$\hbar$

Kako zapreči kvantne pojave in zmagati?

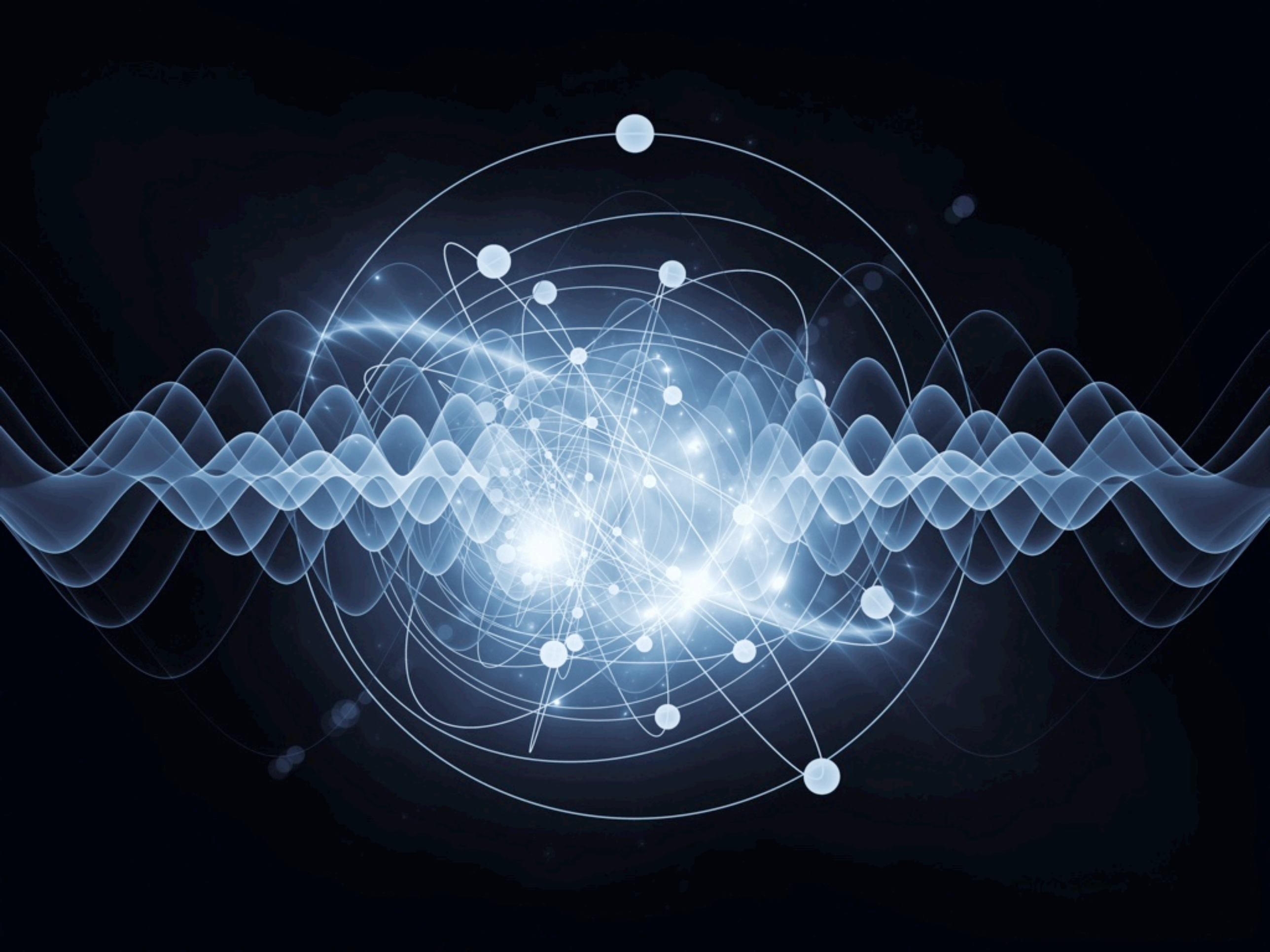
Rok Žitko

institut Jožef Stefan

in

Fakulteta za matematiko in fiziko Univerze v Ljubljani

Ljubljana, 13. 2. 2019



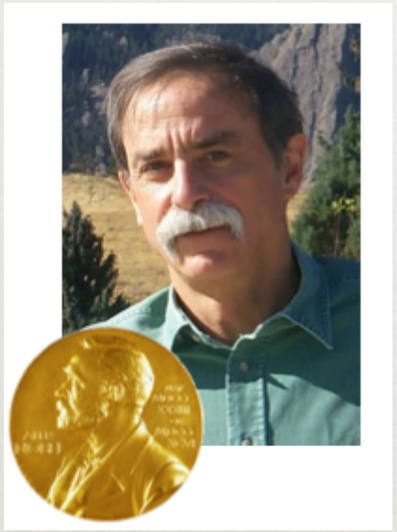
$$-\frac{\hbar^2}{2m}\frac{\partial^2\psi(x,t)}{\partial x^2}+V(x,t)\psi(x,t)=i\hbar\frac{\partial\psi(x,t)}{\partial t}$$

Erwin Schrödinger (1926)

superpozicija: $\psi(x,t)=\alpha\,\psi_1(x,t)+\beta\,\psi_2(x,t)$

“Nikoli ne opravljamo poizkusov z enim samim elektronom ali atomom ali (majhno) molekulo. V miselnih eksperimentih včasih predpostavimo prav to, pa zato vedno znova pridemo do trapastih zaključkov. ... Zato je treba priznati, da ne moremo eksperimentirati s posameznimi delci nič bolj, kot lahko vzgajamo ihtiozavre v živalskih vrtovih.”

