Informacioni dhe Kompjuteri Kuantik

Ervin Kafexhiu

14 Shkurt 2020

Permbajtja

1. Nevoja per Teknologji Kuantike
2. Themelet e Informacionit Kuantik
3. Kompjuteri Kuantik
4. Portat dhe Qarqet Kuantike
5. Zbatime te thjeshta ne Kompjuterin Kuantik IBM-Q
6. Sfidat

Nevoja per Teknologji Kuantike

Kerkese per kompjutera te fuqishem:

- Jetojm ne nje epoke informacioni (IoT, pajisjet "Smart", etj.)
- Pajisjet integrohen me shume ne jeten e perditshme (IoT)

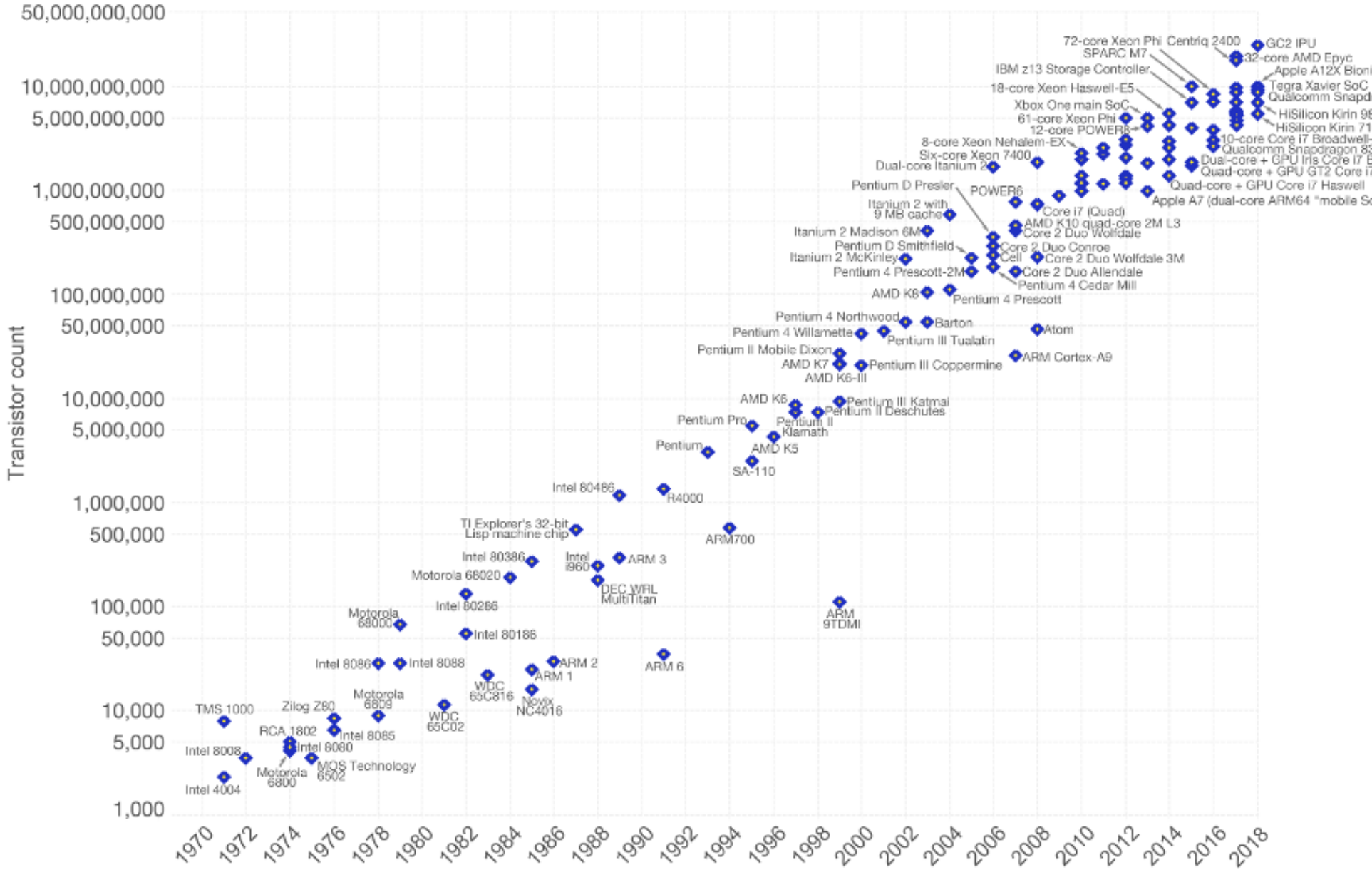
$\Rightarrow$ Kerkese me e madhe per fuqi llogaritese (CPU, GPU etj.)

