# Quantum Computing and Quantum Communication

## Lecture 3

Michal Kloc

http://quantumtheory-bruder.physik.unibas.ch

winter semester 2020

# Outline of the lectures

- building blocks of quantum information
  - quantum bits (qubits)
  - superposition and entanglement
  - gates and universal computation
  - Deutsch algorithm
- decoherence, quantum error correction, no-cloning theorem, quantum teleportation
- quantum cryptography, quantum "hardware"

## References


- N. D. Mermin, *Quantum computer science*, Cambridge University Press
- M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press
- Lecture notes by C. Bruder, R. Tiwari, N. Lörch and M. Koppenhöffer

## Main take-home messages of Lecture 2

- Any realistic quantum computer will be *noisy* due to uncontrolled interaction with environment.
- When information is transmitted we have to face two types of the errors: bit flips and phase flips
- Correction schemes are based on redundancy; to encode one *logical qubit* we need more *physical qubits*
- A quantum state cannot be simply copied from Alice to Bob (no-cloning theorem) but can be teleported provided that Alice and Bob share an auxiliary entangled state.

## Classical private-key cryptography

- Alice wants to send a secret message to Bob
- both have exchanged a random encryption key beforehand

  0 1 0 0 1 1 0 0 1 0 0 0 message

  1 1 0 1 0 1 1 1 0 1 0 0 encryption key

  1 0 0 1 1 0 1 1 1 1 0 0 bitwise sum = encrypted message
- Message transmitted to Bob over public channel

  1 0 0 1 1 0 1 1 1 1 0 0 encrypted message

  1 1 0 1 0 1 1 1 0 1 0 0 encryption key

  0 1 0 0 1 1 0 0 1 0 0 0 bitwise difference = message
- Provably secure if the key is as long as the message

## Safety of key distribution

- if Eve (eavesdropper) gets hold of the encryption key, she may read the encrypted message
- Eve can read the message without Bob's knowledge of the interception of the message

**Quantum cryptography, quantum key distribution (QKD)**

- Quantum mechanics can be used to distribute a provably secure private key over a public channel
- This key can be used for classical private-key cryptography
- The presence of an eavesdropper can be detected

## Quantum cryptography; BB84 protocol

- Alice sends a string of quantum states to Bob:

  she randomly switches between the encodings $0, 1 = |0\rangle, |1\rangle$ and $0, 1 = |+\rangle, |-\rangle$ (encoding is secret)
- Bob measures the qubits:

  he randomly switches between measurements in the $|0\rangle, |1\rangle$ and $|+\rangle, |-\rangle$ basis (measurement basis is secret)
- Alice announces her choice of basis via a public channel
- Alice and Bob keep only bits obtained in the same basis (the bit values are secret)
- Alice and Bob compare the values of a randomly chosen subset of bits via a public channel
- if all compared bits agree, the channel is safe and the remaining secret bits can be used as a private key

**Why can Alice and Bob conclude the channel is safe?**

- to obtain the key, Eve intercepts the qubits on the way to Bob, measures them, and sends a new qubit with her measurement result to Bob
- Eve guesses the basis because she does not know Alice's random choice of basis

  $\Rightarrow$ in 50% of the cases, Eve measures in the wrong basis
- if Bob happens to measure in the same basis as Alice, he gets the wrong bit in 50% of the cases

  $\Rightarrow$ Eve unavoidably corrupts $\approx$ 25% of the bits

## Quantum cryptography; E91 protocol

- BB84 based purely on quantum randomness, no entanglement
- Bob and Alice share the initial singlet state

$$|\psi\rangle = |\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- Both make measurements on their half of the pair.
- Using the same basis, the results are random but perfectly anticorrelated
- Using different bases, they can verify that the state was entangled (Bell test). If Eve inferred, the entanglement would be gone.

## Bell test

### An example of a Bell test based on (CHSH)[1] inequality

- Alice and Bob perform measurements of physical properties of their particles e.g., spin component $\sigma_{\vec{n}}$ along an axis $\vec{n}$
- measurements are performed in two randomly chosen settings
  - $A_1$, $A_2$ for Alice
  - $B_1$, $B_2$ for Bob

  e.g., different directions $\vec{n}$
- outcome of a measurement is $\{a_1, a_2, b_1, b_2\} \in \{+1, -1\}$ e.g., $\{\uparrow, \downarrow\}$ wrt. the chosen direction $\vec{n}$

[1] Clauser-Horne-Shimony-Holt

## Bell test

### An example of a Bell test based on (CHSH) inequality

- Consider $\mathcal{C} = (a_1 + a_2)b_1 + (a_1 - a_2)b_2$
- Either $a_1 + a_2 = 0 \Rightarrow a_1 - a_2 = \pm 2$
- Or $a_1 - a_2 = 0 \Rightarrow a_1 + a_2 = \pm 2$
  $\Rightarrow \mathcal{C} = \pm 2$