E. Schrödinger, *Br. Jl. for Phil of Sci*. 3, 109 (1952)

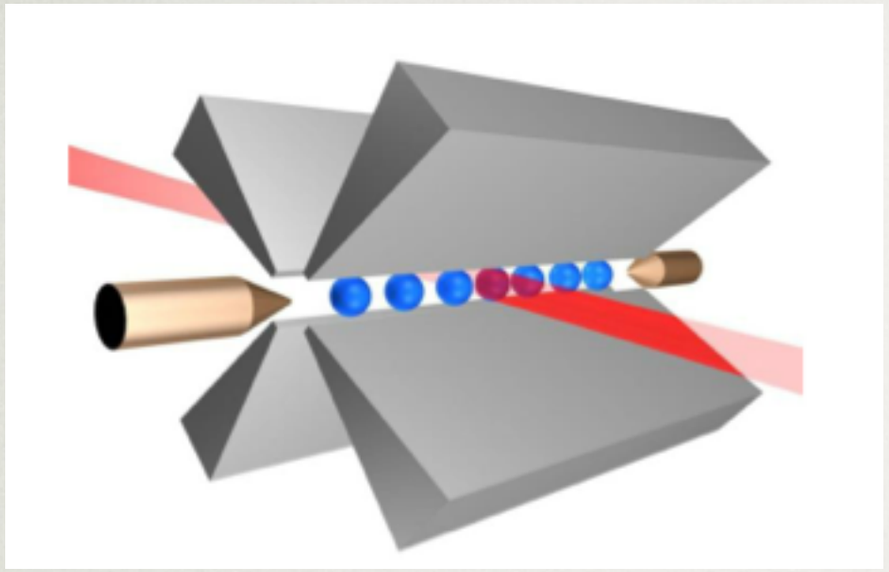


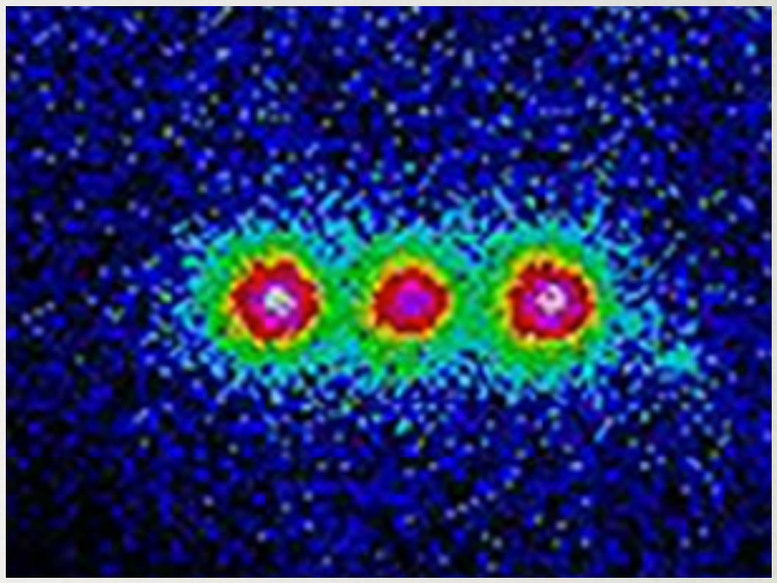
David J. Wineland in Serge Haroche

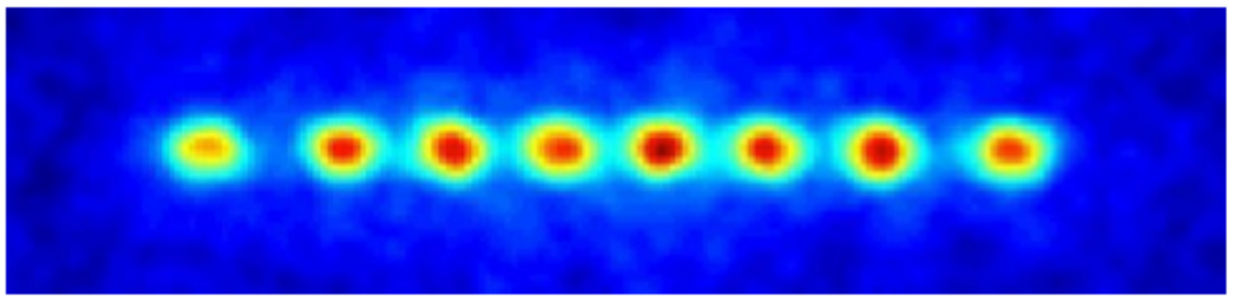
Nobelova nagrada za fiziko 2012

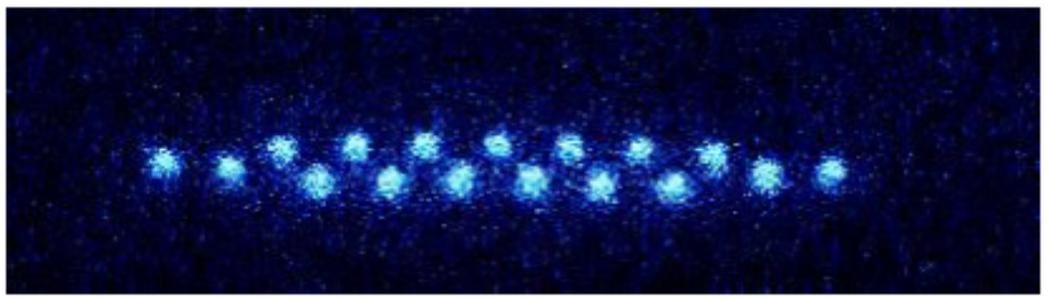
“za prelomne eksperimentalne metode, ki omogočajo merjenje in nadzor nad posameznimi kvantnimi sistemi, pri čemer se ohranijo njihove kvantne lastnosti, → superpozicija kar se je predhodno smatralo kot **nemogoče**”

Ionska past

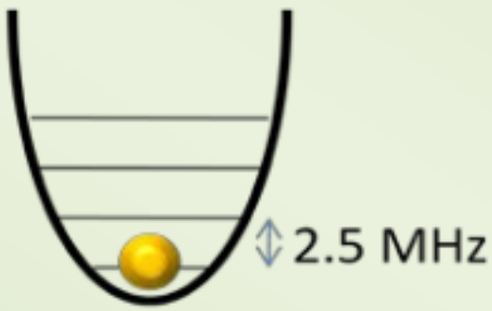


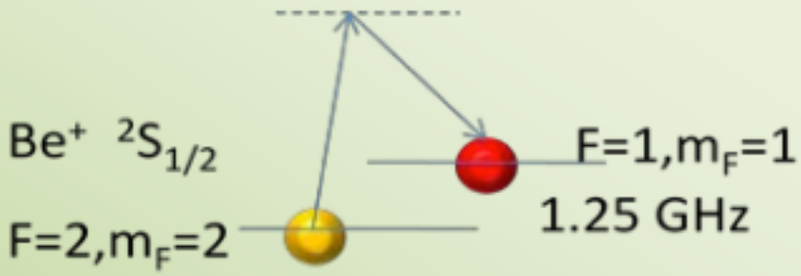






dvonivojski sistem





Weinland (1978, 1981)

KUBIT

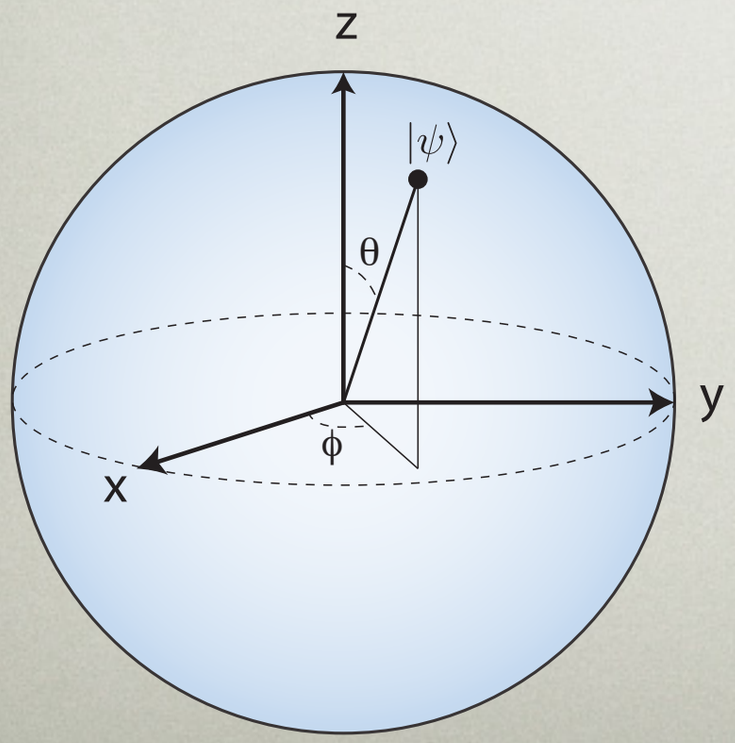
Informacija je neločljivo povezana s svojim fizičnim zapisom.