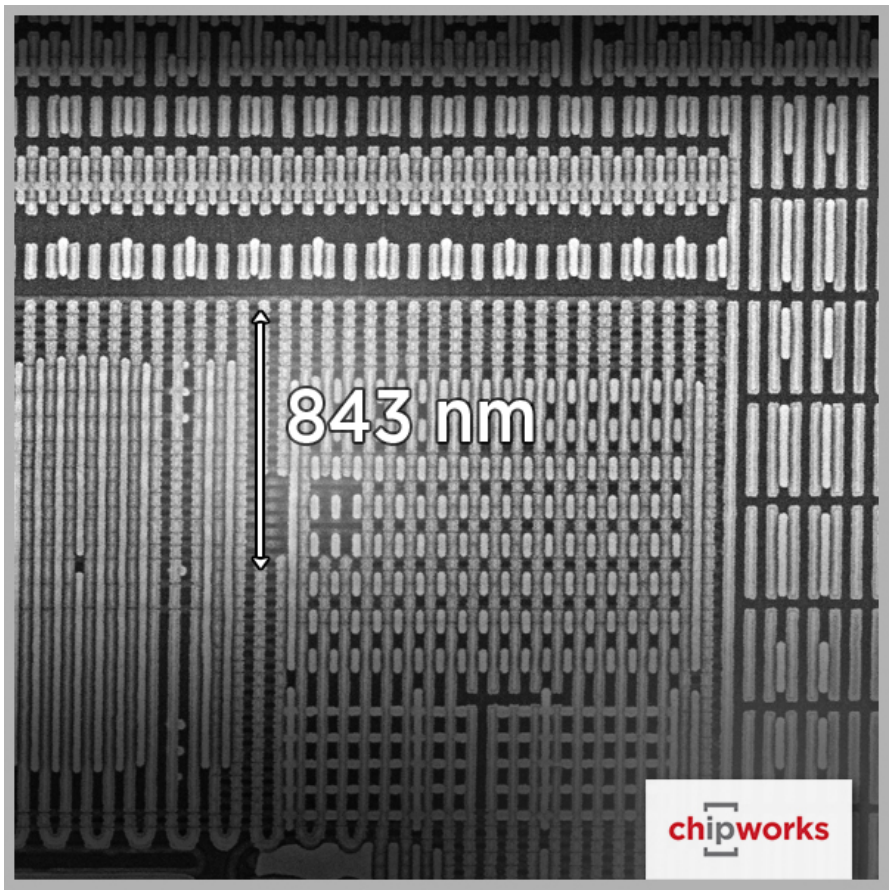
Ligji Moore:

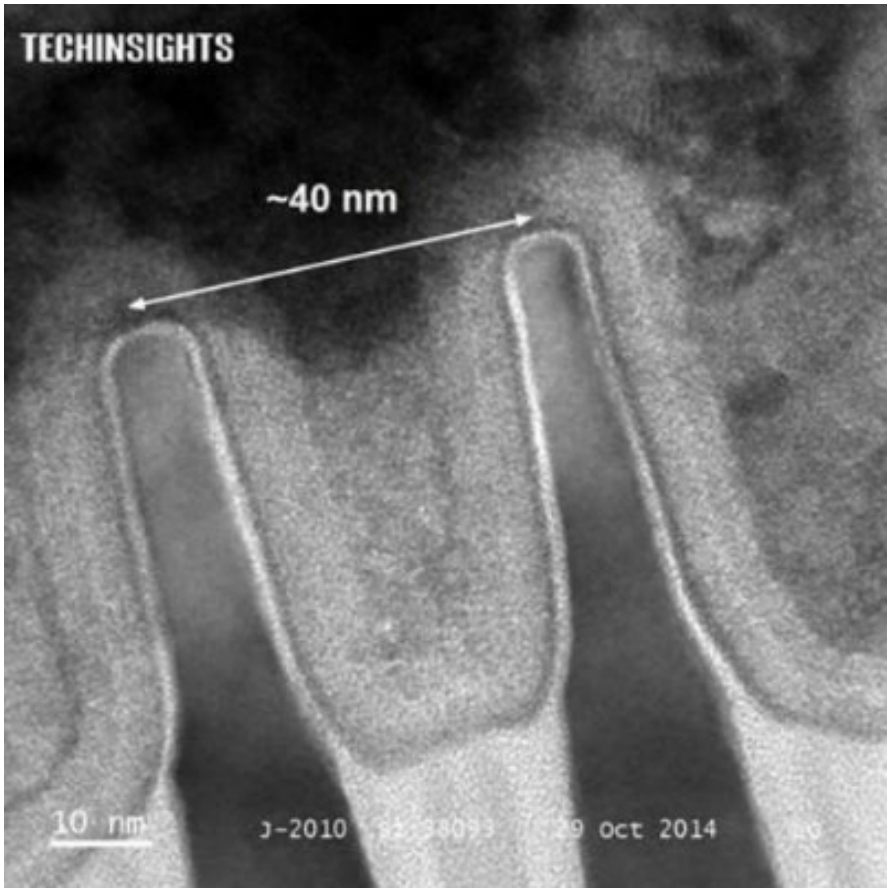
- **"Cdo dy vite dendesia e tranzistoreve te integruar ne nje cip dyfishohet."**

Moore's Law – The number of transistors on integrated circuit chips (1971-2018)

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are linked to Moore's law.




