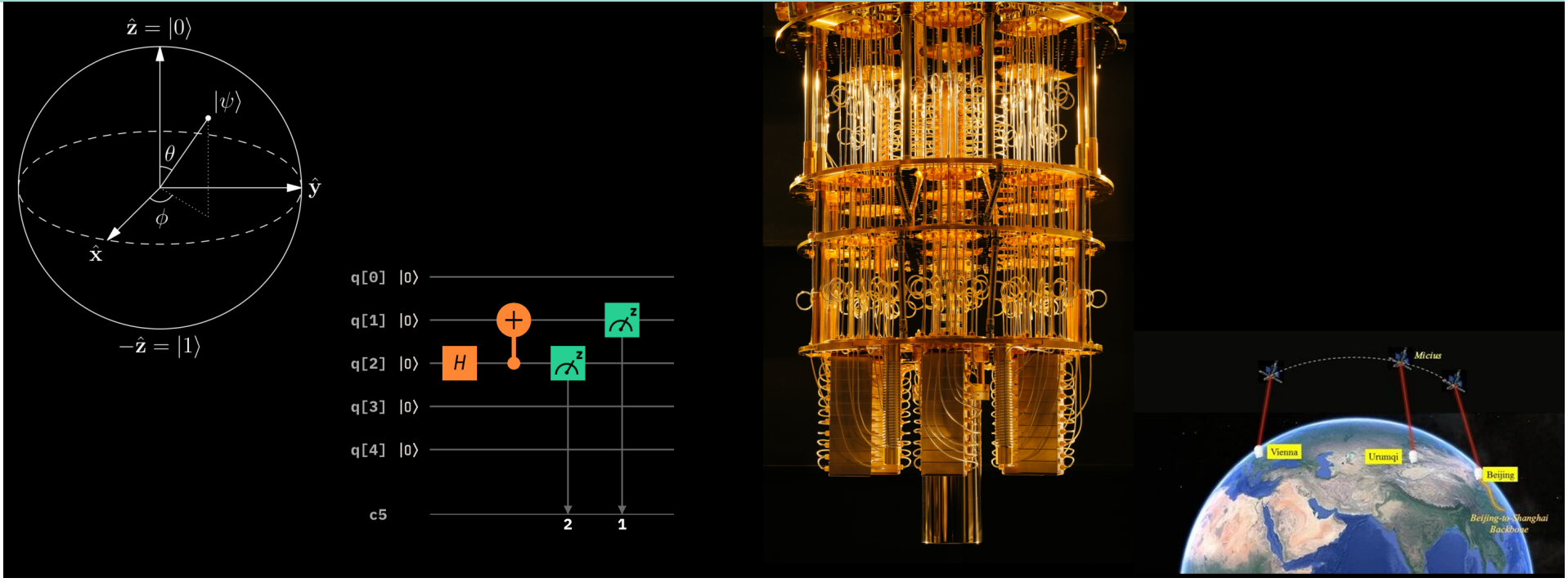
University of Basel

Quantum Computing and Quantum Communication

Martin Koppenhöfer
https://www.quantumtheory-bruder.physik.unibas.ch/



Overview over the lectures

- elements of quantum information
  - quantum bits (qubits)
  - superposition and entanglement
  - gates and universal computation
  - Deutsch algorithm
- no-cloning theorem, quantum error correction, teleportation
- quantum cryptography, Bell tests, 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, and N. Lörch

Classical private-key cryptography

One-time pad method

- 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

Classical private-key cryptography

Problem: 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 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

Quantum cryptography

BB84 protocol

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 get's the wrong bit in 50% of the cases

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

Bell test

Overview

One of these two intuitions about our world is wrong:

Realism: Physical properties have definite values which exist independent of observation

Locality: Performing a measurement at position x does not influence an instantaneous measurement at $y \neq x$

- Way to check this statement: perform a Bell test
- There are many different Bell tests
- Here: Clauser-Horne-Shimony-Holt (CHSH) inequality

Bell test

Clauser-Horne-Shimony-Holt (CHSH) inequality

- Charlie prepares two particles and sends one to Alice and one to Bob
  e.g., electrons
- 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 $\vec{n}$

Bell test

Clauser-Horne-Shimony-Holt (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 realistic theory

- particle is in a certain state before the measurement
- $p(a_1, a_2, b_1, b_2)$ 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 $|\langle \mathcal{C} \rangle| \leq 2$

Bell test

Clauser-Horne-Shimony-Holt (CHSH) inequality

Quantum mechanics

- 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 $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