### Local theory

- particle is in a certain state before the measurement (no correlations between measurements $A$ and $B$)
- $p(a_1, a_2, b_1, b_2)$ is probability to measure
  $A_1 = a_1, A_2 = a_2, B_1 = b_1, B_2 = b_2$

$$|\langle \mathcal{C} \rangle| = |\sum_{a_1, a_2, b_1, b_2} p(a_1, a_2, b_1, b_2) \times \mathcal{C}| \leq \langle |\mathcal{C}| \rangle = 2$$

$\Rightarrow$ classically (or for non-entangled states) one expects $|\langle \mathcal{C} \rangle| \leq 2$

## Quantum mechanics

- $\mathcal{C} \to \hat{\mathcal{C}}$, operator!
- Measure spin $\hat{\sigma}_{\vec{n}}$ along a general direction $\vec{n}(\theta, \varphi)$
- Choose $\varphi = 0$ for simplicity: $\hat{\sigma}_\theta = \sin(\theta)\hat{\sigma}_x + \cos(\theta)\hat{\sigma}_z$ and

$$\hat{\sigma}_\alpha \otimes \hat{\sigma}_\beta = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix} \otimes \begin{pmatrix} \cos(\beta) & \sin(\beta) \\ \sin(\beta) & -\cos(\beta) \end{pmatrix}$$

- Take a *Bell state* $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

$$\langle\beta_{00}|\hat{\sigma}_\alpha \otimes \hat{\sigma}_\beta|\beta_{00}\rangle = \cos(\alpha - \beta)$$

- remember classically: $\mathcal{C} = (a_1 + a_2)b_1 + (a_1 - a_2)b_2$
  Compute $\left\langle\hat{\mathcal{C}}\right\rangle = \langle(\hat{\sigma}_{\alpha_1} + \hat{\sigma}_{\alpha_2}) \otimes \hat{\sigma}_{\beta_1}\rangle + \langle(\hat{\sigma}_{\alpha_1} - \hat{\sigma}_{\alpha_2}) \otimes \hat{\sigma}_{\beta_2}\rangle$

## Quantum mechanics

- Take a *Bell state* $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

$$\langle\beta_{00}|\hat{\sigma}_\alpha \otimes \hat{\sigma}_\beta|\beta_{00}\rangle = \cos(\alpha - \beta)$$

$$\left\langle \hat{\mathcal{C}} \right\rangle = \cos(\alpha_1 - \beta_1) + \cos(\alpha_2 - \beta_1) + \cos(\alpha_1 - \beta_2) - \cos(\alpha_2 - \beta_2)$$

- Choose angles $\alpha_1 = 0$, $\alpha_2 = \frac{\pi}{2}$, $\beta_1 = \frac{\pi}{4}$, and $\beta_2 = -\frac{\pi}{4}$:
  $\Rightarrow |\langle\mathcal{C}\rangle| = 2\sqrt{2}$ violates CHSH inequality
- Violation of the inequality $|\langle\mathcal{C}\rangle| \leq 2$ demonstrates entanglement
  Check that for a non-entangled state (for example $|00\rangle$) the CHSH inequality holds.

**Necessary criteria for quantum computation (DiVincenzo criteria):**

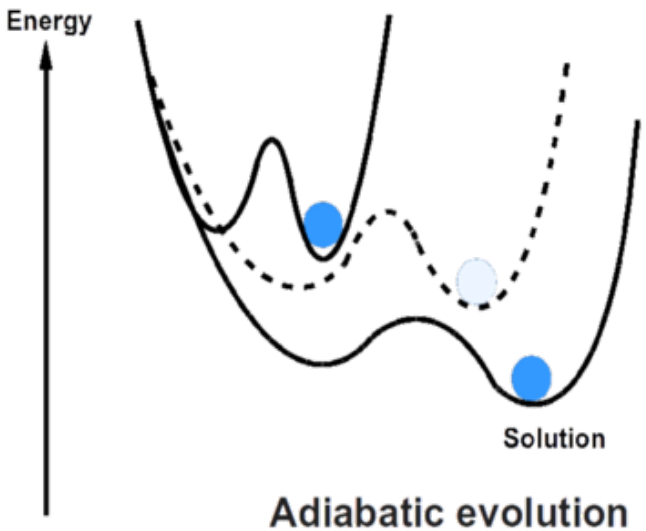
1. scalability: build a large (e.g., $10^9$) number of qubits
2. initialization: prepare a well-defined initial quantum state
3. long coherence time: in comparison to the gate time
4. universal set of quantum gates: to construct all possible quantum gates
5. measurement procedure: to get the result of a calculation