843 nm
chipworks

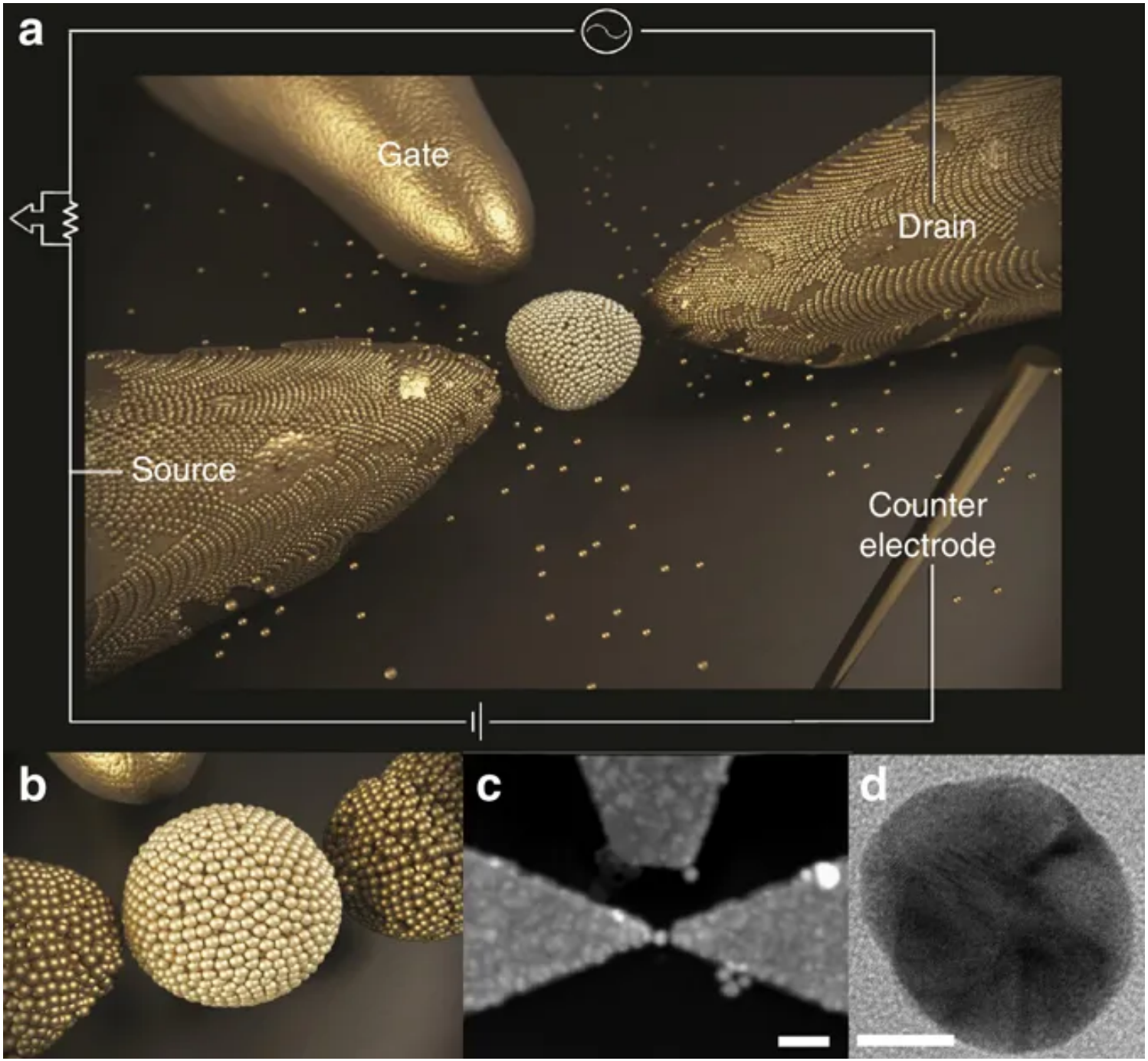

TECHINSIGHTS
~40 nm
10 nm
J-2010
29 Oct 2014

Evolucioni i Permasave te MOSFET:

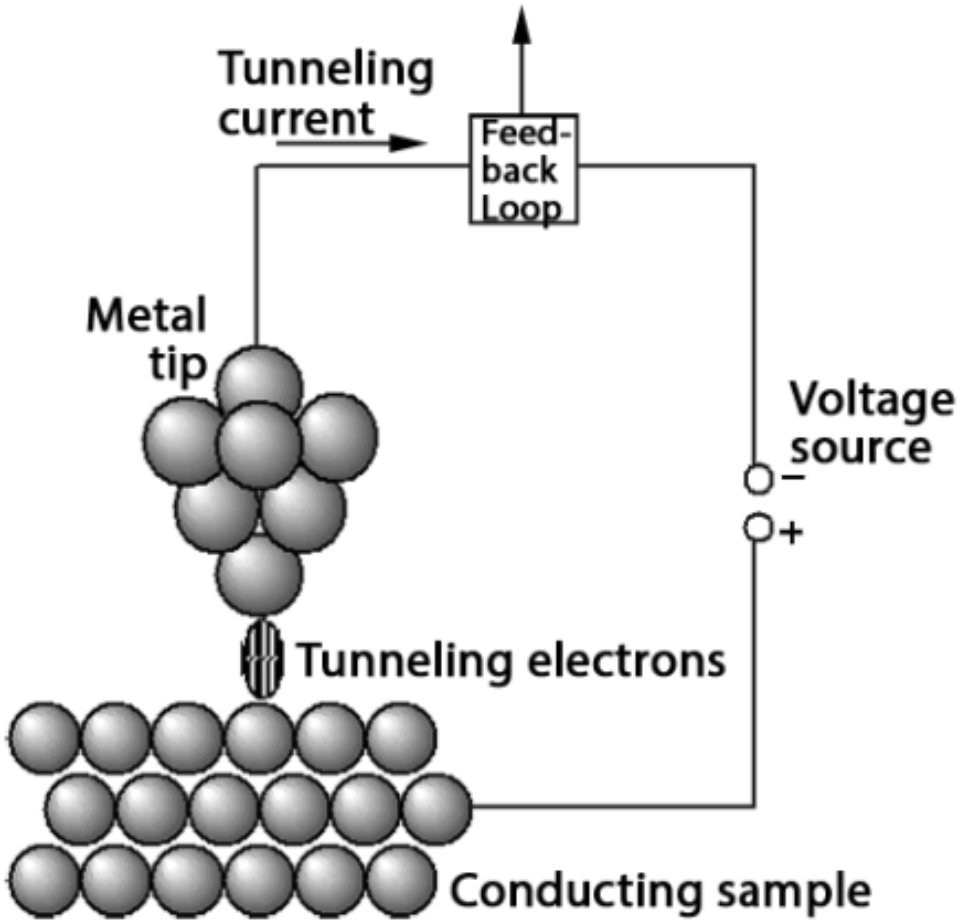
Viti	Dimens.
1971	10 μm
1974	6 μm
1977	3 μm
1981	1.5 μm
1984	1 μm
1987	800 nm
1990	600 nm
1993	350 nm
1996	250 nm
1999	180 nm
2001	130 nm
2003	90 nm