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

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

- 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

Physical implementation of quantum computers

Di-Vincenzo criteria

Necessary criteria for quantum computation:

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

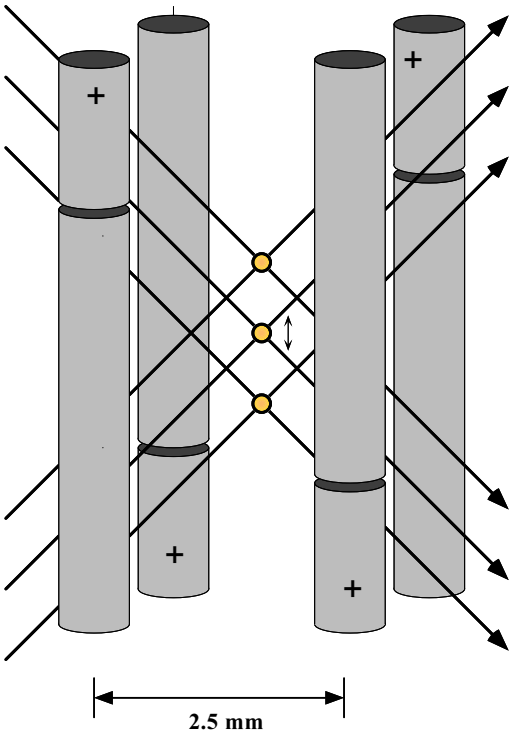
Physical implementation of quantum computers

Overview of quantum-computing platforms

- 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.

Physical implementation of quantum computers

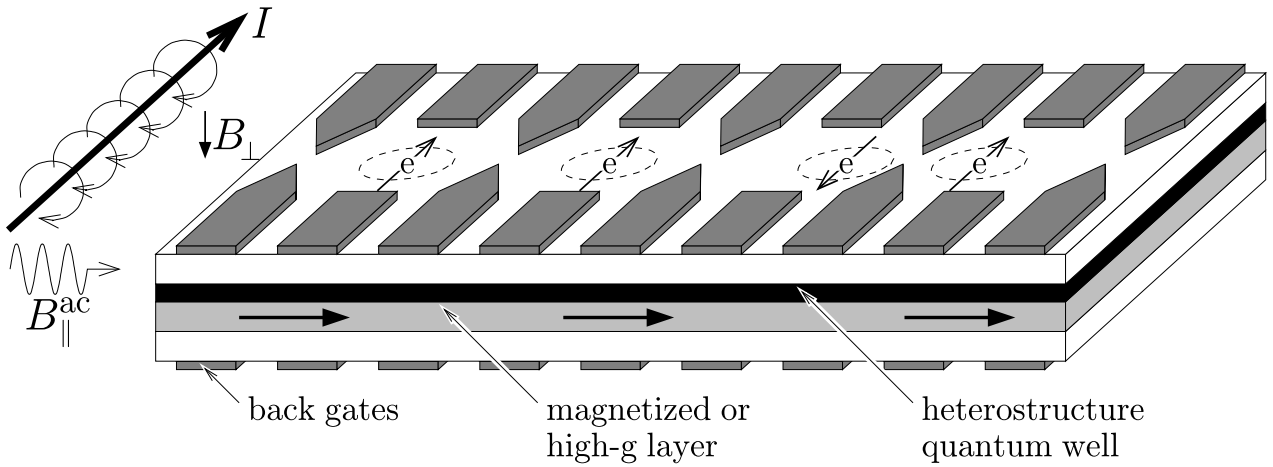
Ions in electromagnetic traps



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

Physical implementation of quantum computers

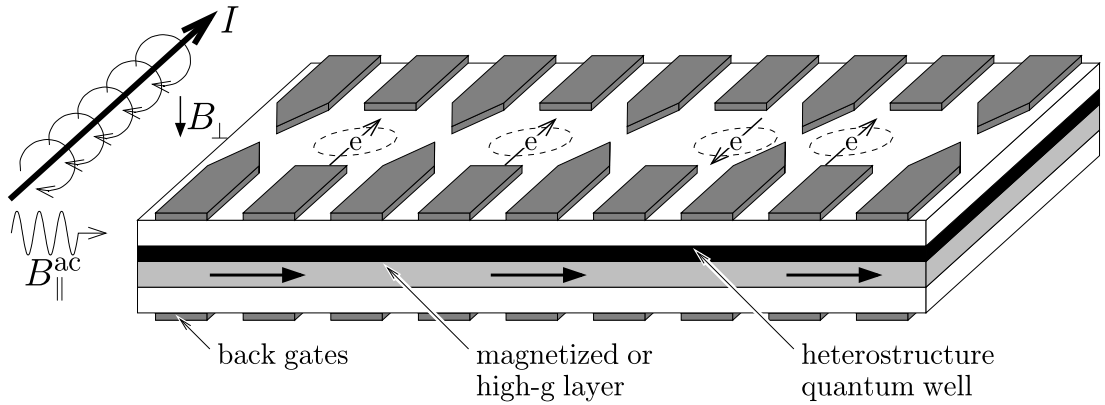
Electron spins in semiconductor quantum dots