Rolf Landauer, Phys. Lett. A 217, 118 (1996)

računska baza: $|0\rangle, |1\rangle$

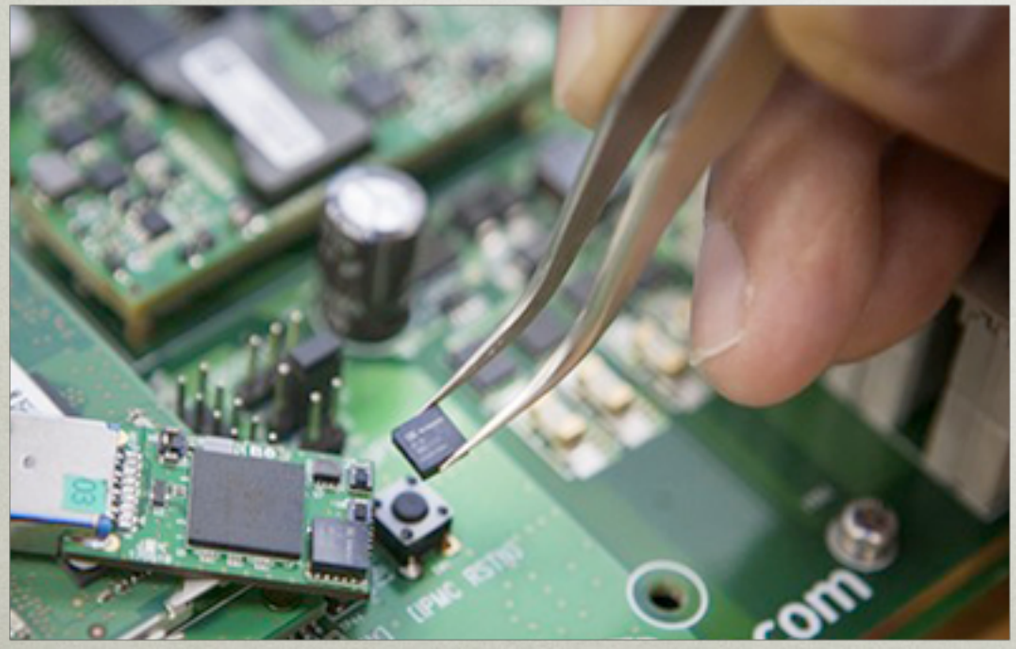
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

verjetnostni amplitudi



$$\alpha = \cos\frac{\theta}{2} \qquad \beta = e^{i\phi}\sin\frac{\theta}{2}$$

Kvantni generator naključnih števil



ID Quantique

Overview | Applications | Resources

- Lotteries & gaming
- Cryptography
- IT Security applications
- Quantum cryptography
- Password & PIN number generation
- Random seed generation
- Mobile prepaid systems
- Numerical simulations
- Statistical research

Kvantna enkripcija (izmenjava ključev)

Cerberis^3 QKD System

State-of-the-art Quantum Key Distribution

- Provably secure key exchange based on Quantum Key Distribution
- Quantum keys ensure long-term protection and forward secrecy
- Fully automated key exchange with continuous key renewal
- Integrated entropy source based on a Quantum Random Number Generator

ID Quantique

"Penetrating hard targets" (projekt NSA)

Excerpts from the "black budget," Volume 2, "Combined Cryptologic Program":

(U) RESEARCH & TECHNOLOGY (U) PENETRATING HARD TARGETS

(U) Project Description

(S//SI//REL TO USA, FVEY) The Penetrating Hard Targets Project provides proof-of-concept technological solutions to *{...}* enable:

{...}

- (S//SI//REL TO USA, FVEY) Breaking strong encryption.

(TS//SI//REL TO USA, FVEY) This Project focuses on meeting those customer requirements that will directly impact the end-to-end SIGINT mission during the next decade and beyond. It provides advanced knowledge of technology trends and opportunities to steer IT products and standards in a SIGINT-friendly direction. This Project contains the Penetrating Hard Targets Sub-Project.

(U) Base resources in this project are used to:

{...}

- (S//SI//REL TO USA, FVEY) Conduct basic research in quantum physics and architecture/engineering studies to determine if, and how, a cryptologically useful quantum computer can be built.

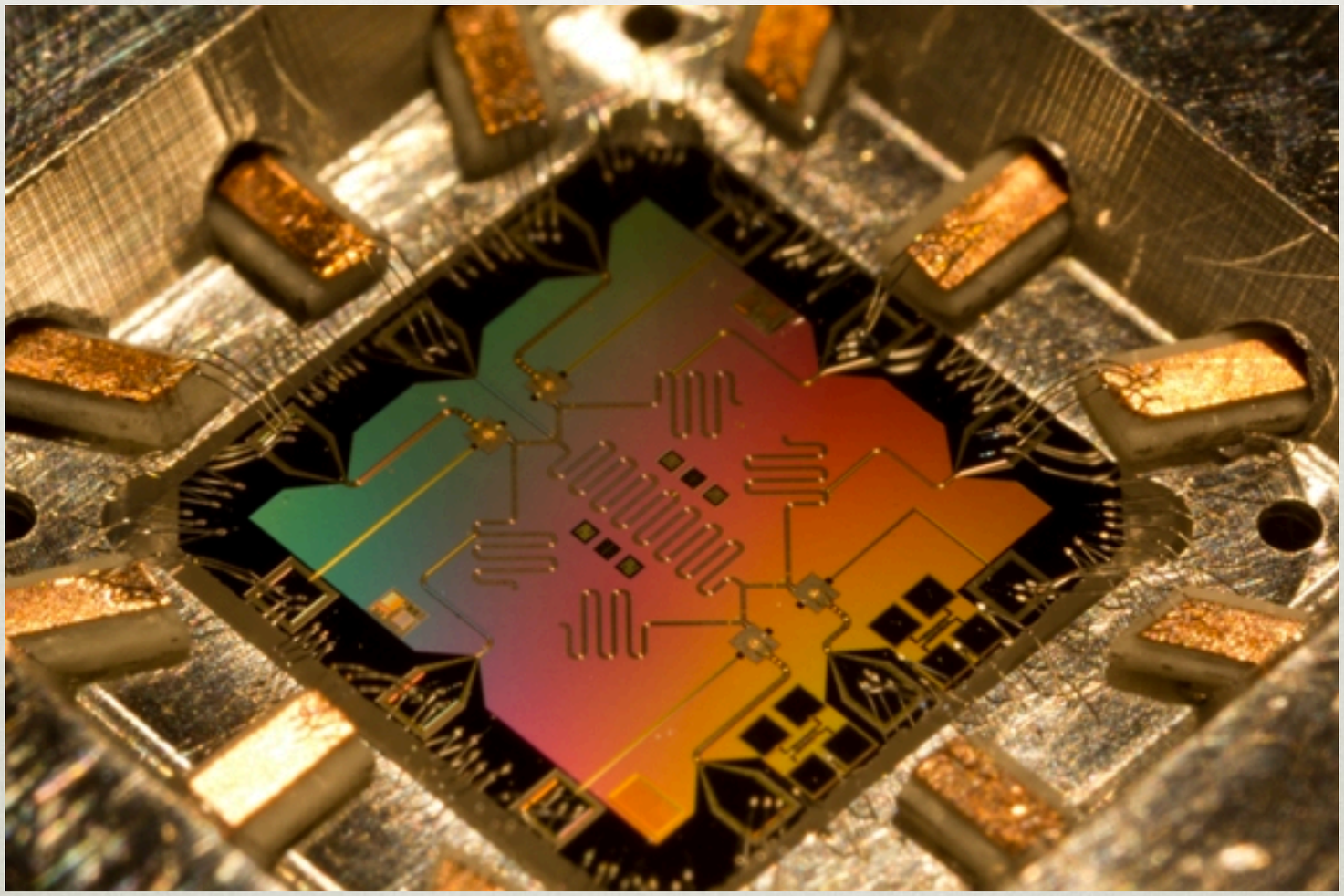
(razkril Snowden)