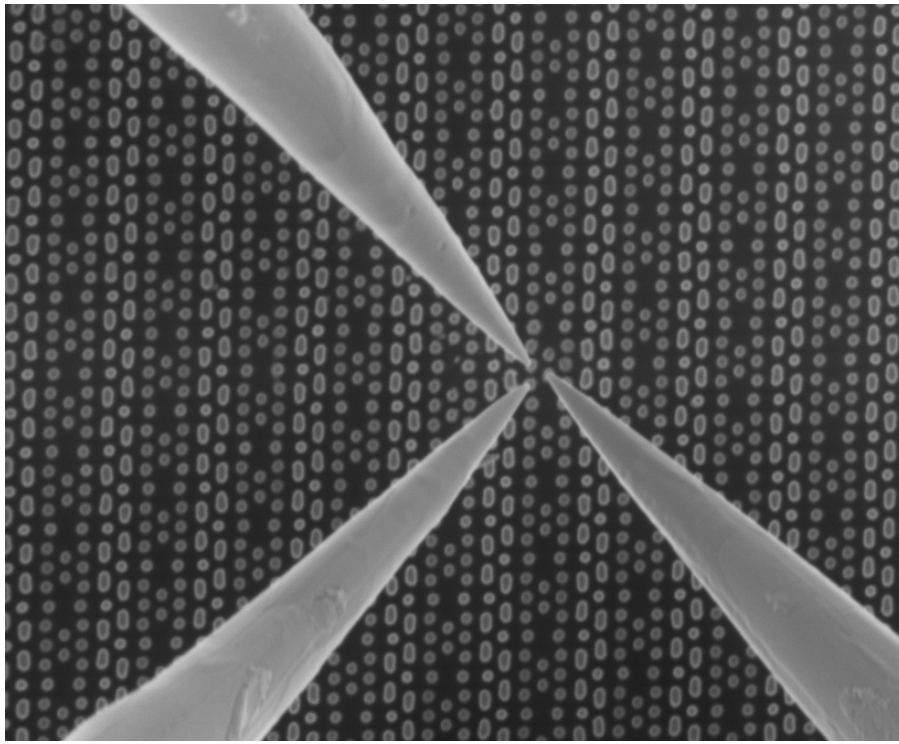
Viti	Dimens.
2005	65 nm
2007	45 nm
2009	32 nm
2012	22 nm
2014	14 nm
2016	10 nm
2018	7 nm
2020	5 nm
2021*	3 nm
2024*	2 nm

Rrjeta Si $a_0 = 0.54$ nm

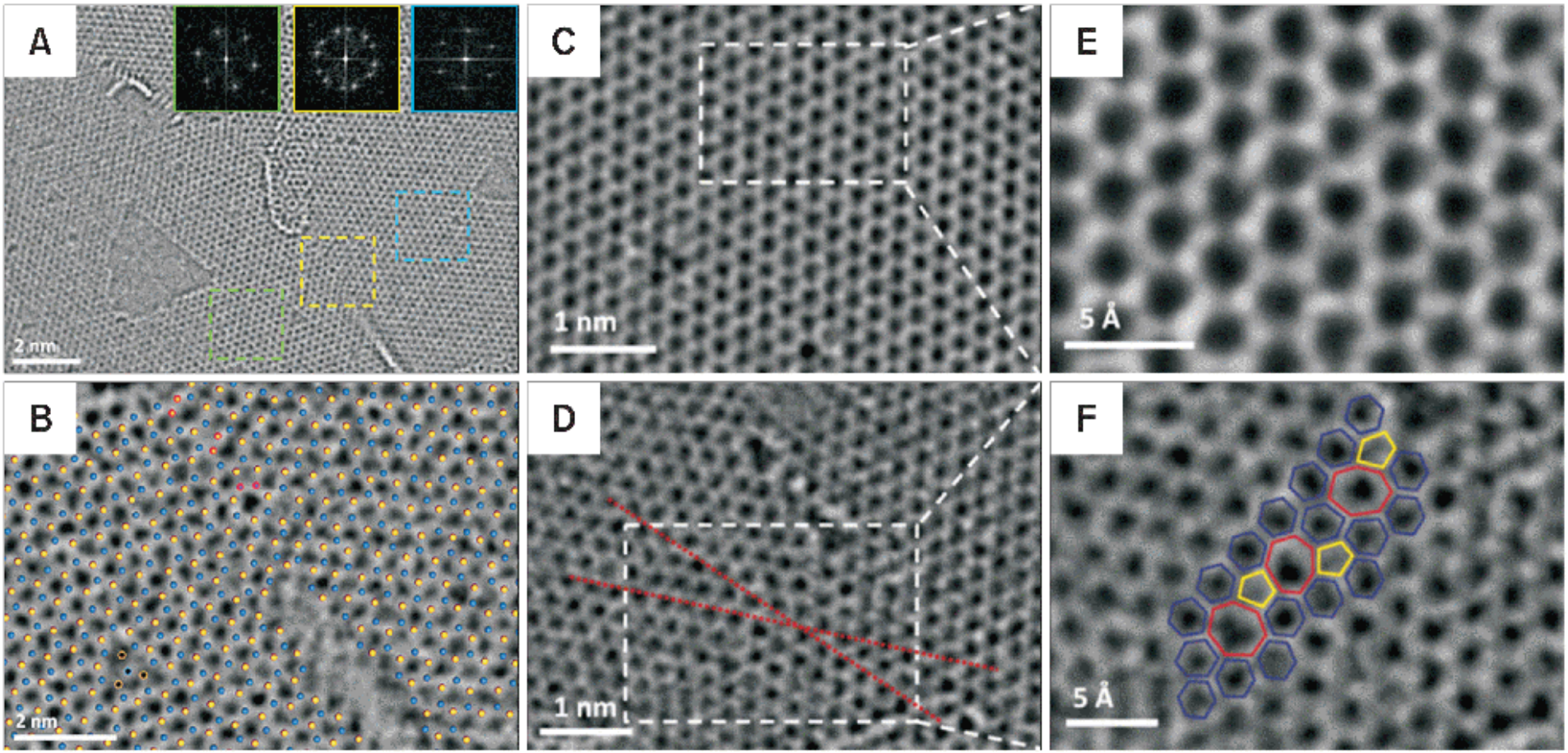

a
Gate
Drain
Source
Counter
electrode
b
c
d

Scanning Tunneling Microscopy (STM) & Atomic Force Microscope (AFM)