## Quantum annealers; quantum adiabatic computation

- Hamiltonian dependent on a control parameter $g \in [0, 1]$:

$$\hat{H}(g) = (1 - g)\hat{H}_{\mathrm{i}} + g\hat{H}_{\mathrm{f}}$$

- ground state of $\hat{H}_{\mathrm{i}}$ is easily accessible
- ground state of $\hat{H}_{\mathrm{f}}$ encodes the solution of a hard computational problem (typically some optimization problems)

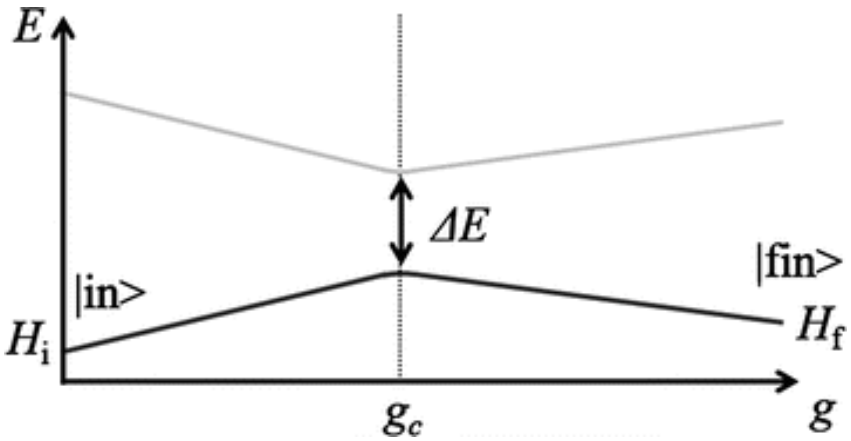



Based on *quantum adiabatic theorem*:

A physical system remains in its instantaneous eigenstate if a given perturbation is acting on it slowly enough and if there is a gap between the eigenvalue and the rest of the Hamiltonian's spectrum.

## Quantum annealers; quantum adiabatic computation

- alternative architecture: no gates applied,
  just slow tuning $g = 0 \to 1$ (for example magnetic field)
- *obstacle*: vanishing gaps in the energy spectrum




For vanishing $\Delta E$ the adiabatic evolution would have to be infinitely slow!

$\Delta E \to 0$ occurs typically in a critical point $g = g_c$ of a *quantum phase transition*

- The first commercially available quantum computer is an annealer (D-Wave, 2015)

# Overview of different qubit realizations

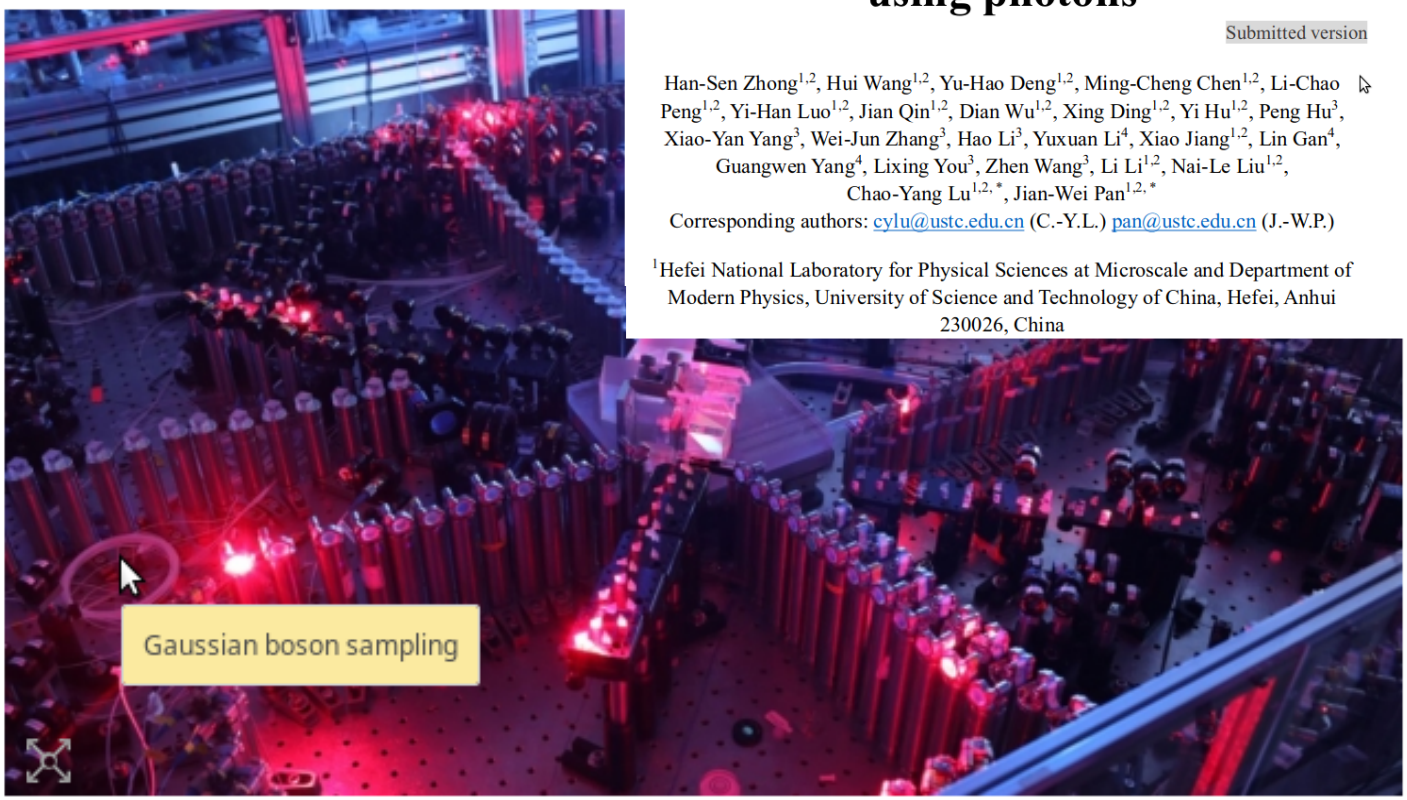
- spins in large molecules + NMR Cory et al., Gershenfeld and Chuang
- ions in electromagnetic traps Cirac and Zoller
- neutral atoms in optical lattices Jaksch et al.
- optical quantum computing Knill, Laflamme, and Milburn
- $^{31}$P donor atoms in silicon Kane
- electron spins in semiconductor quantum dots Loss and DiVincenzo
- superconducting electrical circuits
  - flux qubit Mooij et al., Ioffe et al.
  - charge qubit Schön et al., Averin
  - phase qubit Martinis et al.
  - transmon qubit Koch et al.
- topological qubits Kitaev et al.