The $^{43}Ca^{+}$ ion trap quantum computer

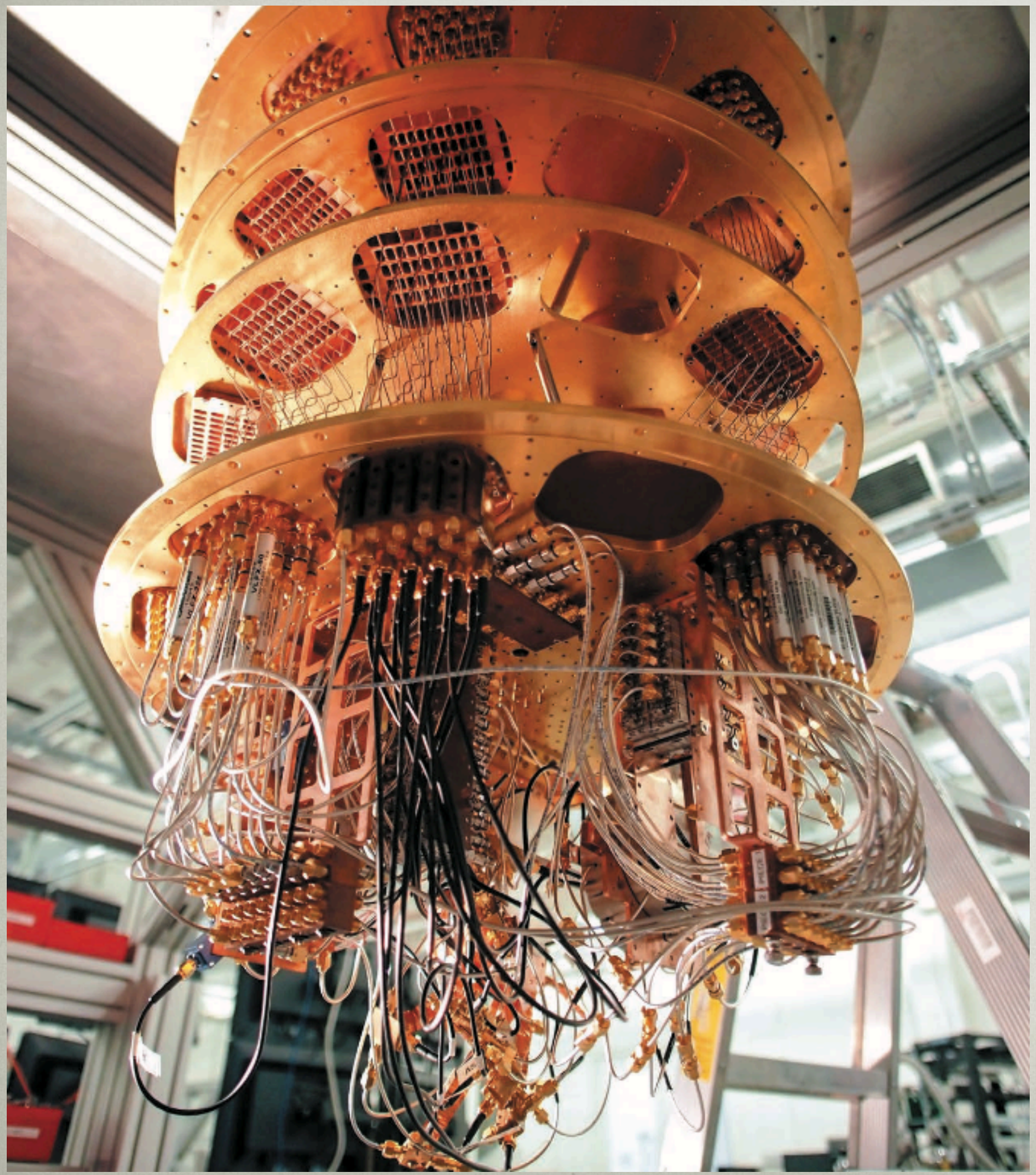
R. Blatt, Innsbruck

Kvantni procesor z gradniki SQUID

SQUID = superprevodniška interferenčna naprava



skupina Johna Martinisa,
Univerza v Kaliforniji v Santa Barbari in **Google**



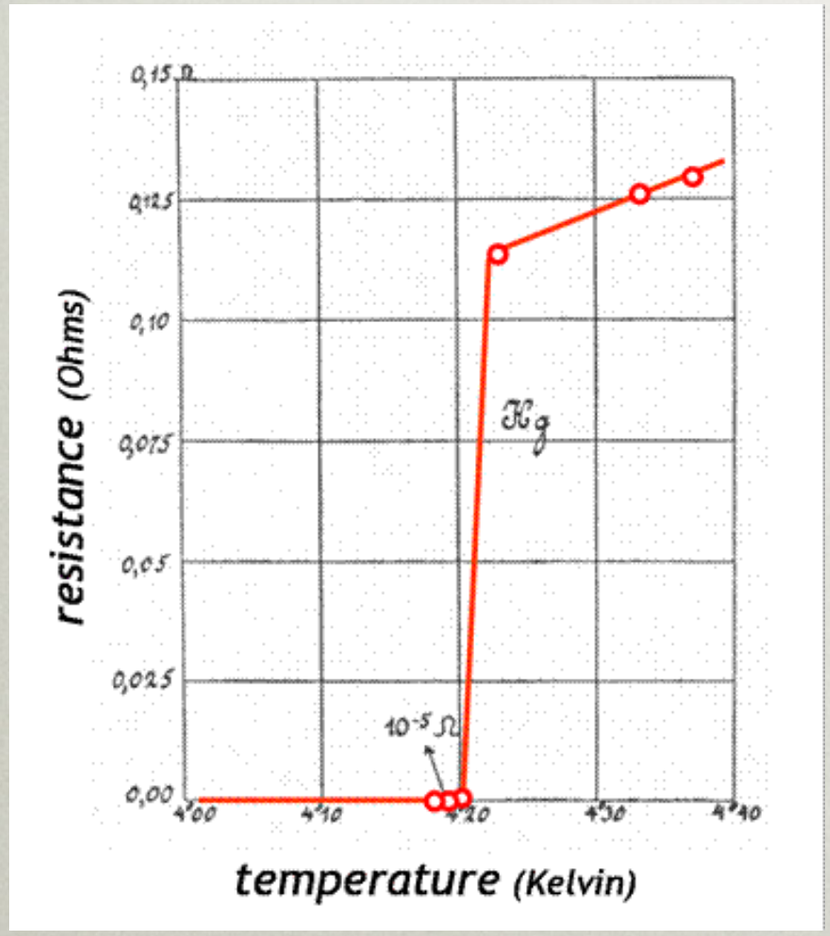
