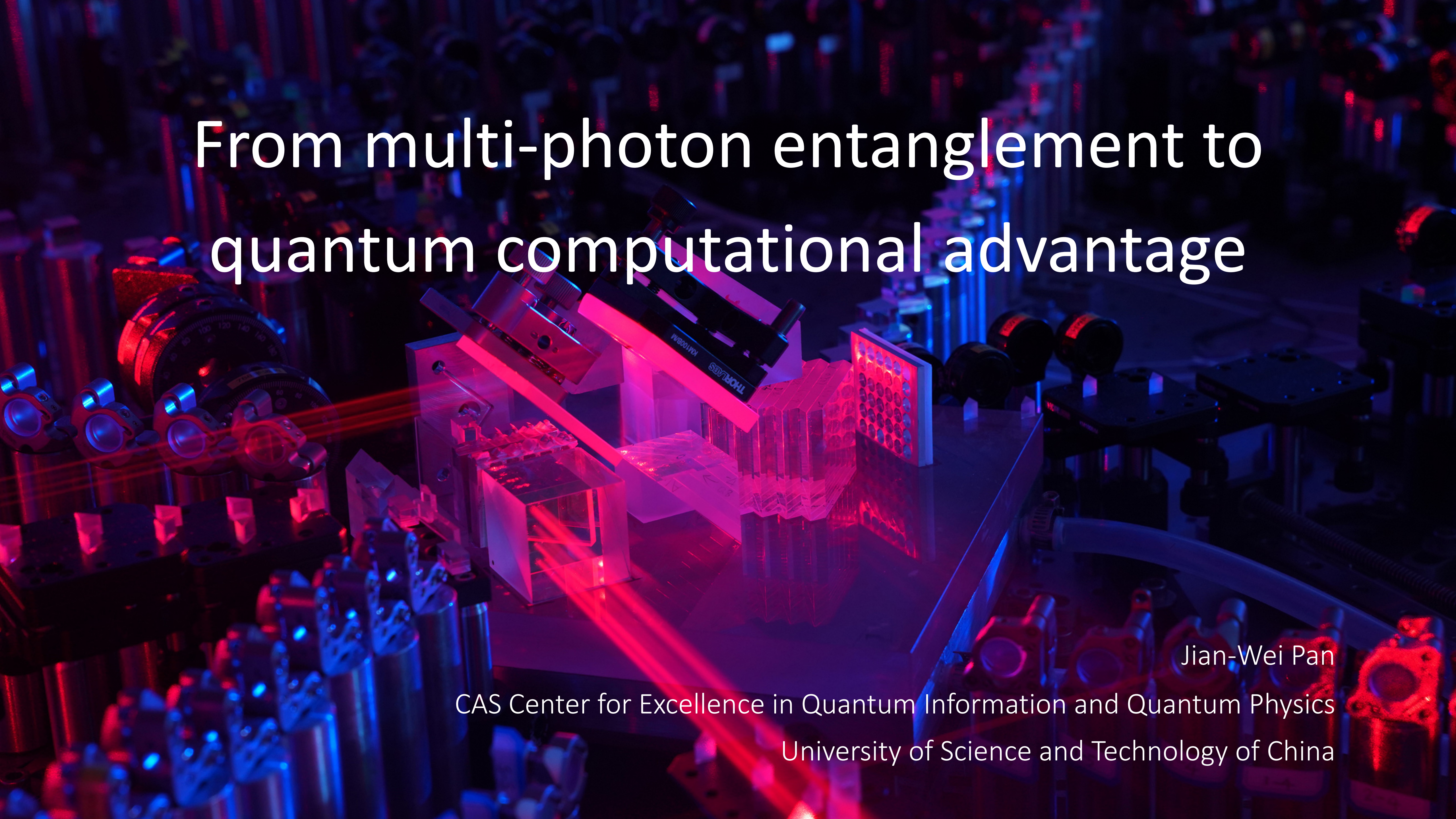
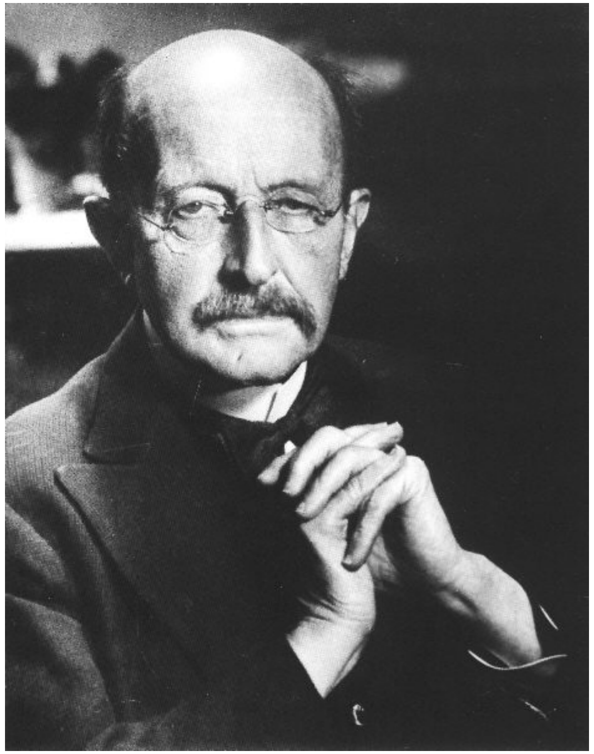


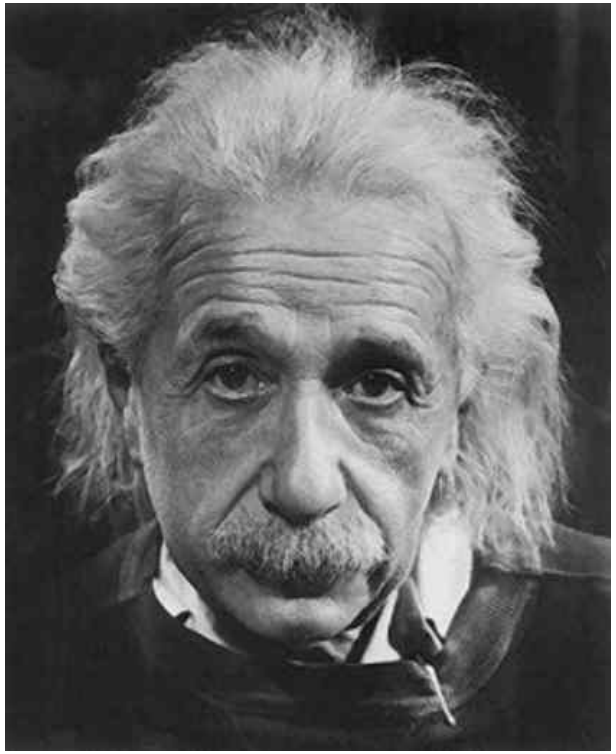
From multi-photon entanglement to quantum computational advantage

Jian-Wei Pan
CAS Center for Excellence in Quantum Information and Quantum Physics
University of Science and Technology of China

Two pillars of modern physics

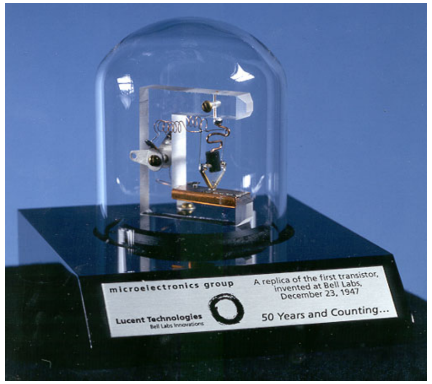


Quantum mechanics

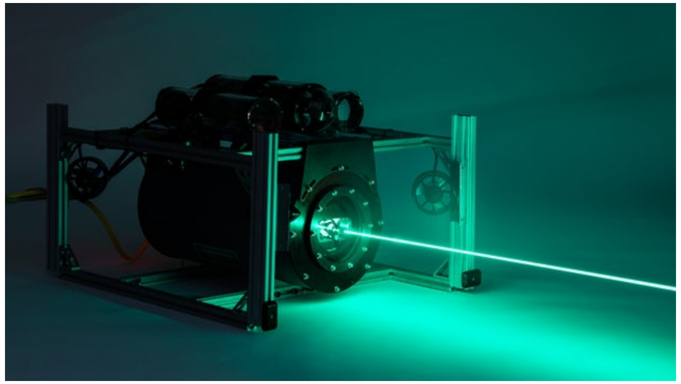


Theory of relativity

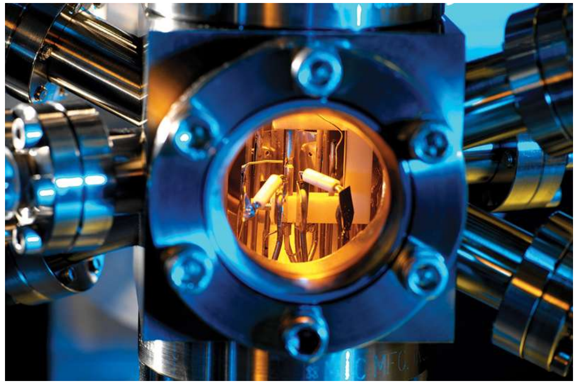
Quantum mechanics and information technologies



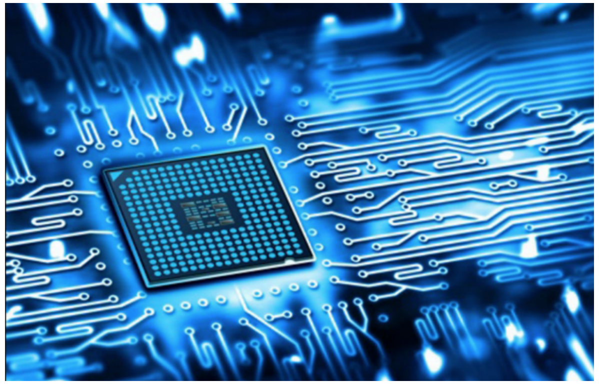
Transistors



Lasers

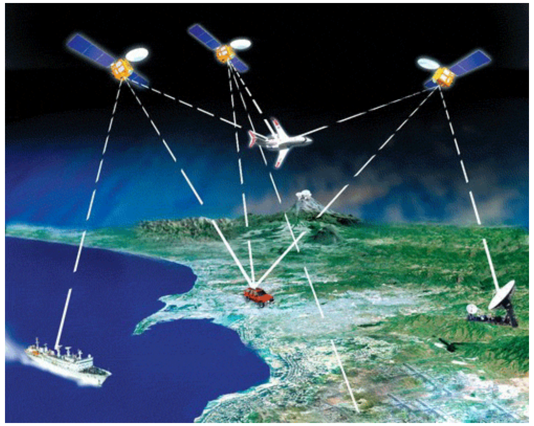


Atomic clocks



Electronic computer

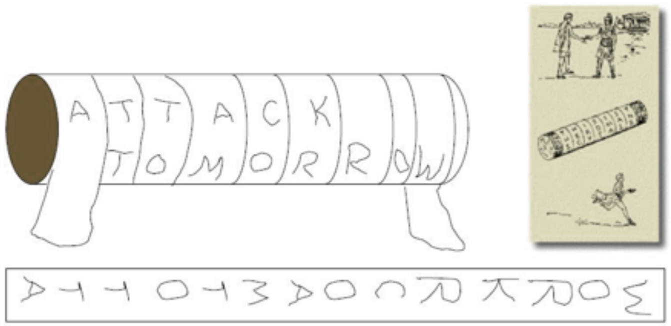
Optical communication and internet



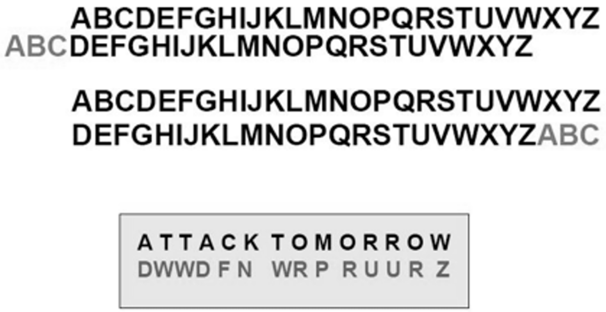
GPS

Challenges: information security

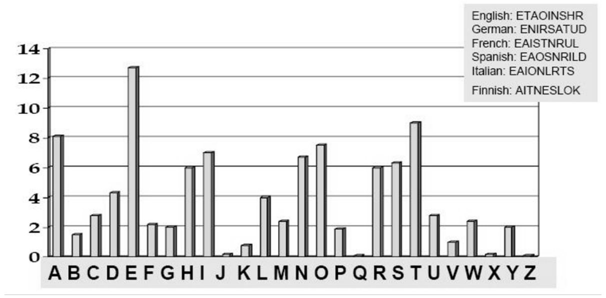
History: every advance in classical cryptography has been defeated by advances in cracking!



Ancient Greek scytale, 700 BC



Caesar cipher, 50 BC



Cracked via variations in the frequency of the occurrence of letters, by Al-Kindi (800-873)

Enigma machine broken by Alan Turing

RSA 512: cracked in 1999

RSA 768: cracked in 2009

RSA 1024: ?

SHA-1: cracked in 2017 by Google

……

Challenges: information security

All the classical encryption methods that depend on computational complexity, can be cracked in principle!

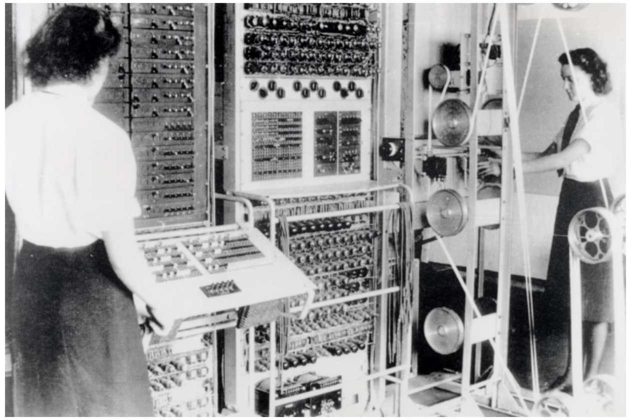
"......human ingenuity cannot concoct a cipher which human ingenuity cannot resolve"

—*A few words on secret writing*, Edgar Alan Poe (1841)

Challenges: computational capacity

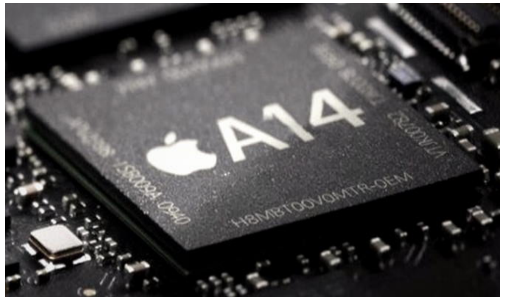
In 1943: "I think there is a world market for maybe five computers"

--Thomas Watson, Chairman of IBM

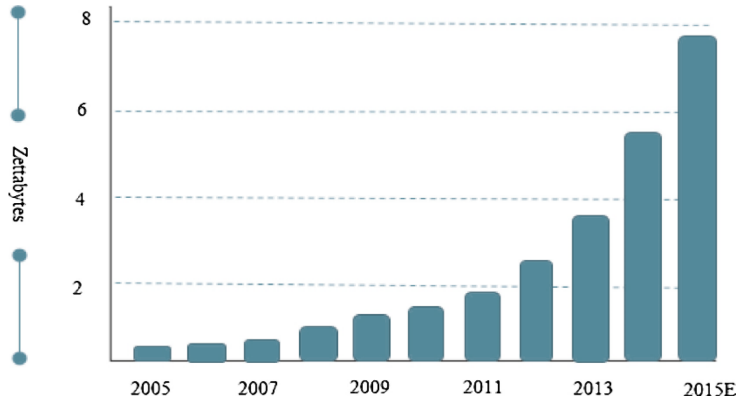


Colossus, weight: 1 ton, power: 8.5kw, 5 kOPS (operations per second)

In 2010's: Almost everyone owns computing power larger than the total computing power used in Apollo Program!



Apple A14, power: <5W, 11 trillion OPS



The world's data volume roughly grow 40% per year

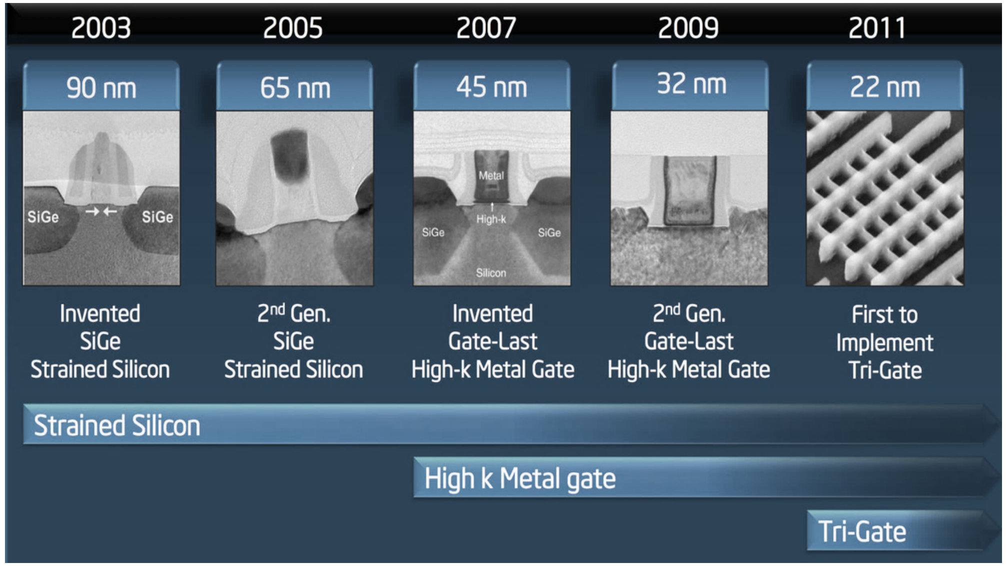
Challenges: computational capacity

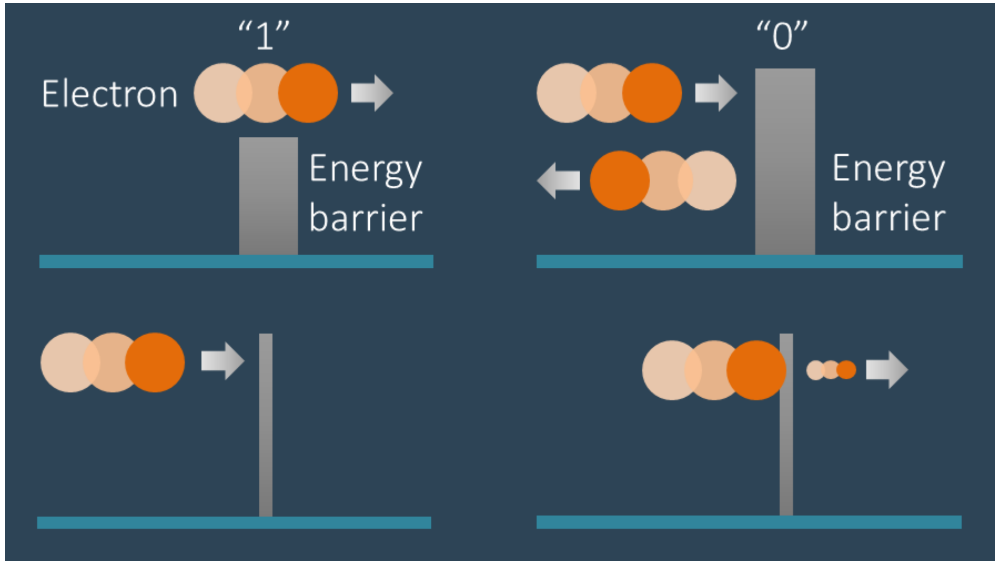
Classical computational bottleneck

The world's total computing power is insufficient to search a target in 2^{90} database within a year

A technological limit

The Moore's law that predicts the transistor density doubles every 18 months has come to an end



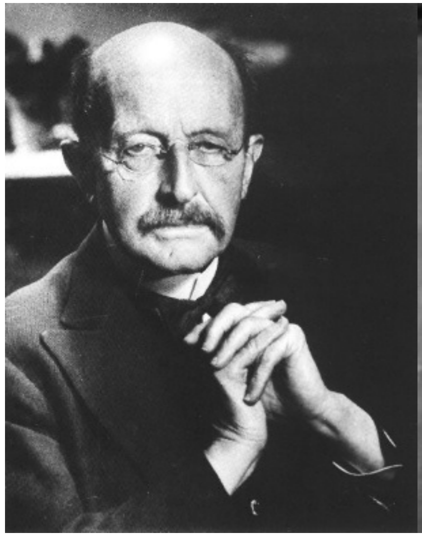


2017, 14 nm ➡ 2022, 4 nm ➡ 0.2 nm (atomic scale) ➡ ???

Tunneling induced leakage ➡

The "0/1" logic in the transistors will fail

Quantum physics, after one century's development, comes to the rescue for the problems confronted in the classical information technologies

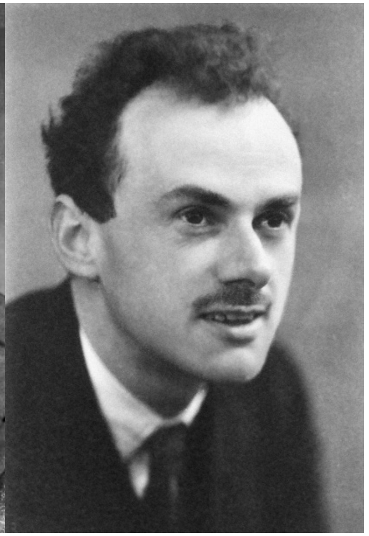

Max Planck


Albert Einstein


Niels Bohr


Erwin Schrödinger


Werner Heisenberg


Paul Dirac

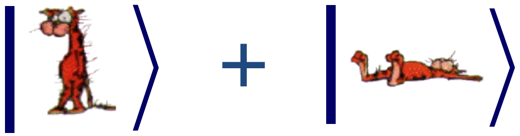
Quantum superposition and qubit

Classical Physics: “bit”

or

0 or 1

Quantum Physics: “qubit”

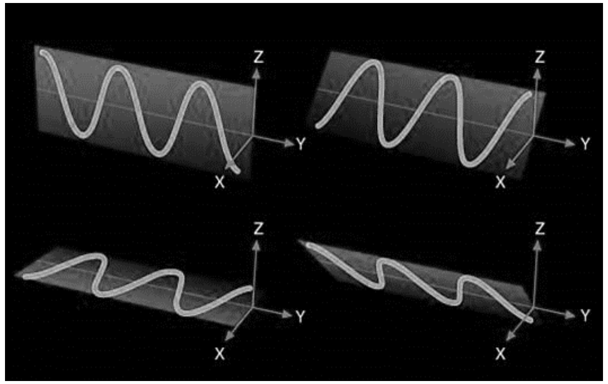


$|0\rangle + |1\rangle$

A qubit encoded in the polarization of a photon

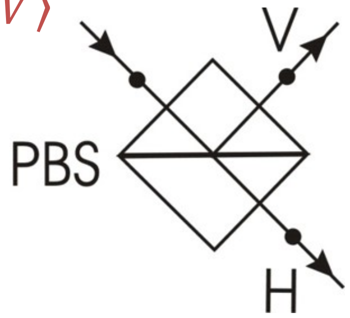
$|H\rangle = |0\rangle$

$|V\rangle = |1\rangle$



$|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$

$|\alpha|^2 + |\beta|^2 = 1$



$P = |\beta|^2$

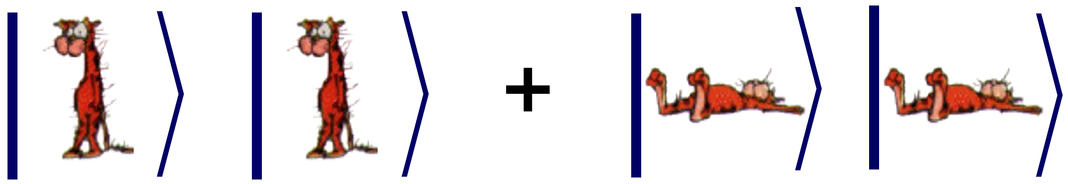
$P = |\alpha|^2$

Non-cloning theorem:

An unknown quantum state can not be copied precisely!