# Breaking News: Quantum supremacy in boson sampling?

QUANTUM COMPUTING | RESEARCH UPDATE

## Quantum advantage demonstrated using Gaussian boson sampling

03 Dec 2020 Hamish Johnston




Quantum advantage: the Gaussian boson sampling experiment at the University of Science and Technology of China. (Courtesy: Chao-Yang Lu)

## Quantum computational advantage using photons

Submitted version

Han-Sen Zhong[1,2], Hui Wang[1,2], Yu-Hao Deng[1,2], Ming-Cheng Chen[1,2], Li-Chao Peng[1,2], Yi-Han Luo[1,2], Jian Qin[1,2], Dian Wu[1,2], Xing Ding[1,2], Yi Hu[1,2], Peng Hu[3], Xiao-Yan Yang[3], Wei-Jun Zhang[3], Hao Li[3], Yuxuan Li[4], Xiao Jiang[1,2], Lin Gan[4], Guangwen Yang[4], Lixing You[3], Zhen Wang[3], Li Li[1,2], Nai-Le Liu[1,2], Chao-Yang Lu[1,2,*], Jian-Wei Pan[1,2,*]

Corresponding authors: cylu@ustc.edu.cn (C.-Y.L.) pan@ustc.edu.cn (J.-W.P.)

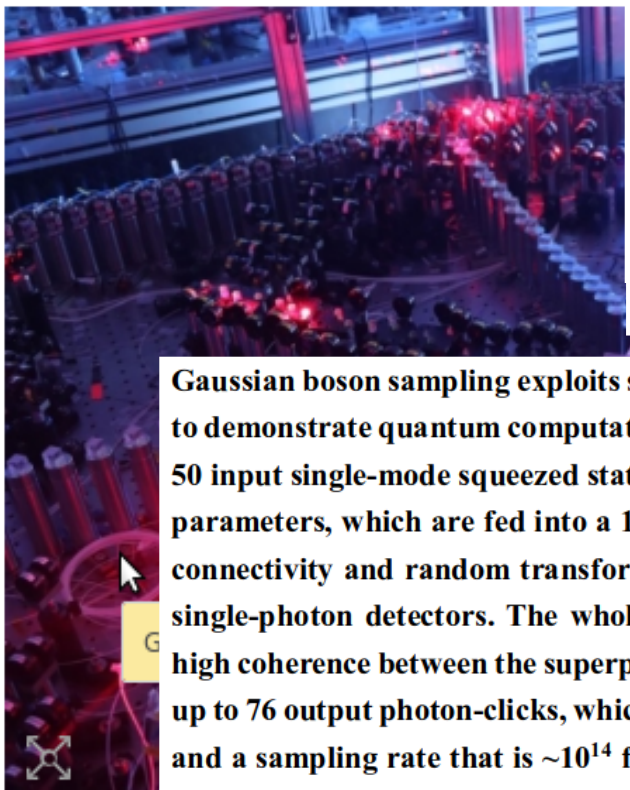
[1]Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