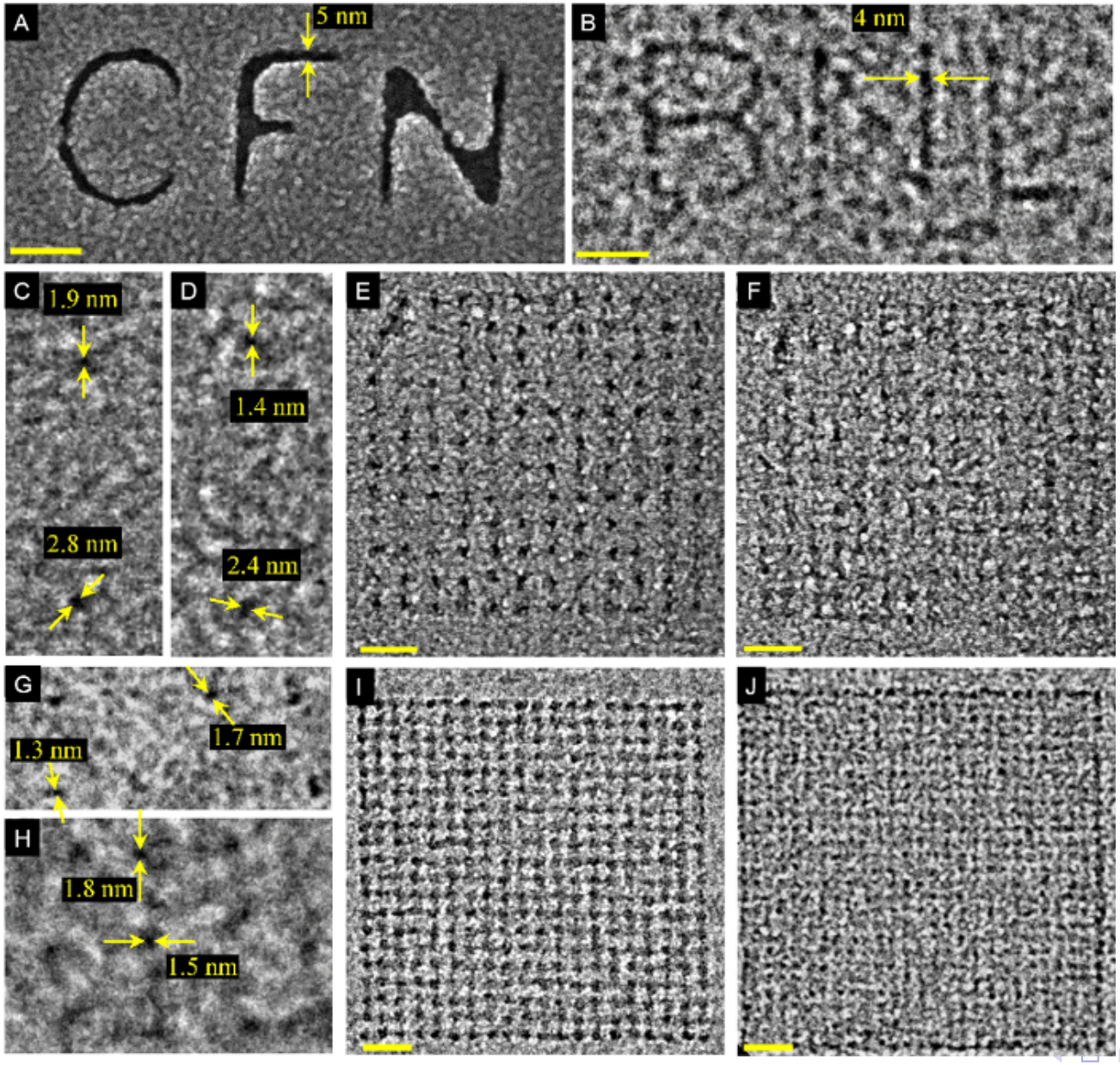




STM dhe AFM lejojne matje ne nivel atomik



STM dhe AFM lejojne manipulim ne nivel atomik



Informacioni Kuantik

Technologjia po perballet me limitet fizike!!!

- Duhen ndertuar tranzistore me madhesi (sub-)atomike (e^-)
- Sjellja kuantike e materies ndryshon rregullat e lojes
- Informacioni "klasik" me bite 0 & 1 humbet vleren
- Gare e forte kush behet i pari ne teknologjine kuantike

Disa fushat kerkimi te informacionit kuantik

- "Quantum Computing" (**kompjuteri kuantik**, algoritmet etj)
- Teoria e informacionit kuantik
- Kriptografi dhe komunikimi kuantik
- Teleportimi kuantik etj...