Quantum entanglement

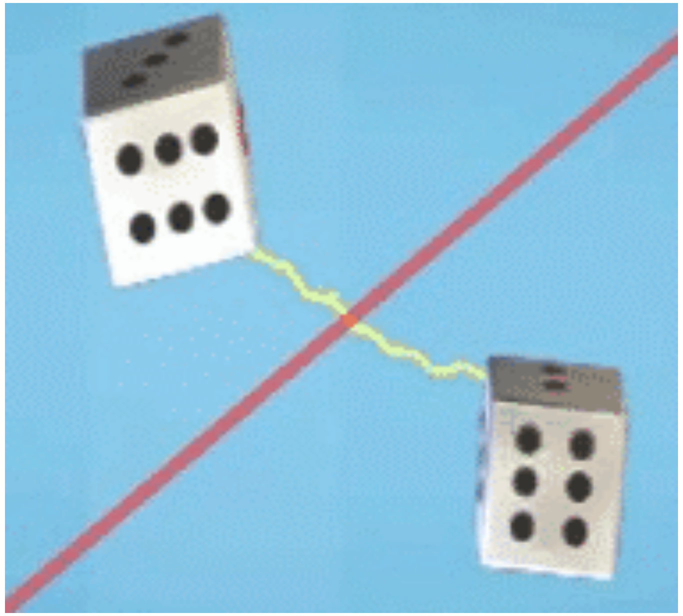
Quantum entanglement:



Bell states – maximally entangled states:

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2)$$

$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2)$$



Spooky action at a distance

—Albert Einstein

Quantum information processing (QIP)

Test of “spooky action at a distance”

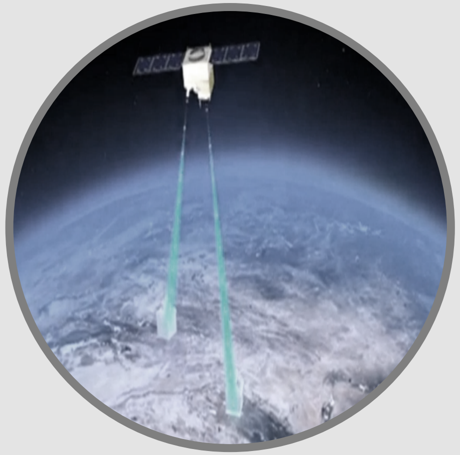
↓

Coherent manipulation of quantum systems

↓

Quantum information processing

Unconditional security



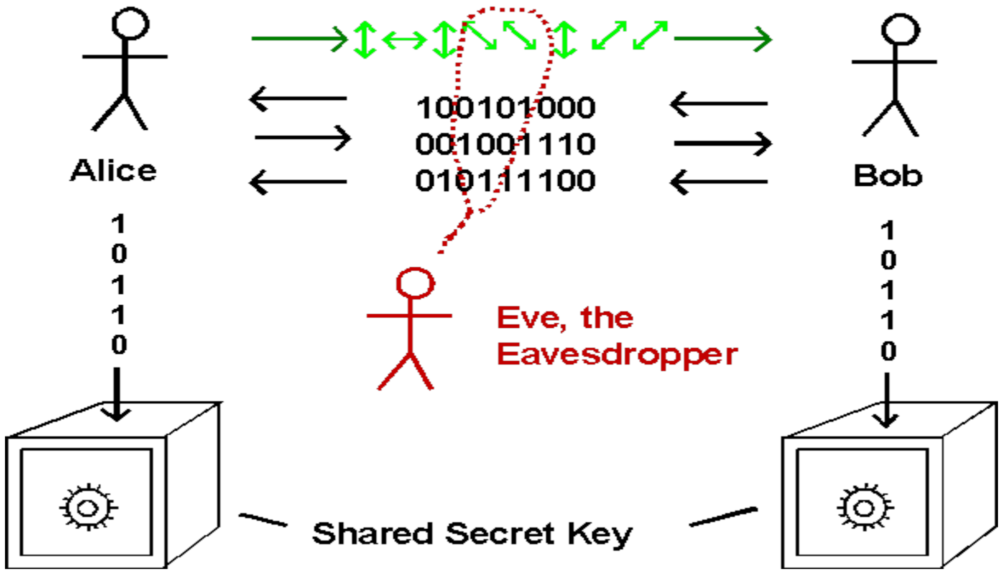
Quantum communication

Computational capacities

Quantum computation and simulation

Quantum key distribution (QKD)

- Single-photon-based key distribution: [Bennett & Brassard 1984 protocol]



Unconditional secure in principle

Any eavesdropping will be detected

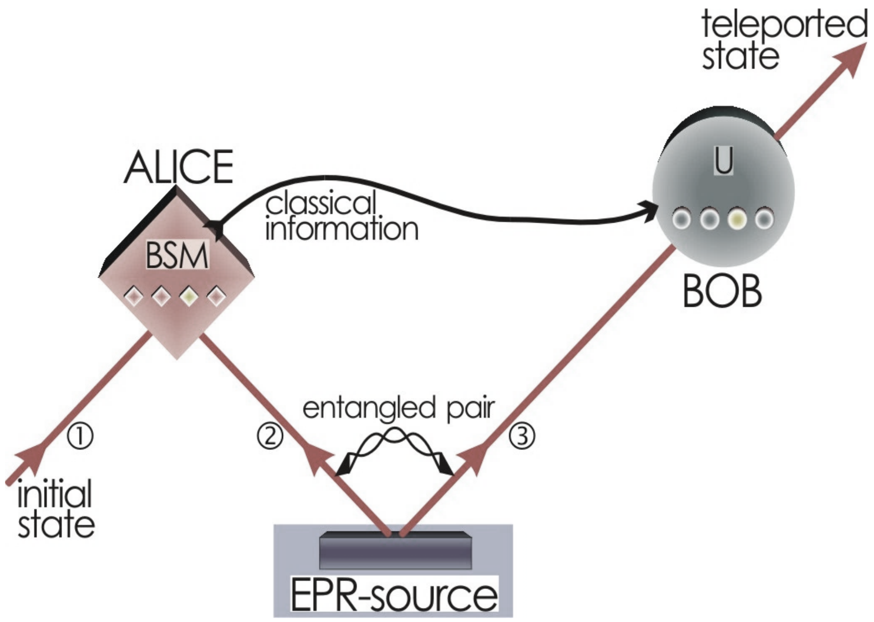
➡ Secure key!

One-time pad encryption

➡ Unhackable!

- Entanglement-based key distribution: [Ekert, PRL 67, 661 (1991)]

Quantum teleportation



Bennett *et al.*, PRL 70, 1895 (1993)

Initial state

$$|\Phi\rangle_1 = \alpha|H\rangle_1 + \beta|V\rangle_1$$

The shared entangled pair

$$|\Phi^+\rangle_{23} = \frac{1}{\sqrt{2}}\left(|H\rangle_2|H\rangle_3 + |V\rangle_2|V\rangle_3\right)$$

$$\begin{aligned}|\Psi\rangle_{123} &= |\Phi\rangle_1 \otimes |\Phi^+\rangle_{23} \\ &= |\Phi^+\rangle_{12} \otimes \left(\alpha|H\rangle_3 + \beta|V\rangle_3\right) + \\ &\quad |\Phi^-\rangle_{12} \otimes \left(\alpha|H\rangle_3 - \beta|V\rangle_3\right) + \\ &\quad |\Psi^+\rangle_{12} \otimes \left(\alpha|V\rangle_3 + \beta|H\rangle_3\right) + \\ &\quad |\Psi^-\rangle_{12} \otimes \left(\alpha|V\rangle_3 - \beta|H\rangle_3\right)\end{aligned}$$

Essential ingredient for quantum computation and distributed quantum network!

Quantum computation

Quantum Parallelism

Bits		Qubits
0 or 1	V. S.	0 + 1
00， 01， 10 or 11		00 + 01 + 10 + 11
000， 001， 010……		000 + 001 + 010 + ……

Evaluating a function f(x) for many different values of x simultaneously

$$U\frac{1}{\sqrt{2^N}}\sum_{i=0}^{2^N-1}|i\rangle|0\rangle = \frac{1}{\sqrt{2^N}}\sum_{i=0}^{2^N-1}|i\rangle|f(i)\rangle$$

→ Exponentially speedup!

Quantum computation

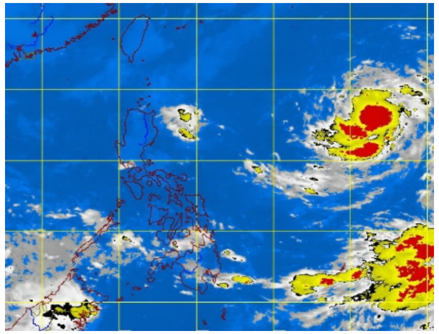
Shor Algorithm (1994):

E.g. factor a 300-digit number with

- Classical THz computer: 150,000 years
- Quantum THz computer: 1 second!

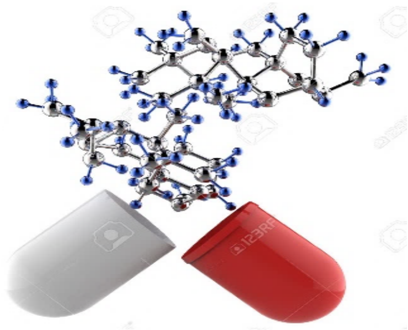
- Code-breaking can be done in minutes, not in millennia
- Public key encryption, based on factoring, will be vulnerable!

Code-breaking



Weather forecast

Financial analysis



Drug design

Quantum simulation

A quantum system of *N* two-level particles

☒ Described by a 2^N (exponentially large) Hilbert space

☒ Hardly accessible for classical computers to simulate its evolution

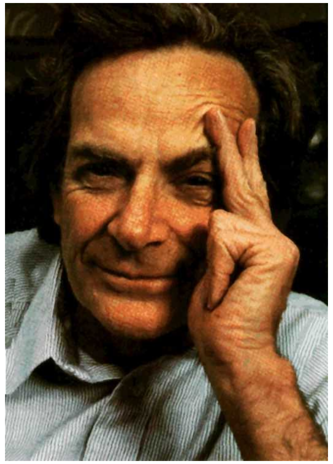
Natural solution: a quantum simulator

Consisting of superposition quantum states engineered to simulate the evolution of a quantum system

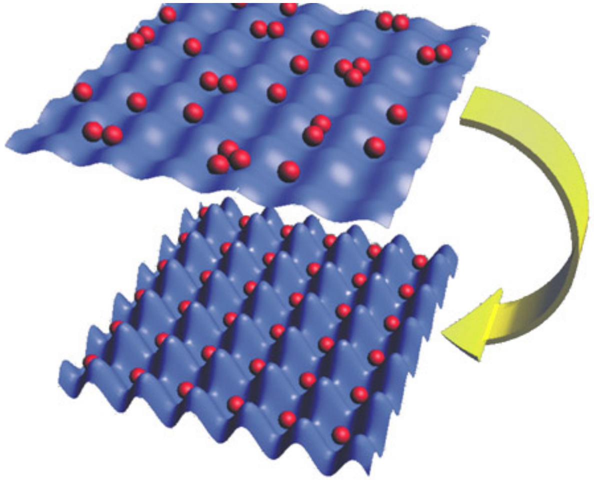
Mimicking condensed matter physics via cold atoms

- High-temperature superconducting
- (fractional) Quantum Hall effect

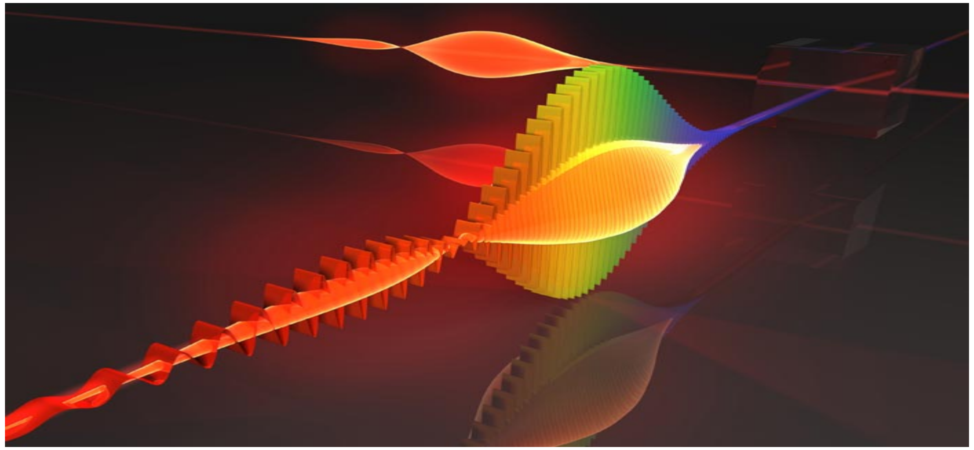
……

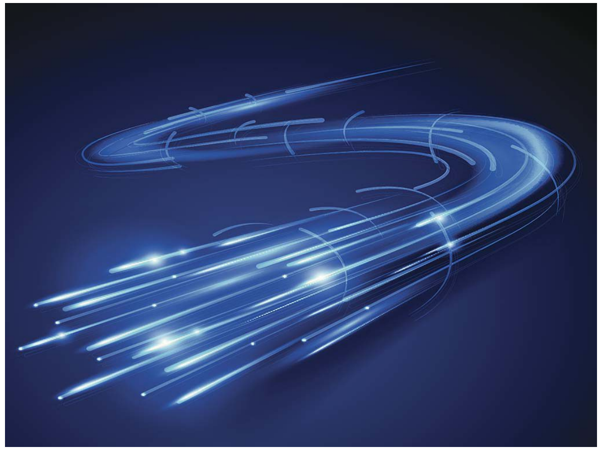


Richard Feynman



Optical quantum information processing





Why do we like photons?

☑ Flying qubit (fastest quantum information transmitter)

☑ Robust qubit (with weak interaction with environment)

☑ High-precision manipulation with off-the-shell devices

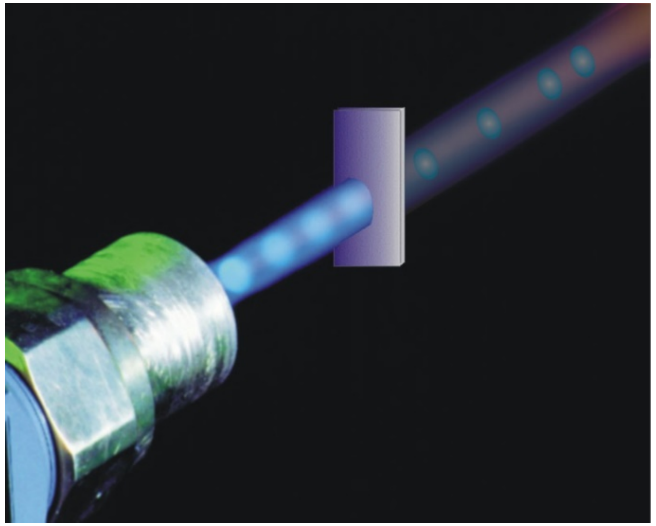
☑ Interconnections between distant physical systems

Elements of optical quantum information processing

Generation of single photons

- Practical singe-photon source is far out of reach within current technologies
- Probabilistic quasi single photon: weak coherence pulse

$$|\psi\rangle \sim \sum_{n=0}^{\infty} \frac{p^n}{\sqrt{n!}} |n\rangle \xrightarrow{p \ll 1} |0\rangle + p|1\rangle$$

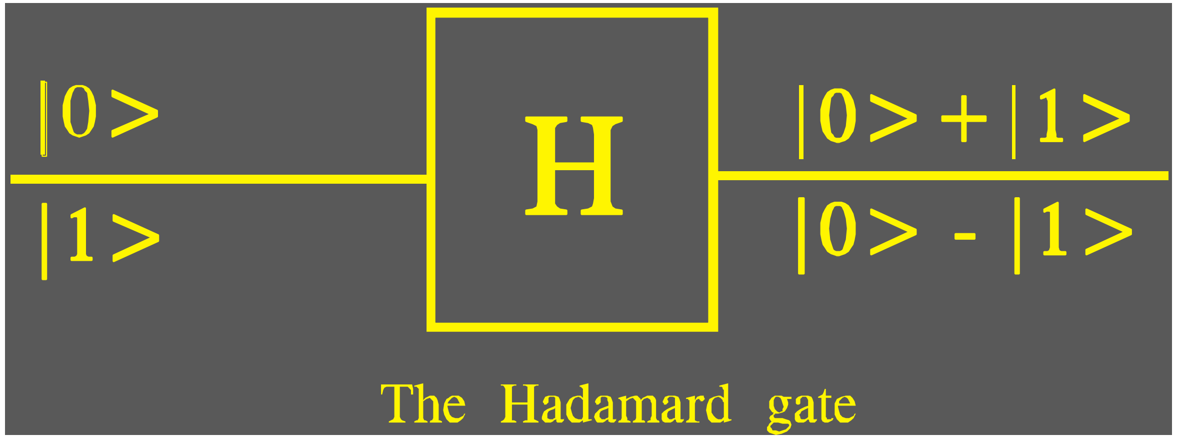


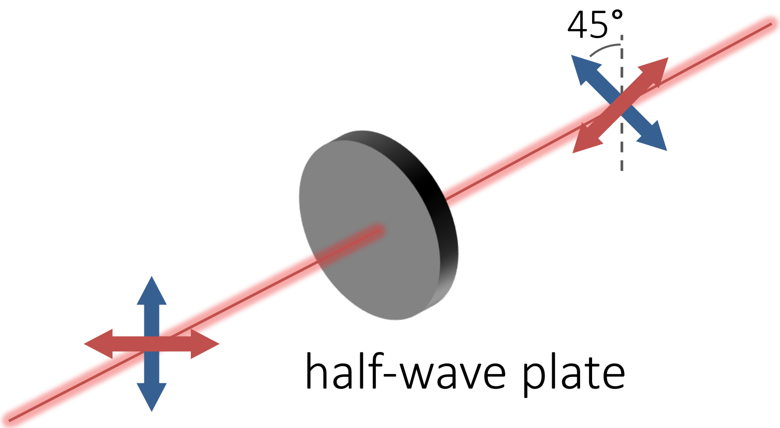
Single photon detector

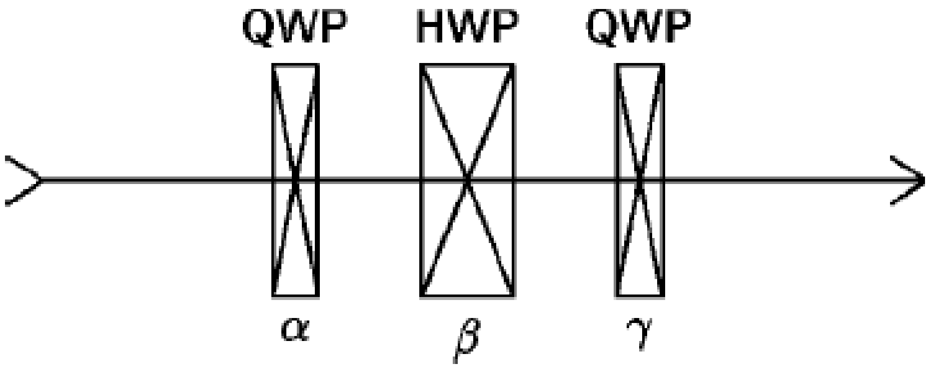
- InGaAs Avalanche photo diode
- Si detector
- Superconducting nanowire detector……

Elements of optical quantum information processing

Single-photon unitary operation





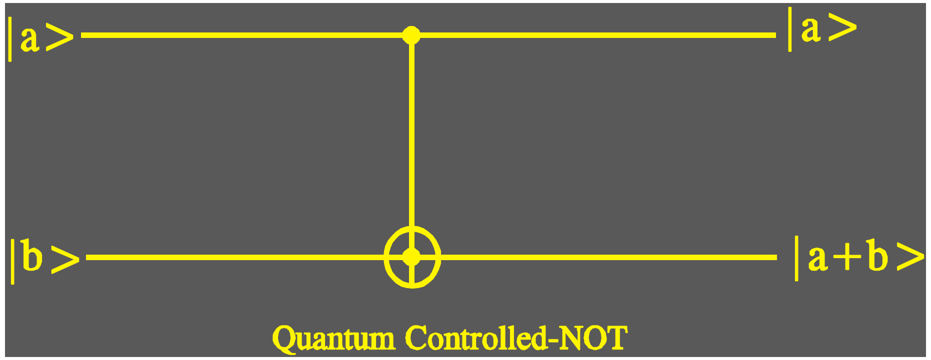


Arbitrary single-qubit unitary operation can be realized undergoing two types of wave plates

- QWP: quarter-wave plate
- HWP: half-wave plate

Elements of optical quantum information processing

Photon-photon logical gate

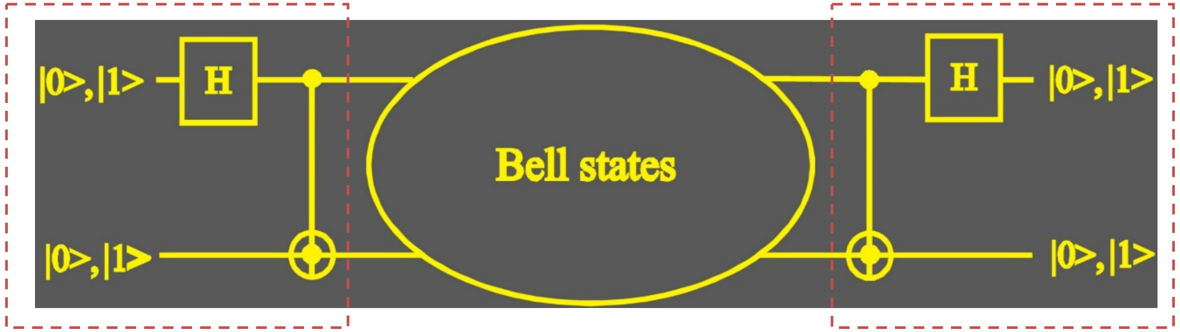


$|00\rangle \rightarrow |00\rangle$ $|10\rangle \rightarrow |11\rangle$

$|01\rangle \rightarrow |01\rangle$ $|11\rangle \rightarrow |10\rangle$

Manipulation of entanglement

Bell states measurement



$|00\rangle \rightarrow |0+1\rangle|0\rangle = |00\rangle + |10\rangle \rightarrow |00\rangle + |11\rangle$

$\rightarrow |00\rangle + |10\rangle = |0+1\rangle|0\rangle \rightarrow |00\rangle$

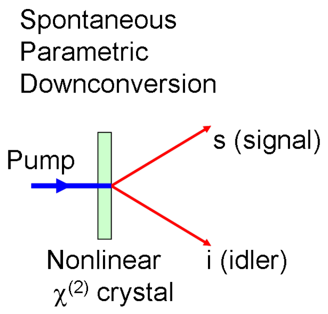
Generating Bell states

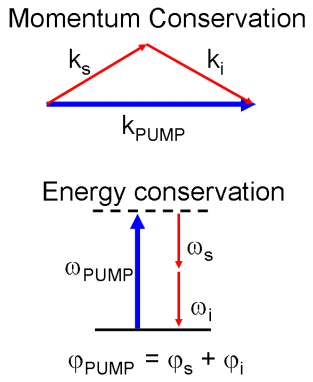
For photons, CNOT gate requires strong non-linear coupling

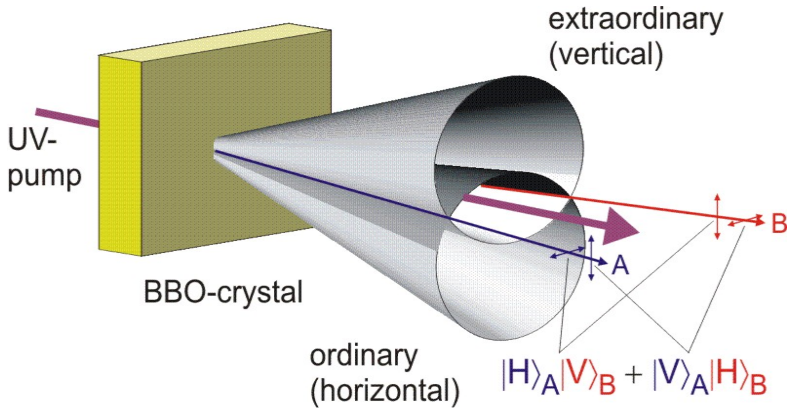
☒ But the coupling between photons is negligibly weak!

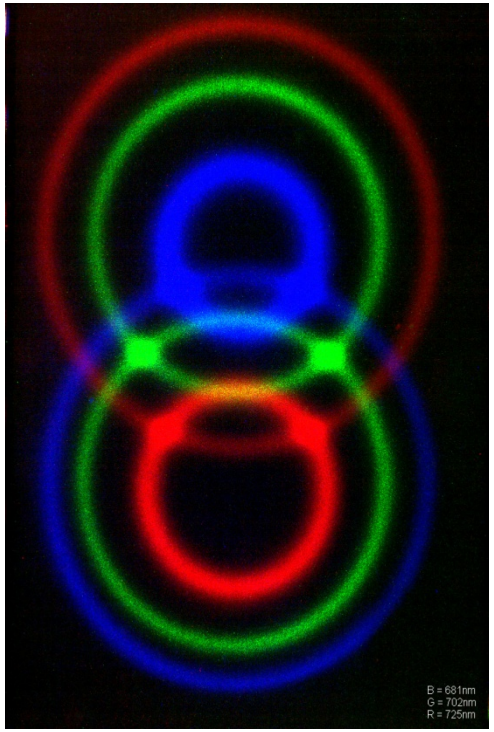
Probabilistic generation of photonic entanglement:

Spontaneous parametric down-conversion (SPDC)









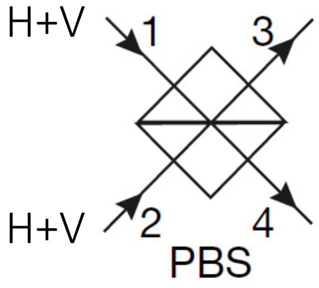
Squeezed vacuum state: $\sum_{k=0}^{\infty} g(k)e^{ik\phi}|k\rangle_1|k\rangle_2$

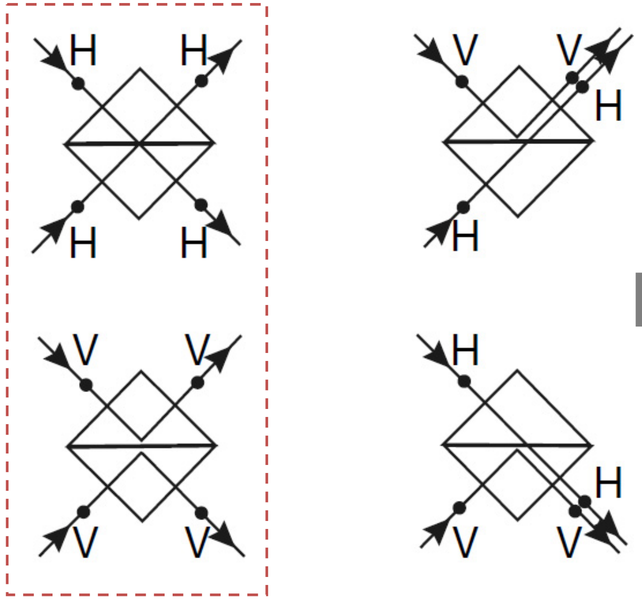
Kwiat *et al.*, PRL 75, 4337 (1995)

Post-selection induced non-linearity

To achieve non-linearity required by CNOT operation:

1. Making independent photons identical in all degrees of freedom ➡ they are indistinguishable even in principle
2. Post-selection





The polarization states of two photons cannot be distinguished: Entangled output state HH+VV

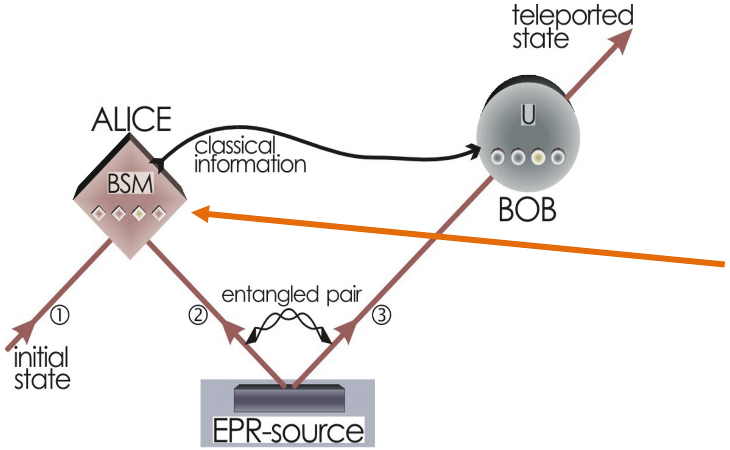
Input two-photon state: (H+V)(H+V)

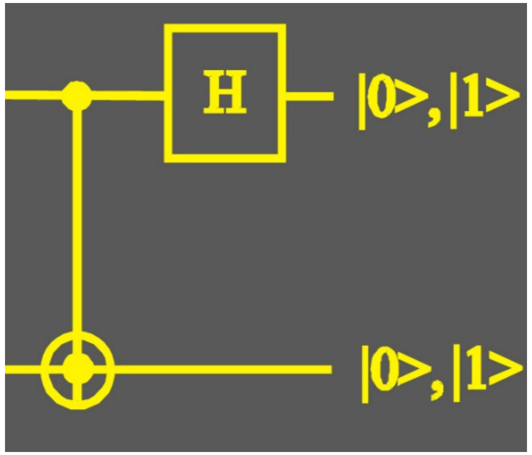
Post-selecting one and only one photon in each of the two output event