# Breaking News: Quantum supremacy in boson sampling?

QUANTUM COMPUTING | RESEARCH UPDATE

## Quantum advantage demonstrated using Gaussian boson sampling

03 Dec 2020 Hamish Johnston



Quantum ad
Technology

## Quantum computational advantage using photons

Submitted version

Han-Sen Zhong[1,2], Hui Wang[1,2], Yu-Hao Deng[1,2], Ming-Cheng Chen[1,2], Li-Chao Peng[1,2], Yi-Han Luo[1,2], Jian Qin[1,2], Dian Wu[1,2], Xing Ding[1,2], Yi Hu[1,2], Peng Hu[3], Xiao-Yan Yang[3], Wei-Jun Zhang[3], Hao Li[3], Yuxuan Li[4], Xiao Jiang[1,2], Lin Gan[4], Guangwen Yang[4], Lixing You[3], Zhen Wang[3], Li Li[1,2], Nai-Le Liu[1,2], Chao-Yang Lu[1,2,*], Jian-Wei Pan[1,2,*]

Corresponding authors: cylu@ustc.edu.cn (C.-Y.L.) pan@ustc.edu.cn (J.-W.P.)

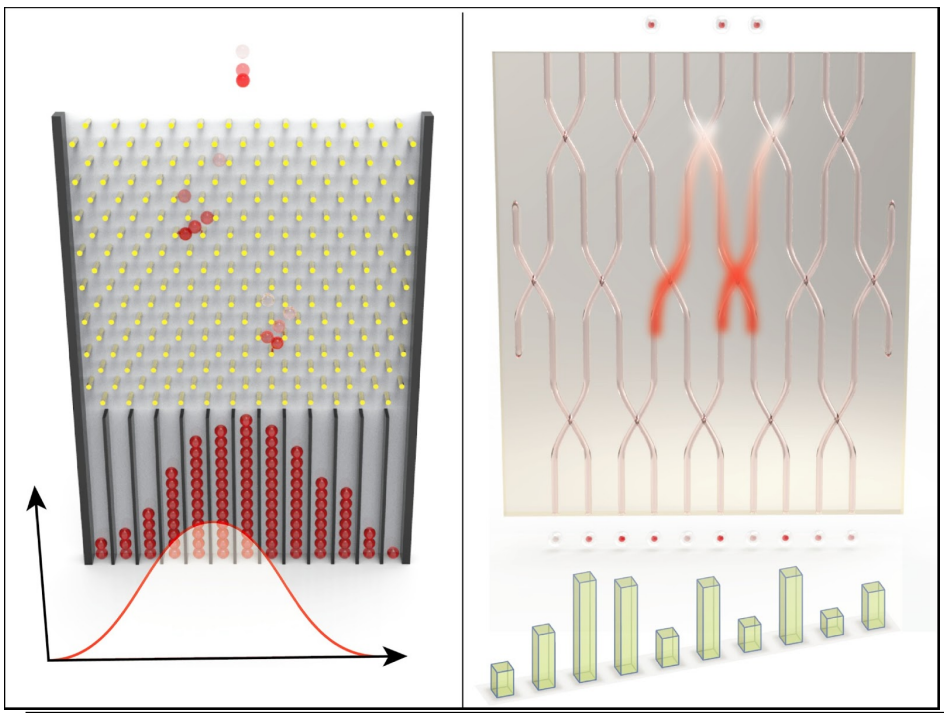
[1]Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

**Gaussian boson sampling exploits squeezed states to provide a highly efficient way to demonstrate quantum computational advantage. We perform experiments with 50 input single-mode squeezed states with high indistinguishability and squeezing parameters, which are fed into a 100-mode ultralow-loss interferometer with full connectivity and random transformation, and sampled using 100 high-efficiency single-photon detectors. The whole optical set-up is phase-locked to maintain a high coherence between the superposition of all photon number states. We observe up to 76 output photon-clicks, which yield an output state space dimension of ~$10^{30}$ and a sampling rate that is ~$10^{14}$ faster than using the state-of-the-art simulation strategy and supercomputers. The obtained samples are validated against various hypotheses including using thermal states, distinguishable photons, and uniform distribution.**