Sistemi kuantik binare

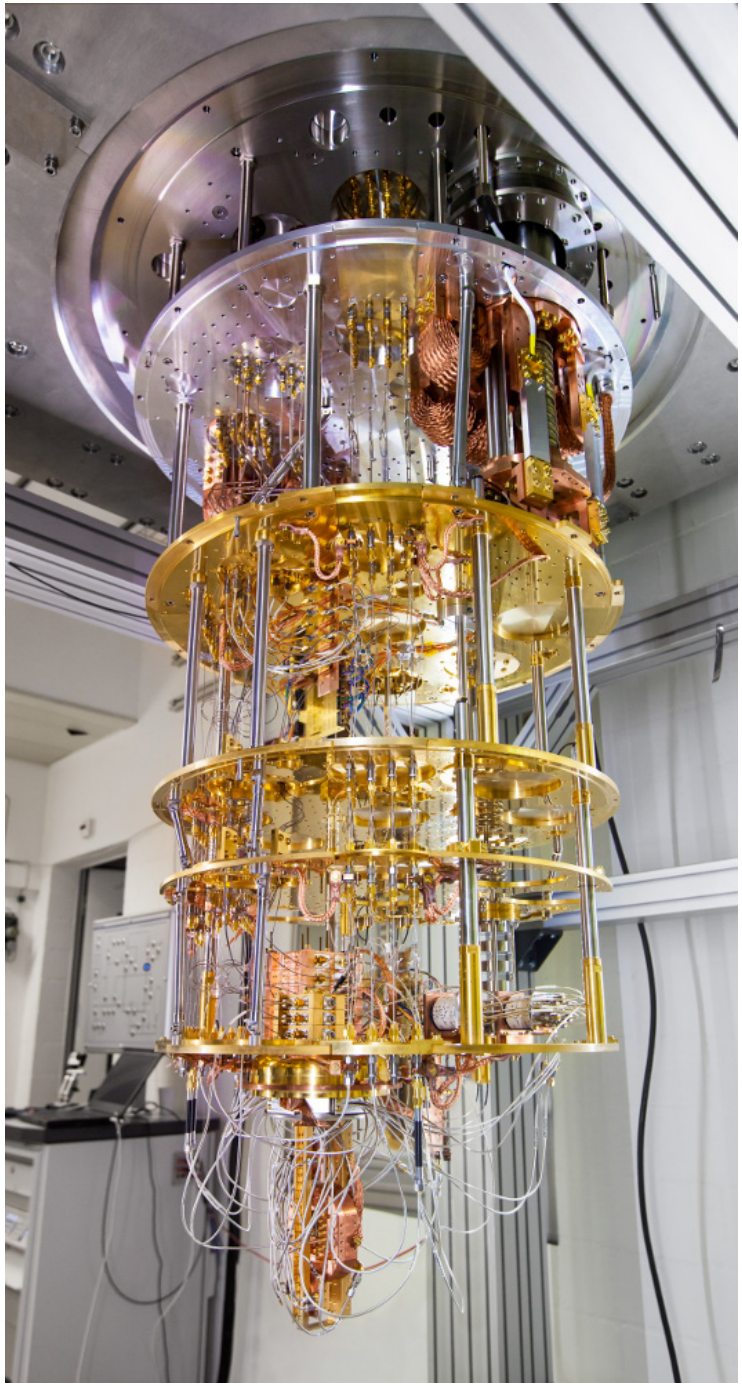
- Konsidero nje sistem me dy gjendje $|0\rangle$ dhe $|1\rangle$.
- Mund te jene:
  1. Dy nivele energjie te nje sistemi (psh atom).
  2. Spini i e^-, $|\uparrow\rangle$ dhe $|\downarrow\rangle$.
  3. Polarizimi photonit $|H\rangle$ & $|V\rangle$ ose $|\circlearrowleft\rangle$ & $|\circlearrowright\rangle$ etj.
- Ne hapsiren Hilbert paraqiten si $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ dhe $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Ne sistemin **klasik** nje gjendjet "0" ose "1" quhet **"bit"** kurse gjendja **kuantike** $|\psi\rangle$ quhen **"qubit"** (quantum bit).

Fenomenet kuantike

- **Superpozimi**: $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ ku $|\alpha_0|^2 + |\alpha_1|^2 = 1$
  Sistemi klasik ka vetem dy gjendje, kurse sistemi kuantik mund te jete ne cdo kombinim linear te ketyre gjendjeve.

- **Entanglement** ("korrelacion" kuantike):
  Hapsira e Hilbert-it per dy qubit paraqitet nga gjendejet e Bell-it
  $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle)$
  $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle)$ ku psh $|00\rangle = |0\rangle_1 \otimes |0\rangle_2$

- **Roli i matjes**: Matja kuantike e "shkatarron" ne menyre te pa kthyeshme superpozimin dhe shemb funksionin valor ne nje nga gjendjet vetjake/pastra. Matjet kan thelbesisht natyre probabilitare.



Kompjuteri Kuantik shfrytezon

- Superpozimin kuantik per te enkoduar me shume informacion
- Entanglement per te komunikuar mes qubit apo ruajtur info.
- Quantum Gates per te manipuluar qubits (jo Logical Gates si kompjuteri klasik)

Kompjuteri Kuantik funksionon ne temperatura te uleta ($T \sim 1$ K) per te mbrojtur sa me gjate sistemin nga dekoherenca ambjentit.

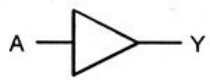
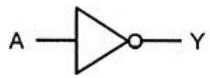
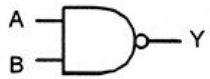
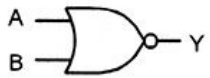
Realizimi Praktik i Kompjuterit Kuantik

- Qarqe superpercjelles (psh. qubit ndertohen me nyje Josephson-i)
- Kurthe Ionesh (qubits ndertohen ne nivelet atomike te joneve te zena kurthe)
- Rrjetat Optike (qubits ndertohen me nivele atomike te nje rrjete optike)
- Quantum dots (qubits ndertohen me spinet e elektroneve te zena ne kurthe te nanogrimcave)
- Rezonance magnetike berthamore (qubitet formohen nga spinet e berthamave atomike)
- Diamantet (qubits formohen nga spinet e elektroneve qe mbesin nga vakancat e N ne diamant)
- etj...

Cfare mund te bej nje kompjuter kuantik?