ohlajeni del dilucijskega hladilnika

$T \approx 10\,\mathrm{mK}$

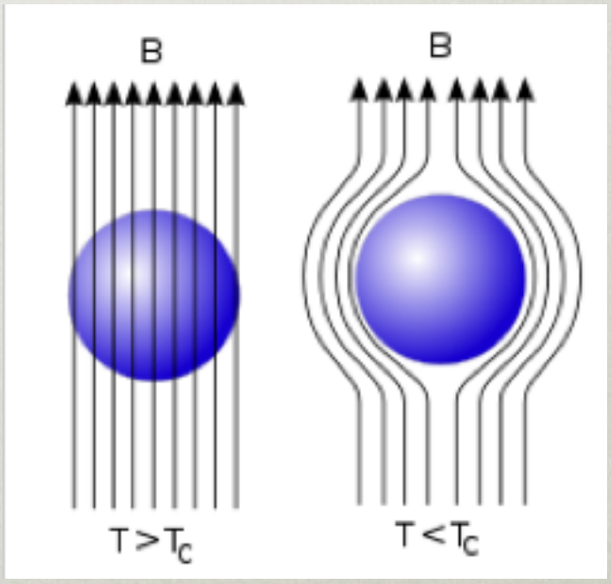
H. K. Onnes

1908: tekoči He
1911: superprevodnost

Nobelova nagrada za fiziko 1913

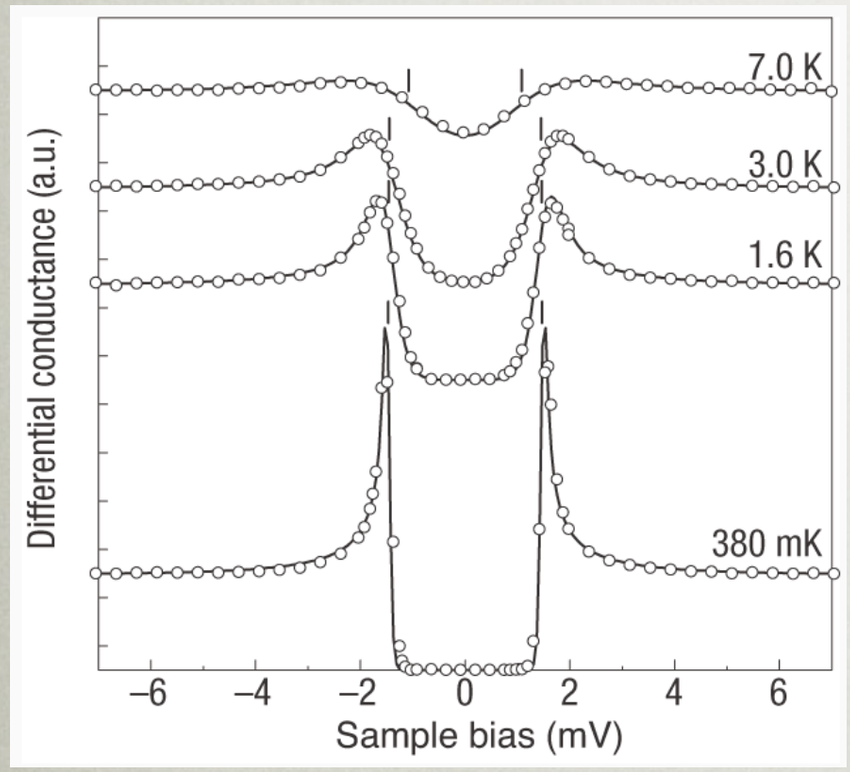


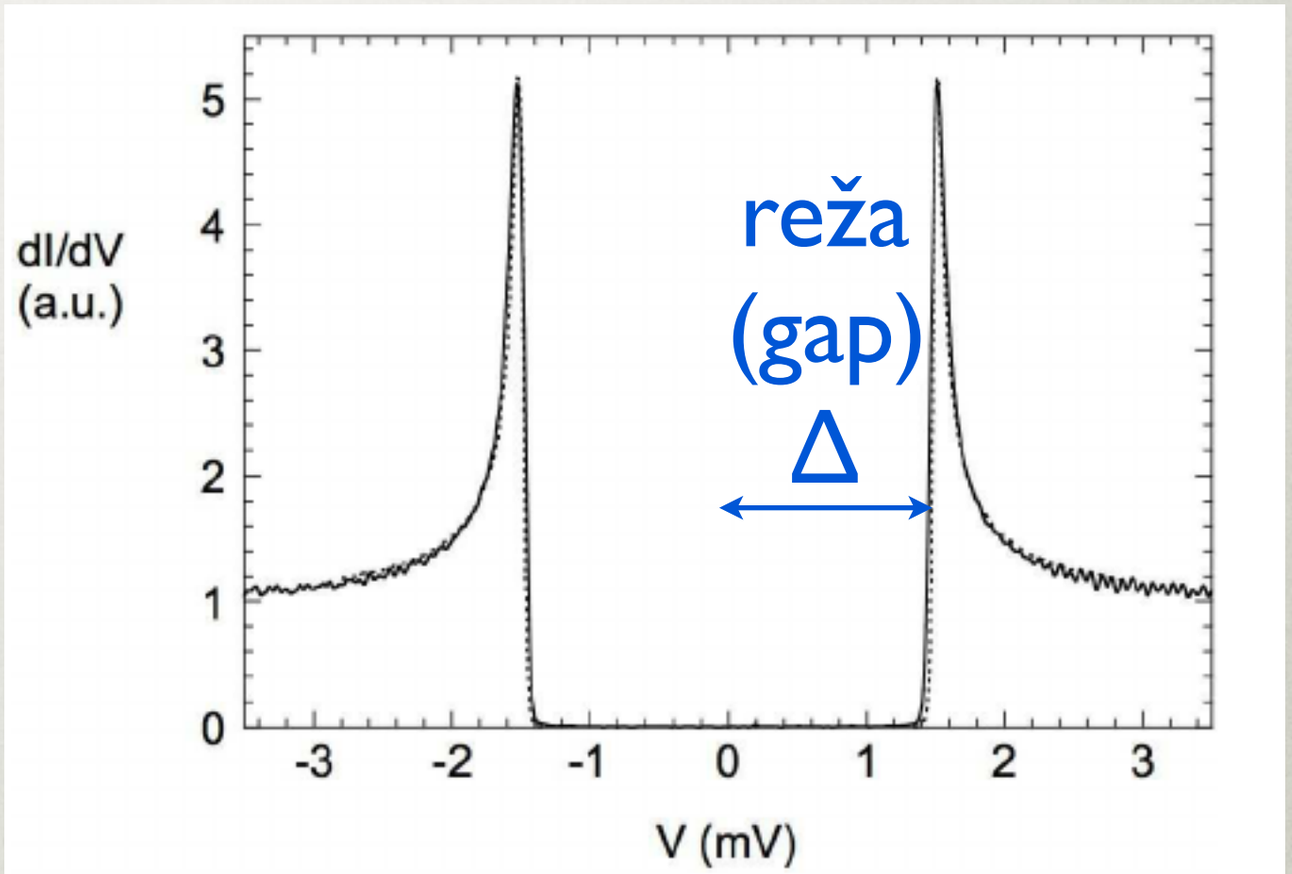
Meissnerjev pojav



Meissner, Ochsenfeld (1933)