## Optical quantum computing

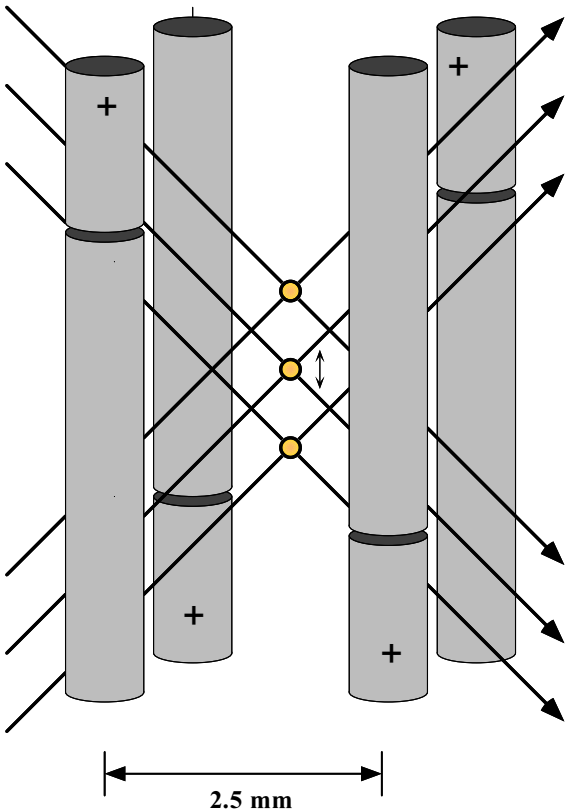
- photons carry information, manipulation only through optical elements (e.g. beamsplitters, mirrors)

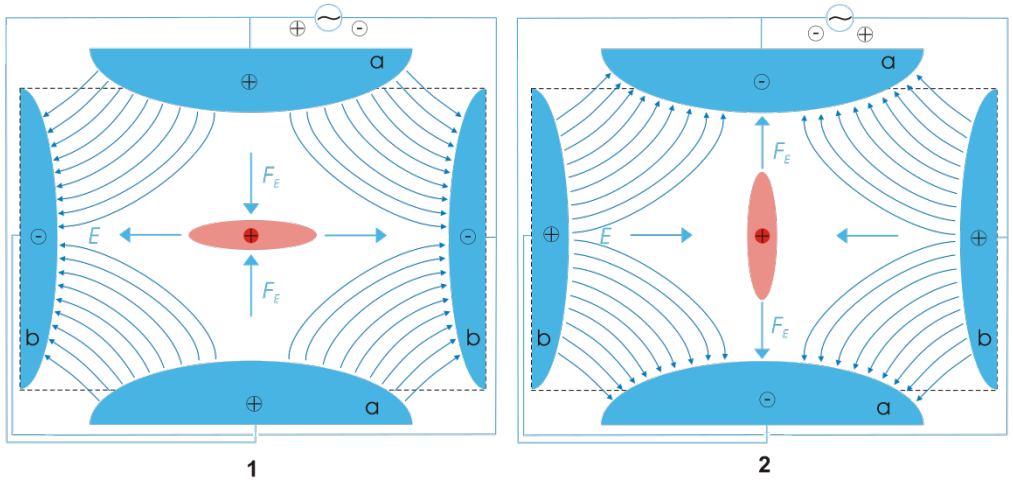
  photons in channels $\leftrightarrow$ qubits, beamsplitters $\leftrightarrow$ superpositions
- in principle optical elements can encode any qubit gate $\rightsquigarrow$ universal computing
- **boson sampling**: non-universal but classically difficult



*task*: model probability that the photodetector in the *n*th outcome channel clicks

# Ions in electromagnetic traps

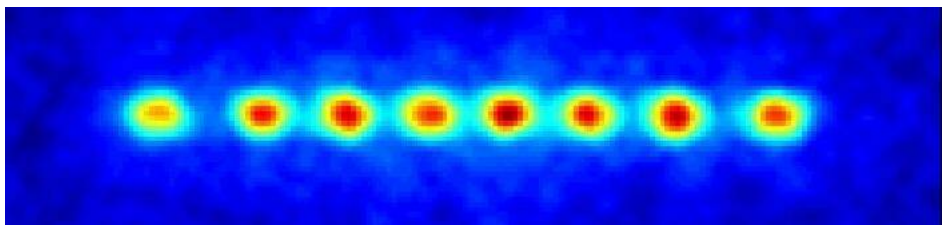



- $N \lesssim 50$ ions (e.g., $^9$Be, $^{40}$Ca) in a harmonic electromagnetic trap (Paul trap)
- qubit is encoded in two long-lived (metastable) internal electron states $\{|g\rangle, |e\rangle\}$ of an ion
- single-qubit gates: laser beams induce transitions $|g\rangle \leftrightarrow |e\rangle$