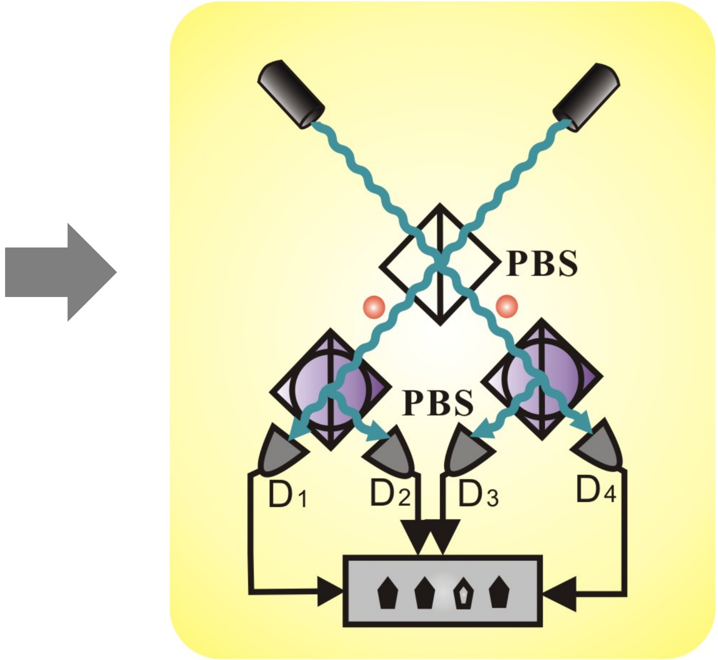
Post-selection induced non-linearity

With the help of linear optics, the required non-linearity of CNOT gate can be effectively induced by post-selection

Bell-state measurement (BSM) required by quantum teleportation can be implemented with linear optics [Pan and Zeilinger, PRA 57, 2208 (1998)]

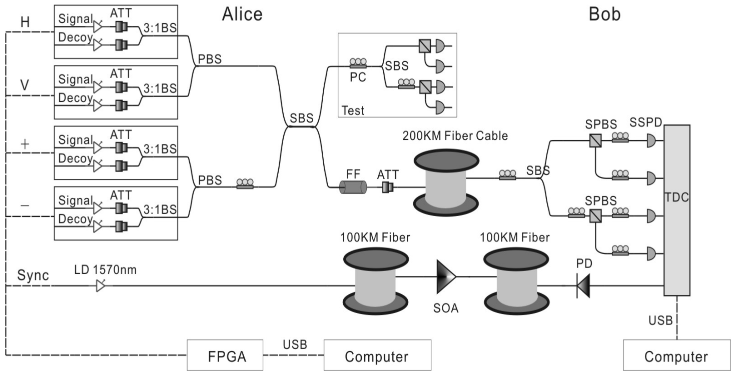


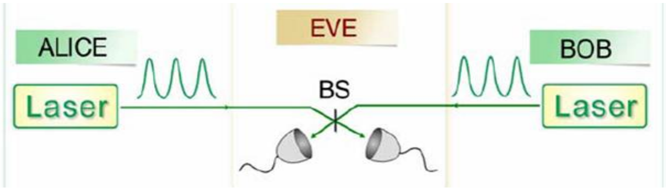


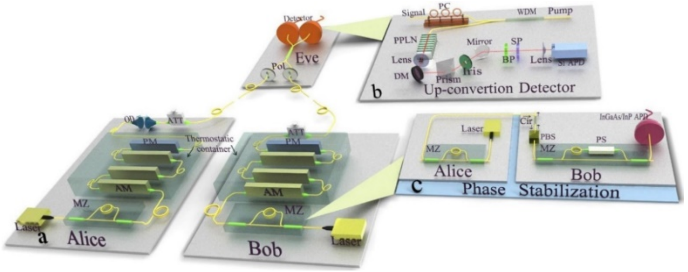


Secure QKD with realistic devices

QKD is the first practical QIP technology since only manipulation of single photon is needed







- **Decoy-state QKD: secure QKD with non-ideal single-photon sources**

  The distance of secure QKD exceeds 100km

  - Rosenberg *et al.*, PRL 98, 010503 (2007)
  - Peng *et al.*, PRL 98, 010505 (2007)

- **Measurement device independent (MDI) QKD: immune to any attack on detection**

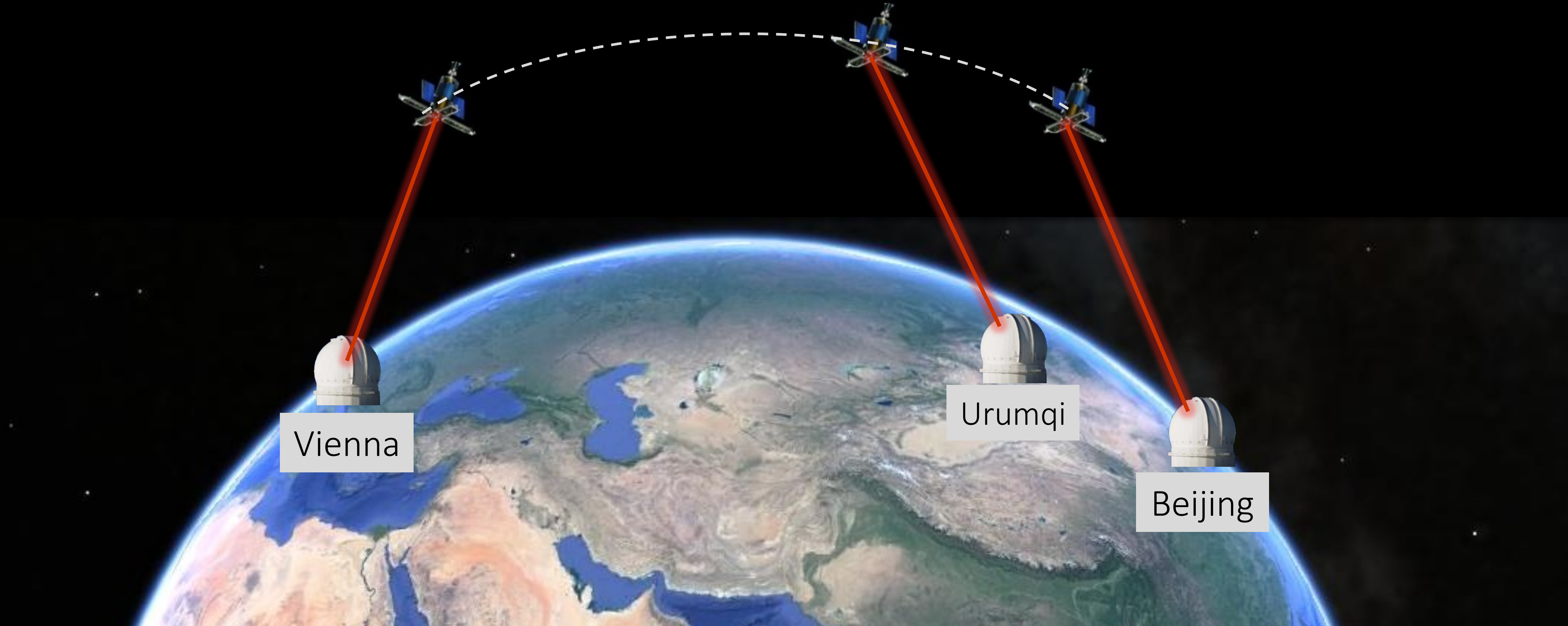
  - First experiment (50km):
    Liu *et al.*, PRL 111, 130502 (2013)
  - Extended distance (400km & 500km):
    Yin *et al.*, PRL 117, 190501 (2016)
    Fang *et al.*, Nat. Photon. 14, 422 (2020)

➡ Making applications of QKD via fiber in metropolitan area feasible!

Toward long-disitance quantum communication

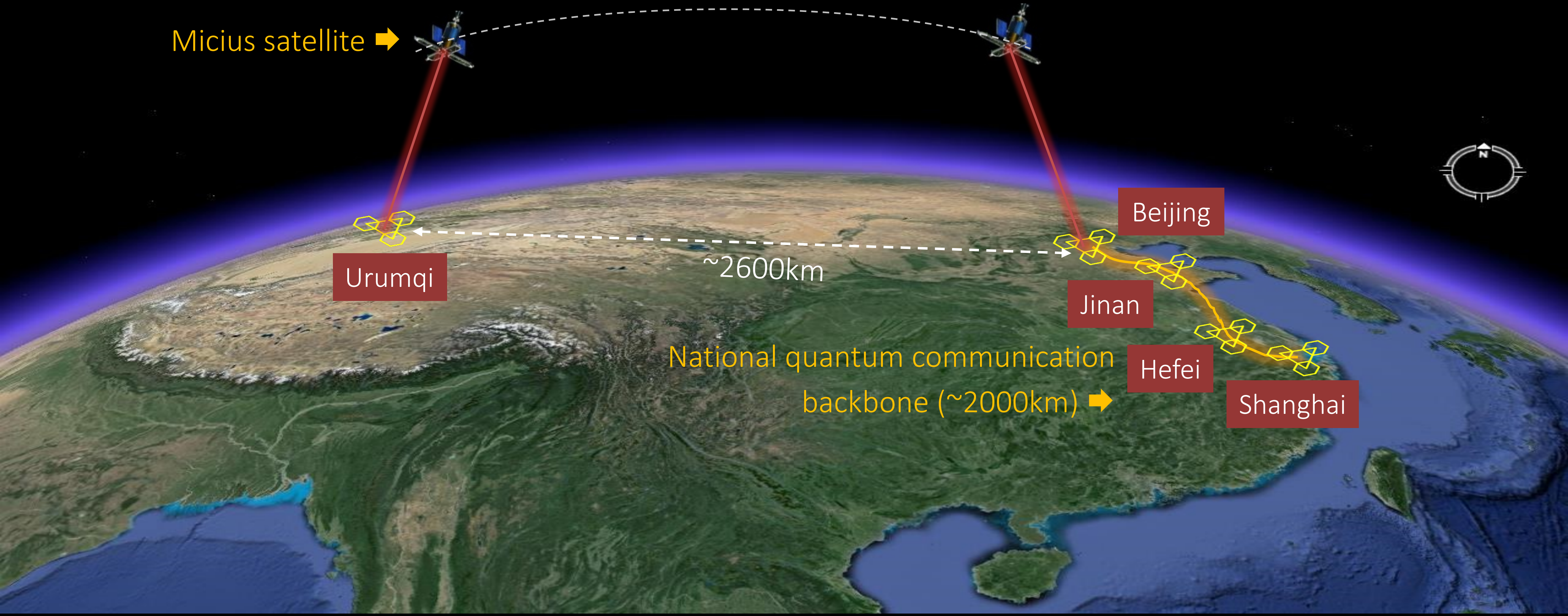
Quantum communication at a distance of 7600km was achieved with Micius satellite (launched in Aug, 2016)

- Liao *et al*., Nature 549, 43 (2017)
- Liao *et al*., PRL 120, 030501 (2018)



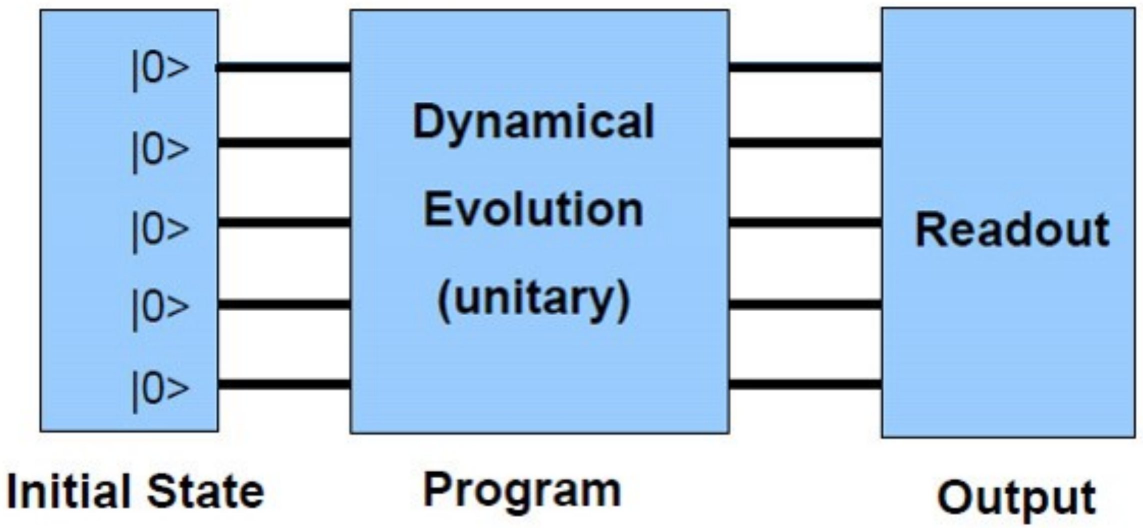
Large-scale quantum communication infrastructure

An integrated space-to-ground quantum communication network over 4,600 kilometres [Chen *et al.*, Nature 589, 214 (2021)]



Are photons sufficient for quantum computing?

Quantum computaiton:
quantum circuit model



Single-qubit unitary gates
+
Two-qubit controlled-NOT gates

→ Universal quantum computation
Lloyd, PRL 75, 346 (1995)

☒ With linear optics, nonlinearity required by CNOT gate can only be induced by post-selection

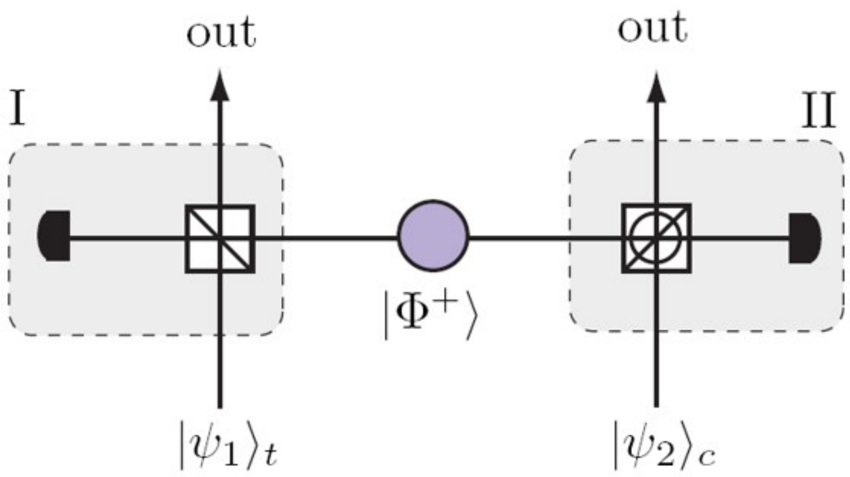
Is it sufficient for efficient quantum computation?

Efficient QIP with linear optics

Knill, Laflamme and Milburn (KLM), Nature 409, 46 (2001)

☑ Non-deterministic quantum logic operations can be performed using linear optical elements

☑ The success rate of the quantum logic can be arbitrarily close to one with the help of multi-photon state



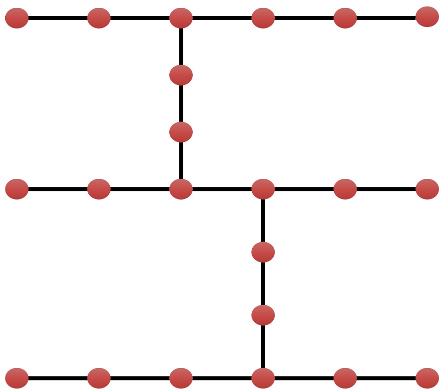
Probabilistic photonic CNOT gate

- O'Brien *et al*., Nature 426, 264 (2003)
- Gasparoni *et al*., PRL 93, 020504 (2004)
- Zhao *et al*., PRL 94, 030501 (2005)

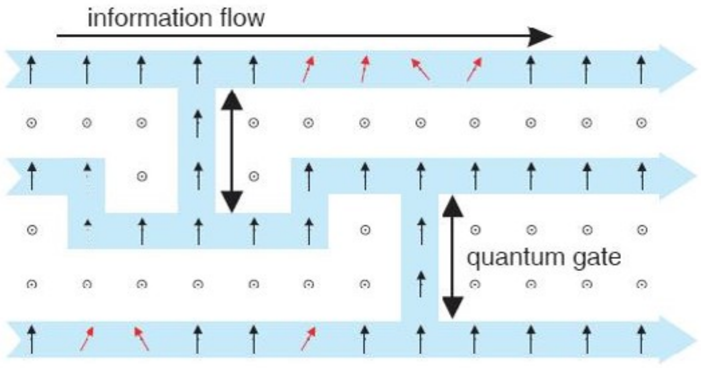
One-way quantum computation model

- Universal QC resource: multi-particle entanglement

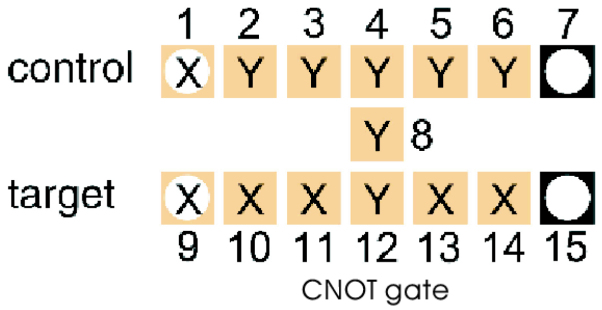
cluster state $|\Phi\rangle_C$:



$$\sigma_x^{(a)} \bigotimes_{a'\in ngbh(a)} \sigma_z^{(a')}|\Phi\rangle_C = \pm|\Phi\rangle_C$$



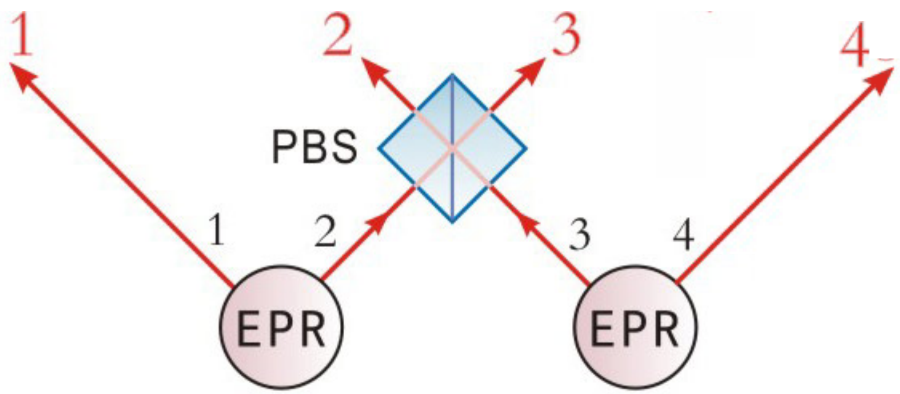
- Quantum gates are implemented by measuring particles in a certain order and in a certain basis

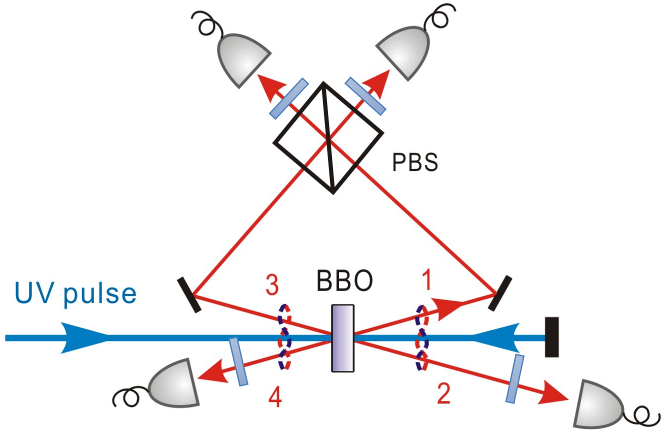


Raussendorf and Briegel, PRL 86, 5188 (2001)

Four-photon entanglement

In 2001, brightness of entanglement source: 2500pair/s@76MHZ ($P\sim3\times10^{-5}$)

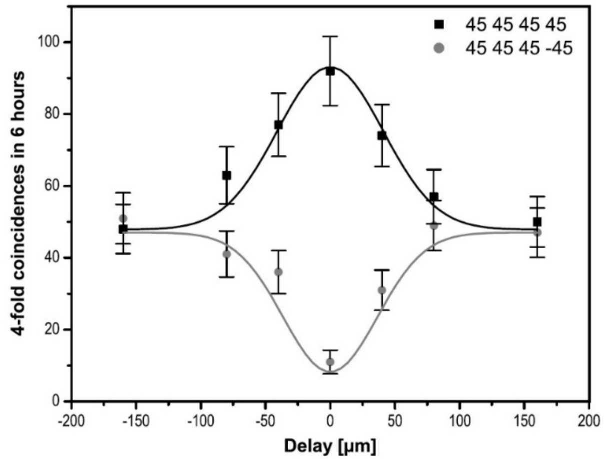




(HH+VV)(HH+VV)

= HHHH+HHVV+VVHH+VVVV

→ HHHH+VVVV

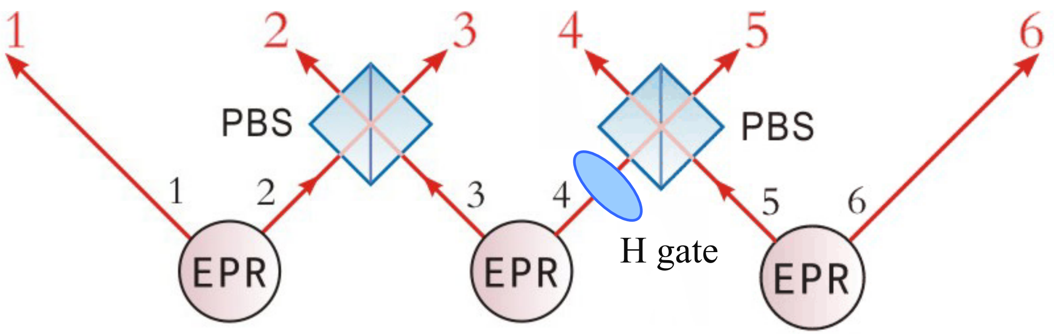


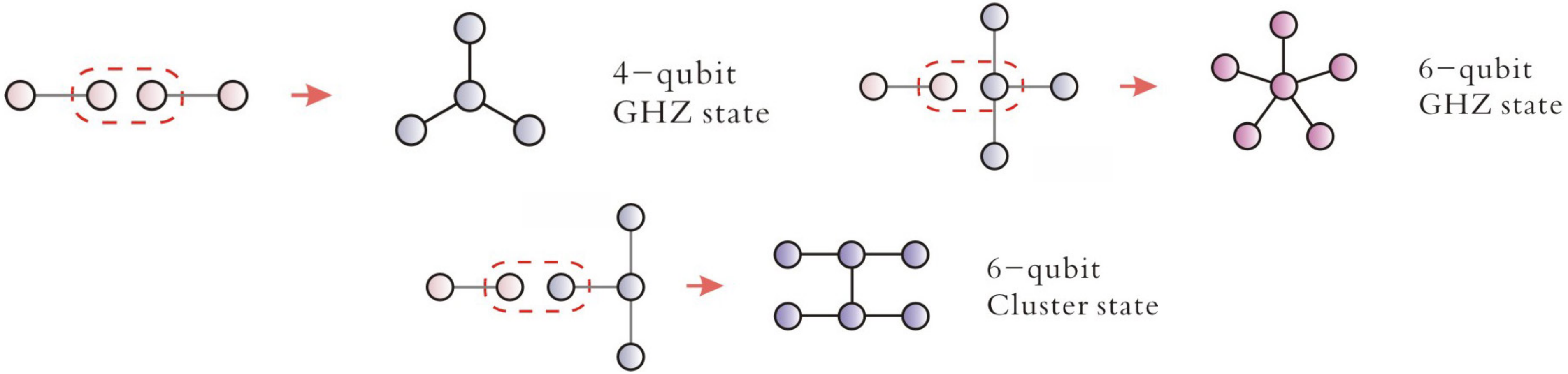
Pan *et al.*, PRL 86, 4435 (2001)

Six-photon cluster states

In 2007, by developing a brighter laser pump source, Verdi 10W → 16W, IR ~ 2.5W

brightness of entanglement source: 93000pair/s@76MHz(P~10^{-3})

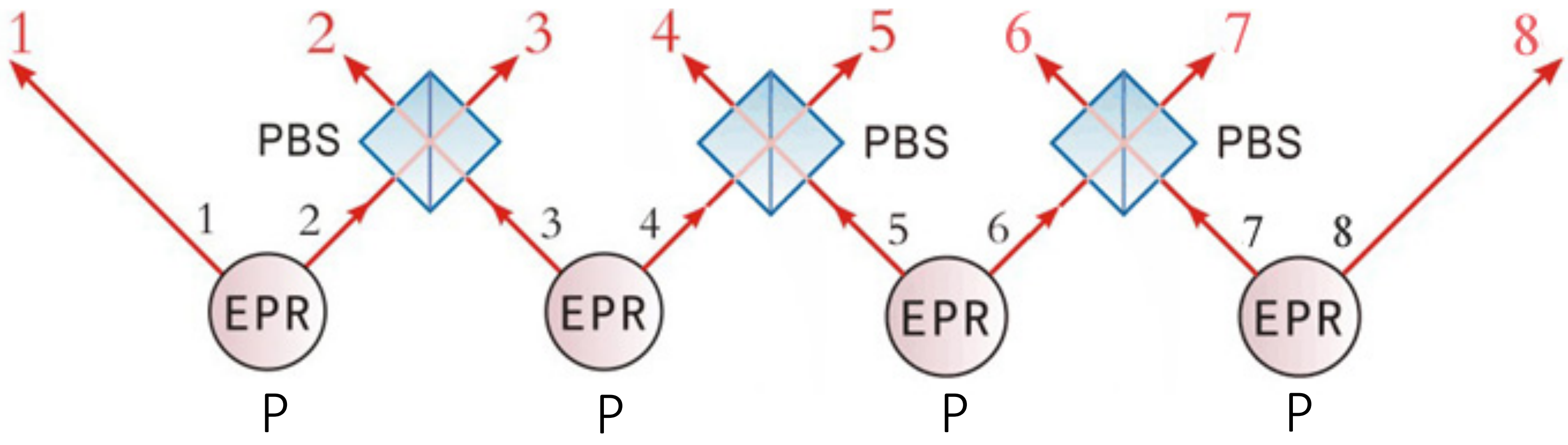




Lu *et al.*, Nature Physics 3, 91 (2007)

Multi-photon interferometry

Essential task: generation and manipulation of multi-photon entanglement



Two-photon entanglement source: P →Four-photon entanglement: $P^2/2$

→ Six-photon entanglement: $P^3/4$ → Eight-photon entanglement: $P^4/8$…

High-brightness entanglement source is needed!

