Materiały i przyrządy półprzewodnikowe

Wykład 13:
Wstęp do informatyki kwantowej.
Komputer kwantowy.

Paweł Szumniak,

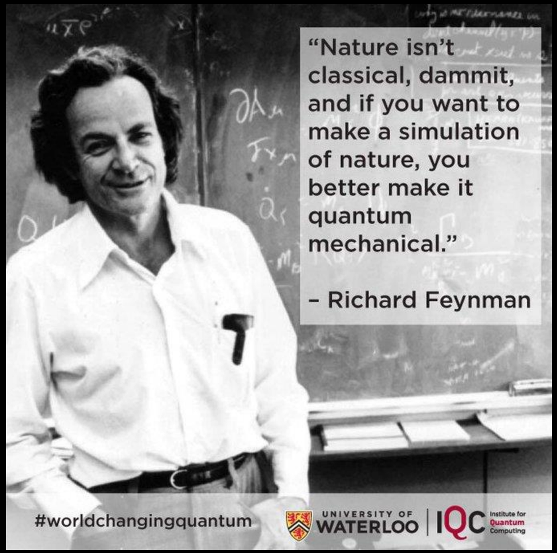
Paweł Wójcik

Plan wykładu:

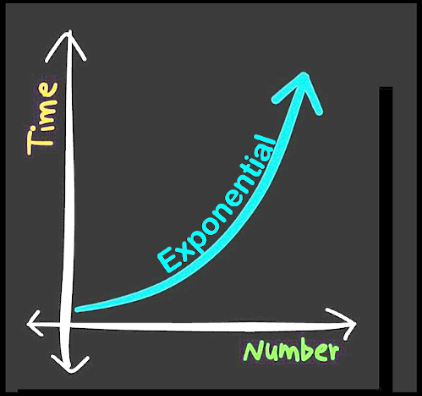
1. Definicja kubitu, sfera Blocha
2. Bramki jednokubitowe
3. Stany dwukubitowe, stany splątane, bramki dwukubitowe
4. Fizyczna realizacja kubitu
5. Przemysłowe badania nad komputerem kwantowym

Motywacja

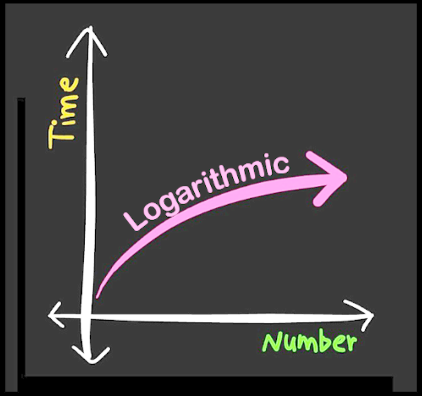
1. Symulacja układów kwantowych



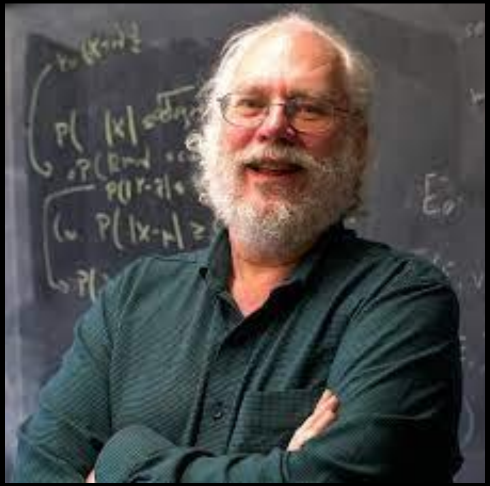
2. Kryptografia kwantowa, łamanie kody RSA (faktoryzacja liczb pierwszych)



CLASSICAL



QUANTUM



3. Kwantowa sztuczna inteligencja

Informatyka kwantowa

1. Symulacje kwantowe
2. Obliczenia kwantowe
3. Kryptografia kwantowa
4. Sieci kwantowe i internet kwantowy
5. Algorytmy kwantowe (Shora, Deutsha, Grovera, itd.)

Teorie matematyczne

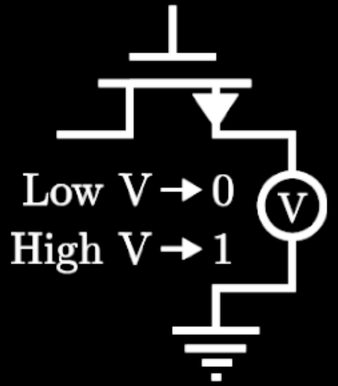
Realizacja fizyczna

Bit vs. kubit

Jednostka informacji kwantowej – Bit kwantowy

Bit klasyczny

$0 \qquad 1$



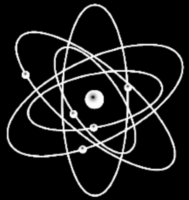
Bit kwantowy - kubit

$$|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

$$\alpha_0, \alpha_1 \in \mathbb{C} \qquad |\alpha_0|^2 + |\alpha_1|^2 = 1$$

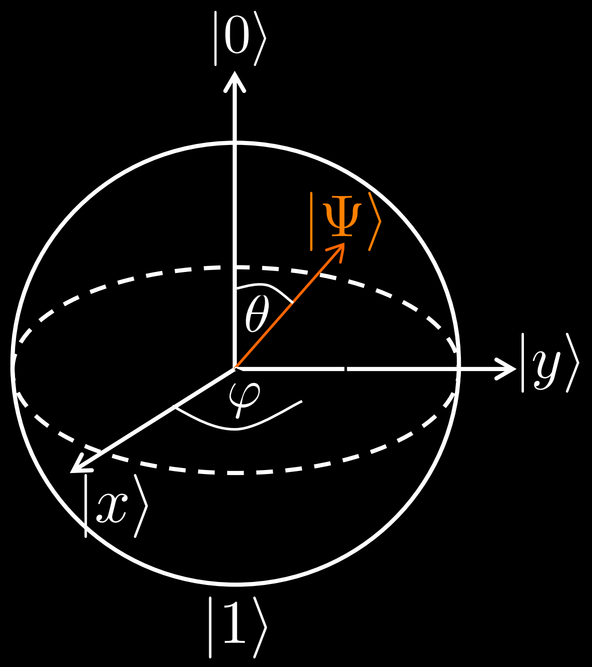
$$|\Psi\rangle \sim e^{i\varphi}|\Psi\rangle \qquad \hat{H}|\Psi\rangle = E|\Psi\rangle$$

$$E_1 \qquad |1\rangle = |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$



$$E_0 \qquad |0\rangle = |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Sfera Blocha



Wektor stanu

$$|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \qquad \alpha_0, \alpha_1 \in C$$

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

$$|\langle 0|\Psi\rangle|^2 = |\alpha_0|^2$$

$$|\langle 1|\Psi\rangle|^2 = |\alpha_1|^2$$

Na sferze Blocha

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

$$\varphi \in [0,2\Pi) \qquad \theta \in [0,\Pi)$$

$$|x\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$$

$$|y\rangle = \frac{1}{2}(|0\rangle + i|1\rangle)$$

Wyprowadzenie na tablicy

Jednokubitowe bramki logiczne

Jednokubitowe kwantowe bramki logiczne reprezentowane są przez unitarny operator U (macierz 2x2) i reprezentują złożenia macierzy obrotu na sferze Blocha

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad UU^\dagger = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix} = I \qquad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \qquad U|0\rangle = a|0\rangle + b|1\rangle$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = c \begin{pmatrix} 1 \\ 0 \end{pmatrix} + d \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \qquad U|1\rangle = c|0\rangle + d|1\rangle$$

Operator obrotu

$$R_{\vec{n}}(\theta) \equiv \exp\left(-i\vec{n}\cdot\vec{\sigma}\frac{\theta}{2}\right) = I\cos(\theta/2) - i(\vec{n}\cdot\vec{\sigma})\sin(\theta/2)$$

Dowód:

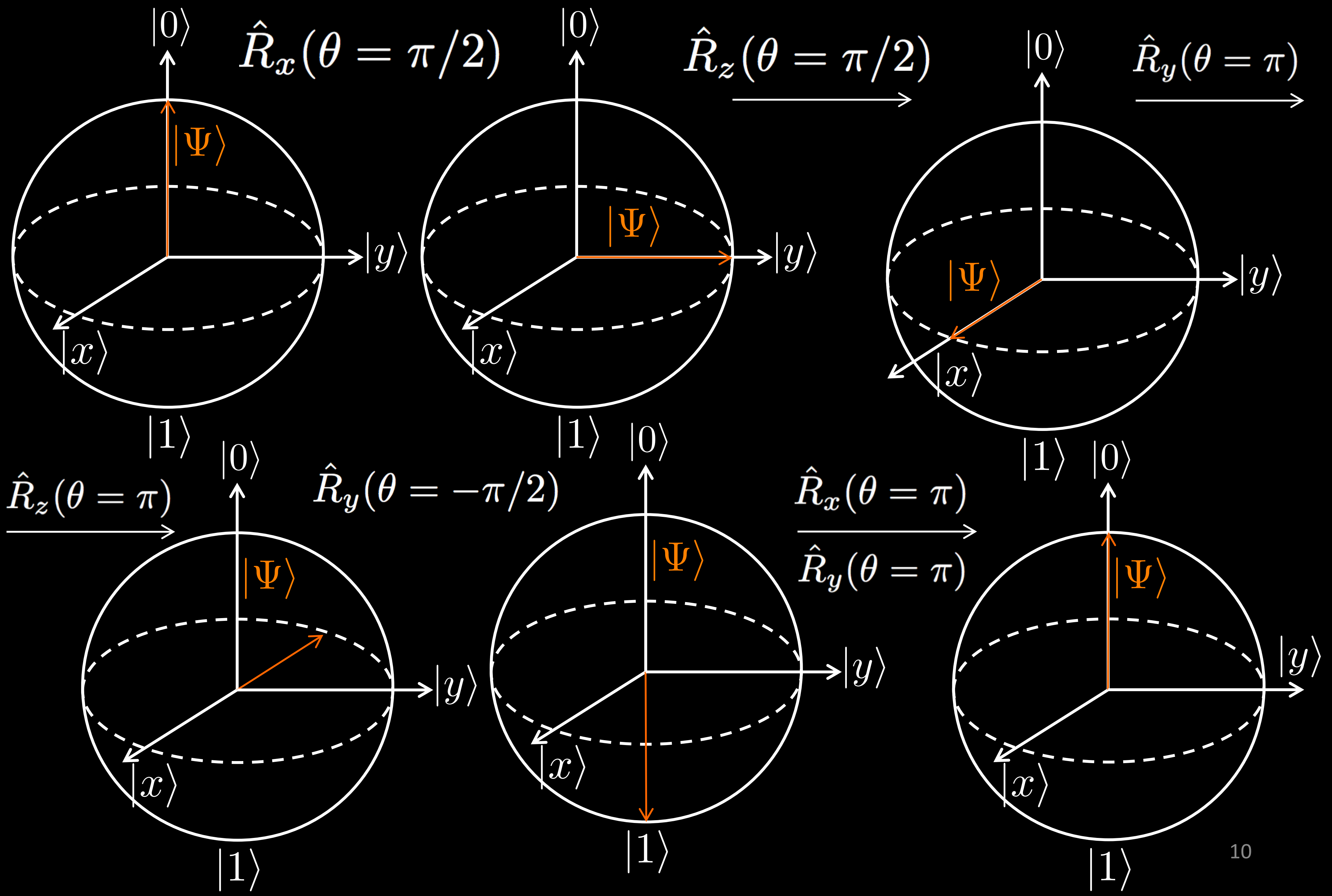
$$\begin{aligned} e^{ia(\hat{n}\cdot\vec{\sigma})} &= \sum_{k=0}^{\infty}\frac{i^k\left[a\left(\hat{n}\cdot\vec{\sigma}\right)\right]^k}{k!} \\ &= \sum_{p=0}^{\infty}\frac{(-1)^p(a\hat{n}\cdot\vec{\sigma})^{2p}}{(2p)!} + i\sum_{q=0}^{\infty}\frac{(-1)^q(a\hat{n}\cdot\vec{\sigma})^{2q+1}}{(2q+1)!} \\ &= I\sum_{p=0}^{\infty}\frac{(-1)^p a^{2p}}{(2p)!} + i(\hat{n}\cdot\vec{\sigma})\sum_{q=0}^{\infty}\frac{(-1)^q a^{2q+1}}{(2q+1)!} \end{aligned}$$

Obroty na sferze Blocha

$$R_x(\theta) = \exp(-iX\theta/2) = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_y(\theta) = \exp(-iY\theta/2) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_z(\theta) = \exp(-iZ\theta/2) = \begin{pmatrix} \exp(-i\theta/2) & 0 \\ 0 & \exp(i\theta/2) \end{pmatrix}$$


$\hat{R}_x(\theta = \pi/2)$
$\hat{R}_z(\theta = \pi/2)$
$\hat{R}_y(\theta = \pi)$
$\hat{R}_z(\theta = \pi)$
$\hat{R}_y(\theta = -\pi/2)$
$\hat{R}_x(\theta = \pi)$
$\hat{R}_y(\theta = \pi)$
$|0\rangle$
$|1\rangle$
$|x\rangle$
$|y\rangle$
$|\Psi\rangle$

Przykłady bramek jednokubitowych

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \sigma_x = \mathrm{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

Bramka Hudamarda

$$\sqrt{X} = \sqrt{\mathrm{NOT}} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{pmatrix}$$

Rejestry dwukubitowe

Stan kwantowy

$$|\Psi\rangle = c_0|0\rangle_A|0\rangle_B + c_1|0\rangle_A|1\rangle_B + c_2|1\rangle_A|0\rangle_B + c_3|1\rangle_A|1\rangle_B$$

$$|\Psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ |01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},\ |10\rangle = |1\rangle \otimes |0\rangle = 0\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix},\ |11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$|\langle 00|\Psi\rangle|^2 = |c_0|^2,\ |\langle 01|\Psi\rangle|^2 = |c_1|^2,\ |\langle 10|\Psi\rangle|^2 = |c_2|^2,\ |\langle 11|\Psi\rangle|^2 = |c_3|^2$$

Warunek normalizacji

$$\langle\Psi|\Psi\rangle = |c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2$$

Rejestry dwukubitowe – stany rozkładalne

$$|\Psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

$$|\Psi_a\rangle = a_0|0\rangle + a_1|1\rangle, \;\; |\Psi_b\rangle = b_0|0\rangle + b_1|1\rangle$$

$$|\Psi\rangle \stackrel{?}{=} |\Psi_a\rangle \otimes |\Psi_b\rangle,$$

$$|\Psi_a\rangle \otimes |\Psi_a\rangle = (a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) =$$

$$= a_0 b_0|00\rangle + a_0 b_1|01\rangle + a_0 b_1|10\rangle + a_1 b_1|11\rangle,$$

Rejestry dwukubitowe – stany nierozkładalne, stany Bella (splątane)

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

Dowód:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

$$|\Psi_a\rangle_A \otimes |\Psi_b\rangle_B = (a_0|0\rangle_A + a_1|1\rangle_A) \otimes (b_0|0\rangle_B + b_1|1\rangle_B)$$

$$|\Psi_a\rangle_A \otimes |\Psi_b\rangle_B = (a_0b_0|0\rangle_A|0\rangle_B + a_0b_1|0\rangle_A|1\rangle_B + a_1b_0|1\rangle_A|0\rangle_B + a_1b_1|1\rangle_A|1\rangle_B),$$

$$a_0b_0 = \frac{1}{\sqrt{2}},\ a_0b_1 = 0,\ a_1b_0 = 0,\ a_1b_1 = \frac{1}{\sqrt{2}}$$

Sprzeczny warunek => stan nierozkładalny

Stany splątane – konsekwencje fizyczne

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

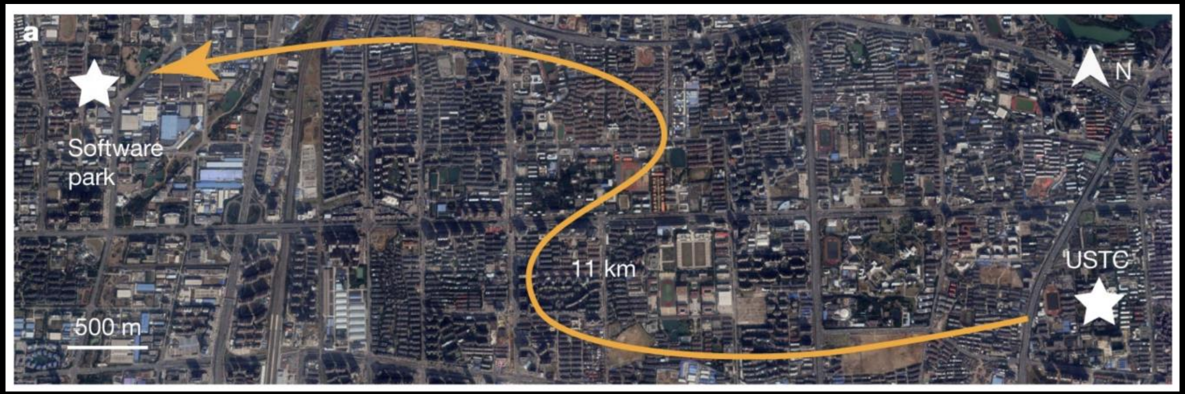
Pomiar cząstki A, otrzymujemy stan: $|0\rangle$

Pomiar stanu odległej cząstki B, pokaże zawsze, że jest ona w stanie $|0\rangle$

Pomiar cząstki A, otrzymujemy stan: $|1\rangle$

Pomiar stanu odległej cząstki B, pokaże zawsze, że jest ona w stanie $|1\rangle$

Pomiar stanu jednej cząstki A determinuje stan drugiej cząstki B, pomimo, że są one odległei nie oddziałują między sobą



Entanglement of two quantum memories via fibres over dozens of kilometres

Yong Yu, Fei Ma, Xi-Yu Luo, Bo Jing, Peng-Fei Sun, Ren-Zhou Fang, Chao-Wei Yang, Hui Liu, Ming-Yang Zheng, Xiu-Ping Xie, Wei-Jun Zhang, Li-Xing You, Zhen Wang, Teng-Yun Chen, Qiang Zhang, Xiao-Hui Bao & Jian-Wei Pan

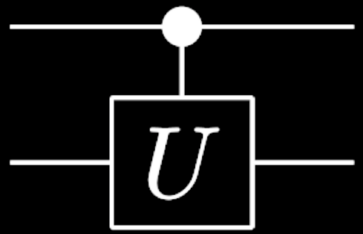
Nature **578**, 240–245 (2020) | Cite this article