Superprevodniška energijska reža





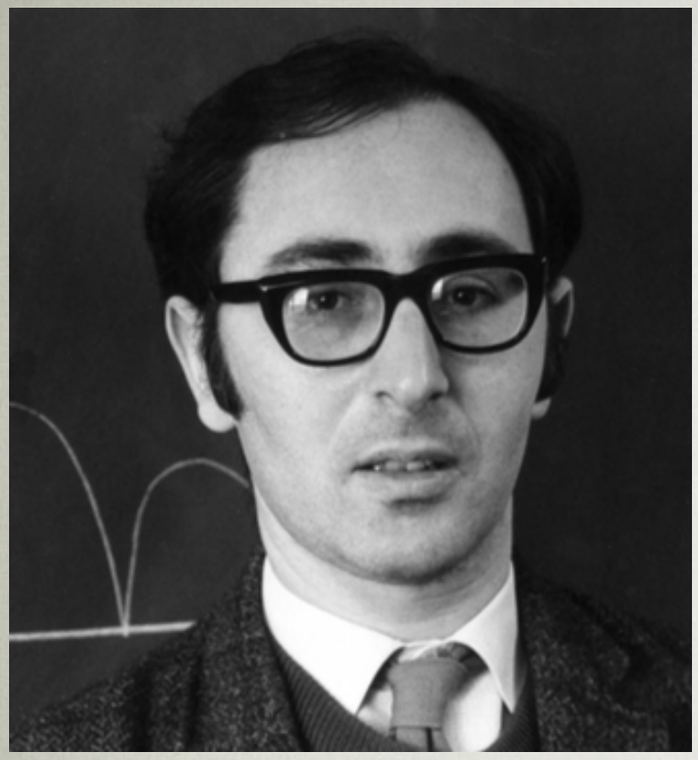
○ meritev

— teorija BCS

Nb, T=170mK, Δ=1.5meV

H. Courtois, Grenoble
PRB (2005)

spektri diferencialne prevodnosti (dI/dV) superprevodnega vzorca izmerjeni z vrstičnim tunelskim mikroskopom (STM)