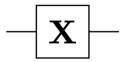
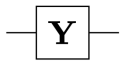
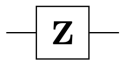
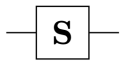
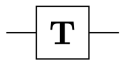
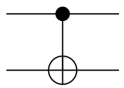
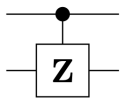
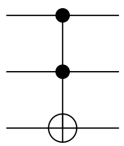
Kompjuterat kuantik pritet te shkelqejne ne:

- Kriptografi (nga teorema e pa klonueshmerise)
- Kerkim databaze (algoritmat kuantike premtojne shpejtesi kerkimi te pa arriteshme nga kompjuteri klasik)
- Simulime kuantike te proceseve fizike dhe kimike qe jan te pamundura nga kompjuteri klasik.
- Inteligjence artificiale
- Parashikime te motit
- Modelimi financiar etj...

Logic function	Logic symbol	Truth table	Boolean expression
Buffer		A | Y 0 | 0 1 | 1	$Y = A$
Inverter (NOT gate)		A | Y 0 | 1 1 | 0	$Y = \overline{A}$
2-input AND gate		A B | Y 0 0 | 0 0 1 | 0 1 0 | 0 1 1 | 1	$Y = A \bullet B$
2-input NAND gate		A B | Y 0 0 | 1 0 1 | 1 1 0 | 1 1 1 | 0	$Y = \overline{A \bullet B}$
2-input OR gate		A B | Y 0 0 | 0 0 1 | 1 1 0 | 1 1 1 | 1	$Y = A + B$
2-input NOR gate		A B | Y 0 0 | 1 0 1 | 0 1 0 | 0 1 1 | 0	$Y = \overline{A + B}$
2-input EX-OR gate		A B | Y 0 0 | 0 0 1 | 1 1 0 | 1 1 1 | 0	$Y = A \oplus B$
2-input EX-NOR gate		A B | Y 0 0 | 1 0 1 | 0 1 0 | 0 1 1 | 1	$Y = \overline{A \oplus B}$

Portat logjike te kompjuterit klasik

Vlerat e ruajtura ne regjister kalojne neper portat logjike edhe japin nje output te caktuar.

Operator	Gate(s)		Matrix
Pauli-X (X)			$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)			$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)			$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)			$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)			$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)			$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)			$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Portat Kuantike

Regjistri kuantik perbehet nga N-qubits, gjendja e te cilit paraqitet me nje funksion valore. Portat kuantike paraqiten matematikisht me matrica apo operator linear unitare qe veprojne mbi qubits ose regjistrin.

Portat dhe Qarqet Kuantike

Hadamard gate

$$-\boxed{H}- = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\langle 1|$$

Pauli-X gate, $\sim$ NOT gate

$$-\boxed{X}- = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = |1\rangle\langle 0| + |0\rangle\langle 1|$$

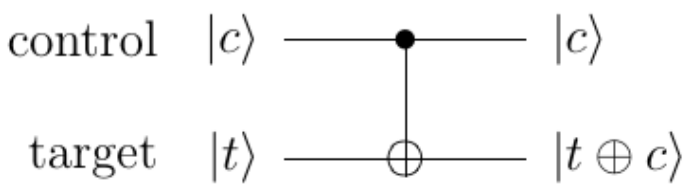
Pauli-Z gate, rrotullim π sipas Z

$$-\boxed{Z}- = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = |1\rangle\langle 0| - |0\rangle\langle 1|$$

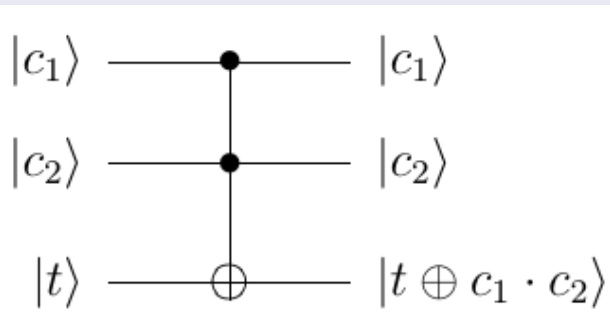
R-gate, ndryshon fazen

$$\boxed{R_\theta} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} = |1\rangle\langle 0| + e^{i\theta}|0\rangle\langle 1|$$

CNOT, NOT i kontrolluar



CCNOT, NOT gate i kontrolluar nga dy qubits

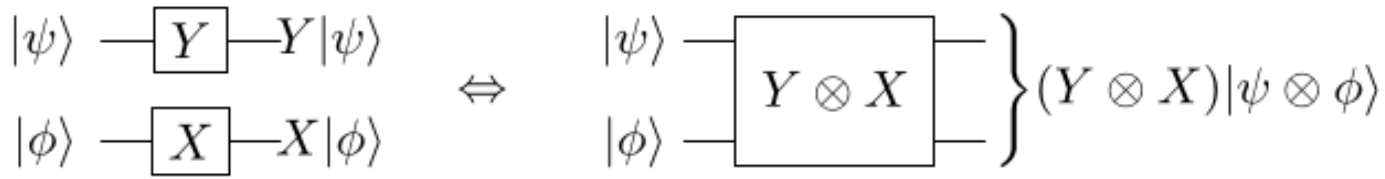


Lidhja seri dhe paralel

Ndryshe nga lidhja seri ku portat veprojne njera mbas tjetres mbi nje qubit, **portat paralele veprojne sipas productit tensorial.**

$$\mathbb{A} \otimes \mathbb{B} = \begin{pmatrix} a_{11}\mathbb{B} \dots a_{1n}\mathbb{B} \\ \vdots \\ a_{n1}\mathbb{B} \dots a_{nn}\mathbb{B} \end{pmatrix}$$