Bramki dwukubitowe

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$|a, b\rangle \mapsto |a, a \oplus b\rangle$$

$$\mathrm{C}_U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}$$



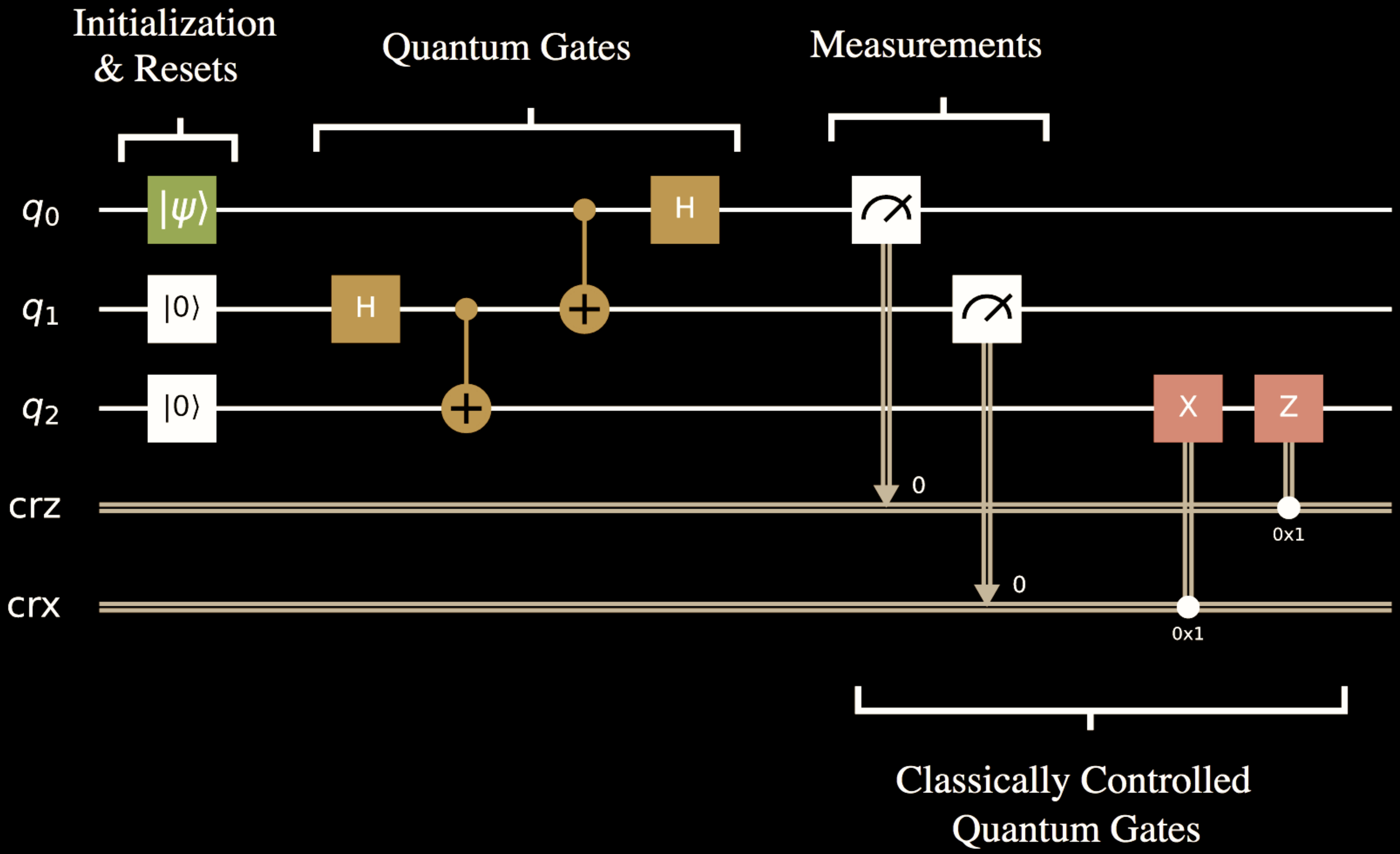
$$|00\rangle \mapsto |00\rangle$$

$$|01\rangle \mapsto |01\rangle$$

$$|10\rangle \mapsto |1\rangle C_U|0\rangle = |1\rangle(u_{00}|0\rangle + u_{01}|1\rangle),$$

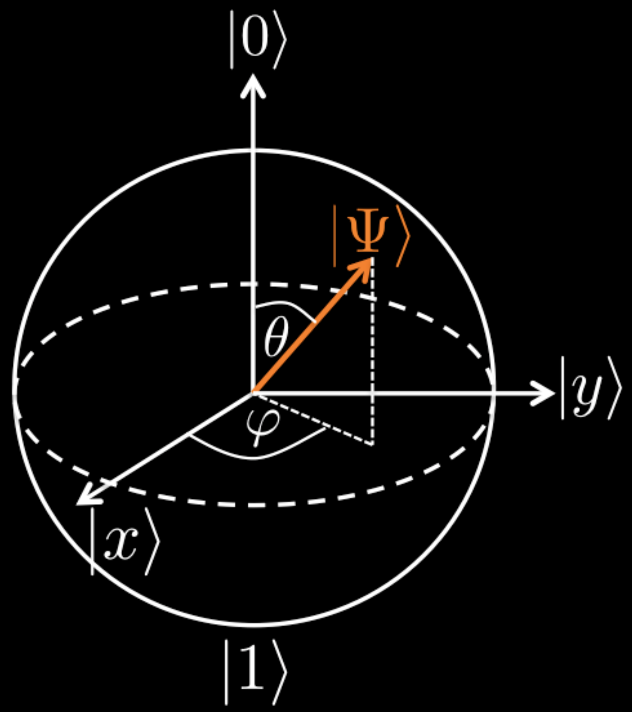
$$|11\rangle \mapsto |1\rangle C_U|0\rangle = |1\rangle(u_{10}|0\rangle + u_{11}|1\rangle),$$

Obwód kwantowy - przykład



Kryteria fizycznej implementacji komputerów kwantowych: DiVicenzo (2000)

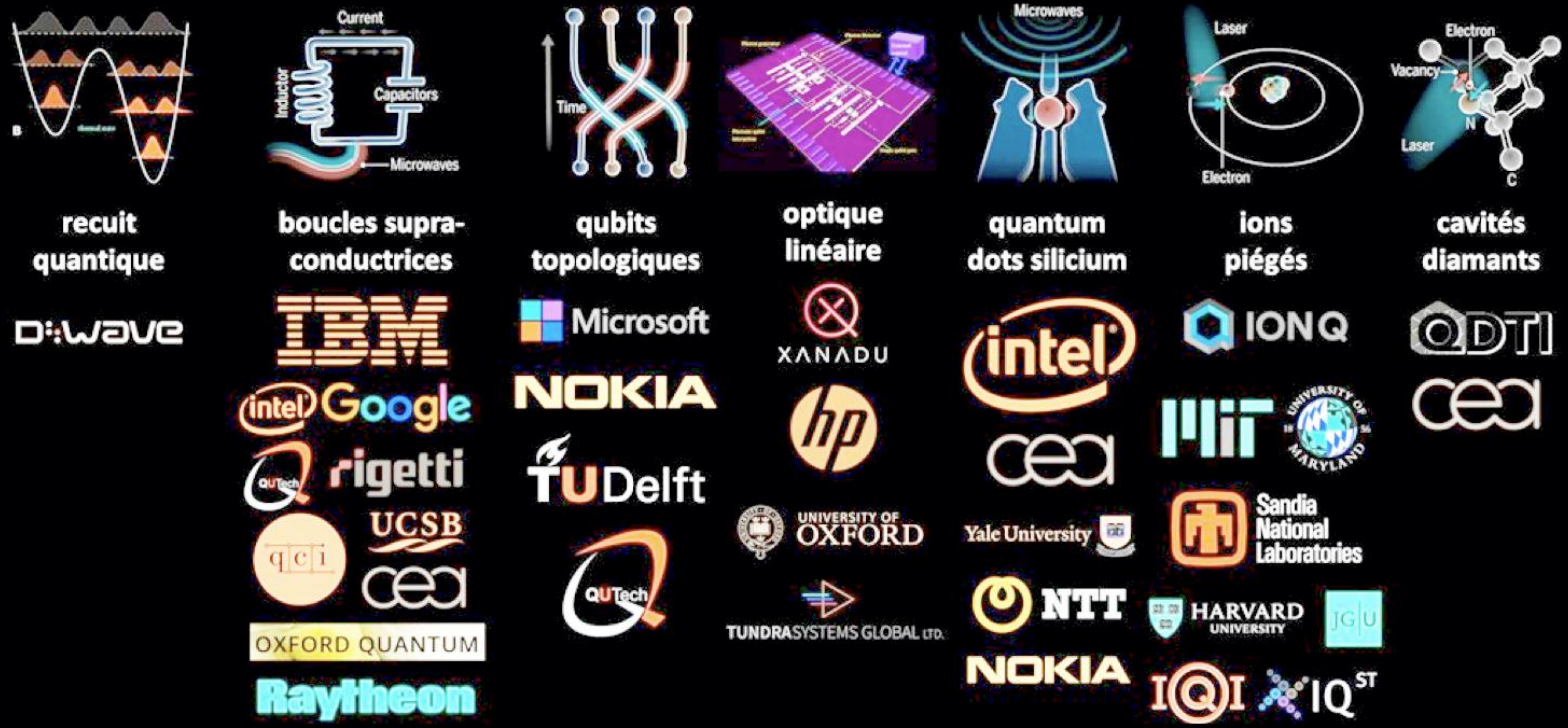
1. Skalowalny układ fizyczny z dobrze zdefiniowanymi kubitami
2. Możliwość ustawiania stanów kubitów na początku algorytmu kwantowego w precyzyjnym stanie (inicjalizacja)
3. Długie czasy koherencji (w porównaniu z czasami działa bramek kwantowych)
4. Uniwersalny zestaw bramek kwantowych
5. Musi istnieć wydajna procedura służąca do pomiaru stanu kubitów na końcu realizacji zadanego algorytmu kwantowego



Pozostałe dwa kryteria konieczne do realizacji kwantowej komunikacji

1. Możliwość konwertowania informacji kwantowej ze stacjonarnych kubitów do mobilnych kubitów
2. Możliwość przesyłania mobilnych kubitów między zadanymi miejscami