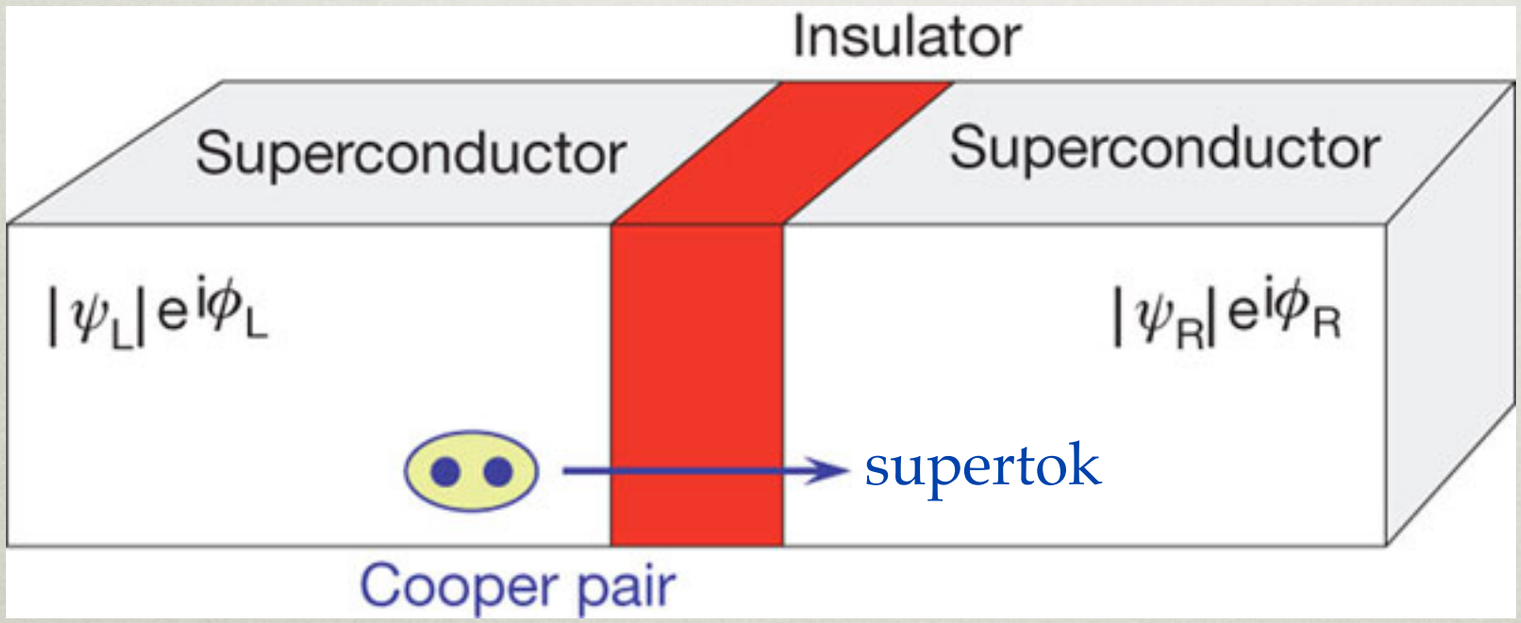


Brian Josephson

teorija: 1962

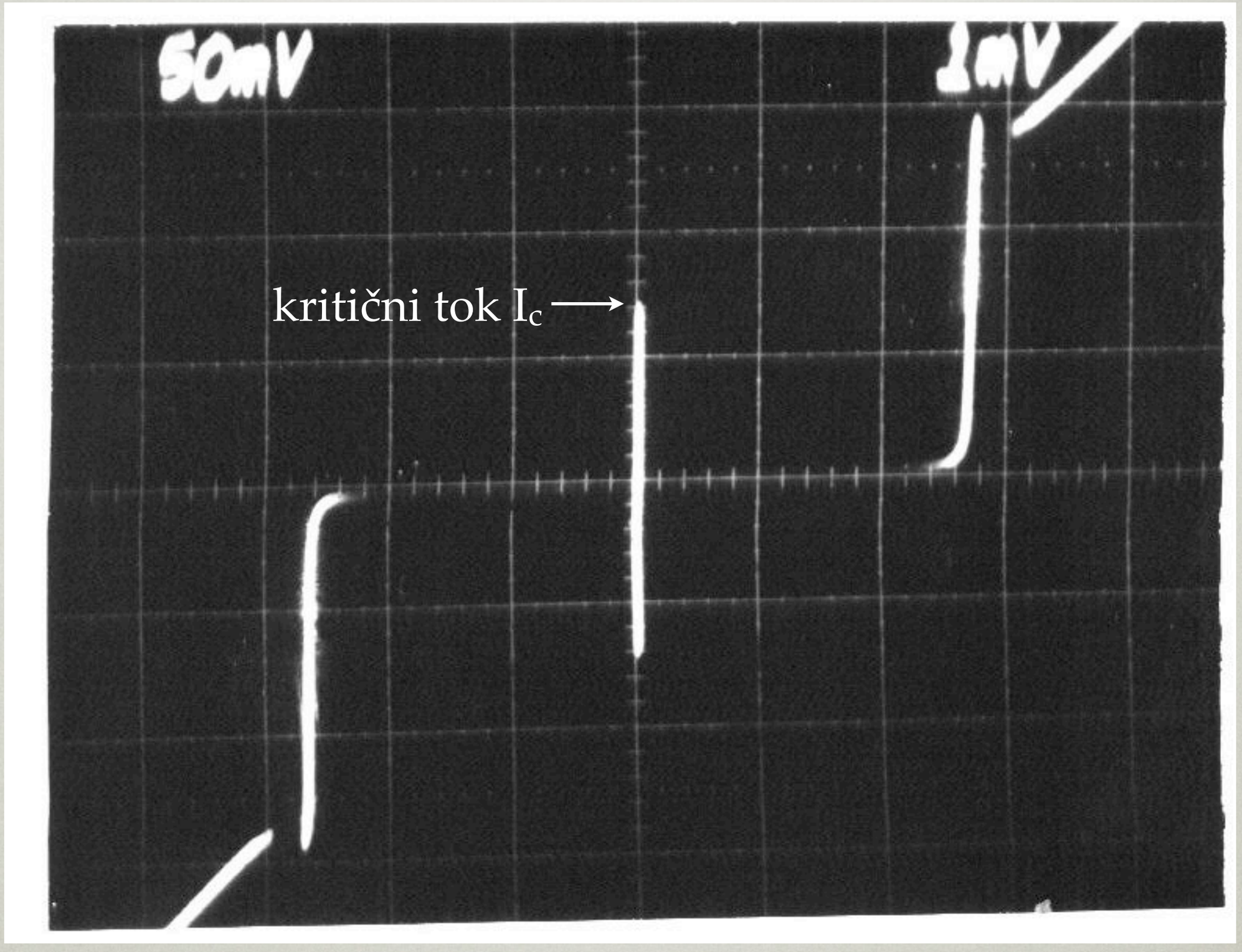
(pri 22 letih)

Nobelova 1973



$$I(t) = I_c \sin[\Delta\phi(t)] \qquad U(t) = \frac{\hbar}{2e}\frac{\mathrm{d}\Delta\phi(t)}{\mathrm{d}t}$$