- 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

Physical implementation of quantum computers

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 μm scales is difficult: use combination of external magnetic field and electric gating
- readout: single-electron transistor or quantum point contact

Physical implementation of quantum computers

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:

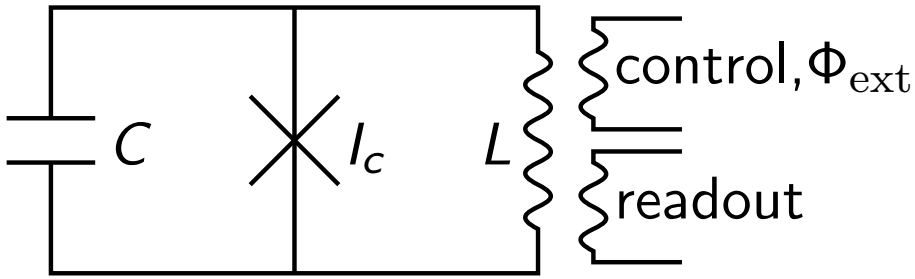
$$I = I_c \sin(\varphi_{\text{left}} - \varphi_{\text{right}})$$

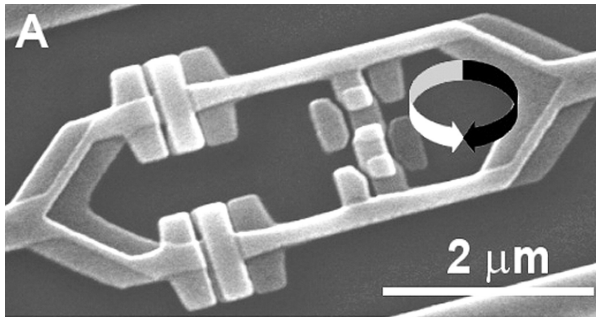
- Hamiltonian describing this current:

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

Physical implementation of quantum computers

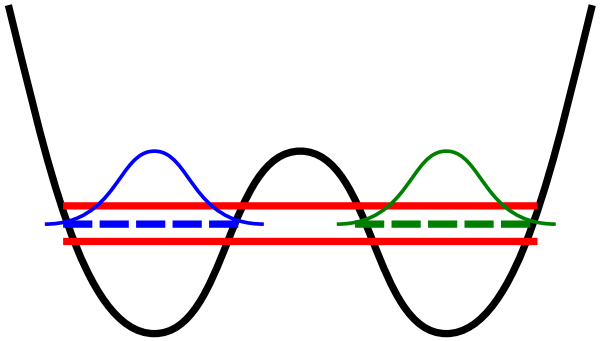
Superconducting electrical circuits: Flux and phase qubit



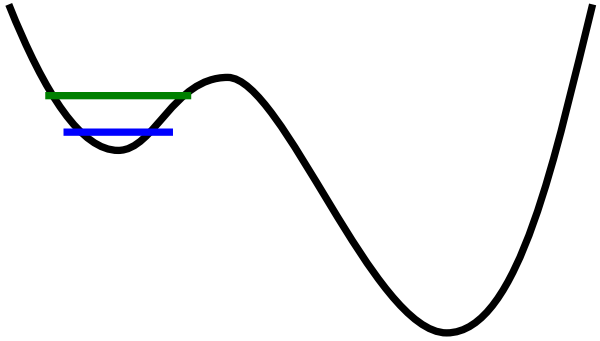


$$\hat{H} = \frac{\hat{Q}^2}{2C} - E_J \cos(\hat{\varphi}) - \frac{(\hat{\varphi} - \Phi_{\text{ext}})^2}{2L}$$

Flux qubit: $\Phi_{\text{ext}} = \frac{\Phi_0}{2}$
superpositions of $|\circlearrowleft\rangle$ and $|\circlearrowright\rangle$