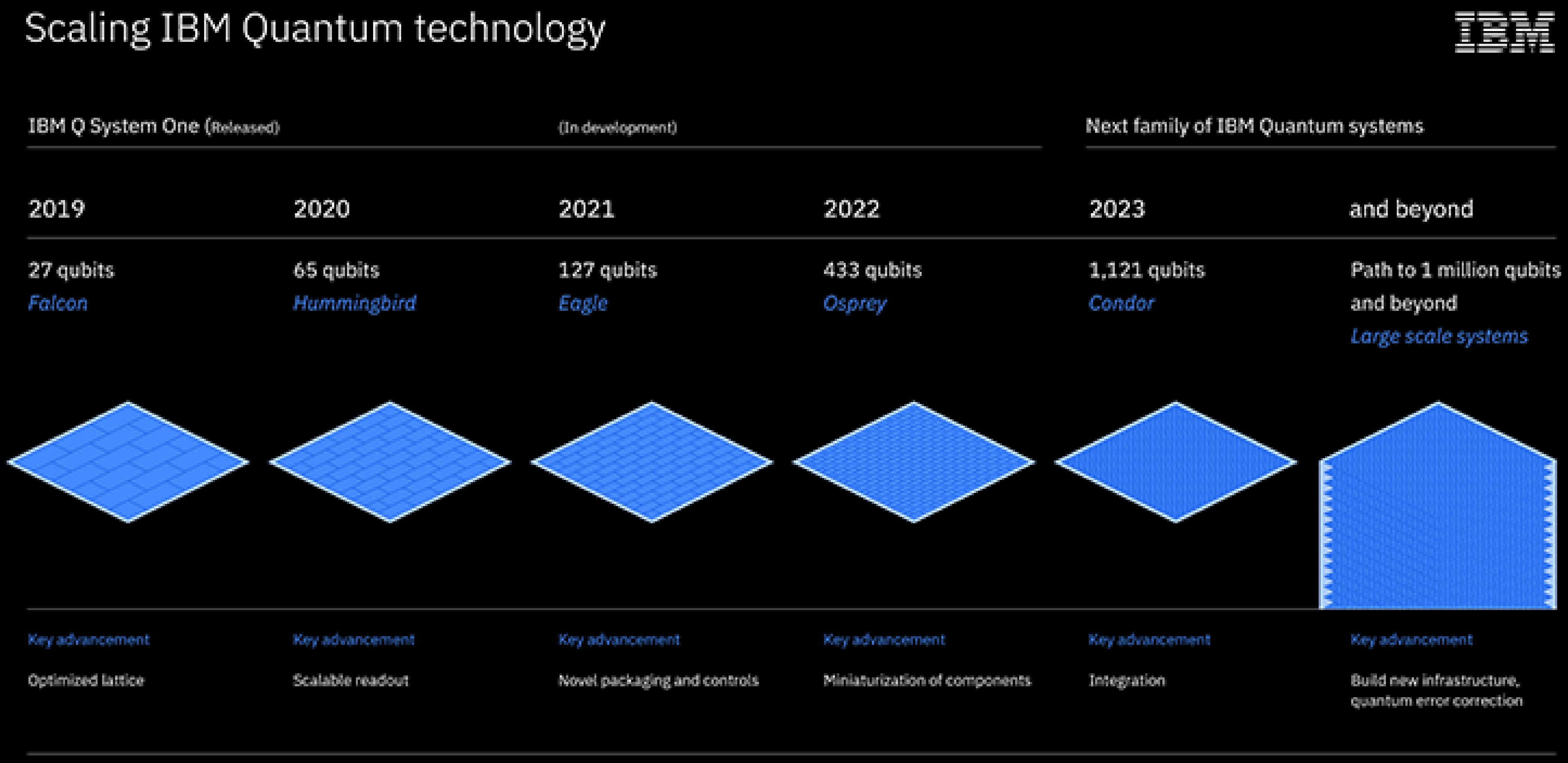
Fizyczna realizacja kubitów



Fizyczna realizacja kubitów

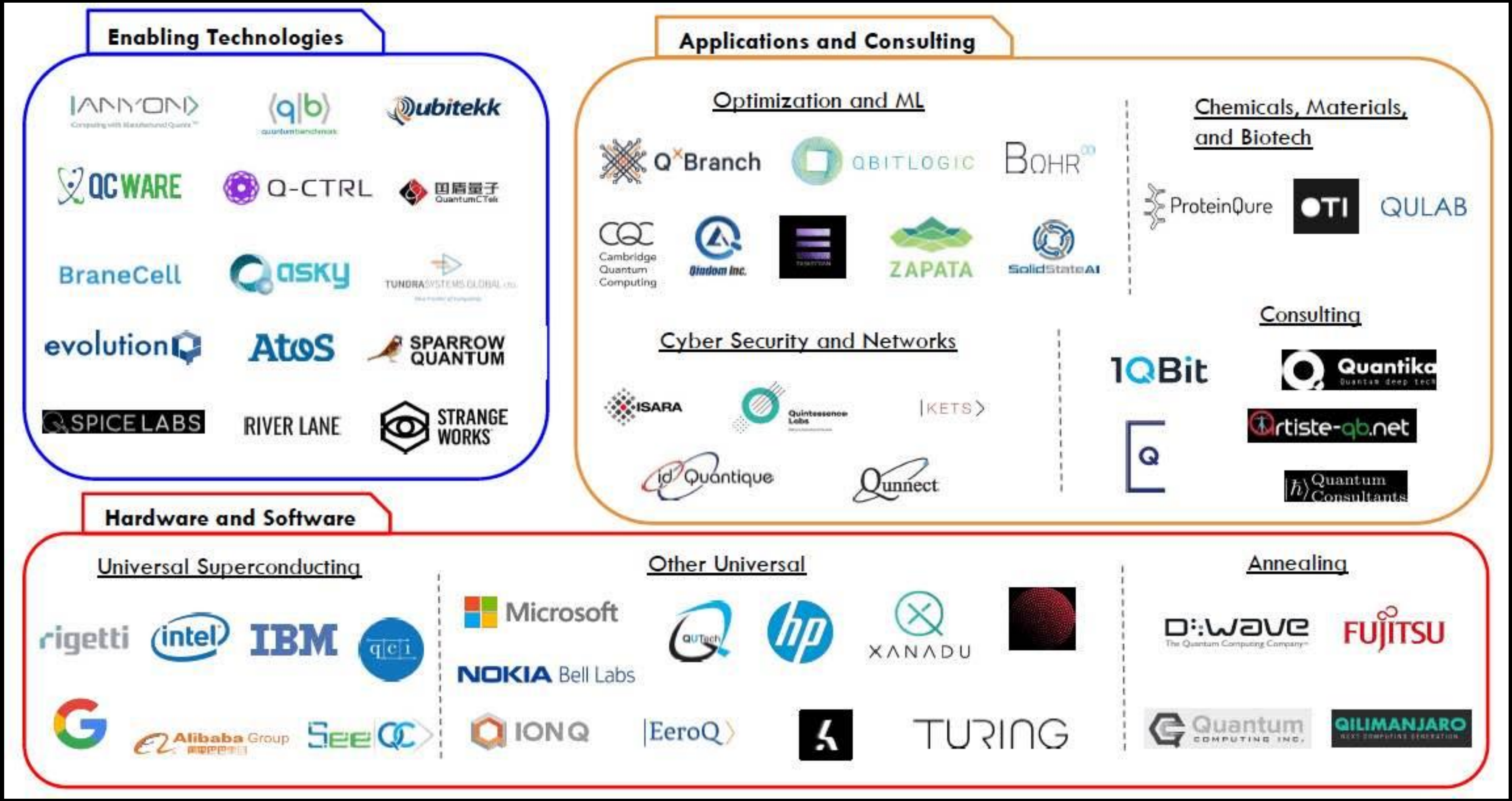
Komputer IBM 2019

Fizyczna realizacja kubitów



20 milion qubits to break RSA 2048, for gate error 10^{-3}

Fizyczna realizacja kubitów



Układy NMR

Zależne od czasu równanie Schroedingera

$$i\hbar \frac{d}{dt}|\Psi(t)\rangle = \hat{H}(t)|\Psi(t)\rangle$$

Dla pojedynczego kubitu (układ dwustanowy)

$$|\Psi(t)\rangle = a(t)|0\rangle + b(t)|1\rangle = \begin{pmatrix} a(t) \\ b(t) \end{pmatrix}$$

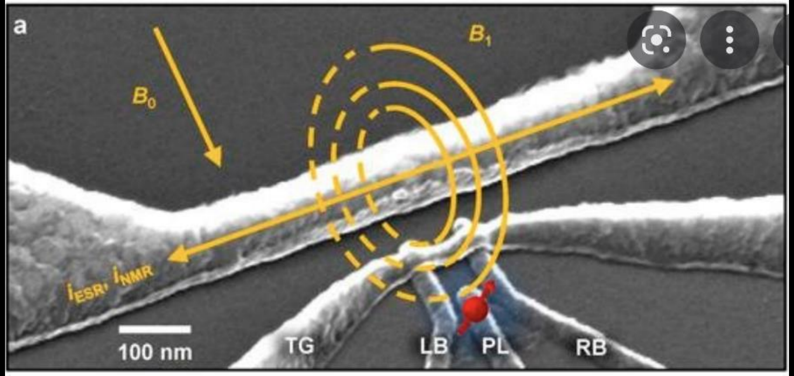
Układ równań różniczkowych zwyczajnych na a(t) i b(t)

$$\begin{cases} i\hbar\dot{a}(t) = h_{11}(t)a(t) + h_{12}(t)b(t) \\ i\hbar\dot{b}(t) = h_{21}(t)a(t) + h_{22}(t)b(t) \end{cases}$$