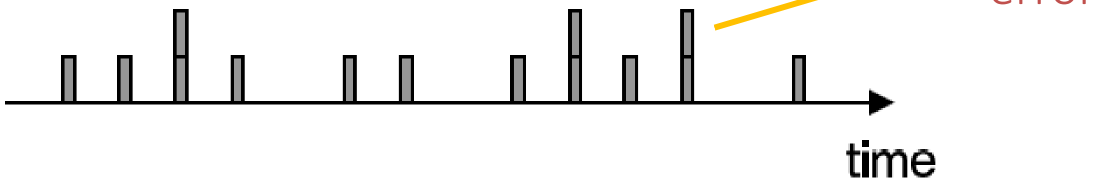
The request for both high brightness & fidelity

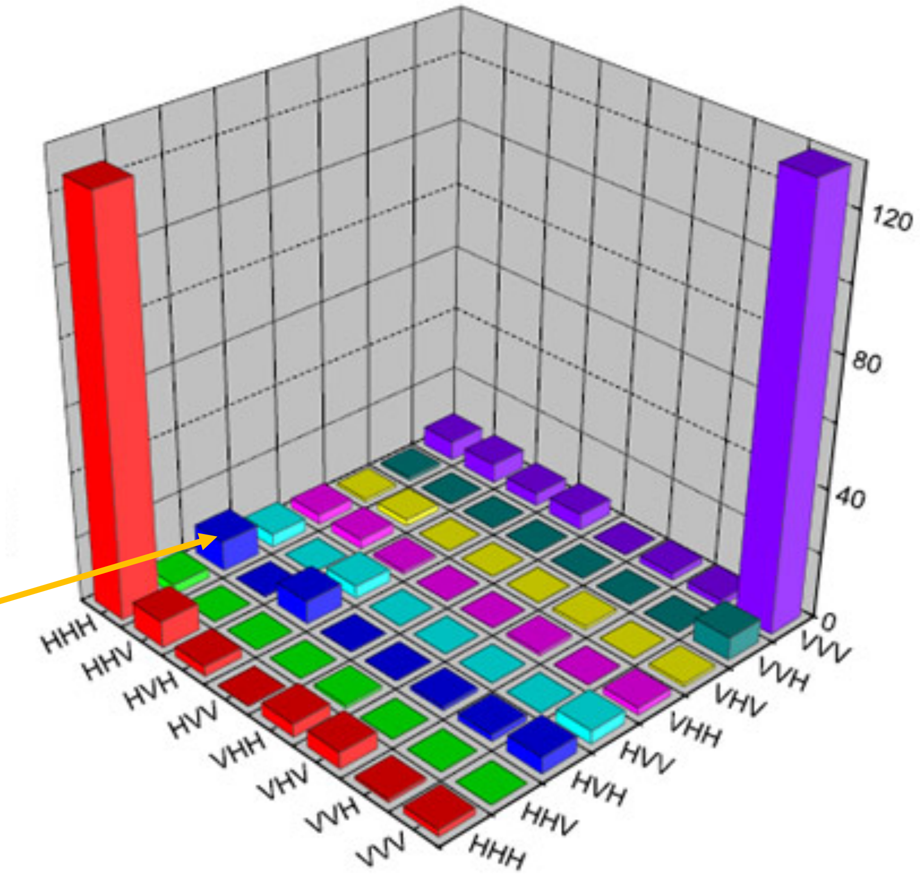
With higher pump

☑ Increase probability

☒ More double pair emissions ➡ degrades fidelity

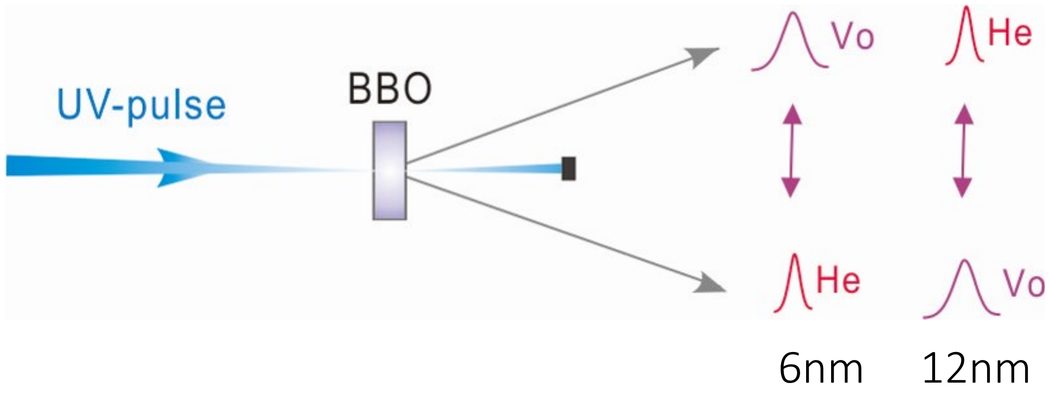
$$P_n = \frac{\mu^n e^{-\mu}}{n!}$$





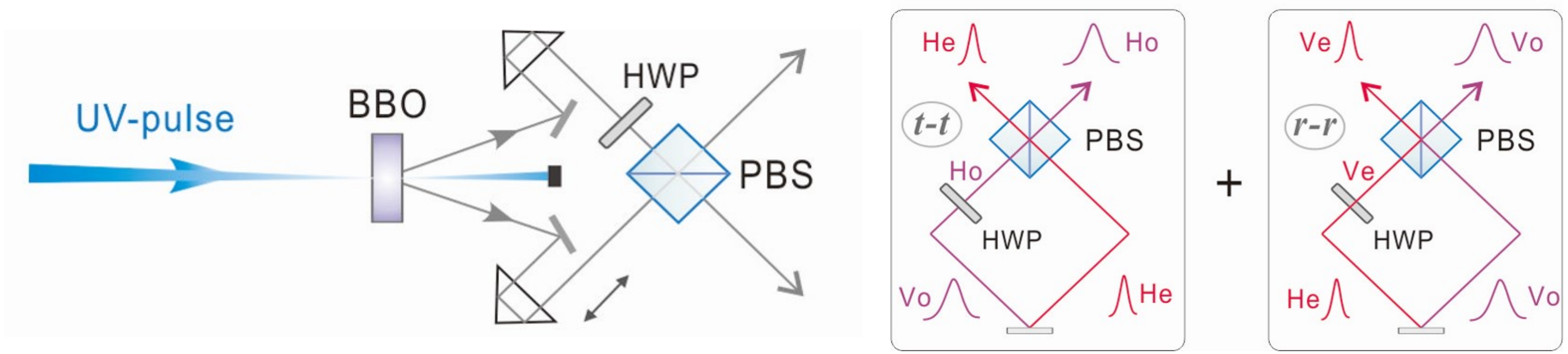
Can we further push the brightness of two-photon entanglement, meanwhile with high fidelity?

Disentangles the timing from the polarization



☒ Different spectral widths, decrease the indistinguishability thus the fidelity

☒ Narrow-band filters (~3nm), causes unnecessary waste of photons

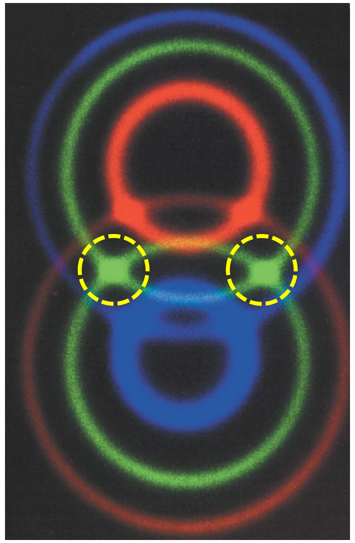


☑ Interferometric Bell-state synthesizer, disentangles the timing from the polarization

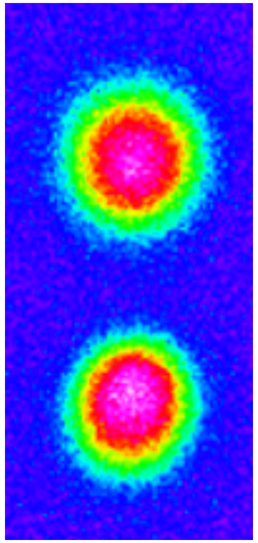
☑ ~1 million coincidence counts per second without filter, with ~90% fidelity ($P \sim 10^{-2}$)

➡ Eight-photon entanglement [Yao *et al.*, Nature Photonics 6, 225 (2012)]

SPDC: driven to perfection



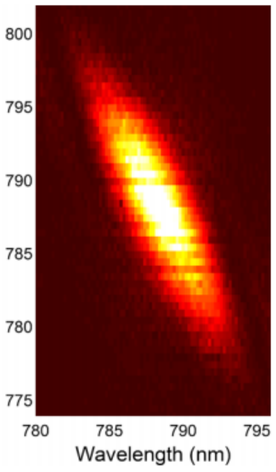
V. S.



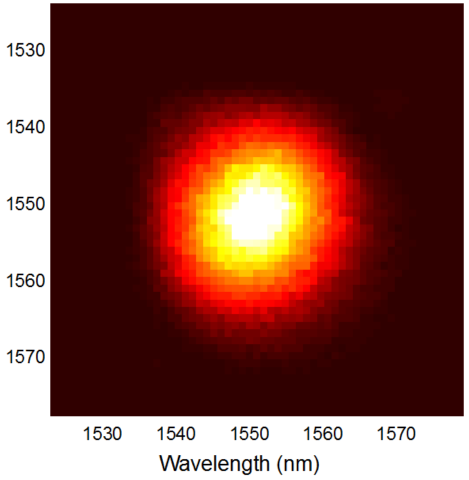
☑ Collect all photons from two separate circular beams ($P \sim 5 \times 10^{-2}$)

Ten-photon entanglement

[Wang et al., PRL 117, 210502 (2016)]



V. S.

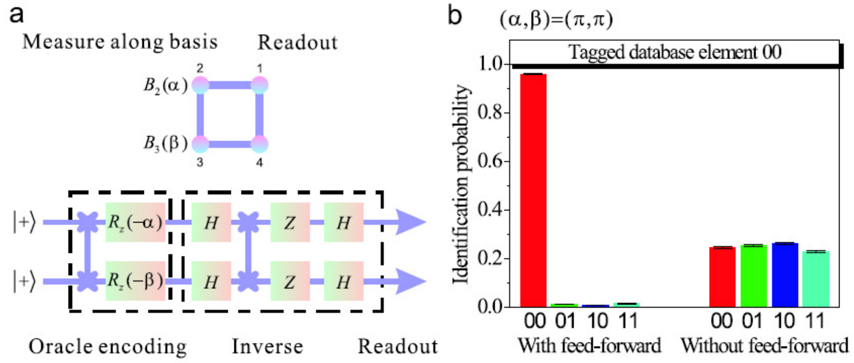


☑ Frequency uncorrelated, no narrowband filtering loss ($P \sim 7 \times 10^{-2}$)

12-photon entanglement

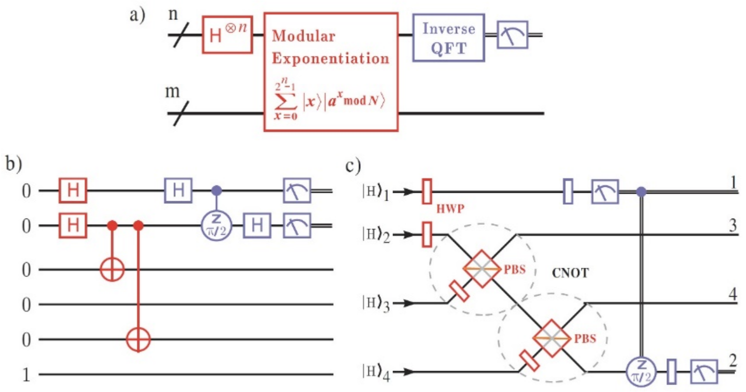
[Zhong *et al*., PRL 121, 250505 (2018)]

Demonstrations of quantum algorithms



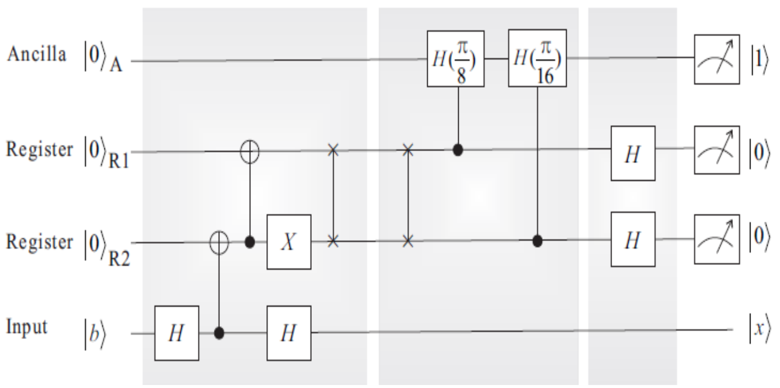
Gover's searching algorithm

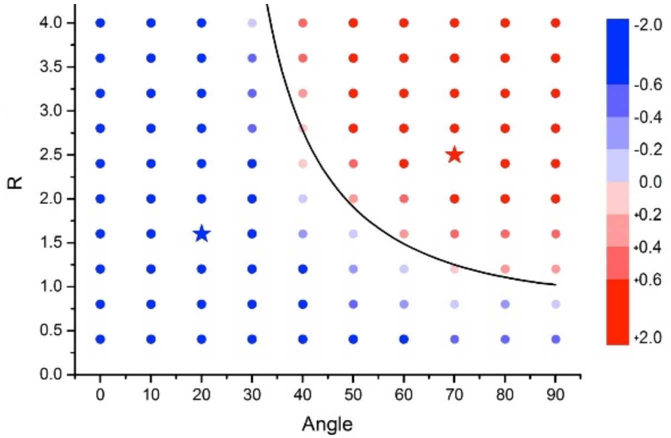
Chen *et al.*, PRL 99, 120503 (2007)



Shor's factoring algorithm (15 = ? X ?)

Lu *et al.*, PRL 99, 250504 (2007)





Solving linear systems of equations

Cai *et al.*, PRL 110, 230501 (2013)

- Classical: *O* (*N*) steps
- Quantum: *O* (log(*N*)) steps

Quantum machine learning

Cai *et al.*, PRL 114, 110504 (2015)

Quantum error correction

Inevitable noise ➡ qubit error during quantum computation

- Bit flip error: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$
- Phase flip error: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle - \beta|1\rangle$
- Mixed error: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle - \beta|0\rangle$

Error-correction code：

Similar to redundant coding in classical computing

$|0\rangle \rightarrow |000\rangle, |1\rangle \rightarrow |111\rangle$

Superposition: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$

Some quantum error-correction code schemes:

- Shor, PRA 52, R2493 (1995) 9 qubits
- Steane, PRL 77, 793 (1996) 7 qubits
- Laflamme *et al.*, PRL 77, 198 (1996) 5 qubits

Challenge: require error rate of single qubit $< 2\times10^{-5}$!

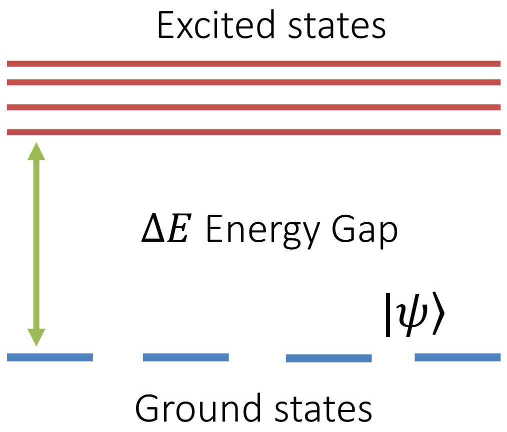
Topological quantum error correction

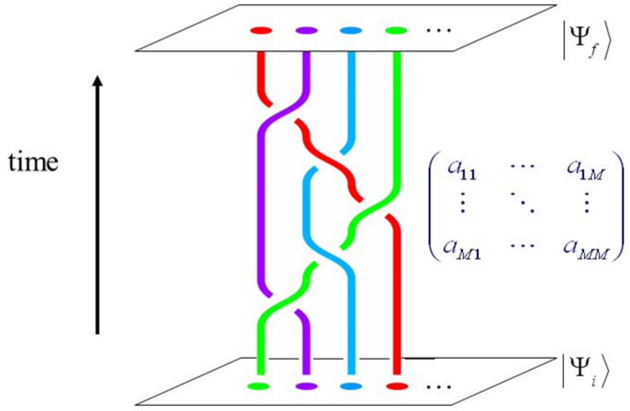
Protect quantum bits/gates at the physical level

- Kitaev, Ann. Phys. 303, 2 (2003); Ann. Phys. 321, 2 (2006)
- Raussendorf *et al*., Ann. Phys. 321, 2242 (2003)
- Nayak *et al*., RMP 80, 1083 (2008)

➡ Relax the error threshold rate from 10^{-5} to 10^{-2}

Protect qubits with energy gap



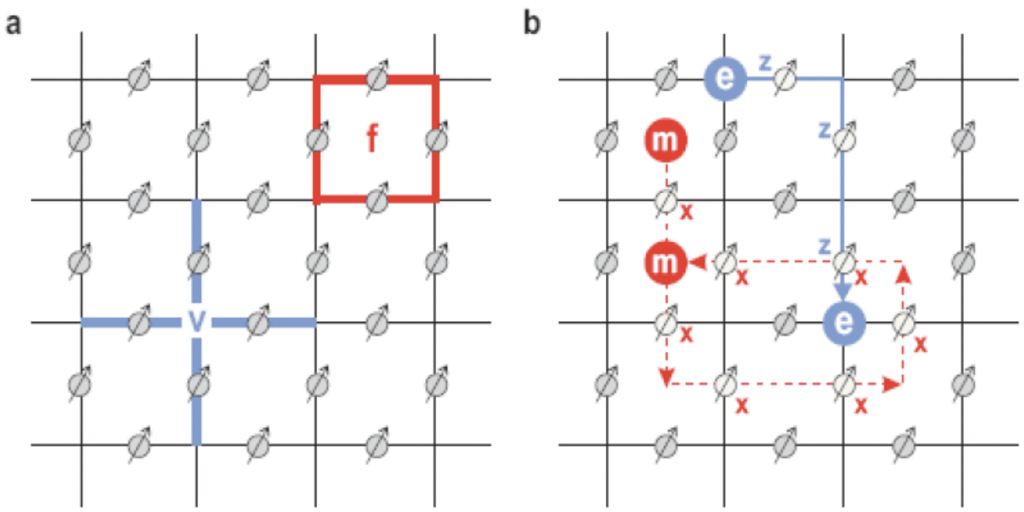


Quantum gates: Braiding Anyons

Topological quantum error correction

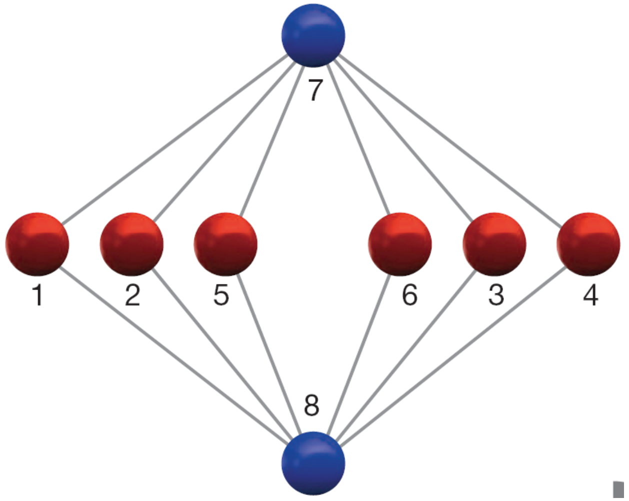
- Revealing fractional statistics of Anyons with 6-photon entanglement

  Lu *et al.*, PRL 102, 030502 (2009)

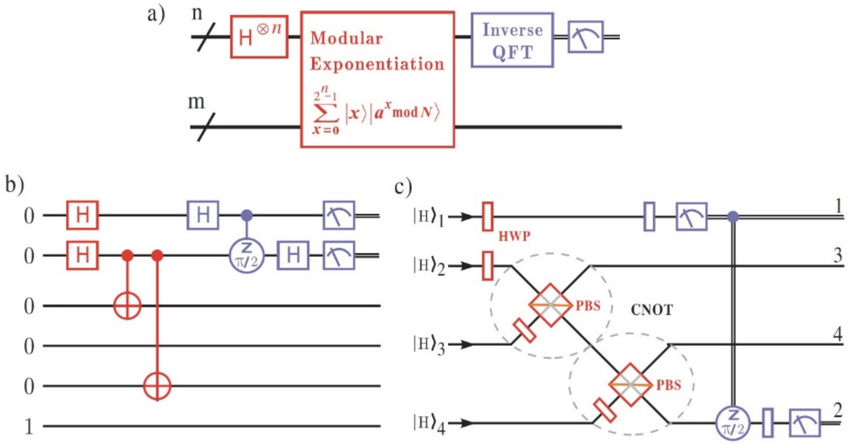


- Demonstration of simplest example of topological quantum error correction with 8-photon entanglement

  Yao *et al.*, Nature 482, 489 (2012)



- There are huge technical challenges in scalable quantum computing
- So far one has only verified the possibility of quantum computing……

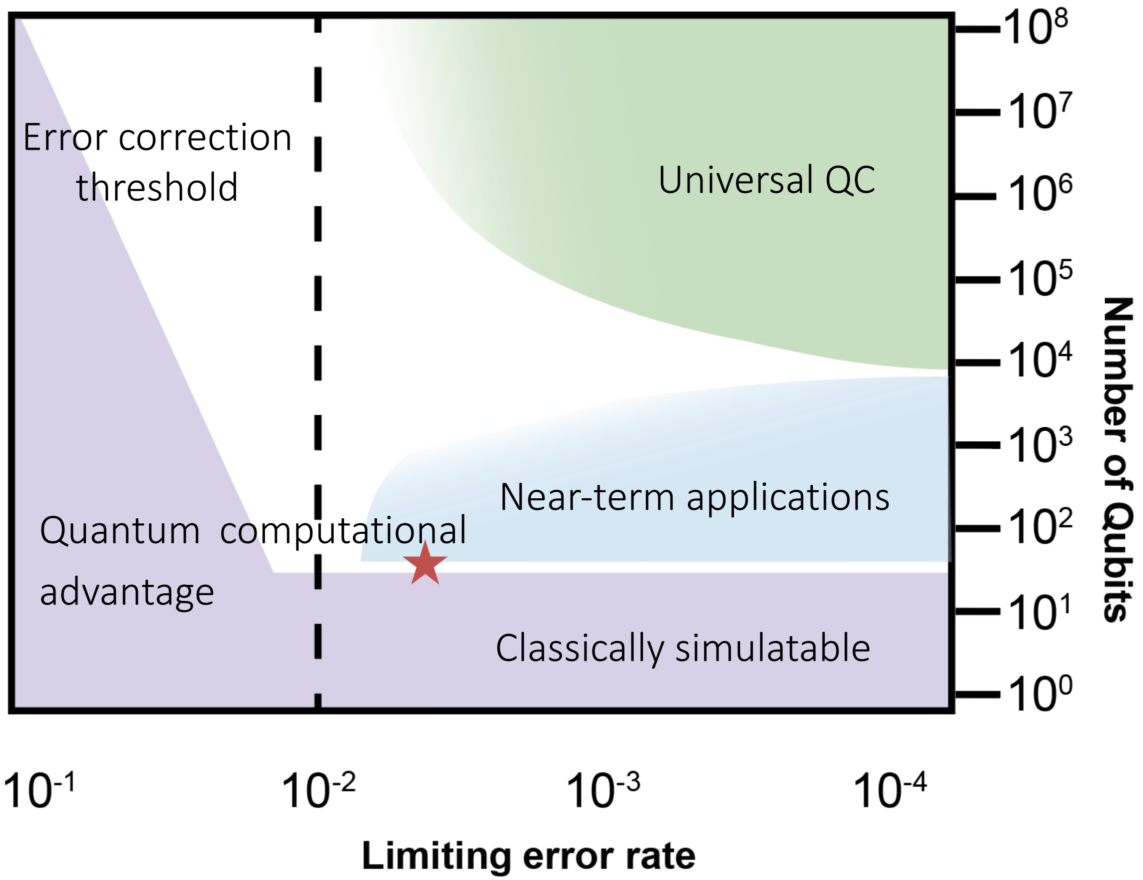


Shor’s factoring algorithm (15 = ? × ?)

How to show quantum computational advantage?