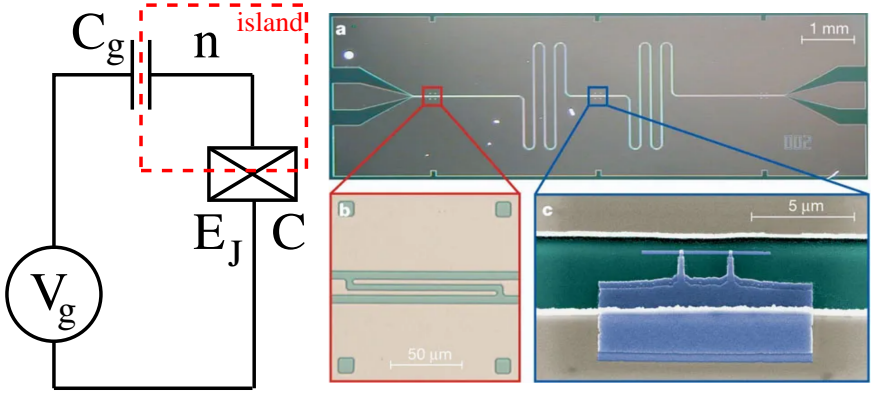


Phase qubit: $\Phi_{\text{ext}} \approx \Phi_0 = \frac{h}{2e}$
states $|0\rangle$ and $|1\rangle$ in same well



Physical implementation of quantum computers

Superconducting electrical circuits: Charge and transmon qubit

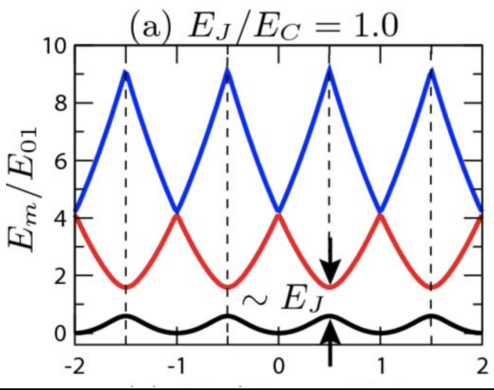


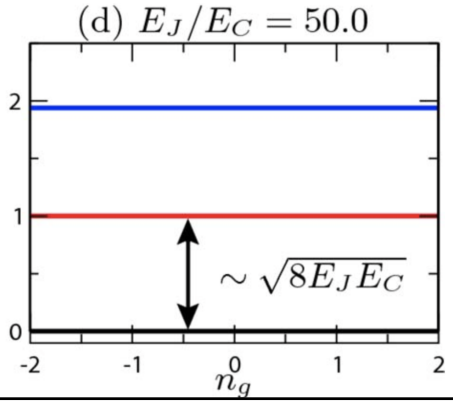
control & readout

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

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

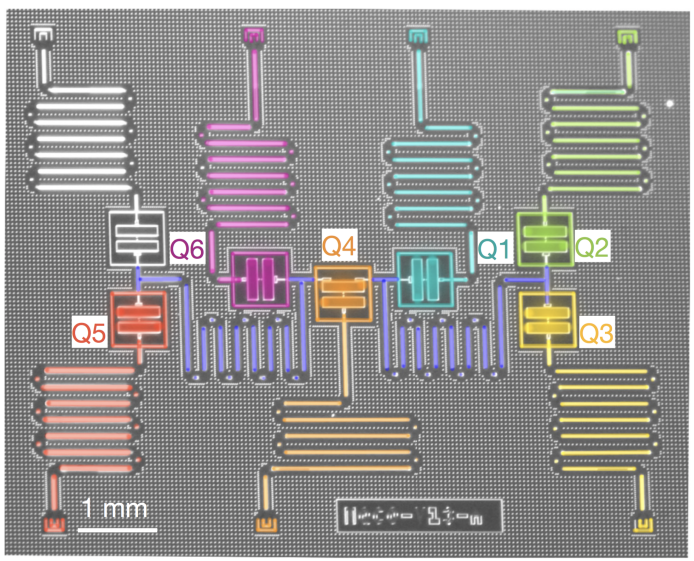




Physical implementation of quantum computers

Review of different platforms

	superconducting qubit	electron spin qubit	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	$10\,mK$	$100\,mK$	μK	$300\,K$
single-qubit gate time τ_1	$\approx ns$	$10\,ns$	μs	ms
two-qubit gate time τ_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)]

$$5\,GHz \approx 250\,mK$$

Physical implementation of quantum computers

Operating a quantum processor