Układy NMR – oscylacje Rabiego

Hamiltonian Zeemana

$$\hat{H} = -\vec{\mu} \cdot \vec{B} \qquad \vec{\mu} = \frac{1}{2}\gamma_p \vec{\sigma}, \quad \gamma_p = 5.59 \frac{q_p \hbar}{2m_p}$$



$$\vec{B}_1(t) = (\cos(\omega t), -\sin(\omega t), 0)$$

$$\vec{B}_0(t) = (0, 0, B_0)$$

$$\vec{B}(t) = (\cos(\omega t), -\sin(\omega t), B_0)$$

$$\hat{H}(t) = -\frac{1}{2}\gamma_p B_0 \sigma_z - \frac{1}{2}\gamma_p B_1 \left(\cos(\omega t)\sigma_x - \sin(\omega t)\sigma_y\right)$$

$$\hbar\omega_0 = \gamma_p B_0 \qquad \hbar\omega_1 = \gamma_p B_1$$

$$\boxed{\hat{H}(t) = -\frac{\hbar}{2}\omega_0 \sigma_z - \frac{\hbar}{2}\omega_1 \left(\cos(\omega t)\sigma_x - \sin(\omega t)\sigma_y\right)}$$

Układy NMR – oscylacje Rabiego

Hamiltonian Zeemana

$$\frac{\hbar\omega_0}{2} \quad |1\rangle = |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$-\frac{\hbar\omega_0}{2} \quad |0\rangle = |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\hat{H}(t) = -\frac{\hbar}{2}\begin{pmatrix} \omega_0 & \omega_1 e^{i\omega t} \\ \omega_1 e^{-i\omega t} & -\omega_0 \end{pmatrix}$$

$$P_{|0\rangle\to|1\rangle}(t) = \left(\frac{\omega_1}{\Omega}\right)^2 \sin^2\left(\frac{\Omega t}{2}\right)$$

$$P_{|0\rangle\to|1\rangle}(t) = \sin^2\left(\frac{\omega_1 t}{2}\right), \qquad \omega = \omega_0$$

$$\Omega = \sqrt{(\omega-\omega_0)^2 + \omega_1^2}$$

$$\frac{\omega_1 t}{2} = \frac{\pi}{2}, \qquad t = \frac{\pi}{\omega_1}$$

$$\frac{\omega_1 t}{2} = \frac{\pi}{4}, \qquad t = \frac{\pi}{2\omega_1}$$

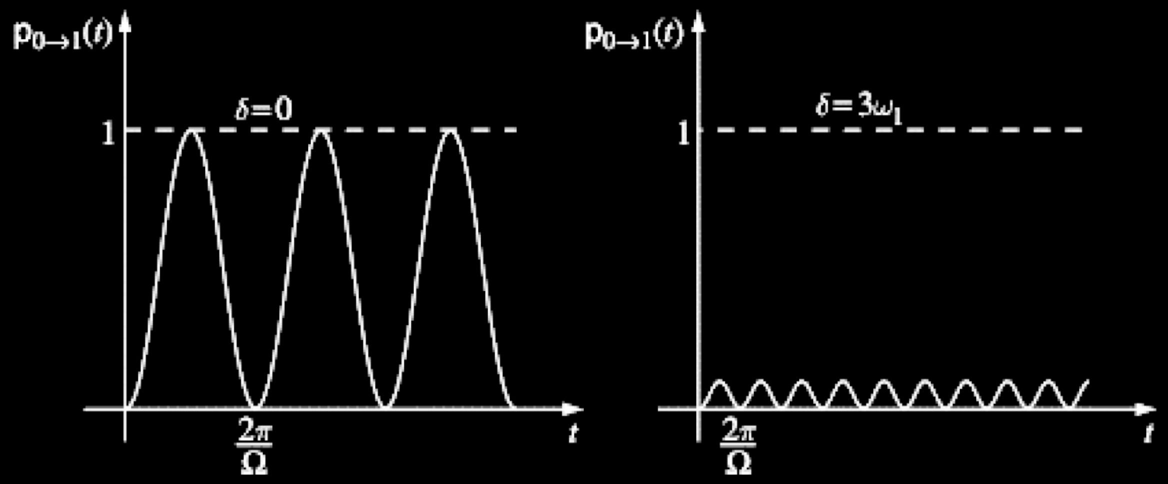
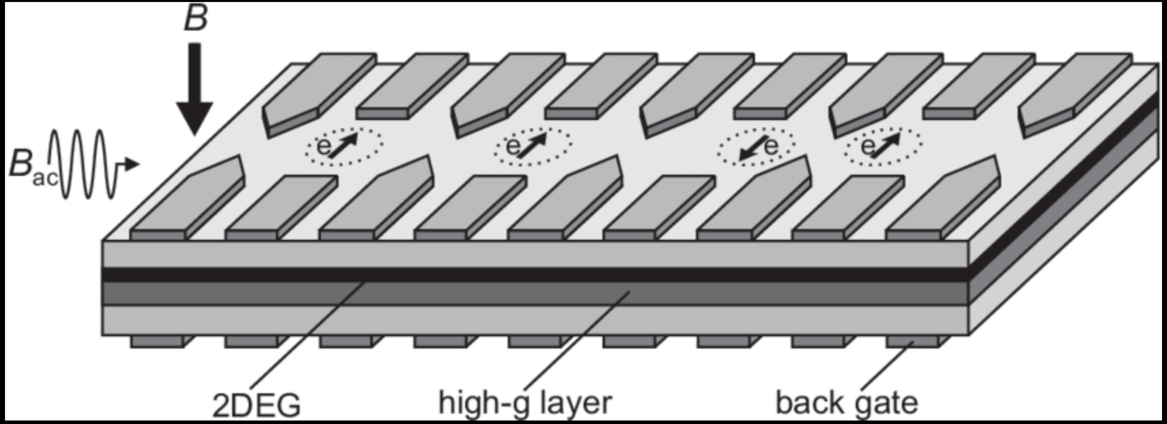


Figure 3.4 Rabi oscillations. The *detuning* δ is defined as $\delta = \omega - \omega_0$.

Oscylacje Rabiego

Układy kropek kwantowych



Daniel Loss

DP DiVincenzo

$$H = \sum_{\langle ij \rangle} J_{ij}(t) S_i \cdot S_j + \sum_i (g_i \mu_B B_i)(t) \cdot S_i$$

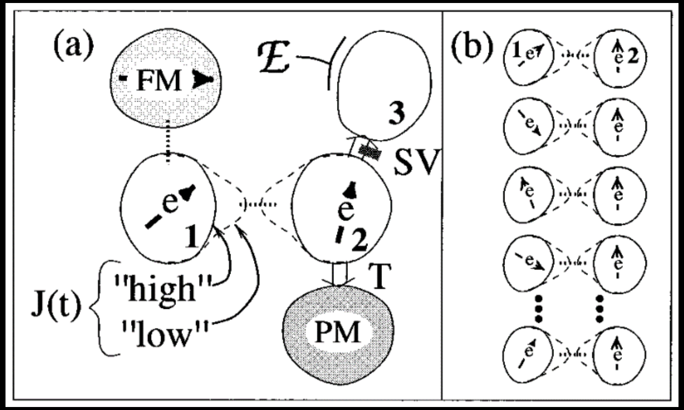
$$|\Psi\rangle = \alpha |\uparrow\rangle + \beta |\downarrow\rangle$$

$$|1\rangle = |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

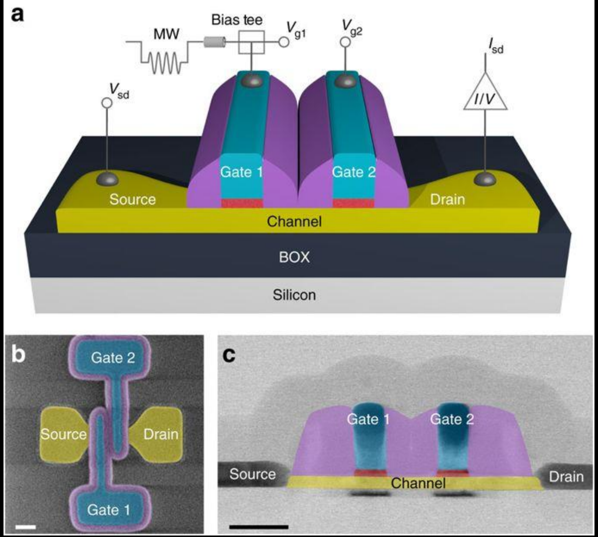
$$S_i = \frac{\hbar}{2} \sigma_i$$

$$|0\rangle = |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

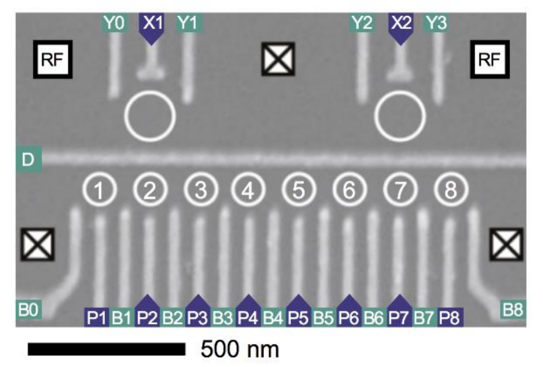
Quantum computation with quantum dots
D Loss, DP DiVincenzo PRA **57** (1), 120 (1997)