Veprimi paralel mbi 2 qubit



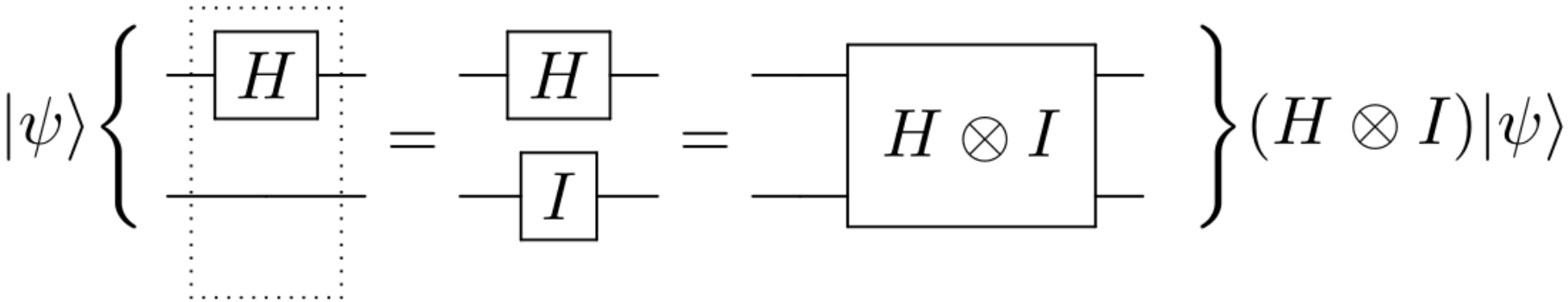
Paraqitja matricore

$$Y \otimes X = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix}$$

and $|\psi \otimes \phi\rangle =$

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

Veprimi paralel mbi 2 qubit



Veprimi paralel i Hadamard Gate

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

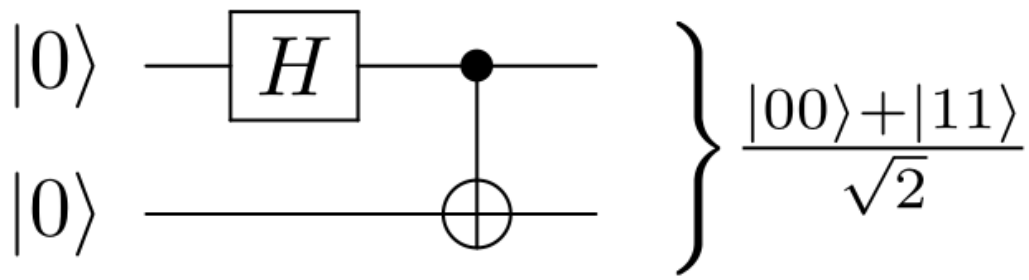
Veprimi paralel i 2 Hadamard Gate

$$H_2 = H \otimes H = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_2 |00\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{|00\rangle + |10\rangle + |01\rangle + |11\rangle}{2}$$

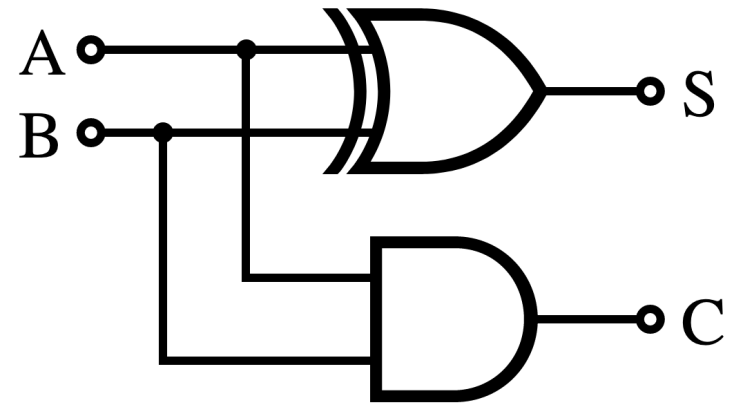
Zbatime te thjeshta ne Kompjuterin Kuantik IBM-Q

Entanglement

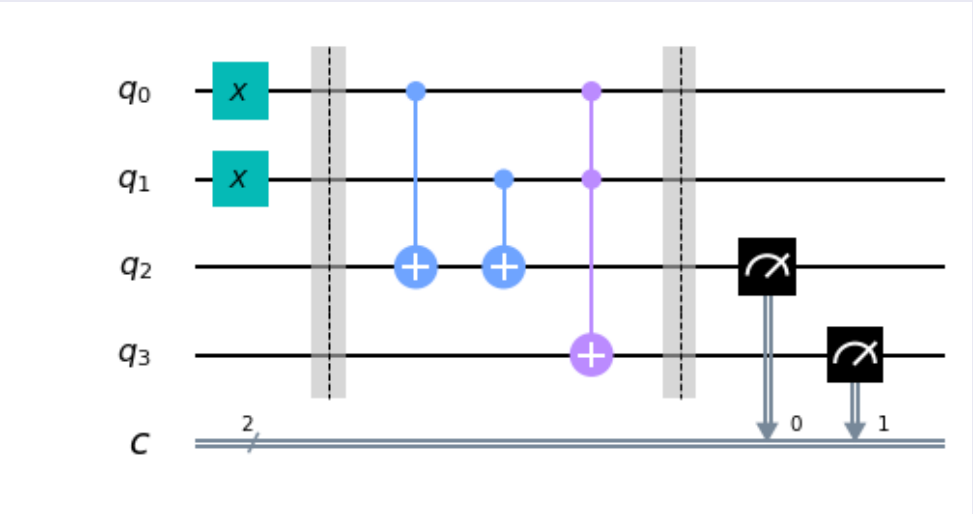


$$CNOT(H \otimes I)|00\rangle = \frac{|00\rangle+|11\rangle}{2}$$

Mbledhja dy biteve klasike



Mbledhja dy qubiteve



Sfidat

- Ndertimi me shume qubits
- Lidhshmeri me e madhe (entanglement) mes qubits
- Gabime me te vogla dhe korrektim me i mire (pershkak te dekoherences kuantike)
- Funksionim ne temperature me te larta (jo-kriogjenike)
- Ulje te kostove