Roadmap of quantum computing

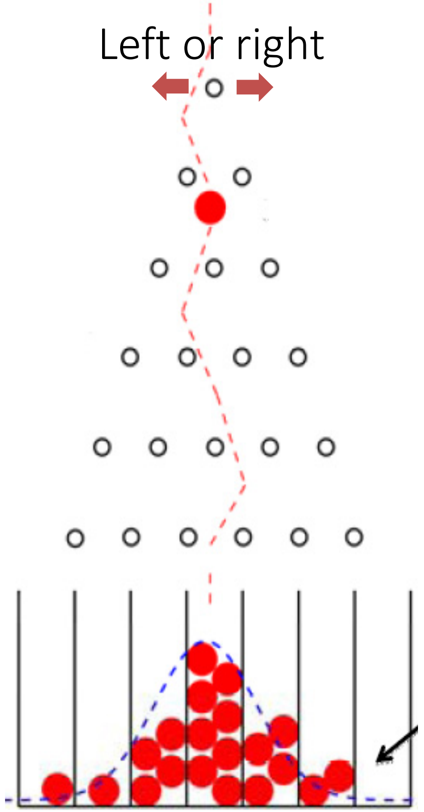
- Milestone 1: Beating classical supercomputer in specific tasks (quantum computational advantage)



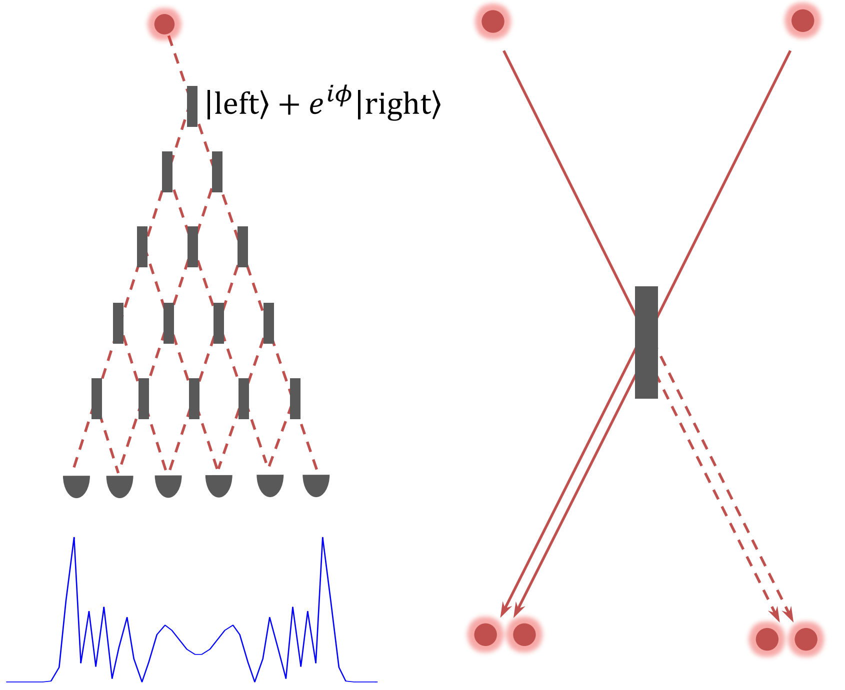
- Milestone 2: Quantum simulation to reveal the microscopic mechanism of condensed matter physics (e. g., high temperature superconductivity, etc.)
- Milestone 3: Universal and programmable quantum computers

Boson sampling

Boson sampling [Aaronson and Arkhipov, *Theory of Computing*. 9, 143 (2013)]

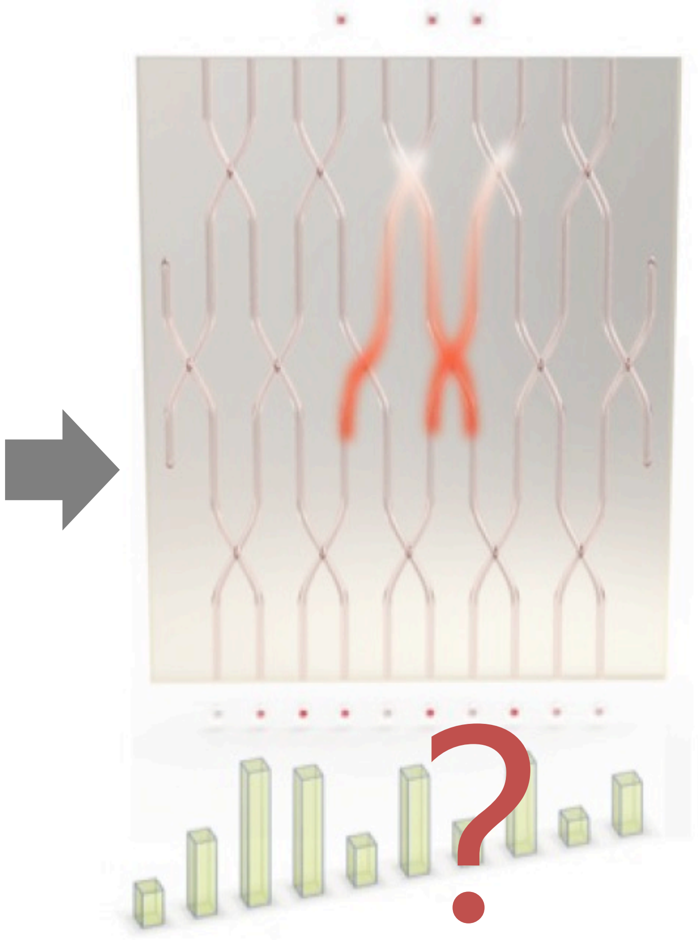


Classical Galton Board



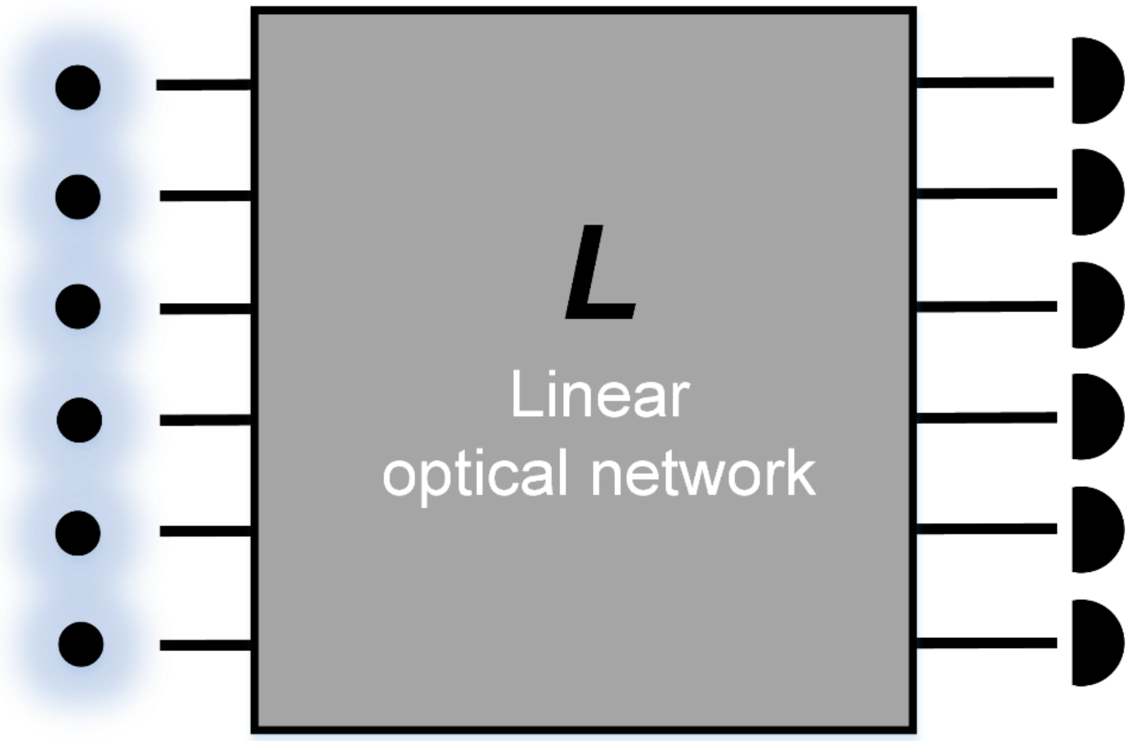
Single-photon interference

Two-photon interference



How to classically predict the outcome of boson sampler?

m input single photons into an N-mode interferometer (N>m)



Calculation:
Permanent of $m \times m$ matrix U

$$\mathrm{Per}(U) = \sum_{\sigma \in S_m} \prod_{i=1}^{m} U_{i,\sigma(i)}$$

S_m is the set of all permutation of m elements

e.g., $\mathrm{Per}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad + bc$

$\mathrm{Per}\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh + ceg + bdi + afh$

Bosons VS Fermions

Identical Bosons

$$\begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix} \; ?$$

$$aei + afh + bdi + bfg + cdh + ceg$$

$$= \mathrm{perm}\,(M)$$

Bosons commute:

Hard

Identical Fermions

$$\begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix} \; ?$$

$$aei - afh - bdi + bfg + cdh - ceg$$

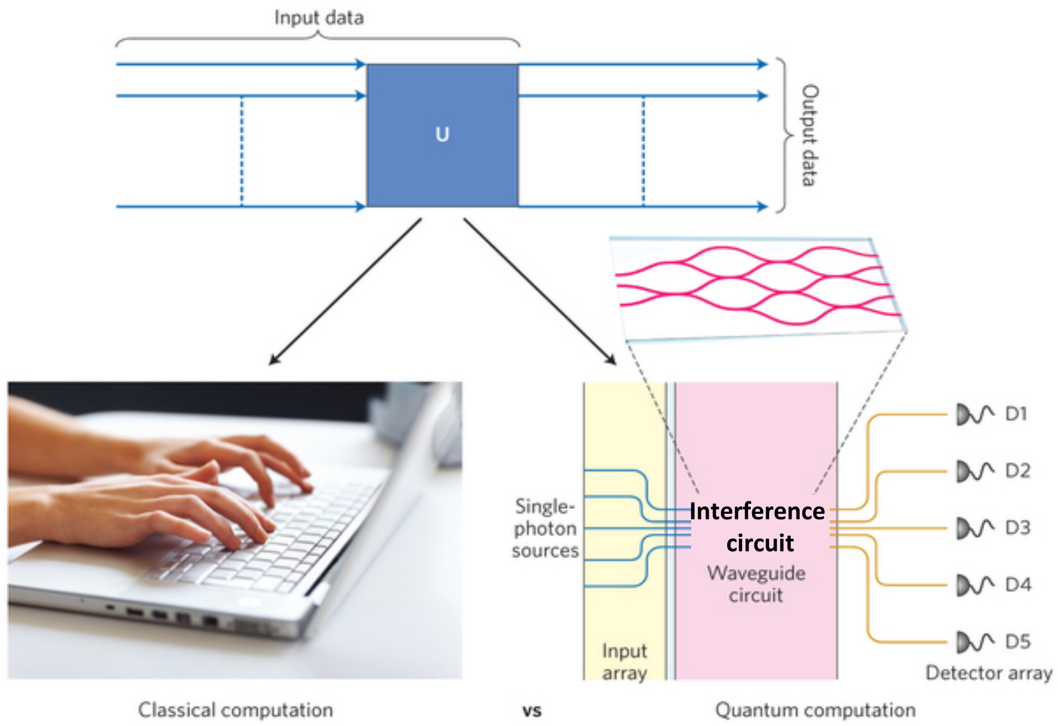
$$= \det\,(M)$$

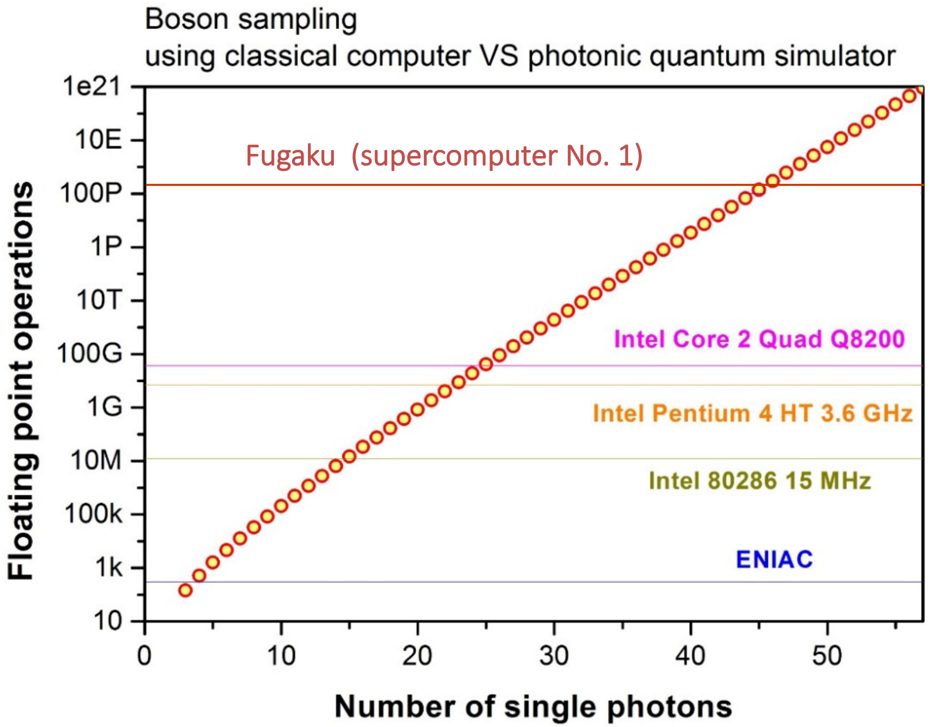
Fermions anti-commute

Easy

Demonstrating quantum computational advantage

- Classical algorithm needs $O(m^2 2^{m+1})$ steps, sharp P-complete problem!
- With ~50 input single photons, the complexity will challenge fastest supercomputer today! [Nat. Phys. 13, 1153 (2017)]

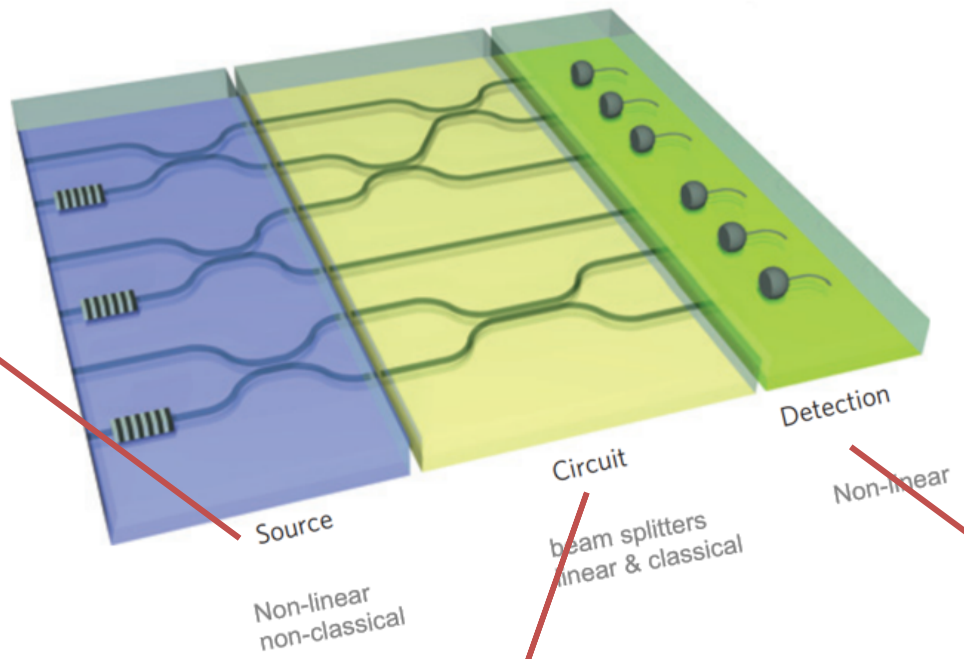




Quantum computer: directly detect the distribution of output photons

Coherent manipulation of ~50 photons to archive quantum computational advantage!

Challenges for large-scale Boson sampling



- High efficiency, high indistinguishability

- Multi-mode interferometer with high transmission rate and random matrix—phase stable, Harr-random matrix, very large mode volume

- High-efficiency and fast single-photon detection

- Validation of the obtained samples
  - Unlike Shor's algorithm where its solution can be efficiently verified
  - For Boson sampling a full certification of the outcome is strongly conjectured to be intractable for classical computation

How to increase the number of manipulated photons?

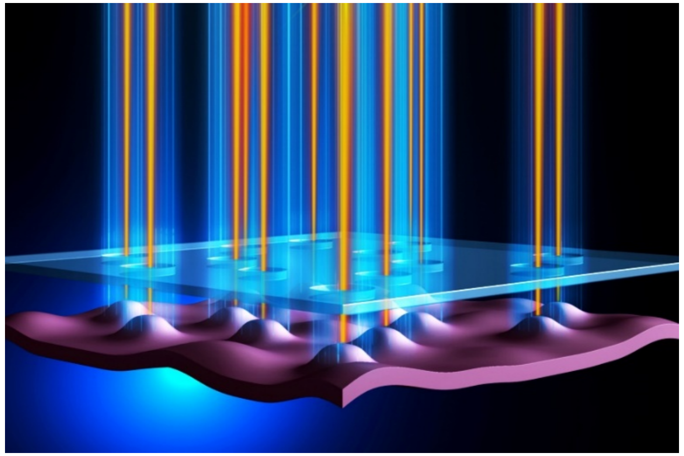
☒ To increase number of entangled photons is extremely hard due to probabilistic source

In 2013:

- Counts ~600,000/s
- Indistinguishability ~90%
- Source efficiency ~0.8%
- Circuit efficiency: 10%-30%
- Detection efficiency: best 90%

50-photon rate $\sim 10^{-150}$ Hz

☑ Possible solution: manipulation of multi deterministic single photons emitted from quantum dots!



Check list for a perfect single-photon source

1. High efficiency

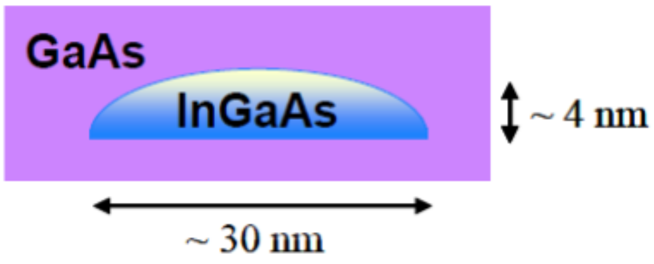
- Quantum efficiency: the decay of excited states should predominantly result in an emitted photon
- Deterministic generation: upon a pulsed excitation, the source should deterministically emit one photon in a push-button fashion
- High collection efficiency: the radiated photons should be extracted with a high efficiency to a single spatial mode

2. High purity—the emission should have a vanishing multi-photon probability, $G^2(0)=0$

3. High indistinguishability—individual photons emitted at different trials should be quantum mechanically identical in all degree of freedom (time, frequency etc.)

Resonant excitation of a single quantum dot

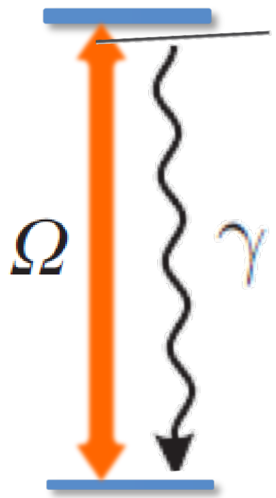
Pulsed resonance fluorescence → 99.5% indistinguishability



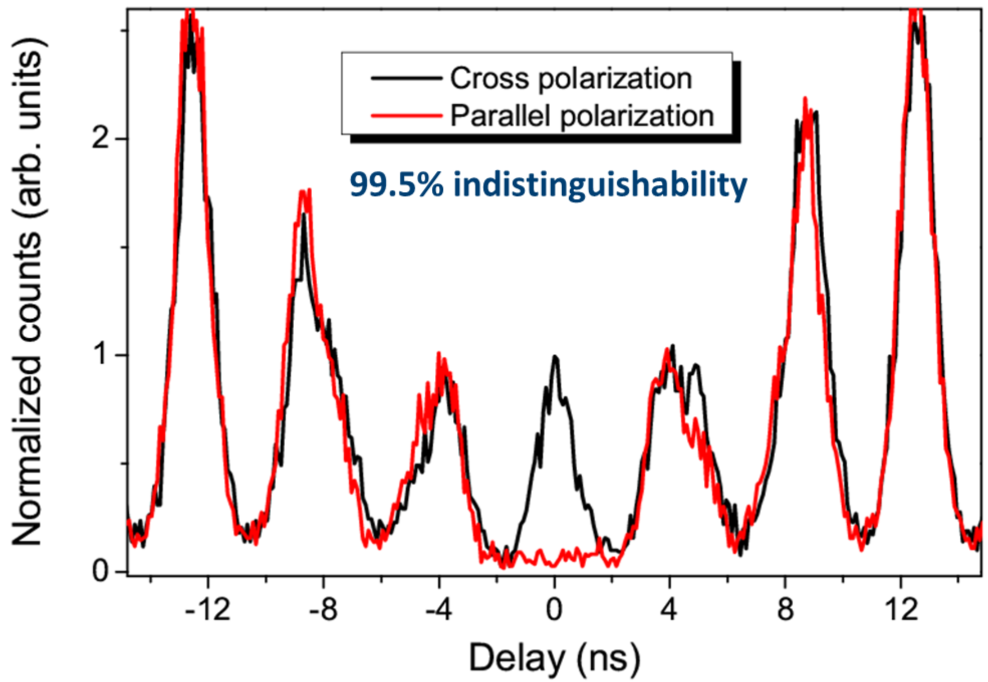
Quantum dots:

InGaAs embedded in GaAs

Coherent drive, no time jitter

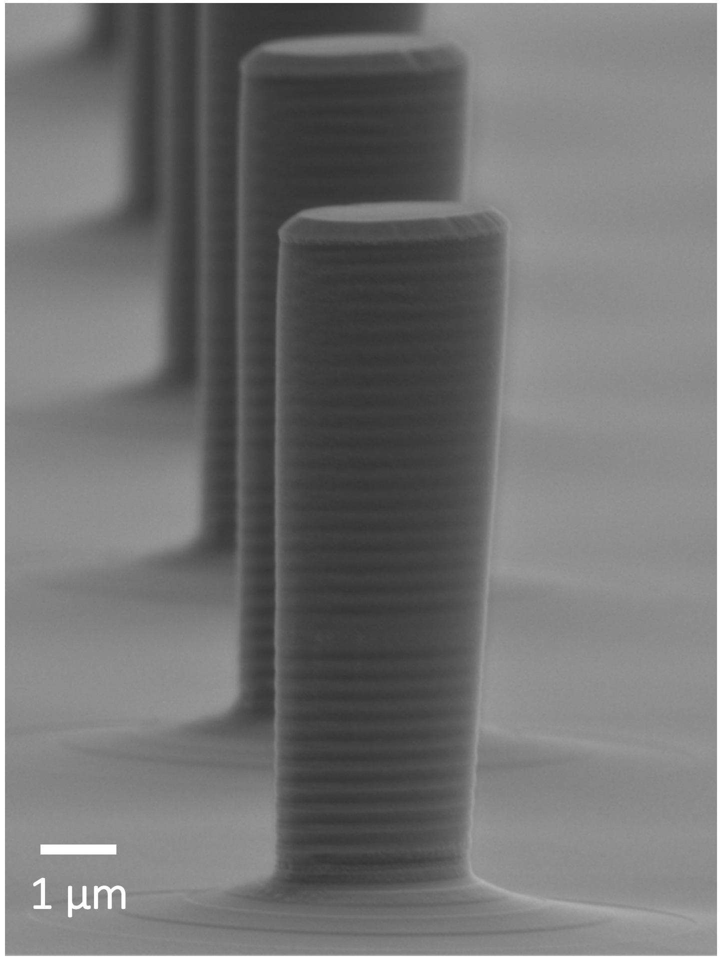


Deterministic drive



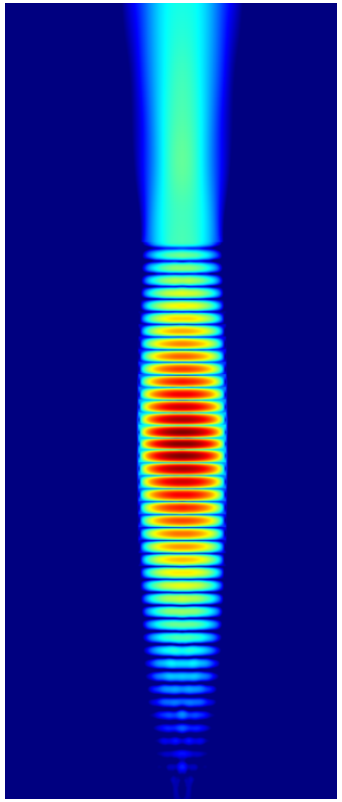
He *et al.*, Nature Nanotechnology 8, 213 (2013)

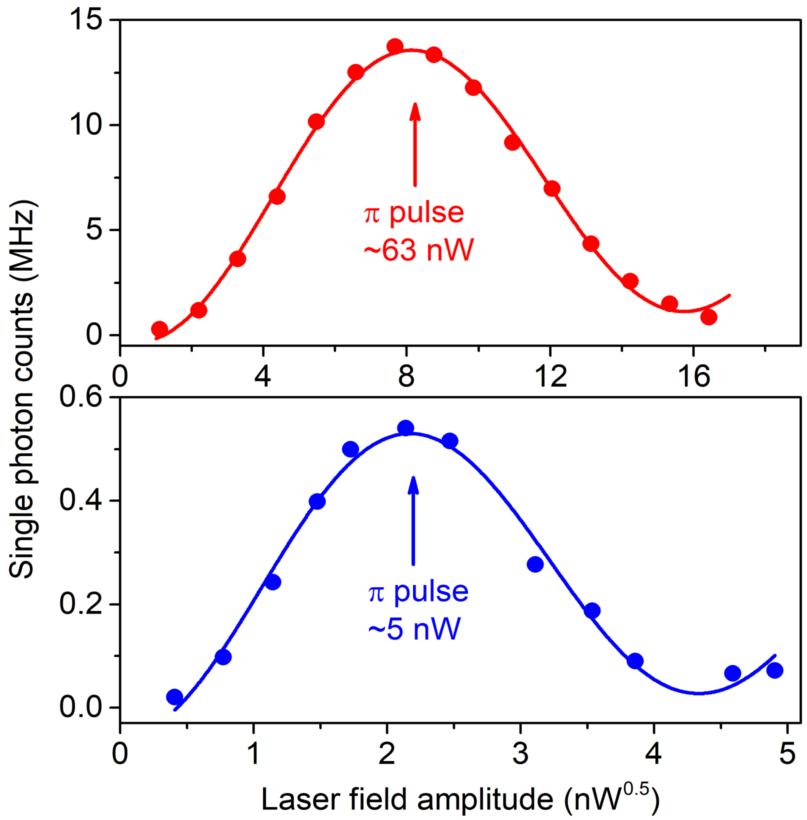
Efficient single photons quantum dot-microcavity



Coherent drive + Purcell enhancement

Both high extraction efficiency and indistinguishability



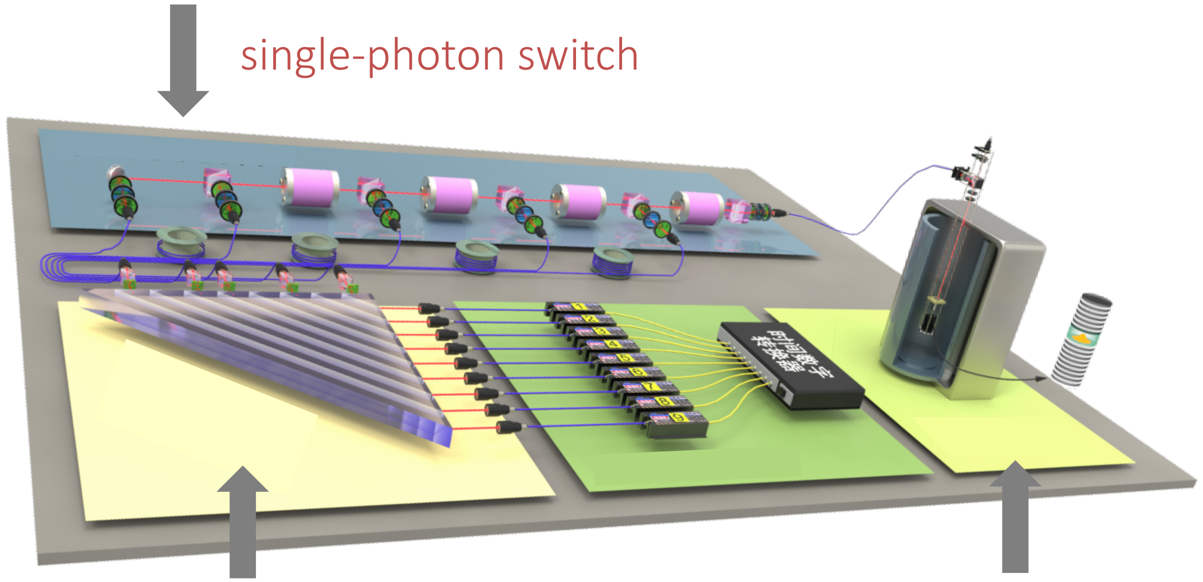


Ding *et al.*, PRL 116, 020401 (2016)

Wang *et al.*, Nature Photonics 13, 770 (2019)