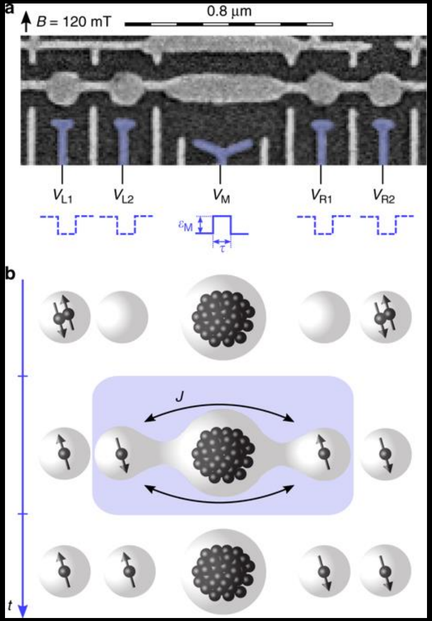
Układy kropek kwantowych



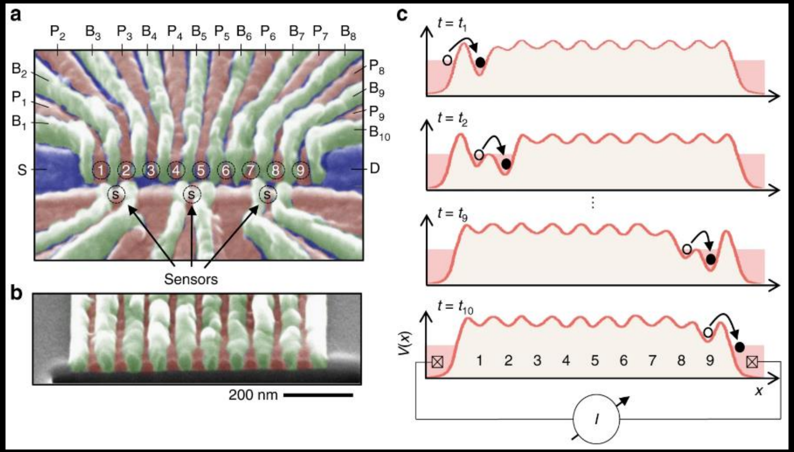
A CMOS silicon spin qubit
R. Maurand,... & S. De Franceschi
Nat. Com. 7, 13575 (2016)



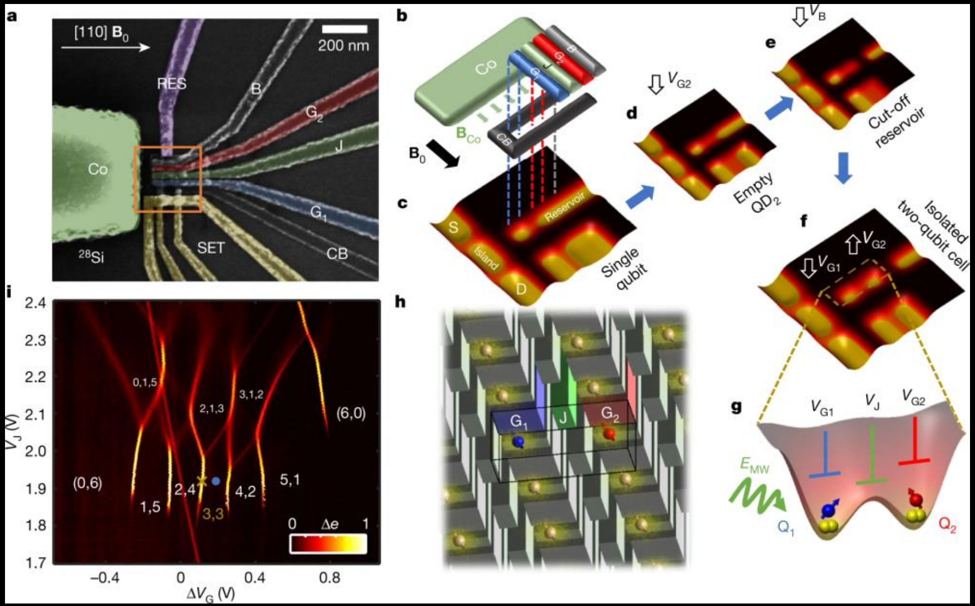
Loading a quantum-dot based "Qubyte" register
L.M.K. Vandersypen
arXiv:1901.00426 (2019)

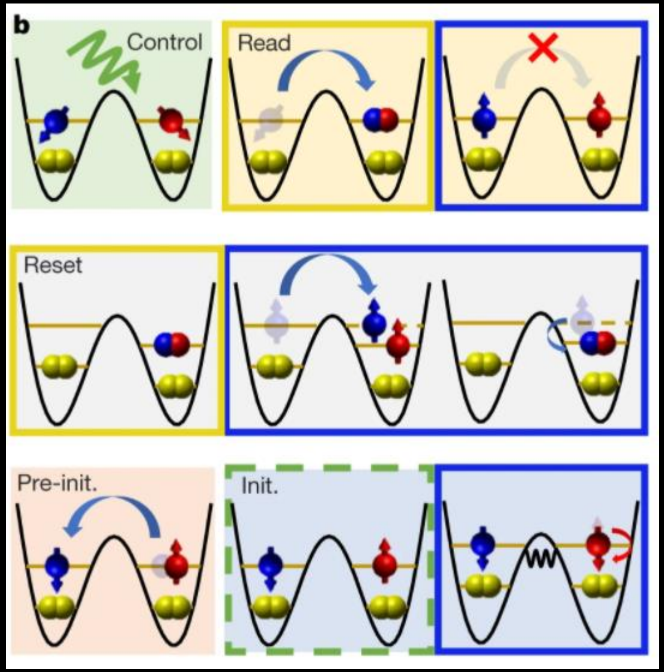


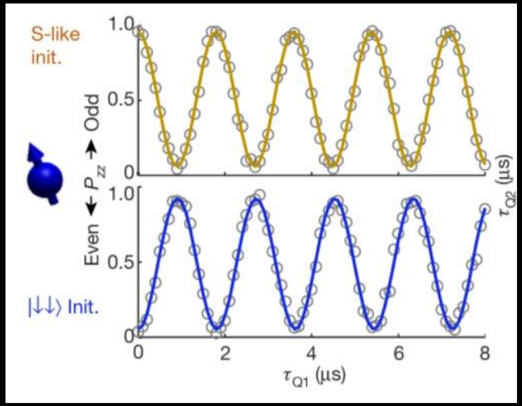
Fast spin exchange across a multielectron mediator
Filip K., ... , Charles M. Marcus
Nat. Com. 10, 1196 (2019)

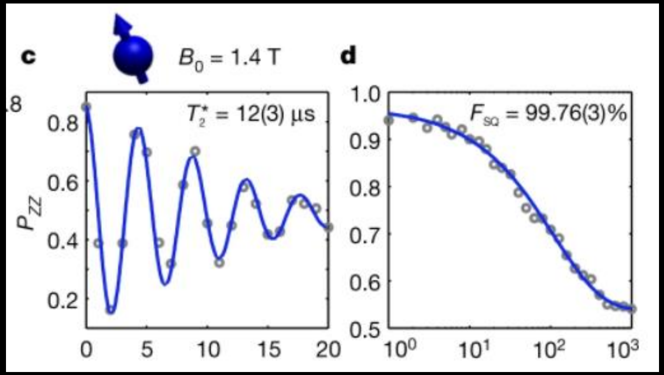


Układy kropek kwantowych









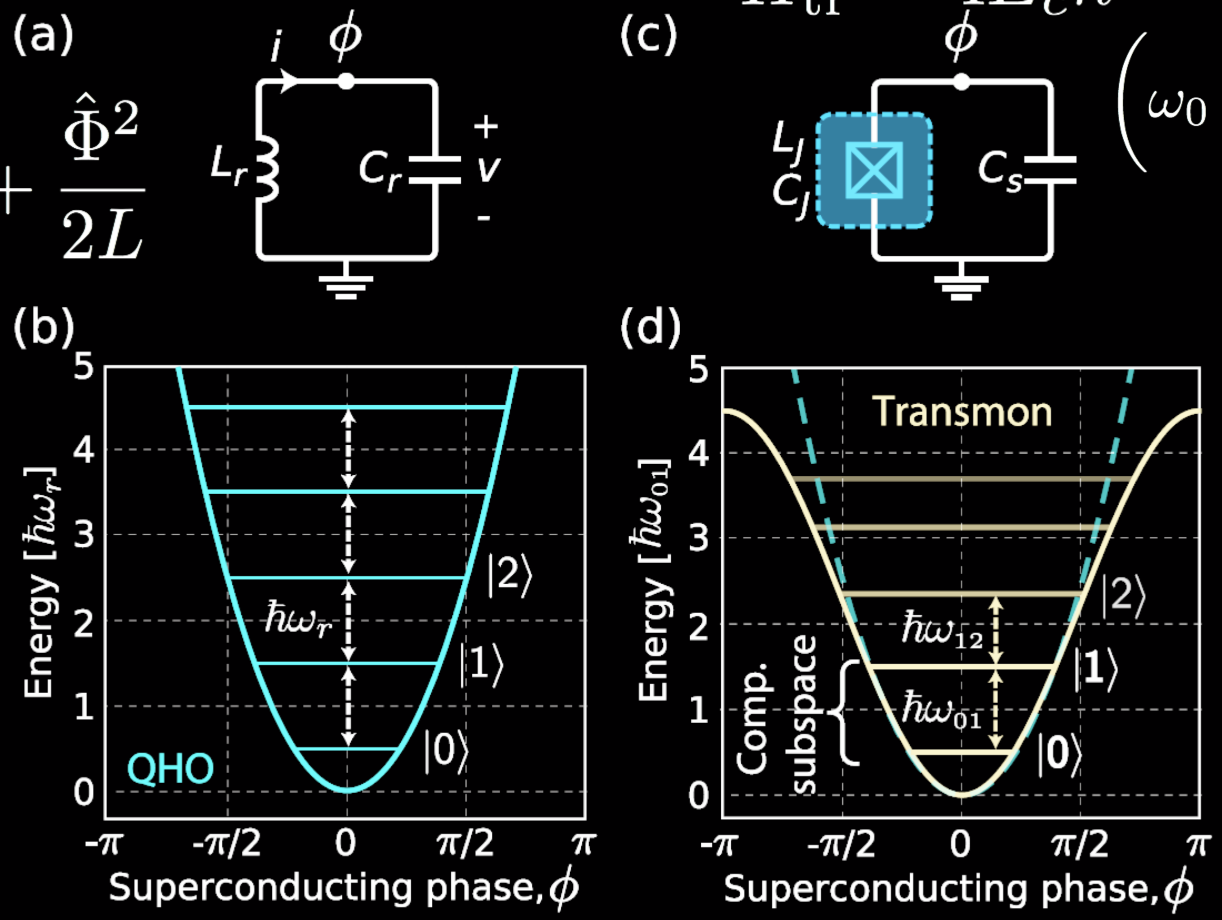
Operation of a silicon quantum processor unit cell above one kelvin, A. S. Dzurak, Nature London, 580, (2020)