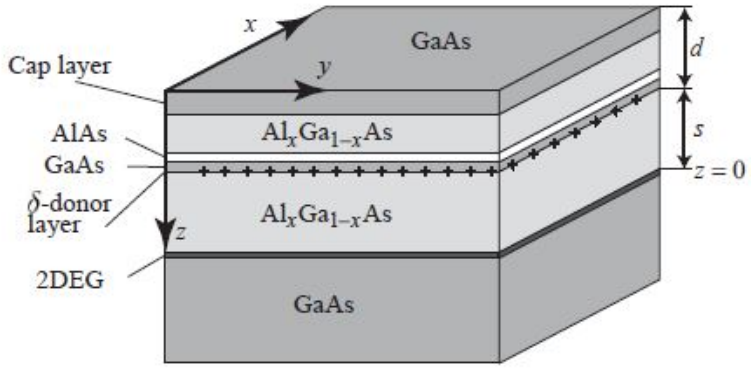
## Ions in electromagnetic traps

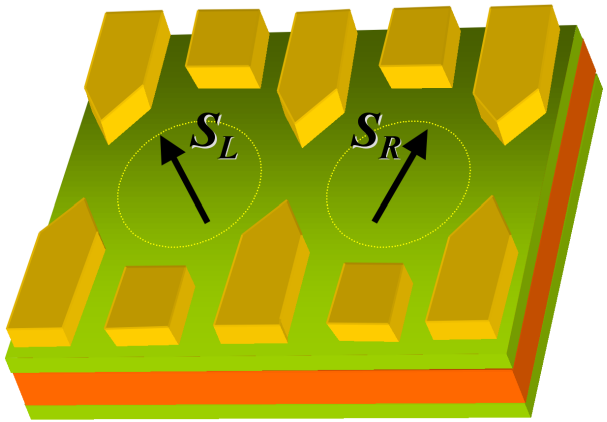
- multi-qubit gates: ions repel each other $\Rightarrow$ phonon-like oscillation modes along the chain, useful for qubit-qubit interaction
- readout: drive transition from $|e\rangle$ to a short-lived state $|r\rangle$, detect photon emitted during relaxation $|r\rangle \rightarrow |e\rangle$ through CCD camera.



- pros: long coherence times $(10 - 100s)$, individual addressing, high fidelity gates, generation of entanglement in the chain
- cons: relatively slow gates $(\approx \mu s)$, poor scaling properties

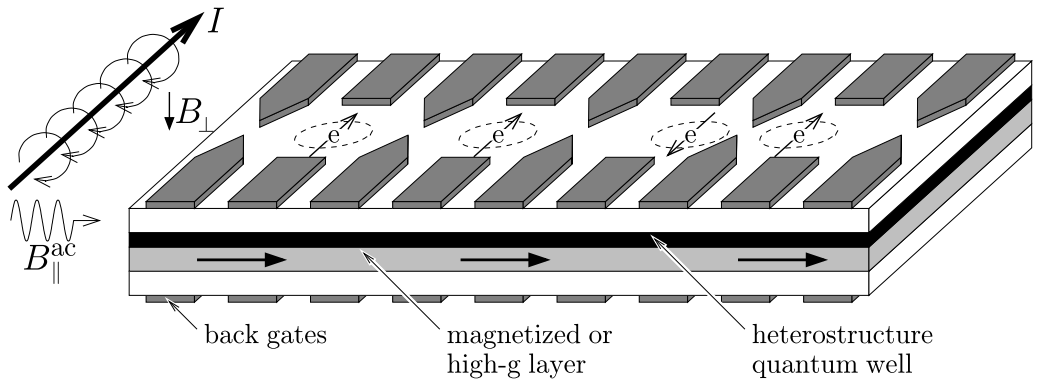
# Electron spins in semiconductor quantum dots




- A two-dimensional electron gas (2DEG) can be realized in semiconductor heterostructures
- 2DEG can be structured by gate electrodes (negative potential repels electron gas under the electrode)
- quantum dots may be formed which contain a small number or only a single electron

# Electron spins in semiconductor quantum dots




- $B_\perp$ defines quantization axis of the spins and energy splitting
- single-qubit gates using $B_\parallel(t)$
- two-qubit gates using exchange interaction between spins of neighboring dots $\hat{H}_{\rm ex} = \sum_{\langle i,j\rangle} J_{ij} \hat{S}_i \cdot \hat{S}_j$, coupling strength $J_{ij}$ depends on gate voltages
- Control of magnetic field on scales $\mu$m is difficult: use combination of external magnetic field and electric gating
- readout: sensitive charge detector

  (single-electron transistor or quantum point contact)

## Superconducting electrical circuits

- superconductors are macroscopic quantum systems that show infinite conductivity below a critical temperature $T_c$
- microscopic picture: electrons form Cooper pairs
- superconducting phase is characterized by a macroscopic wavefunction $\Psi = \sqrt{n_s} e^{i\varphi}$
- two superconductors separated by an insulating oxide barrier form a tunnel junction or Josephson junction
- Josephson effect: even in the absence of a voltage across the Josephson junction, a supercurrent $I$ can flow through it:

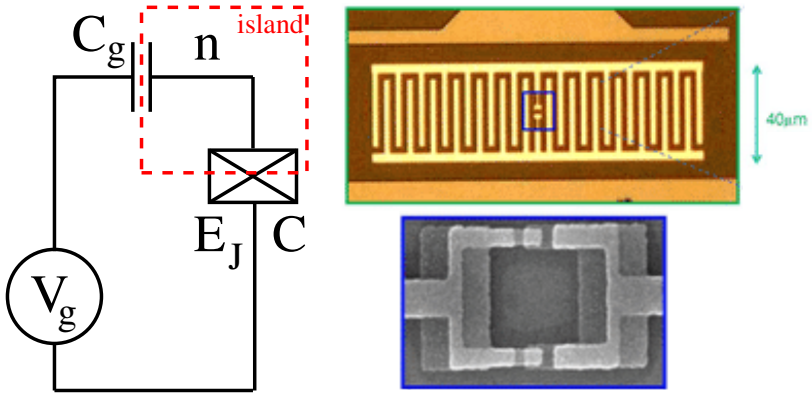
$$I = I_c \sin(\varphi_{\text{left}} - \varphi_{\text{right}})$$

- Hamiltonian describing this current:

$$\hat{H} = -E_J \cos(\varphi_{\text{left}} - \varphi_{\text{right}})$$

- non-linear, non-dissipative electrical element

# Charge and transmon qubit

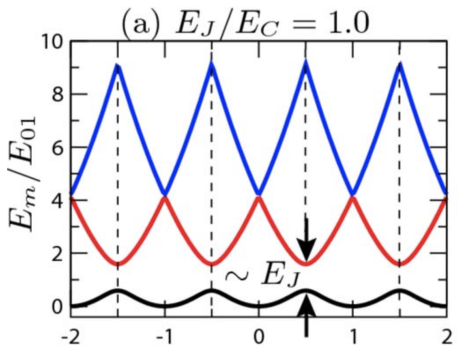



$$\hat{H} = E_C(\hat{n} - n_g)^2 - E_J \cos(\hat{\varphi})$$

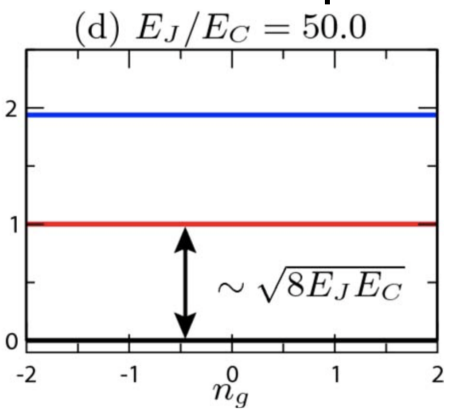
$E_C$: charging energy of the island,
$\hat{n}$: number of Cooper pairs

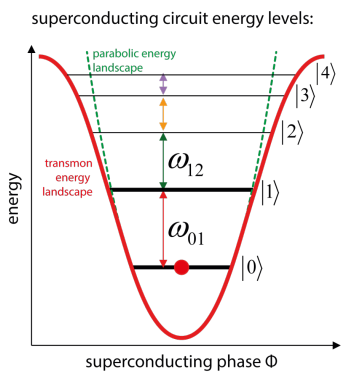
$n_g \propto V_g$

**Charge qubit**: $E_C \gg E_J$
superpositions of 0 or 1 Cooper pairs on the island




**Transmon**: $E_C \ll E_J$
Lowest eigenstates in an anharmonic potential



# Review of different platforms

| | supercond. qb | electron spin qb | trapped ions | NMR |
|---|---|---|---|---|
| footprint | $\approx \mu$m | 0.1 $\mu$m | spacing 10 $\mu$m | mm |
| **scalability** | yes | yes | costly | no |
| energy gap | $1-20$ GHz | $1-10$ GHz | $10^5-10^6$ GHz | MHz |
| temperature | 10 mK | 100 mK | $\mu$K | 300 K |
| single-qubit gate time $\tau_1$ | $\approx$ ns | 10 ns | $\mu$s | ms |
| two-qubit gate time $\tau_2$ | $10-50$ ns | 0.2 $\mu$s | 100 $\mu$s | 10 ms |
| **coherence time** $T_2$ | $10-100\mu$s | ms $-$ s | 0.1 s | 10 s |
| 1-qubit gate fidelity (%) | $98-99.9$ | $98-99.9$ | $99.1-99.9999$ | $98-99$ |
| 2-qubit gate fidelity (%) | $96-99.4$ | $89-96$ | $97-99.9$ | 98 |
| **initialization** | yes | yes | yes | ensemble |
| **readout fidelity** (%) | 99 | 97 | 99.99 | ensemble |

Xiang et al., Rev. Mod. Phys. **85**, 623 (2013)
Resch et al., arXiv:1905.07240 (2019)
Keith et al., Phys. Rev. X **9**, 041003 (2019)

$5\,\mathrm{GHz} \approx 250\,\mathrm{mK}$