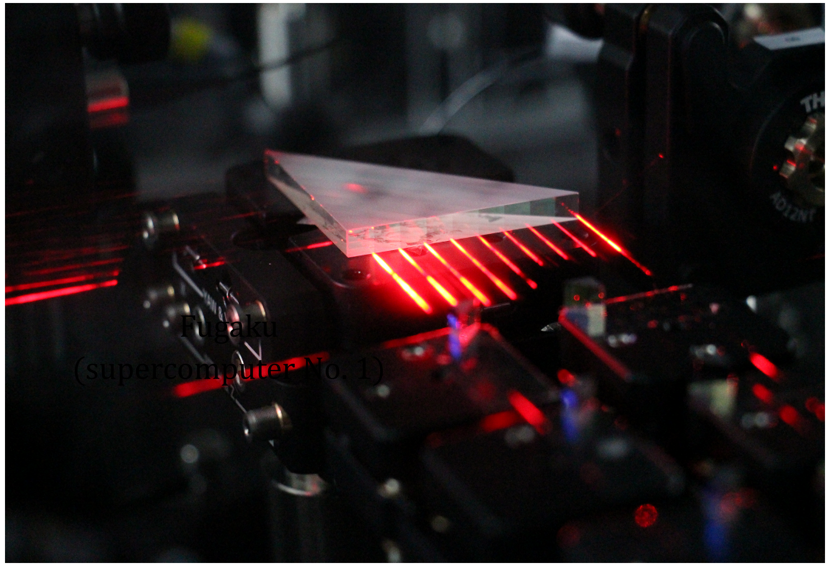
Prototype quantum computer for Boson sampling

single-photon switch



low-loss multi-photon interferometer

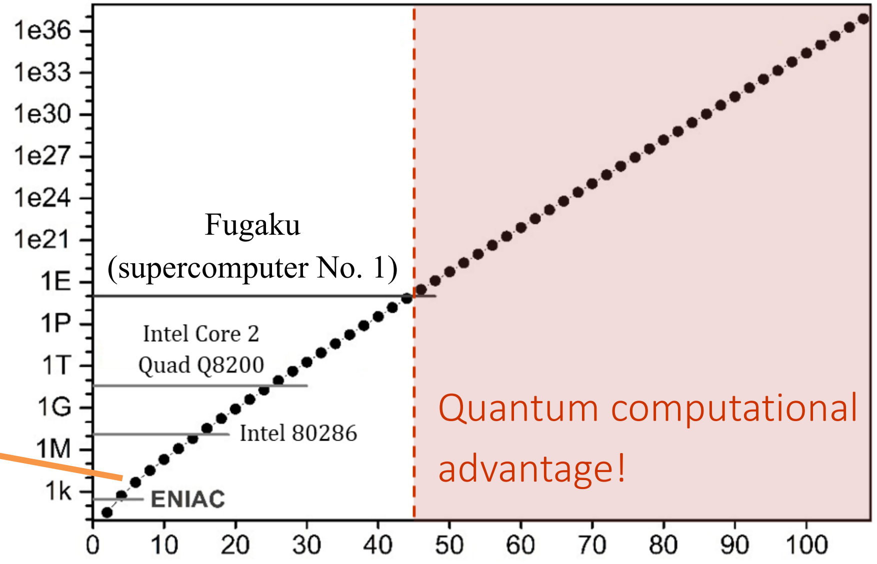
high-efficient single-photon source



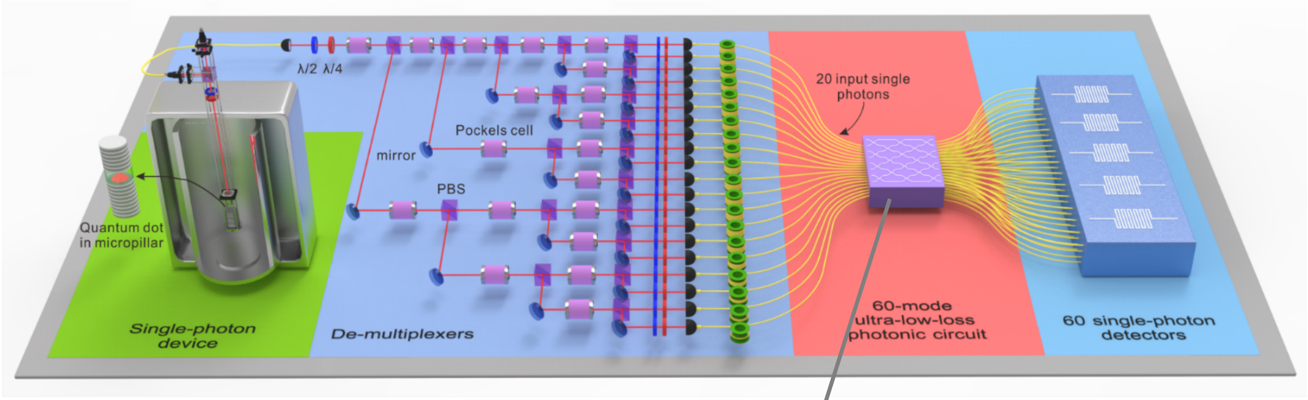
5-photon Boson sampling machine

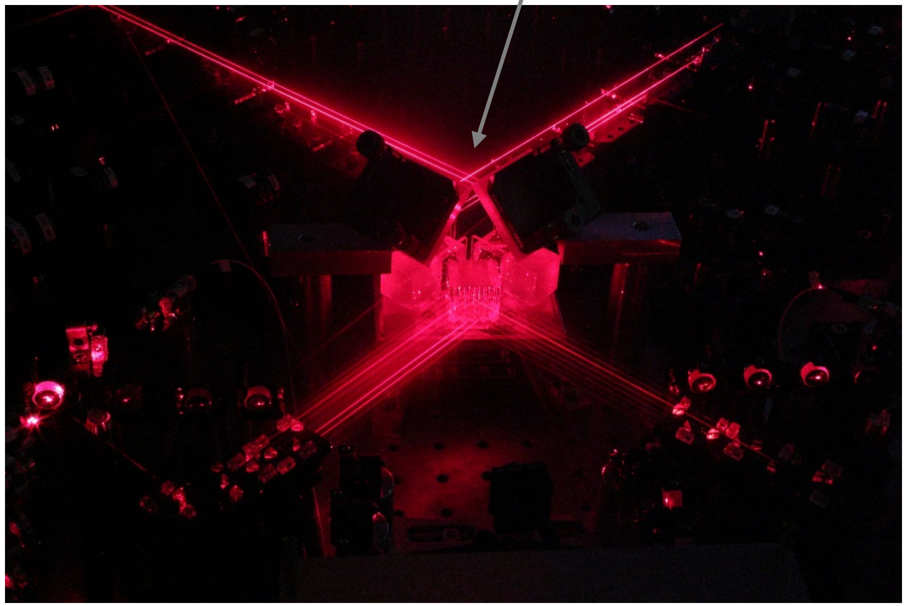
Wang *et al.*, Nature Photonics 11, 365 (2017)

Provably faster than ENIAC and TRADIC for the first time



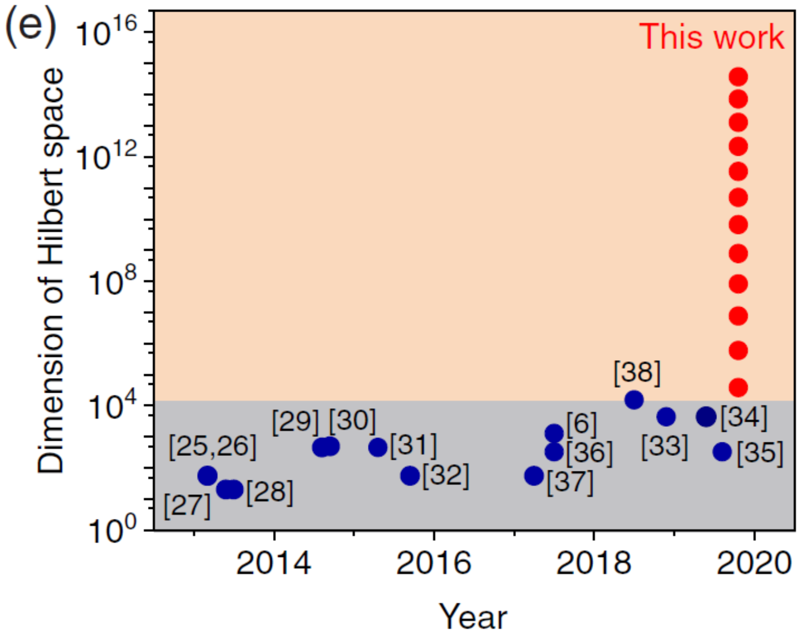
Prototype quantum computer for Boson sampling



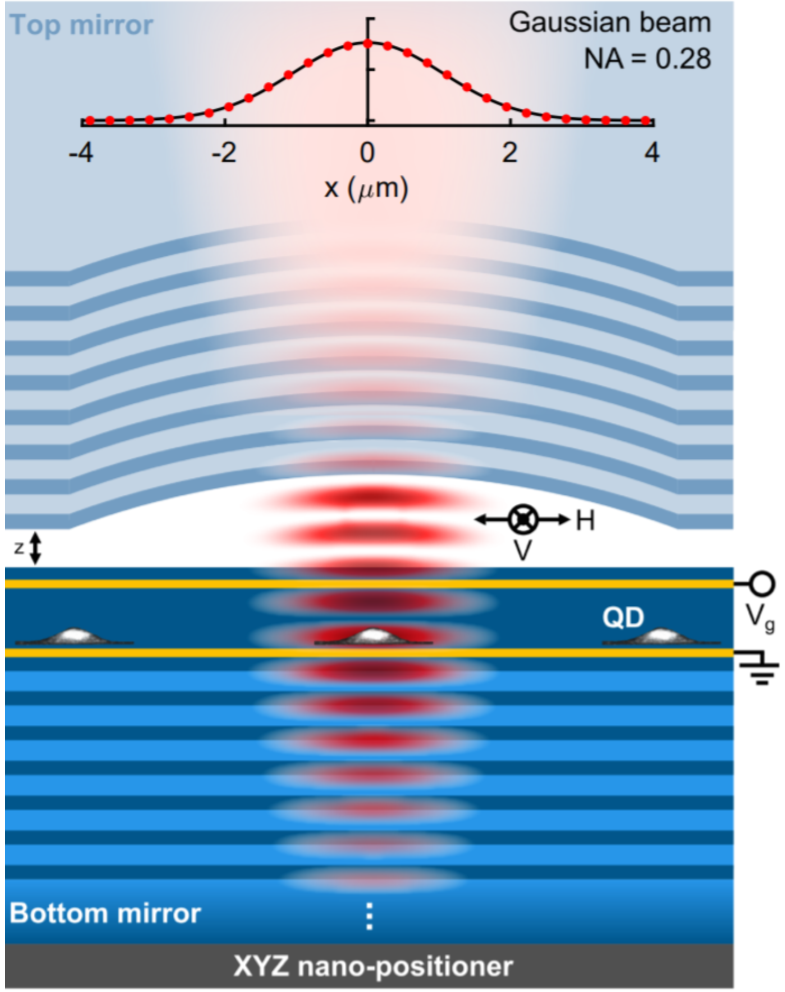


Boson sampling with 20 single photon input 60 modes [PRL 123, 250503 (2019)]

With output state space dimension of 2^{48}, approaching to quantum computational advantage regime



Prototype quantum computer for Boson sampling



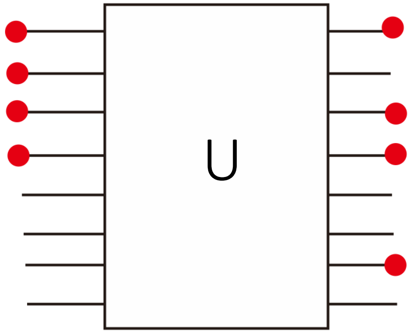
Single quantum dot in a tunable open cavity

- Now single-photon rate ~30 million/s
- Improvement to >40 million/s in progress

Will support boson sampling with ~30 photons, with will outperform the best laptop by 10,000 times, but still cannot beat a supercomputer

Gaussian Boson sampling (GBS)

Boson sampling:



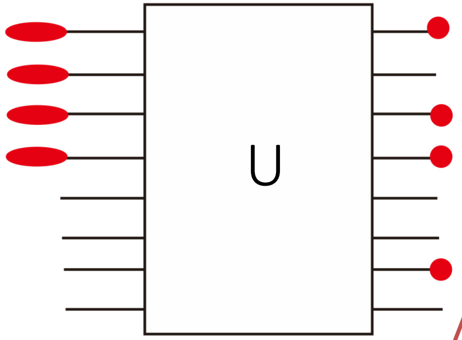
Input N single photons

$$|\text{single photon}\rangle_{\text{input}} = |1\rangle$$

$$\mathrm{P}_N = \left|\sum \text{all possible paths lead to N-photon count}\right|^2$$

$$= \left|\text{Permanent(submatrix)}\right|^2$$

Gaussian Boson sampling:
(with same order of classical
computational complexity)



Input N squeezed vacuum states

$$|\text{squeezed vacuum}\rangle_{\text{input}} = \sum_{k=0}^{\infty} g(\mathrm{k})\, \mathrm{e}^{ik\phi} |2k\rangle$$

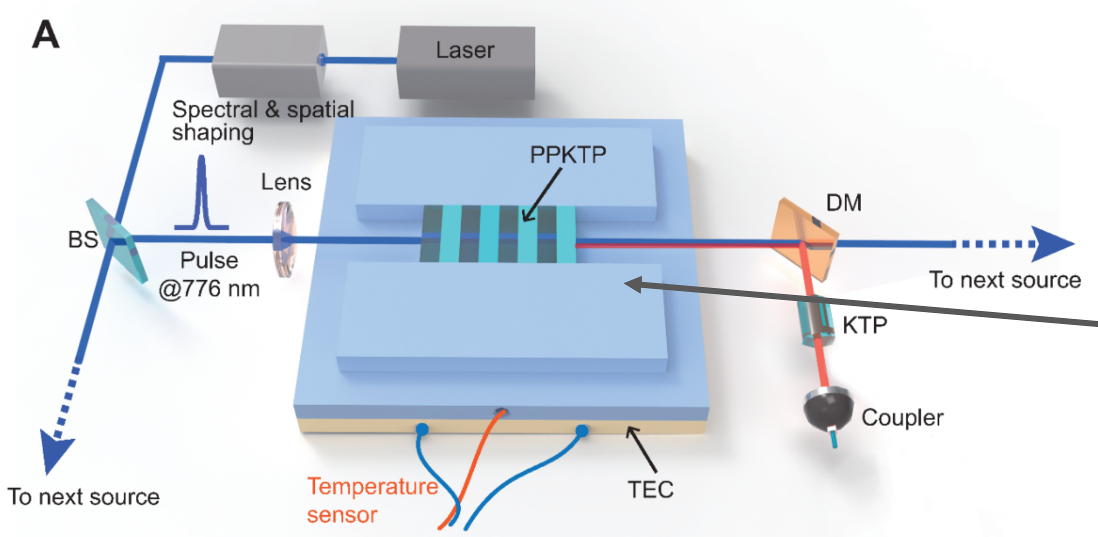
$$\mathrm{P}_N = \left|\sum \text{all possible input photon-number combination} \sum \text{all possible paths}\right|^2$$

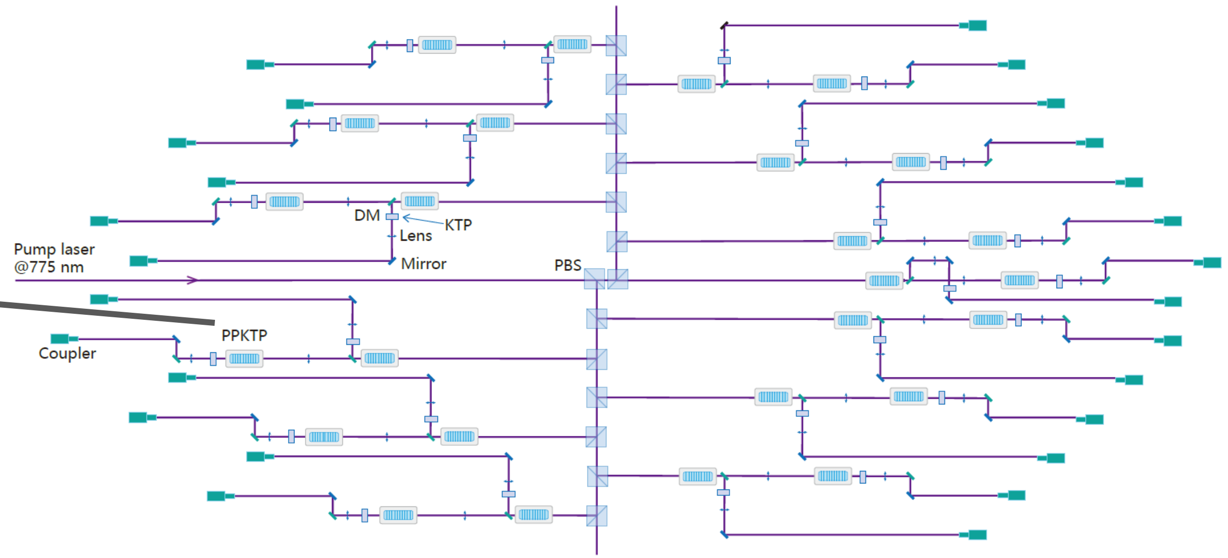
$$= \left|\text{Hafnian[submatrix}(\gamma, \phi, \mathrm{U})]\right|^2$$

GBS makes full use of SPDC!

Hamilton *et al.*, PRL 119, 170501 (2017)
Quesada *et al.*, PRA 98, 062322 (2018)

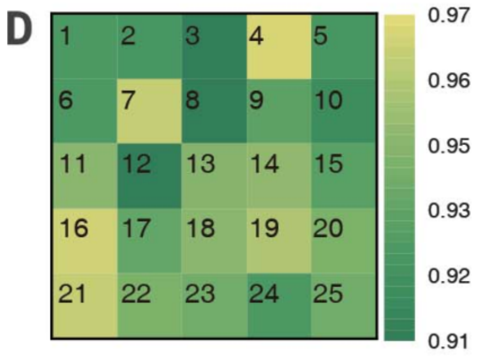
Quantum light sources for GBS



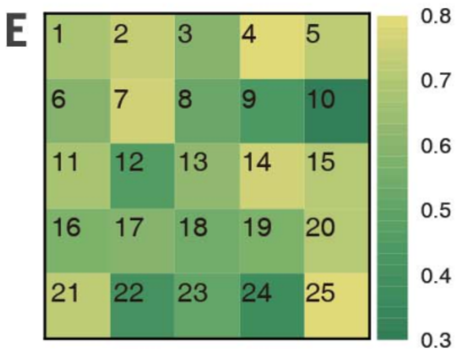


☑ Two mode squeezed state (TMSS) with high squeezing parameters (mean photon number per pulse ~5)

☑ 25 TMSS equivalent to 50 single mode squeezed state (SMSS)



Purities of 25 TMSSs

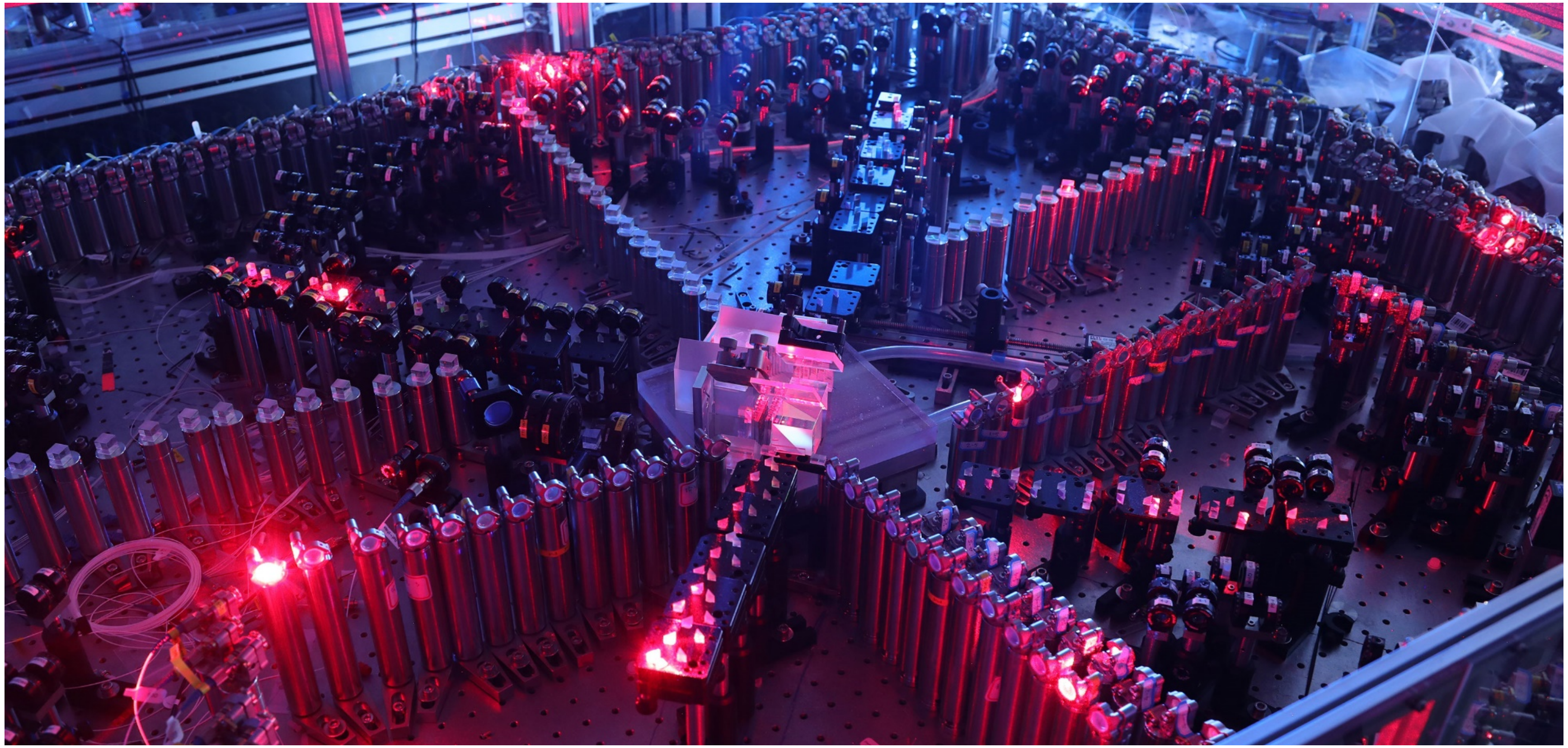


Efficiencies of 25 TMSSs

☑ High purities and efficiencies

Large-scale interferometer

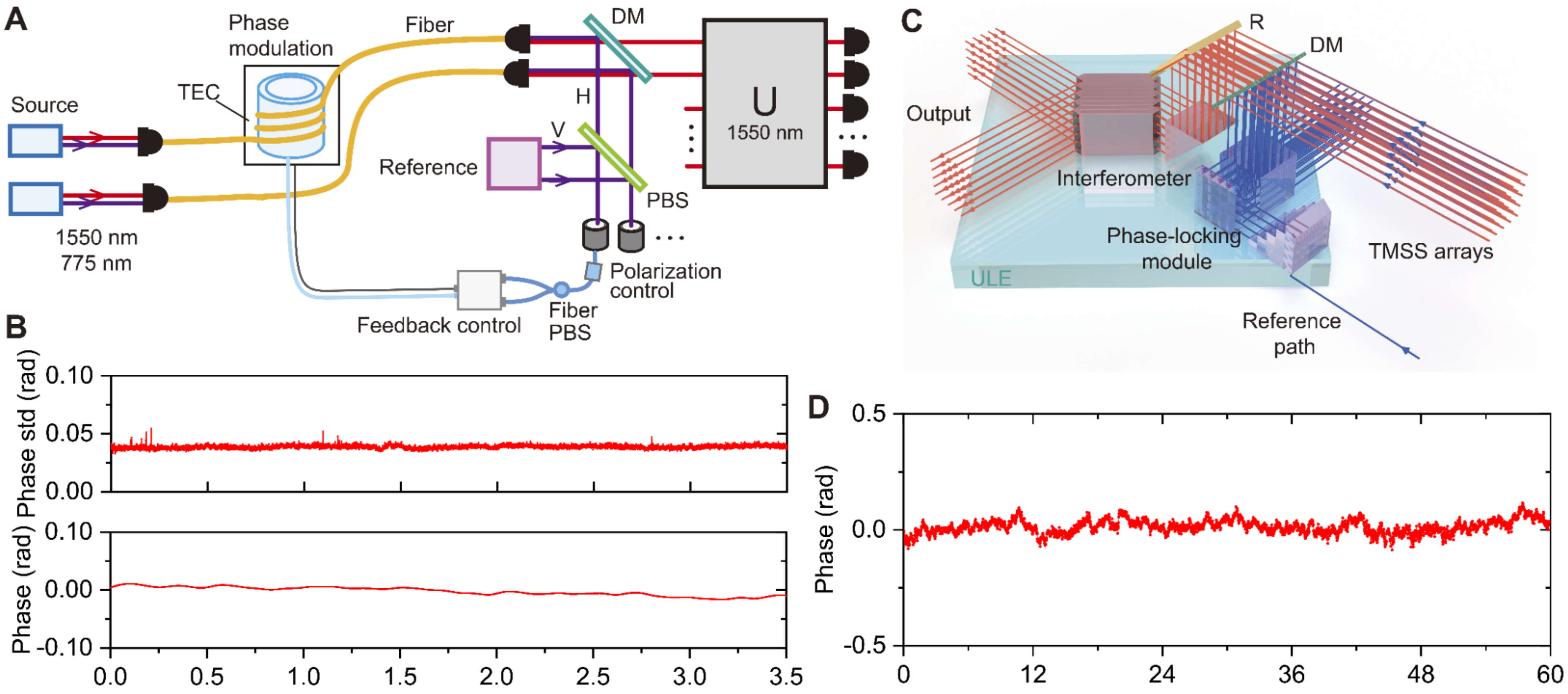
- ☑ Size 100×100 Haar-random matrix,
  fully connected (arbitrary input can goes to arbitrary output),
  phase stable, wave-packet overlap >99.5%, transmission rate >98%



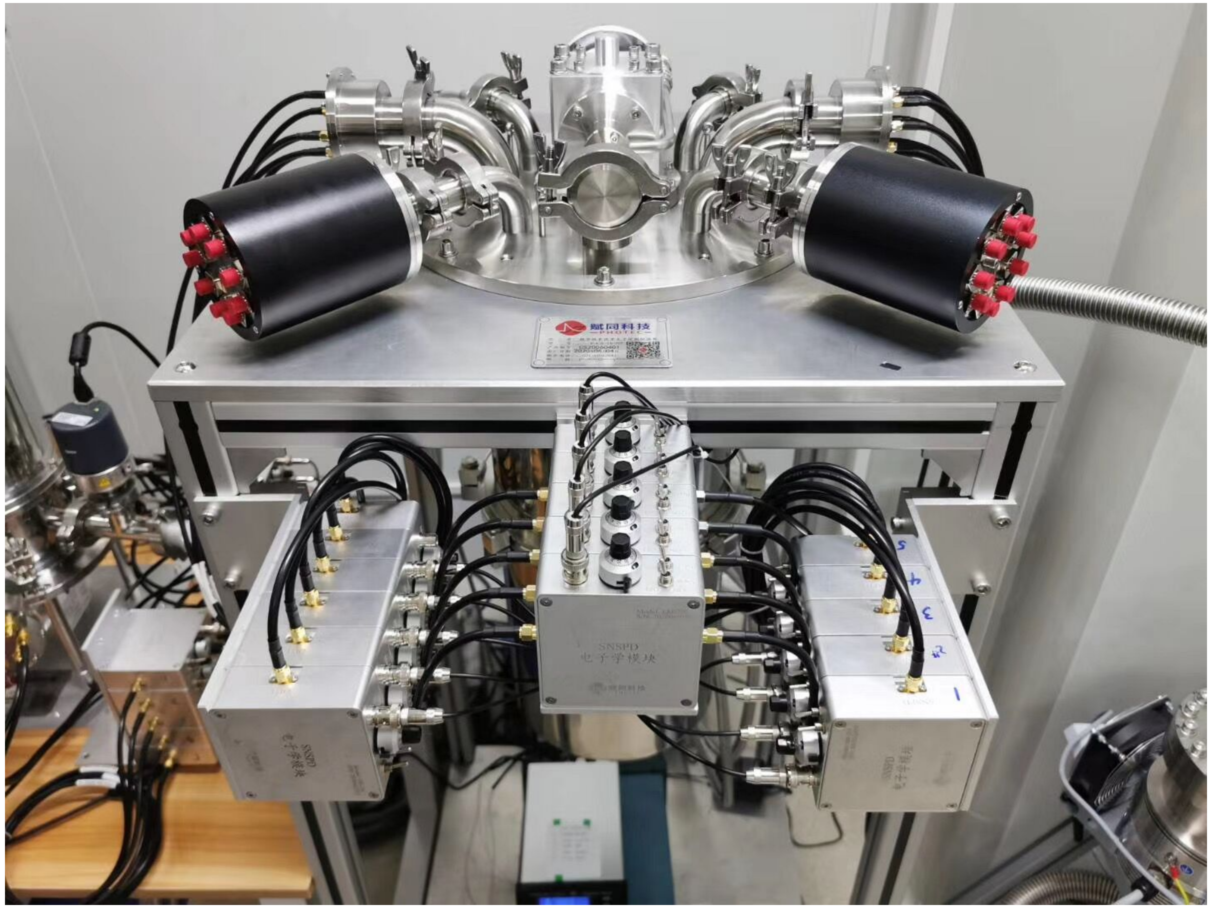
Phase locking of the whole optical setup

