2}\sum_{n_A, n_B} |P(n_A, n_B\,|U) - P(n_A, n_B\,|L)| \leq \sqrt{1 - \frac{(1-\chi^2)^{2M}}{|\det(I - \chi^2 L U^\dagger)|^2}} \leq \epsilon$$

## Summary

- Boson sampling: The problem of sampling from the output probability distribution of linear-optical networks for input single photons. Simple realization but classically hard and can demonstrate quantum supremacy!




- Open question: Verification of boson sampling in the presence of errors?

- Randomized boson sampling and a novel application of entanglement that can be used for other protocols as well.

Thank you for your attention!