Transmon quantum bit

$$\hat{H}_{\mathrm{tr}} = 4E_c\hat{n}^2 - E_J\cos\hat{\phi}$$

$$\hat{H} = \frac{\hat{Q}^2}{2C} + \frac{\hat{\Phi}^2}{2L}$$

$$\left(\omega_0 + \frac{\delta}{2}\right)\hat{c}^\dagger\hat{c} + \frac{\delta}{2}(\hat{c}^\dagger\hat{c})^2$$



$$H_{\mathrm{QHO}}$$

$$\hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)$$

$$\omega_{01} \quad 4 - 8\mathrm{GHz}$$

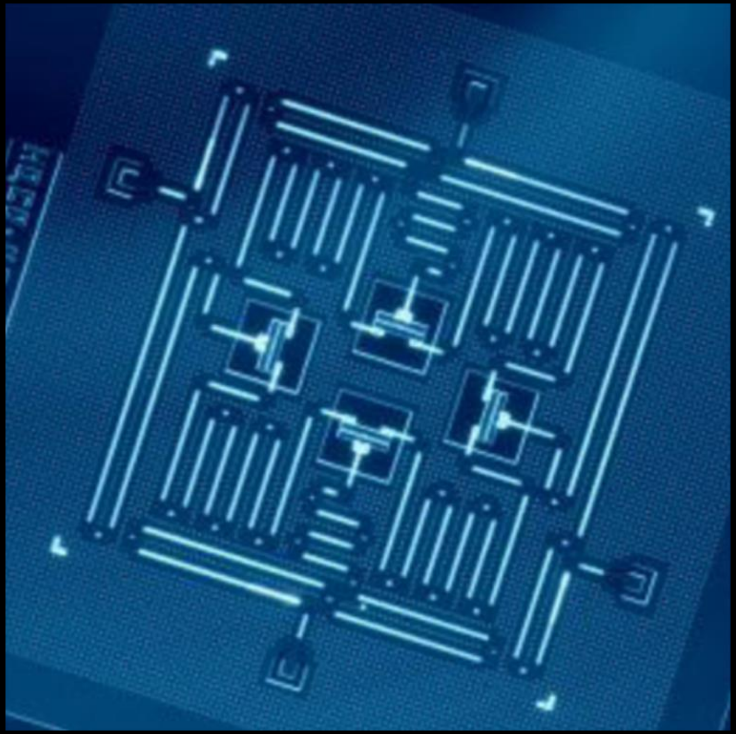
$$250mK$$

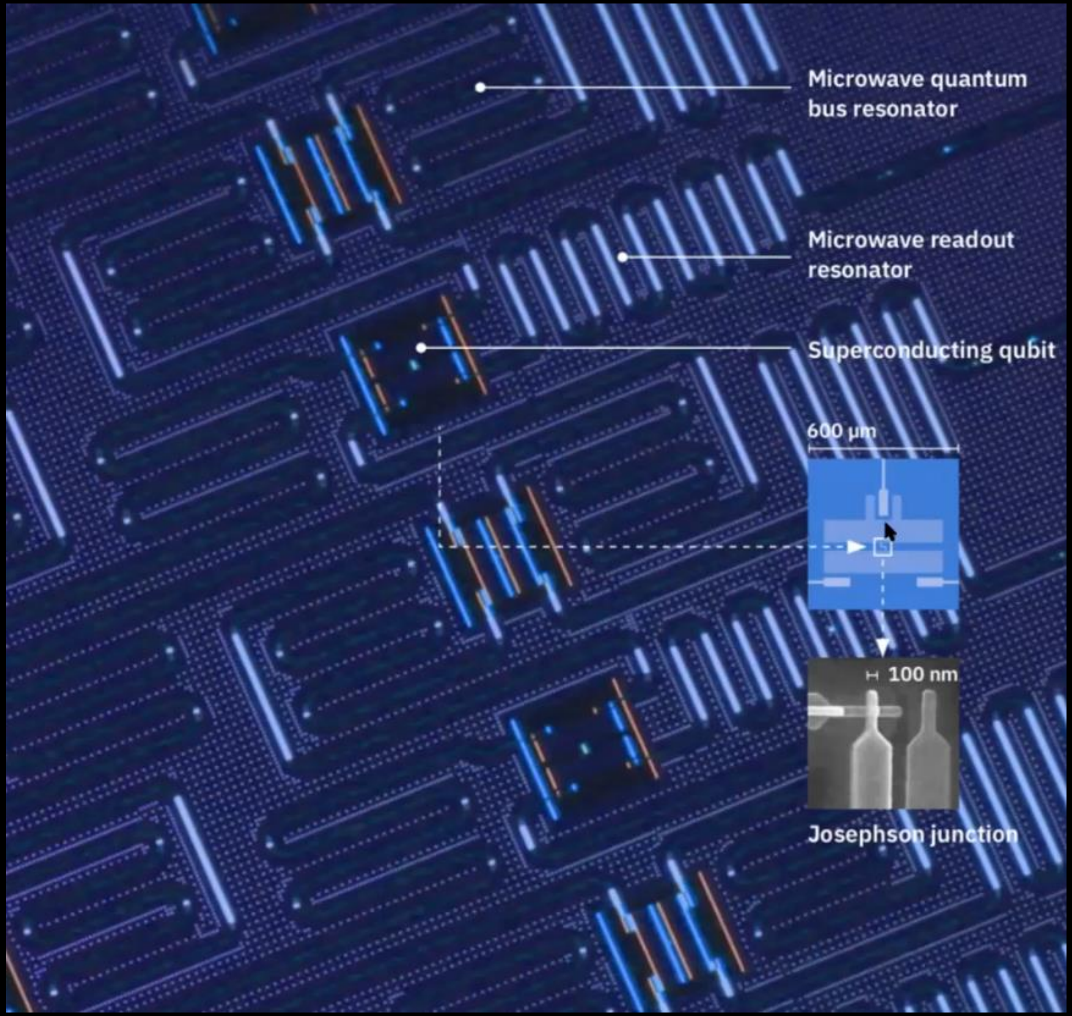
Transmon quantum bit

Building logical qubits in a superconducting quantum computing system

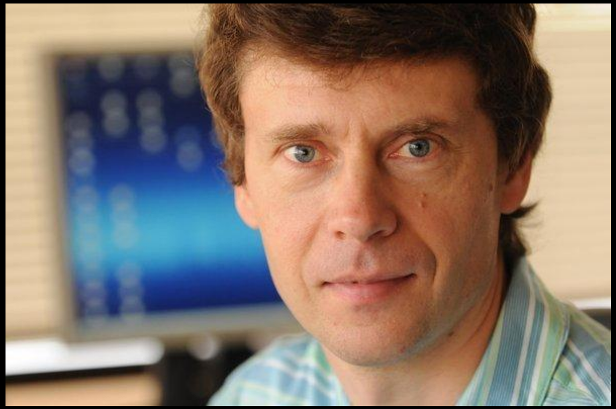
Jay M. Gambetta, Jerry M. Chow & Matthias Steffen