☑ 50 independent paths, each with 2m free space +20m optical fiber

Locking precision: 25nm

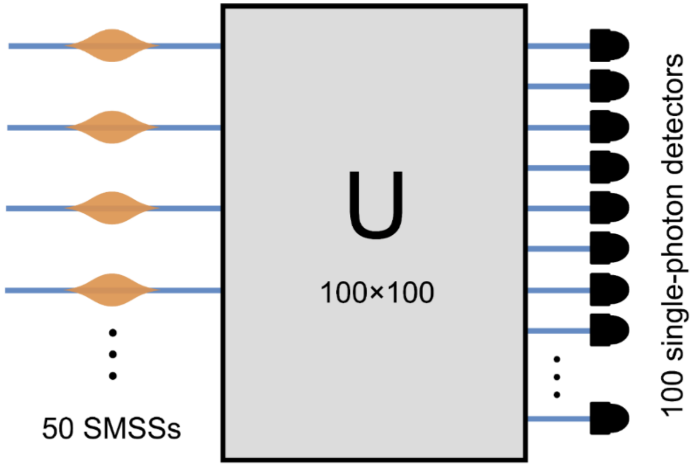


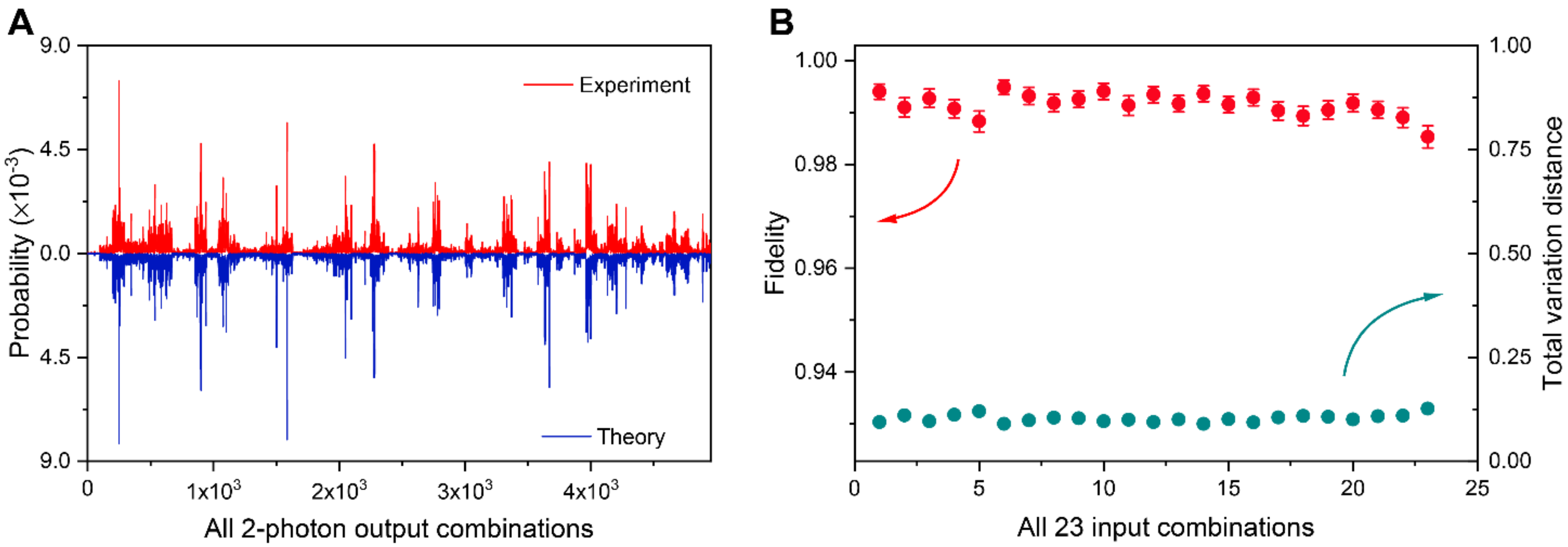
High-efficiency single photon detectors



☑Superconducting nanowire single-photon detector (SNSPD) with efficiency >80%

System calibration



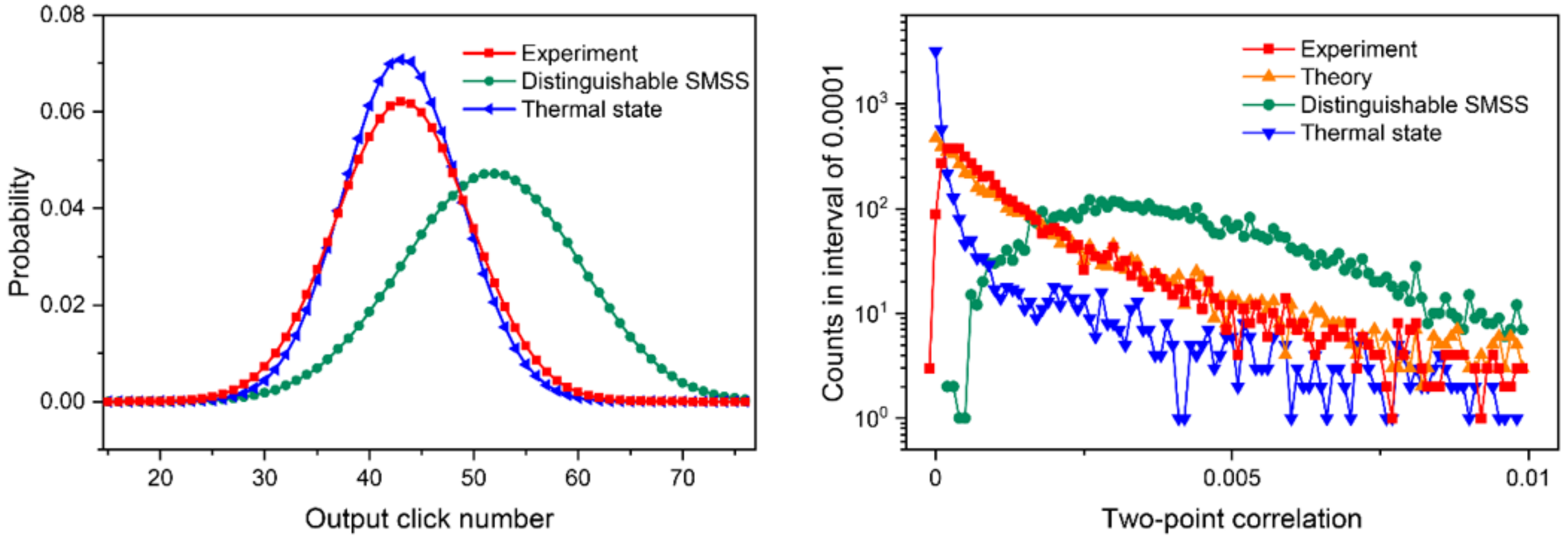


Validation and benchmarking

How to validate GBS?

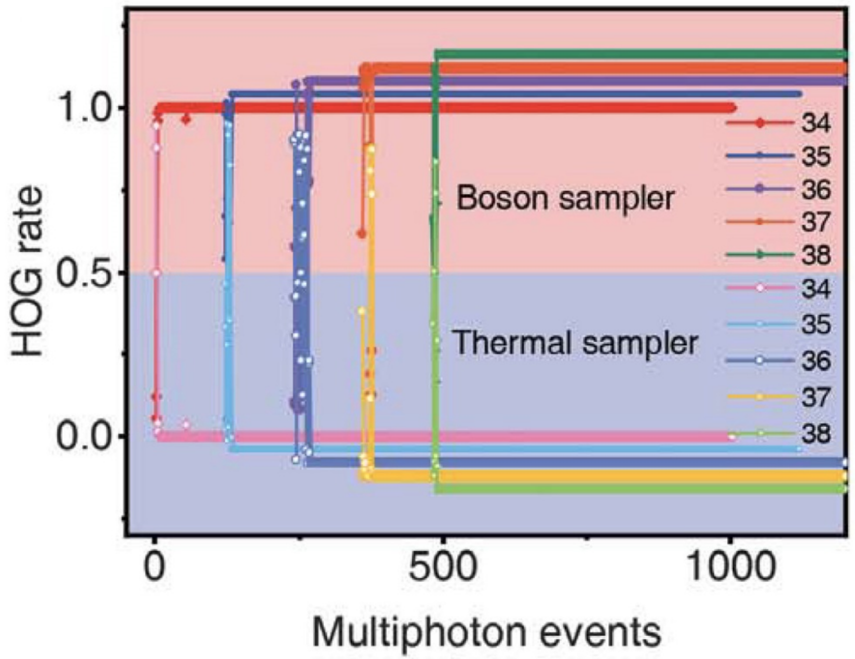
Gathering circumstantial evidence while ruling out possible hypotheses plausibly to occur:

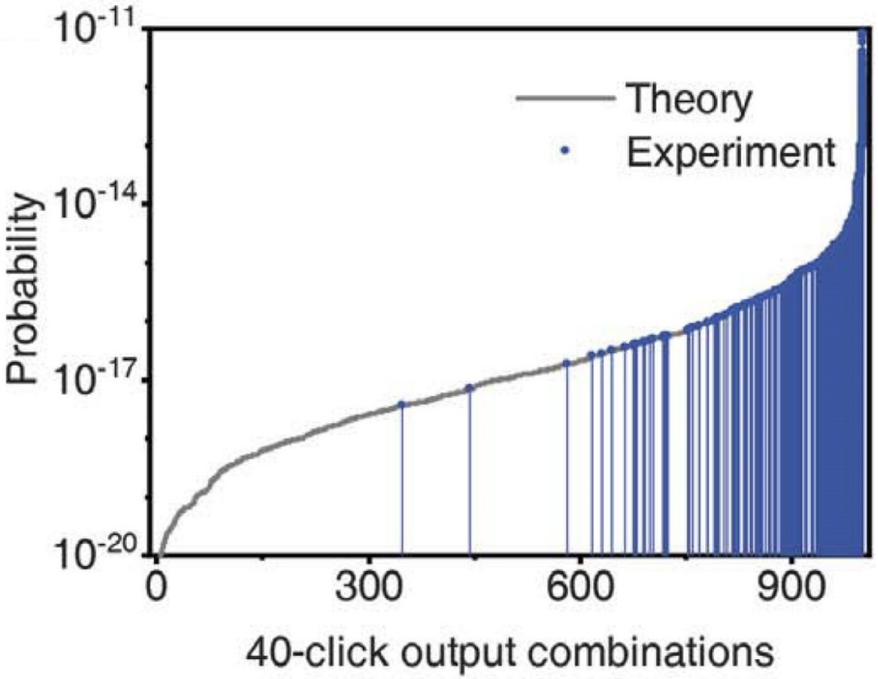
- Thermal states—would result from excessive photon loss
- Distinguishable—would be caused by mode mismatch



☑ Photon number distributions and two-photon correlation statistics deviate from thermal state and distinguishable hypothesis

Validation and benchmarking



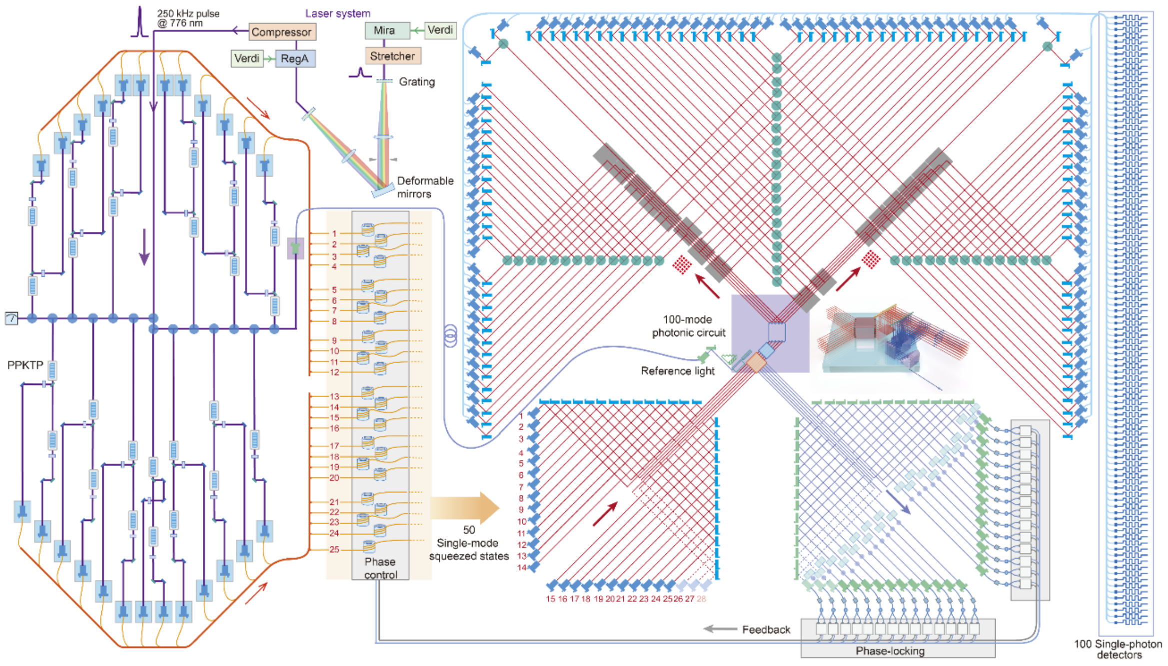


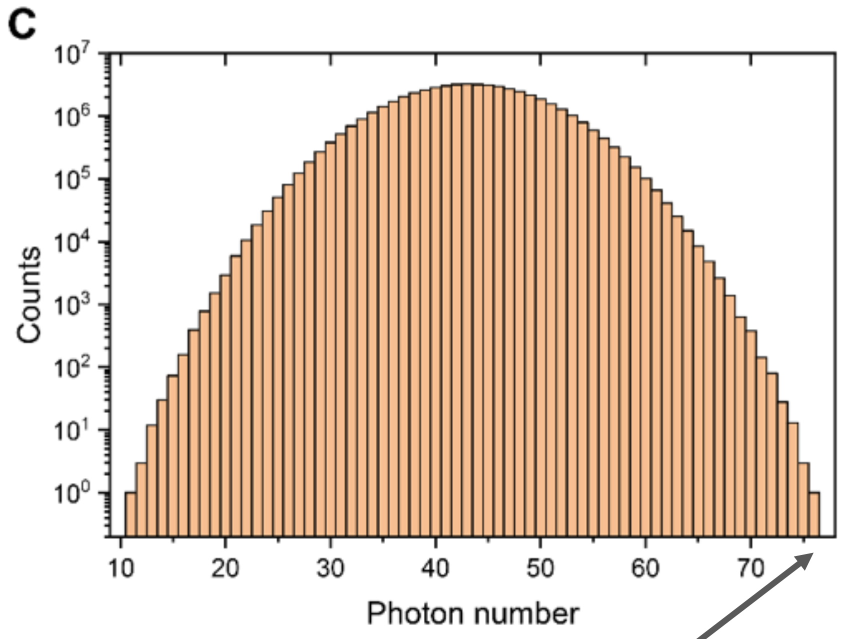
☑ Validation against thermal state hypothesis with detected photon number 34 to 38

☑ Validation against uniform distribution

(classical computing results were calculated by supercomputer Taihu-light)

Quantum computational advantage using photons



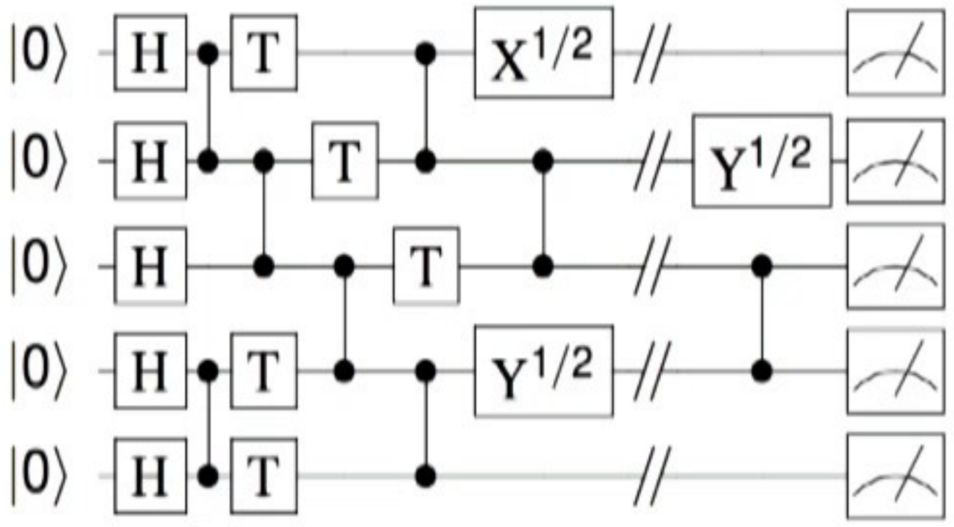


“Jiuzhang（九章）”：Gaussian Boson sampling with up to 76 photons [Science 370, 1460 (2020)]

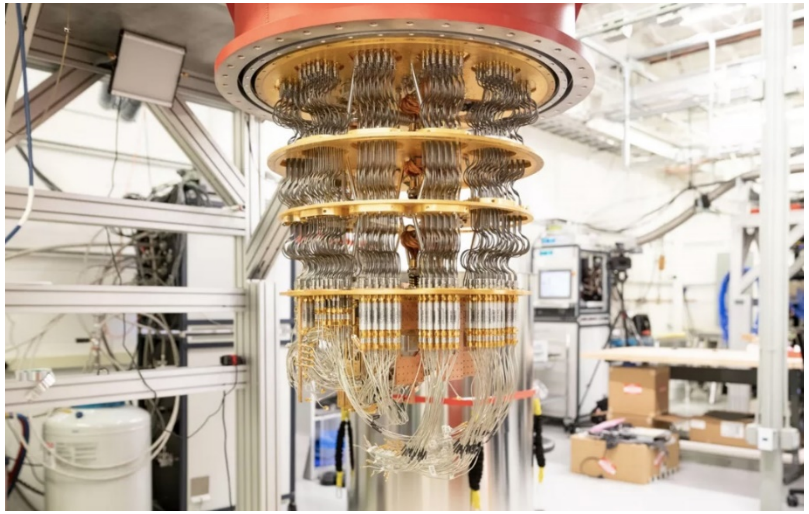
Sampling rate about 10^{14} times faster than classical supercomputer with currently known optimal algorithm [PRA 98, 062322 (2018)]

Google's quantum computational advantage

Random circuit sampling



Aaronson & Chen, In *32nd Computational Complexity Conf.* (2018)



Google's quantum processor "Sycamore" with 53 superconducting qubits

Arute *et al.*, Nature 574, 505 (2019)

- Classical computer: cost a few days to compute all the 2^{53} probability amplitudes
- Sycamore: generated a million (2^{20}) noisy samples in 200 seconds

  But what about 2^{30} samples? 2^{40} samples?

Comparison with Google's "Sycamore"

Random circuit sampling in Sycamore

Sample size	quantum	Classical super-
1 million	200 s	2 days
10 billion	20 days	2 days

The computational advantage would be reversed with larger size of samples!

→ Sample-size-dependent loophole

- Sycamore's state-space: 10^{16}
- Operating temperature: -273.12℃ (30mK)

Gaussian Boson sampling in Jiuzhang

Sample size	quantum	Classical super-
50 million	200 s	0.6 billion years
10 billion	10 hours	120 billion years

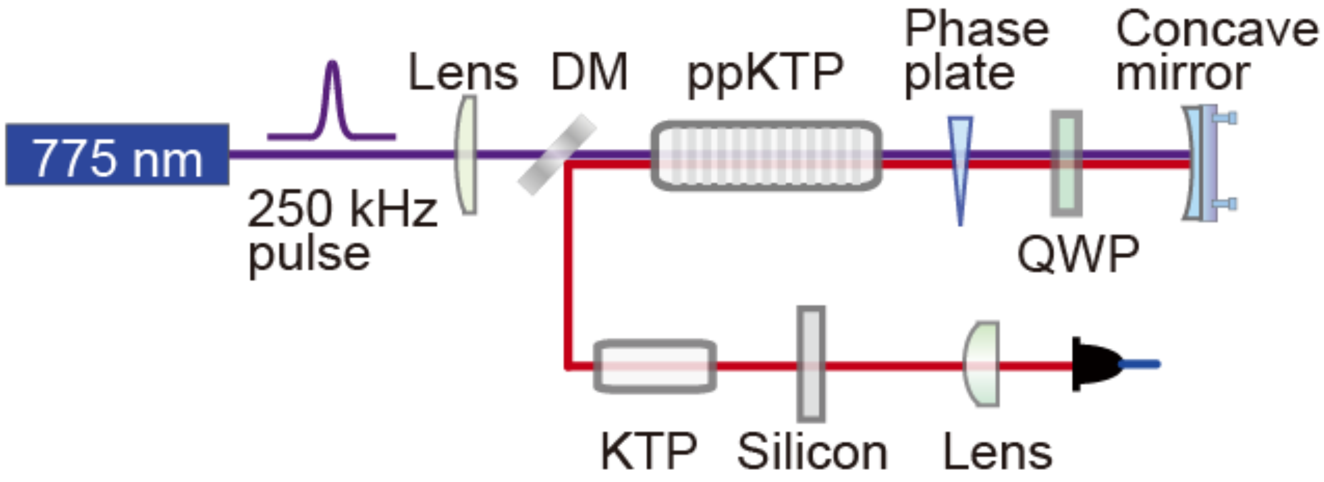
The computational advantage does not rely on the size of samples!

→ Closed the sample-size-dependent loophole!

- Jiuzhang's state-space: 10^{30}
- Room temperature

Recent progress: GBS with 108 detected photons

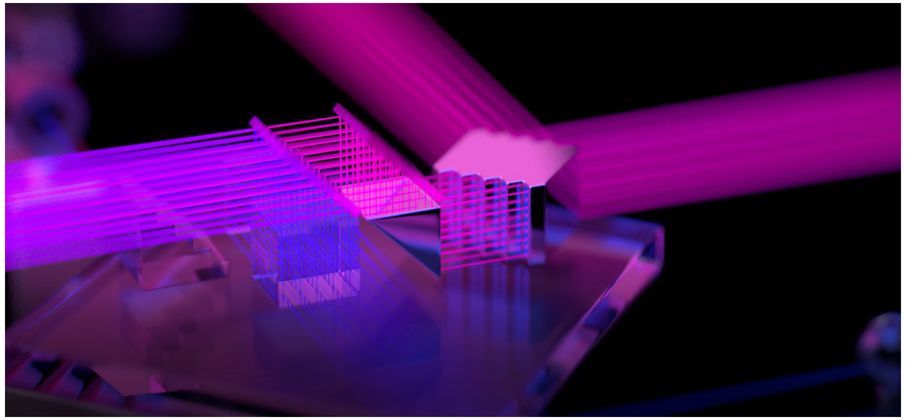
Stimulated PDC: same laser power, 4 times brighter squeezed light

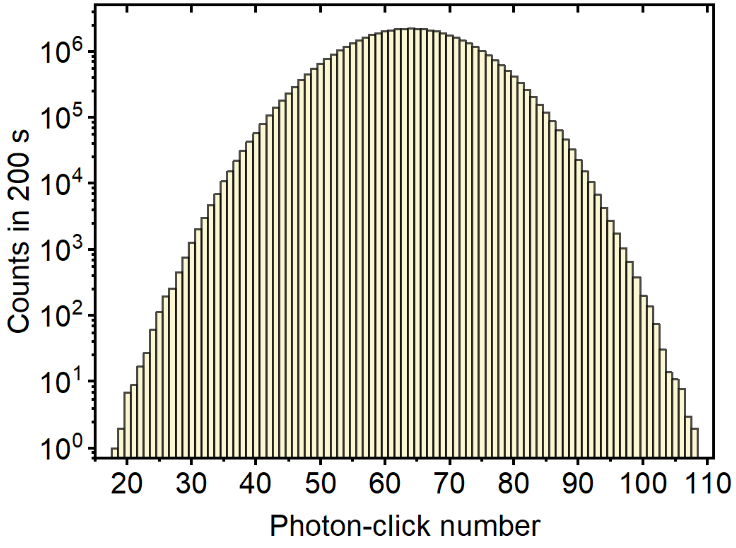


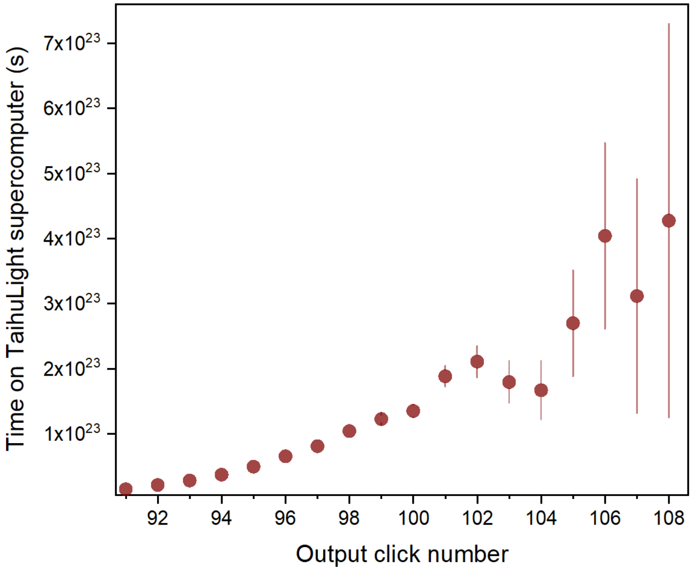
Next steps:

- Tunable interferometer
- More compact set-up
- Seek applications…

144-mode interferometer

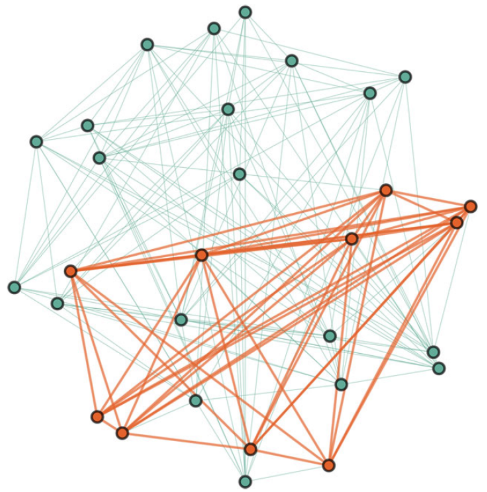


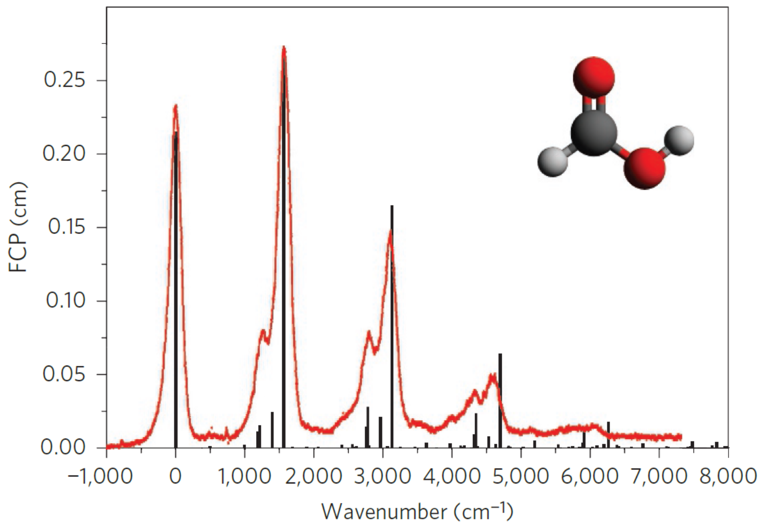


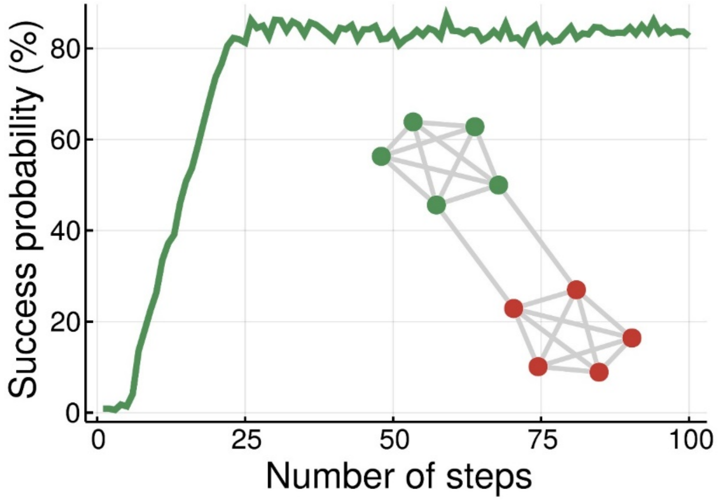


Potentially practical applications

- Now Jiuzhang can only solve GBS problem
- But GBS links to potentially practical applications:

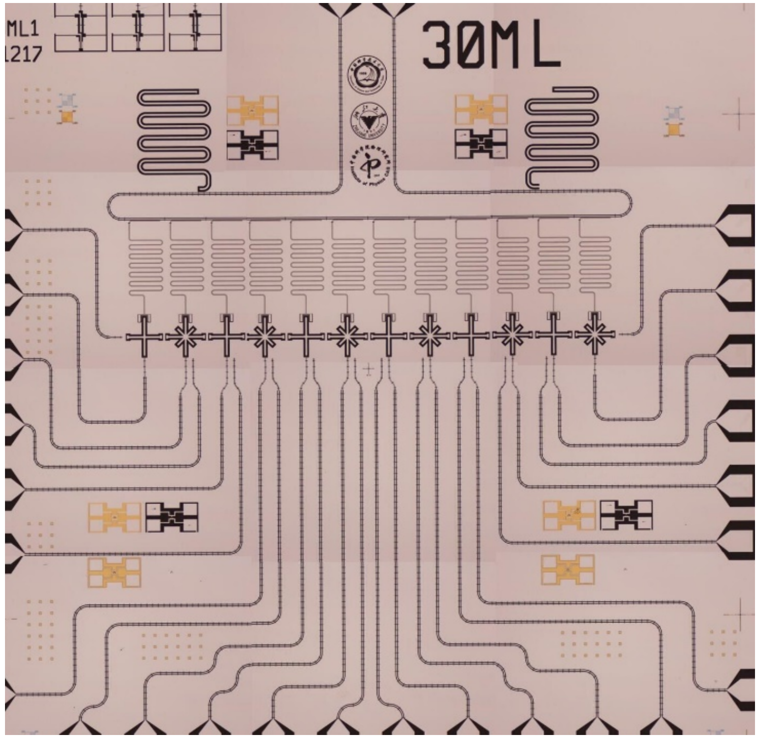




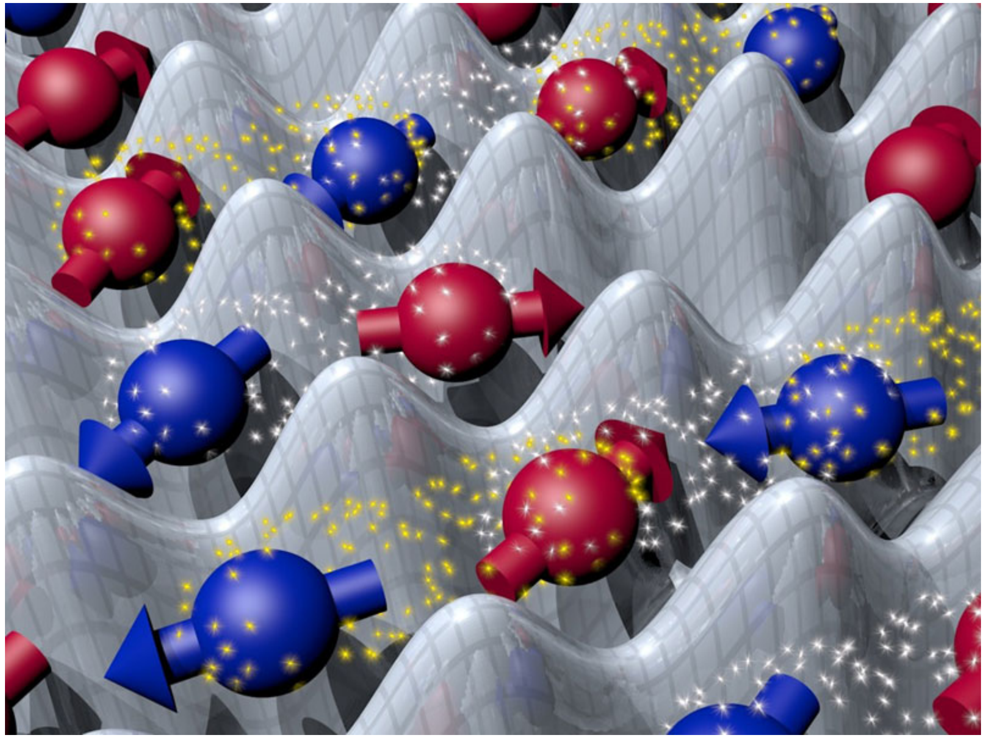


- Graph-related problems: optimization, graph similarity, point process
  [PRL 121, 030503 (2018), PRA 98, 012322 (2018), PRA 98, 032310 (2018), PRA 101, 032314 (2020)]
- Quantum chemistry: simulation of molecular vibration spectrum and molecular docking
  [Nat. Photon. 9, 615 (2015), Sci. Adv. 6, eaax1950 (2020)]
- Quantum machine learning [PRA 102, 012417 (2020)]
- ……

Other candidates of quantum computing



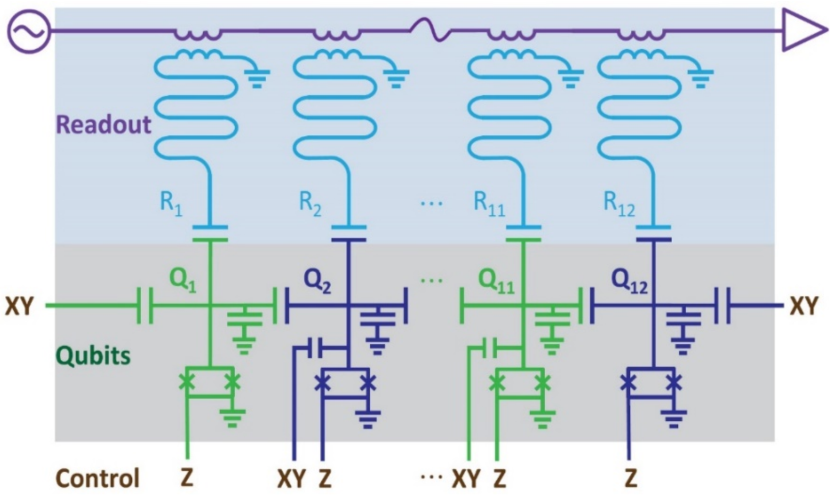
Superconducting quantum circuit

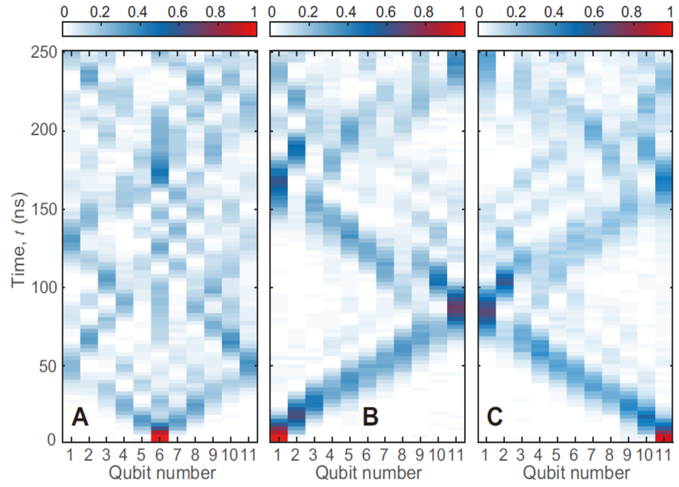


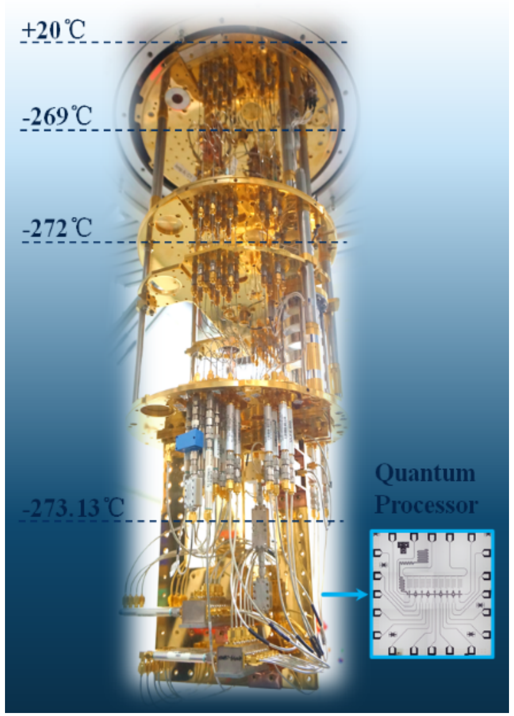
Ultra-cold atoms in optical lattices

Scalability and high-precision quantum manipulation

Superconductor quantum computing



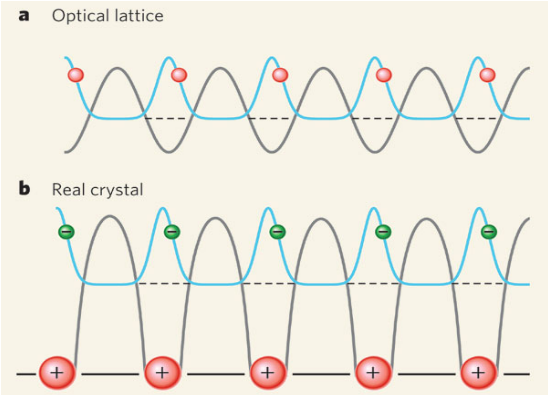




- Entanglement of 10 and 12 superconducting qubits
  [PRL 119, 180511 (2017); PRL 122, 110501 (2019)]
- Demonstration of topological robustness of Anyonic braiding statistics [PRL 121, 030502 (2018)]
- Strongly correlated quantum walks with 12-qubit superconducting processor
  [Science 364, 753 (2019)]

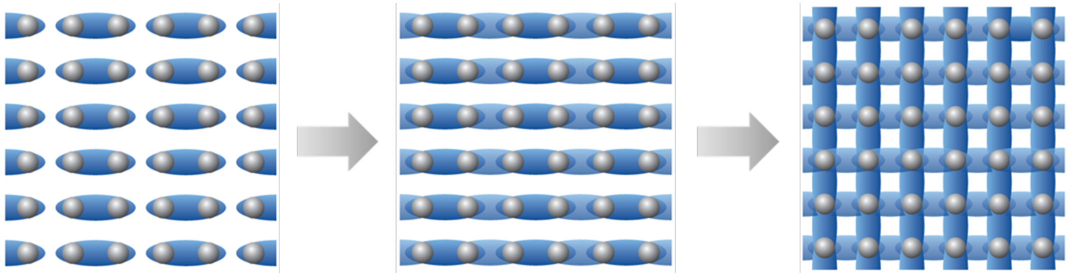
Fabrication and measurement of 66-qubit device for random circuit sampling in progress

Quantum computation and simulation with ultracold atoms



Ultracold atoms is a novel system for quantum simulation

"Quantum engineering" of Hamiltonians



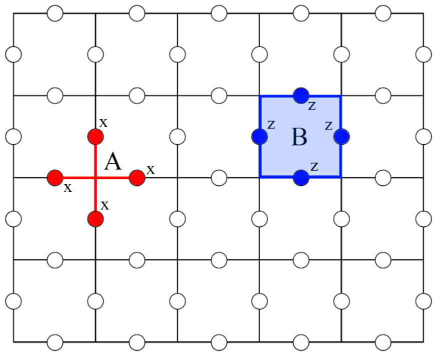
Atom-atom entanglement in optical lattices

~600 pairs: Nature Physics 12, 783 (2016)

$$H_0 = -\sum_s A_s - \sum_p B_p$$

$$A_s = \prod_{j \in \mathrm{star}(s)} \sigma_j^x$$

$$B_p = \prod_{j \in \mathrm{boundary}(p)} \sigma_j^z$$

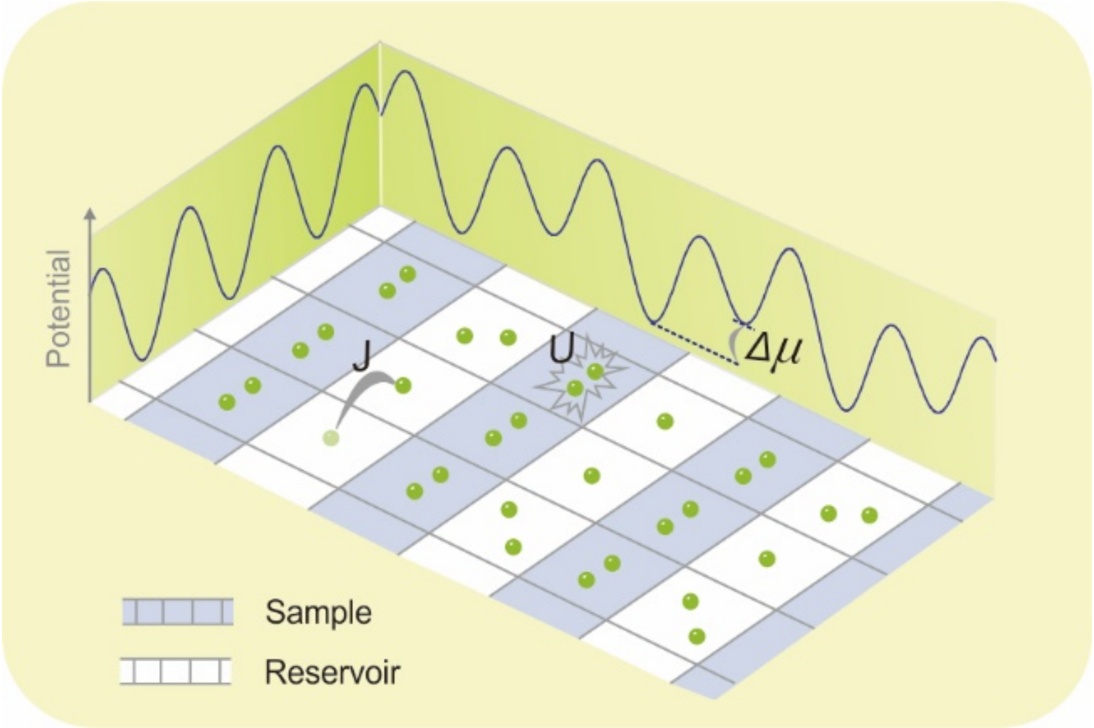


Demonstration of Toric-code Hamiltonian and the Anyonic fractional statistics

Nature Physics 13, 1195 (2017)

Quantum computation and simulation with ultracold atoms

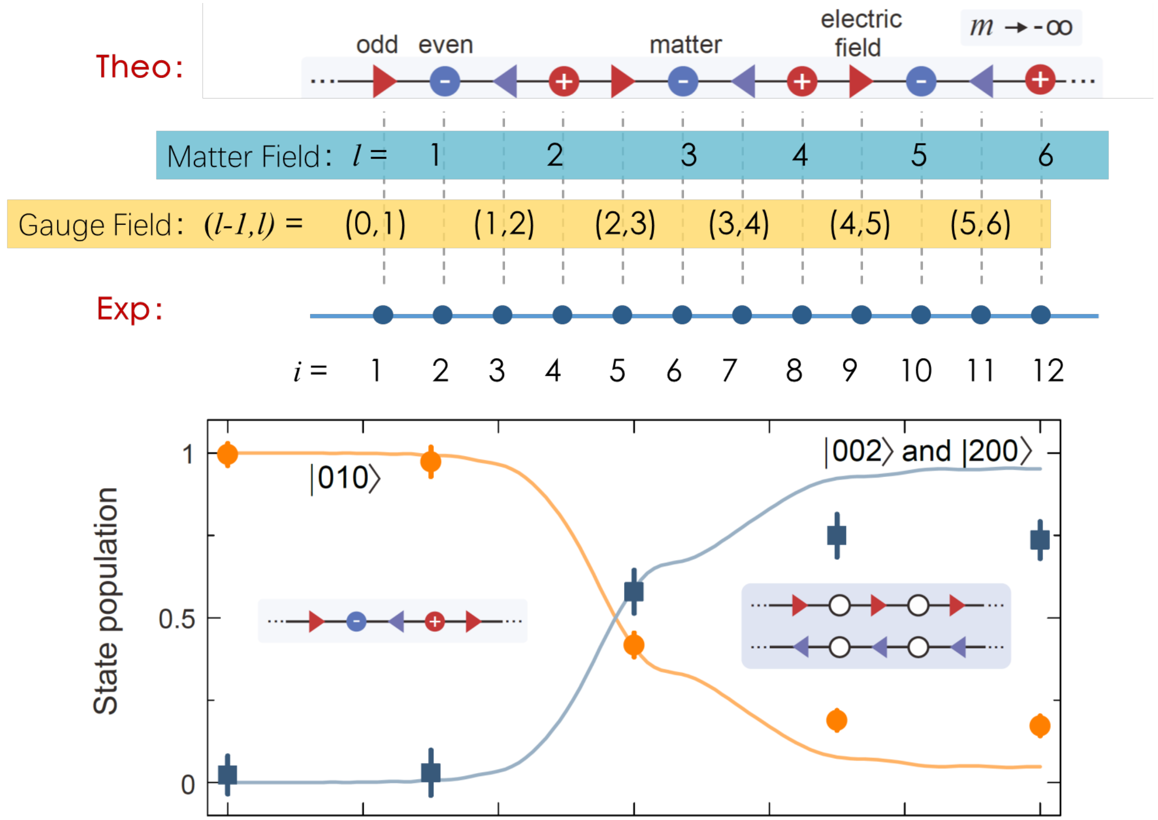
- Staggered-immersion cooling defect-free optical lattice



- Filling factor: 99.2%
- ~1200 pairs of atom-atom entanglement with high fidelity (99.3%)

Science 369, 550 (2020)

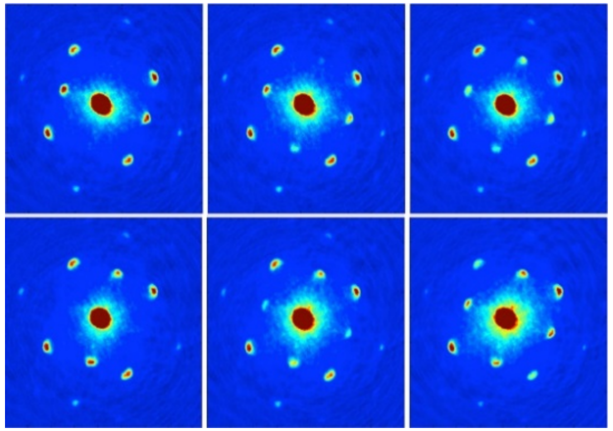
- Simulating a LGT theory with a 71-site quantum simulator



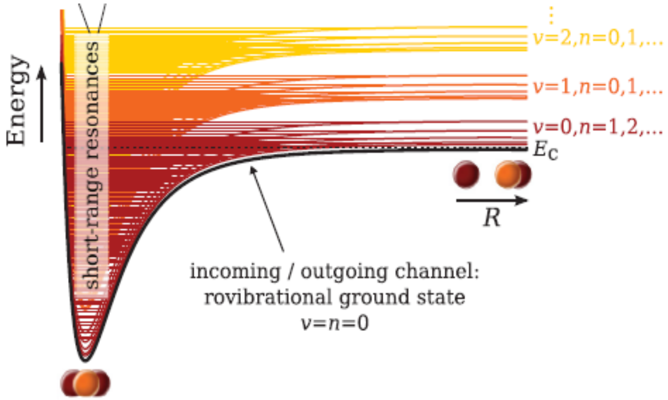
- Schwinger equation is simulated
- Guass's law is verified in the experiment

Nature 587, 392 (2020)

Quantum computation and simulation with ultracold atoms



- Quantum simulation of Gauge potential with neutral atoms
  - Phase diagram of 1D spin-orbit coupling [PRL 109, 115301 (2012)]
  - Realization of 2D SOC [Science 354, 83 (2016)]



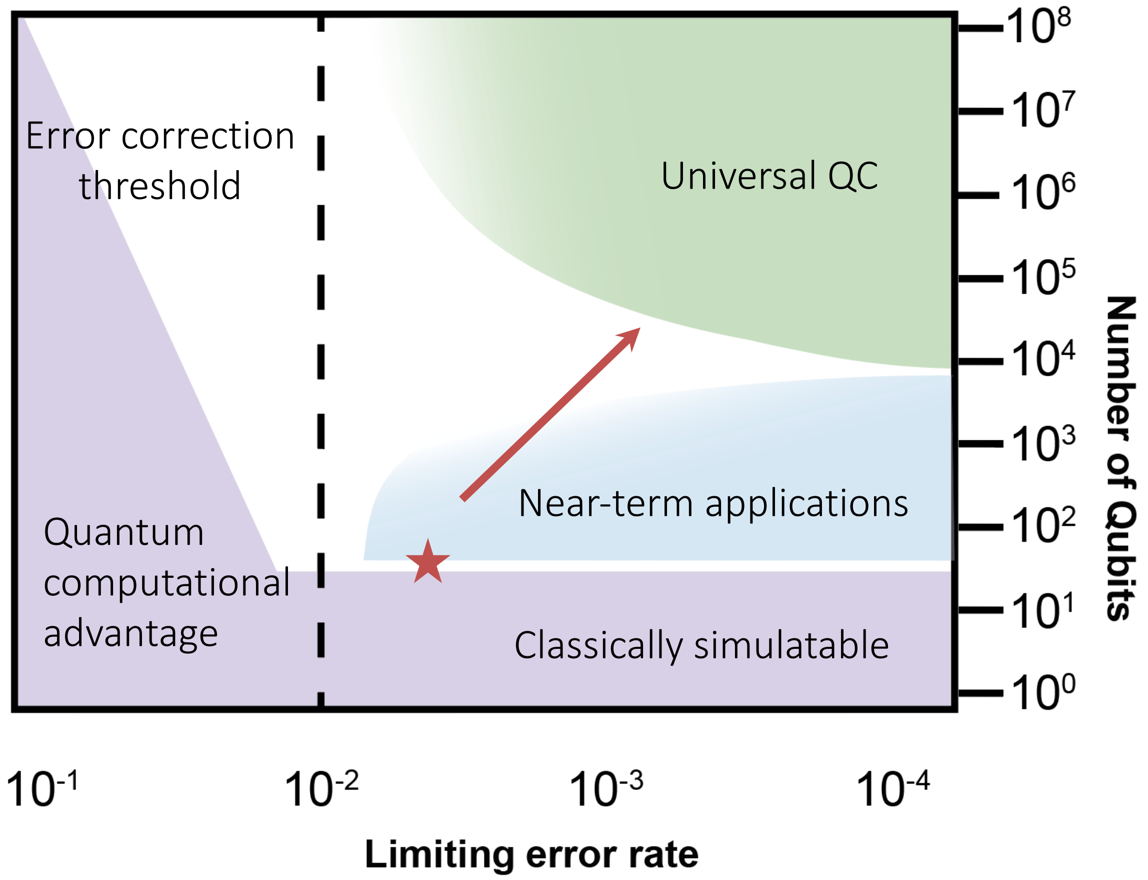
- Quantum simulation with ultracold molecules

Obtaining information of potential energy of triatomic molecule containing 49 electrons (cannot be obtained by solving multi-electron Schrödinger equation with classical numerical simulation) [Science 363, 261 (2019)]

Next step:

- Coherent manipulation of an entangled state of ~100 atoms
- Mimicking strongly correlated topological matter, phase diagram of Fermi-Hubbard model, dynamics of ultracold chemistry......

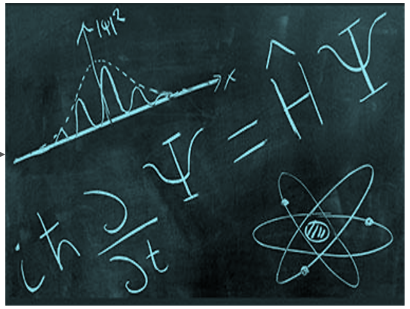
Future prospects



- In next 5-10 years: coherent manipulation of a few hundreds to thousands qubits ➡ study the mechanism of high-temperature superconducting, quantum hall effect and so on
- In next 15-20 years: quantum computer with millions of qubits ➡ realize universal and programmable quantum computers with the help of quantum error correction

Future prospects

Nature has two outstanding achievements

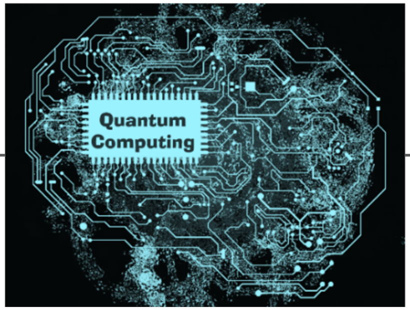


Quantum laws

Human's intelligence

Match nature!

Match human brains!



Quantum computing

Artificial intelligence

To understand or to create new intelligence, maybe we can go beyond Nature!

Thanks for your attention!