npj Quantum Information 3, Article number: 2 (2017) | Cite this article





Bity chronione topologicznie

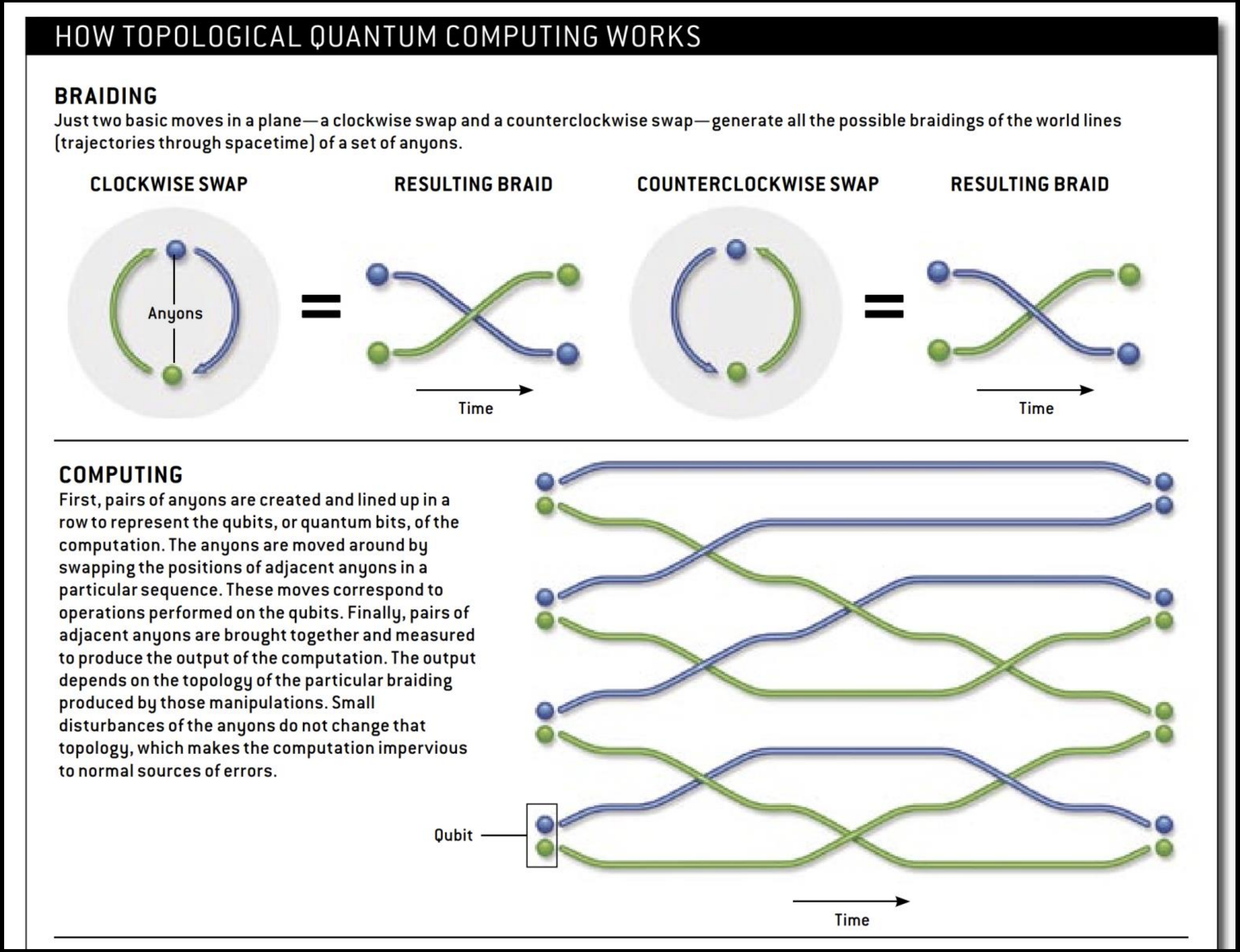


Alexei Kitaev, arXiv:quant-ph/9707021 (1997)' A two-dimensional quantum system with anyonic excitations can be considered as a quantum computer. Unitary transformations can be performed by **moving the excitations around each other**. Measurements can be performed by **joining excitations in pairs and observing the result of fusion**. Such computation is **fault-tolerant by its physical nature**.

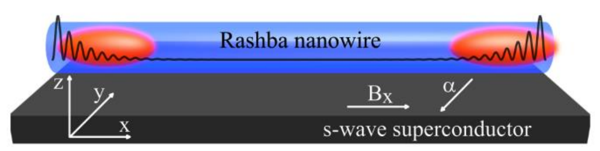
Anyons – cząstki podlegające statystyce w której zamian cząstek miejscami powoduje przemnożenie funkcji falowej przez czynnik fazowy.
Nie są one ani bozonami ani fermionami.

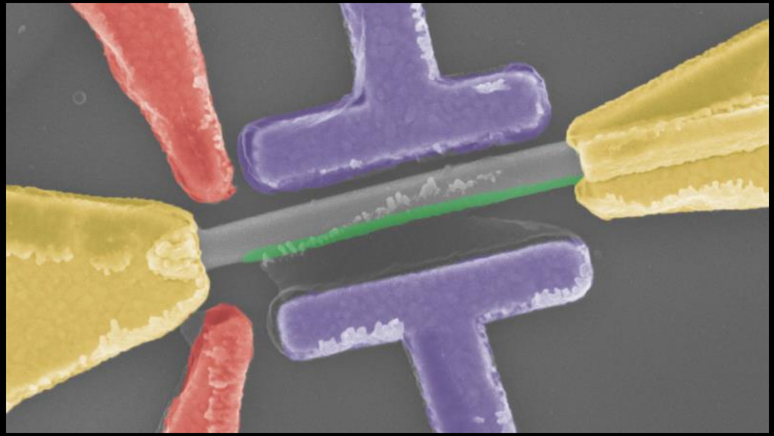
Braiding

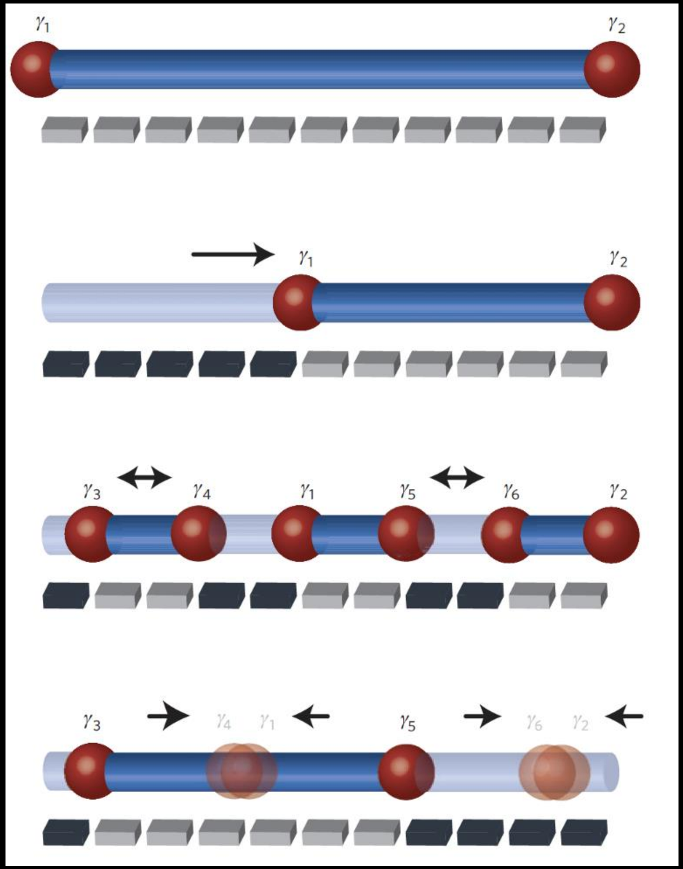

TO BEAT BACTERIA, STOP MUTATIONS • GLOBALIZATION AND POVERTY
SCIENTIFIC AMERICAN
How to Save Millions of Children from Rotavirus
BIZARRE PARTICLES AND SPACETIME BRAIDS SOLVE IMPOSSIBLE PROBLE
COMPUTING WITH QUANTUM KNOTS
Cultured Apes and Evolving Intelligence
Magnetic Triggers of Solar Flares
Plugged-In Hybrid Cars

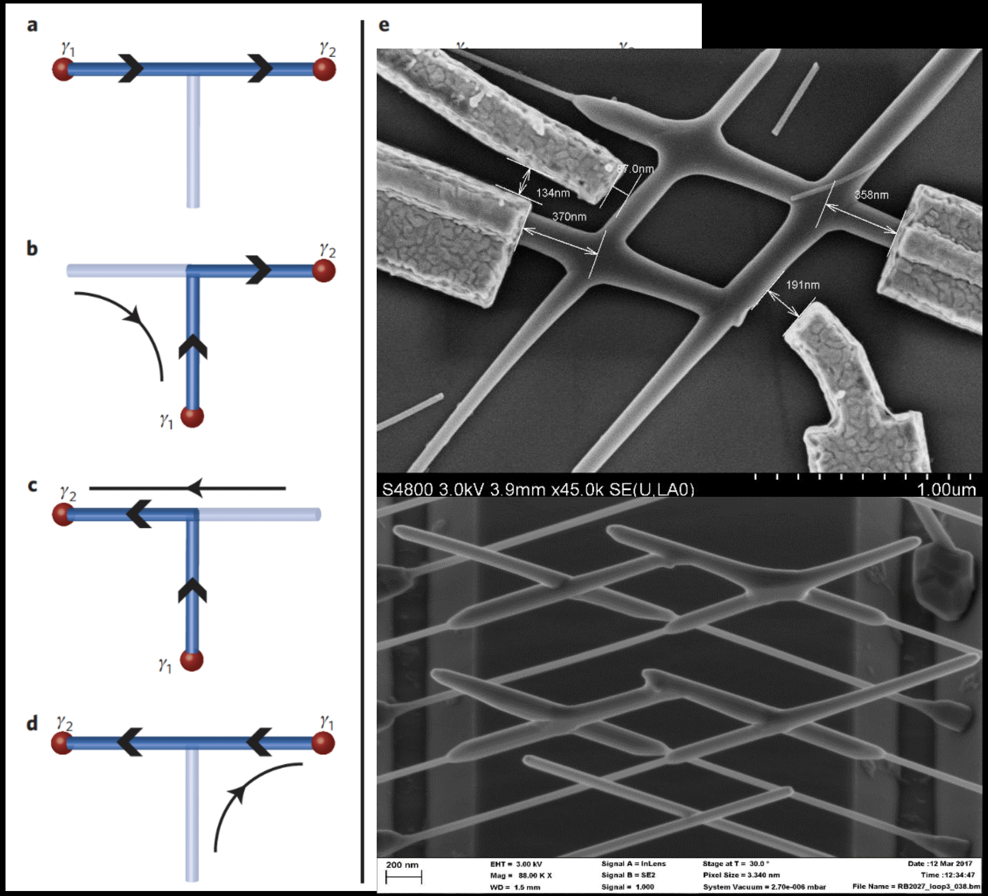

HOW TOPOLOGICAL QUANTUM COMPUTING WORKS
BRAIDING
Just two basic moves in a plane—a clockwise swap and a counterclockwise swap—generate all the possible braidings of the world lines (trajectories through spacetime) of a set of anyons.
CLOCKWISE SWAP
Anyons
=
RESULTING BRAID
Time
COUNTERCLOCKWISE SWAP
=
RESULTING BRAID
Time
COMPUTING
First, pairs of anyons are created and lined up in a row to represent the qubits, or quantum bits, of the computation. The anyons are moved around by swapping the positions of adjacent anyons in a particular sequence. These moves correspond to operations performed on the qubits. Finally, pairs of adjacent anyons are brought together and measured to produce the output of the computation. The output depends on the topology of the particular braiding produced by those manipulations. Small disturbances of the anyons do not change that topology, which makes the computation impervious to normal sources of errors.
Qubit
Time

Fermiony Majorany









Jason Alicea, Yuval Oreg, Gil Refael, Felix von Oppen & Matthew P. A. Fisher Nature Physics volume 7, pages412–417(2011)

Podsumowanie

Wydaje się, że jesteśmy na progu nowej rewolucji technologicznej związanej z rozwojem komputerów kwantowych oraz kwantowych metod przetwarzania informacji.

Dziękuję za uwagę przez cały semestr