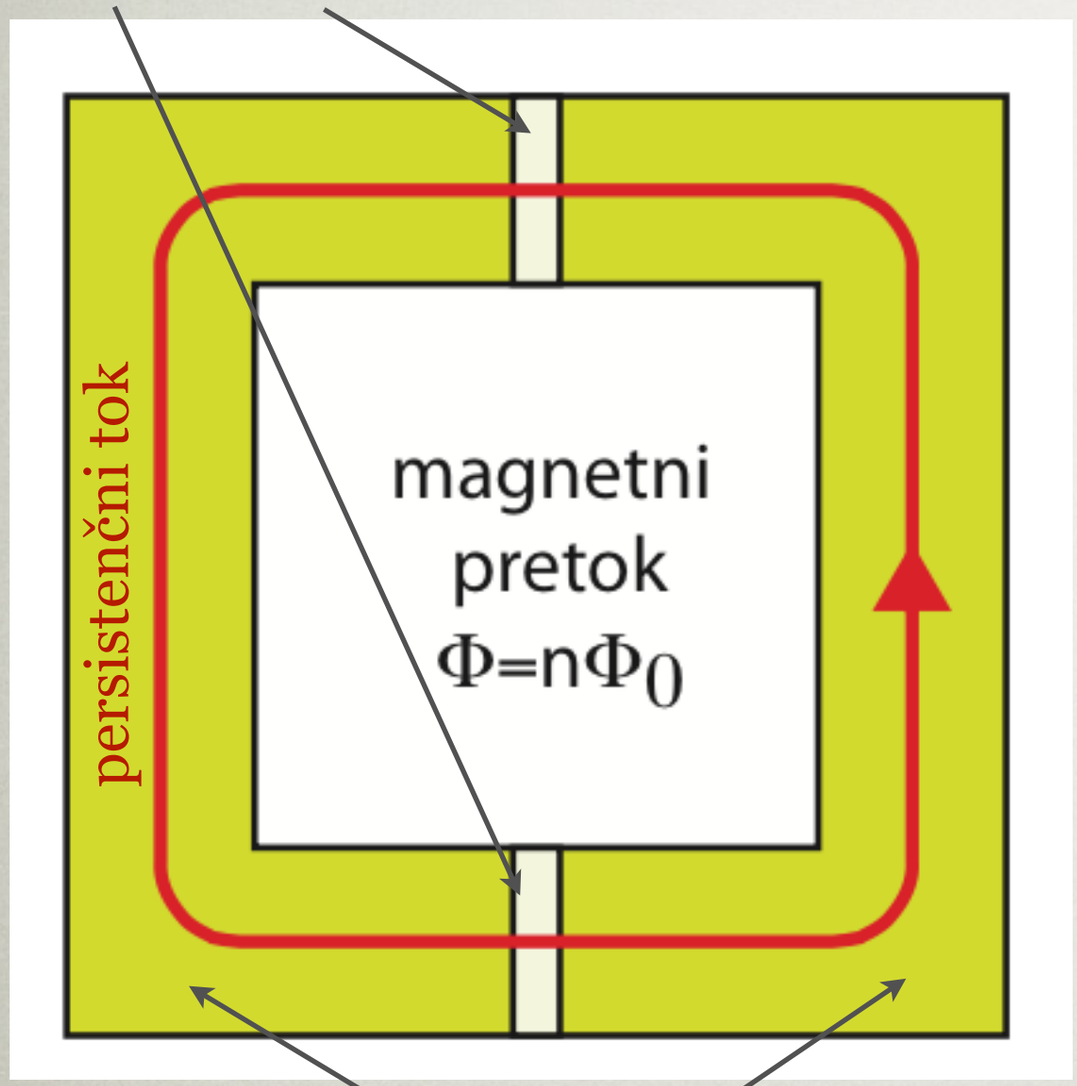
$$I(t) = I_c \sin[\Delta\phi(t)]$$



tok

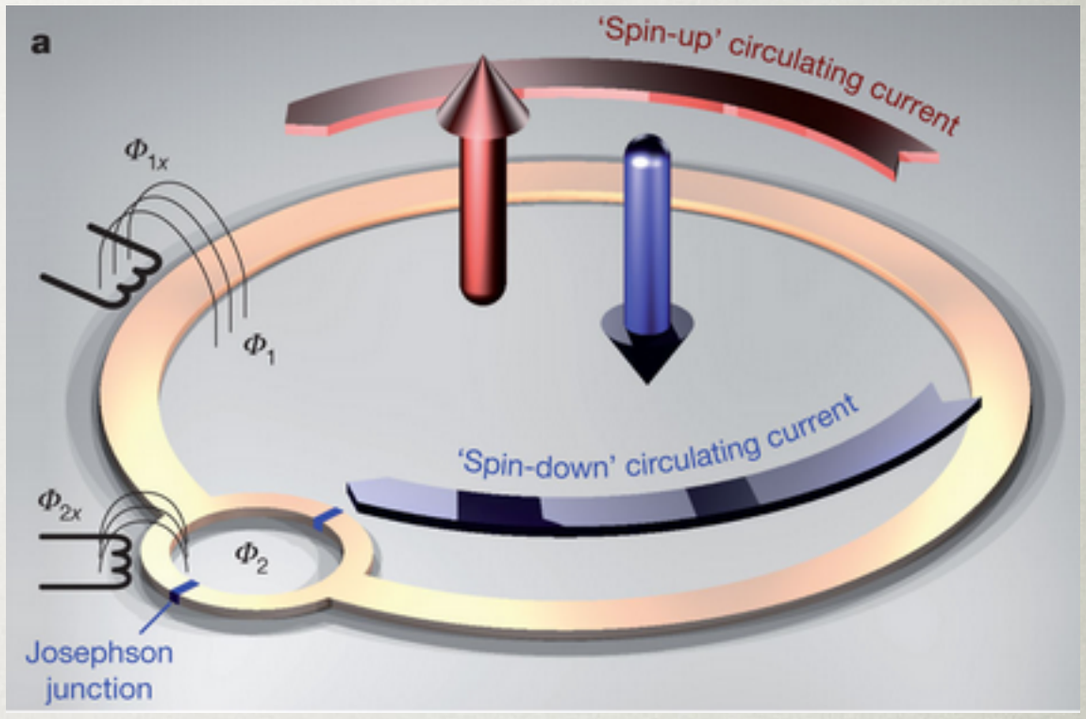
napetost

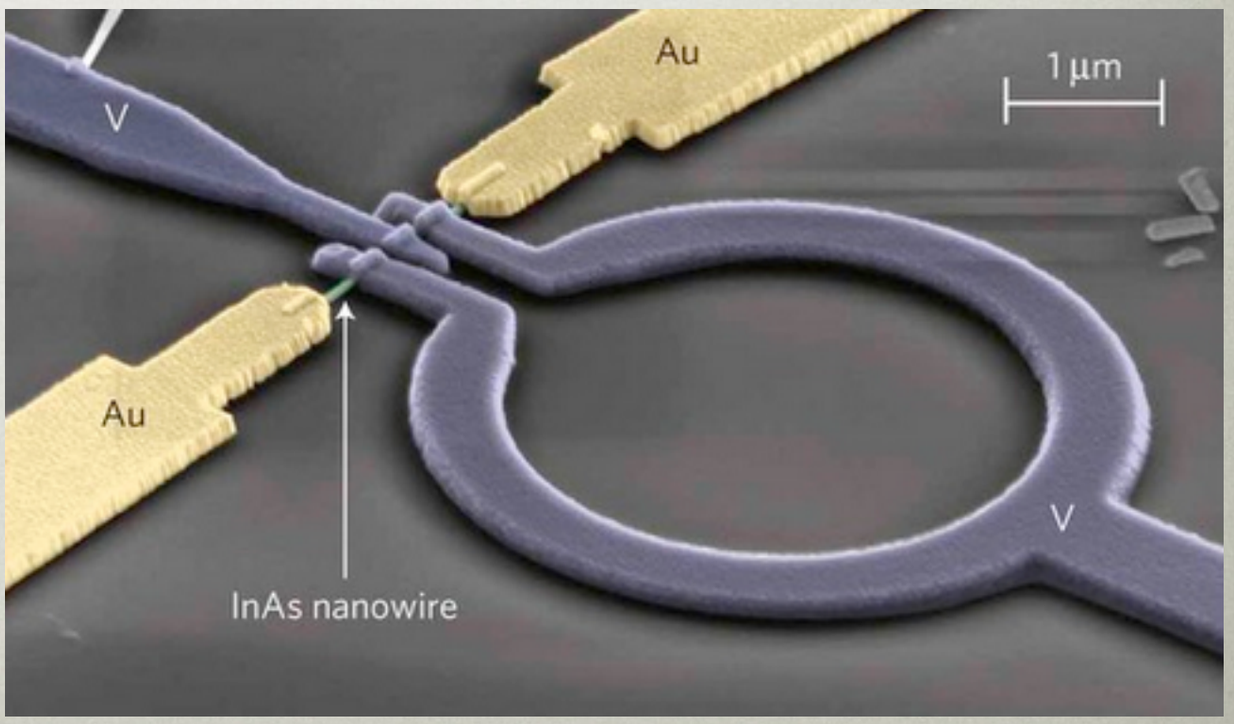
SQUID = superprevodniška interferenčna naprava



$$\Phi = B \times S$$

$$\Phi_0 = \frac{h}{2e}$$ kvant fluksa





Giazotto et al. (2011)

KVANTNI REGISTER VELIKOSTI N

nabor N kubitov = tenzorski produkt dvonivojskih sistemov

$\dim = 2^N$

primer: N=2

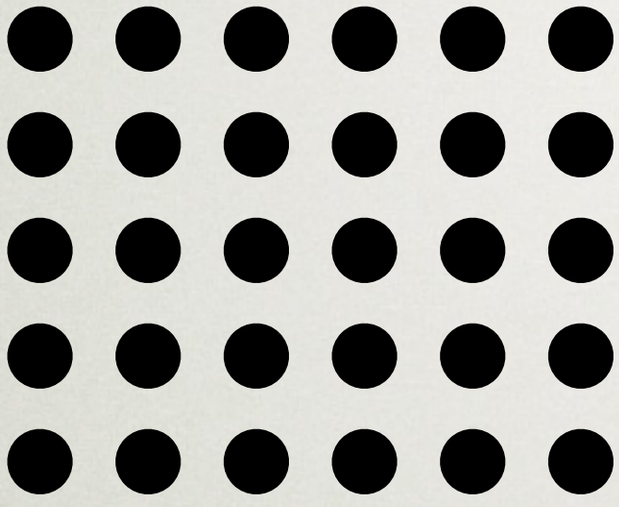
$$\psi = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

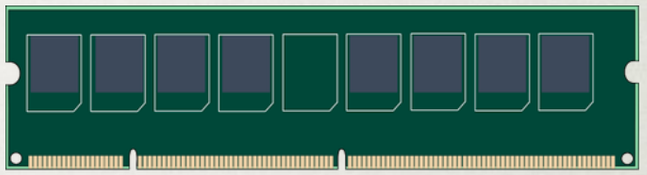
6 realnih parametrov

vs.

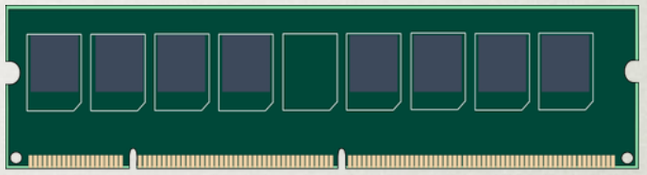
2×2=4 realni parameteri za dva neodvisna in ločena kubita

dodatna "skrita" informacija





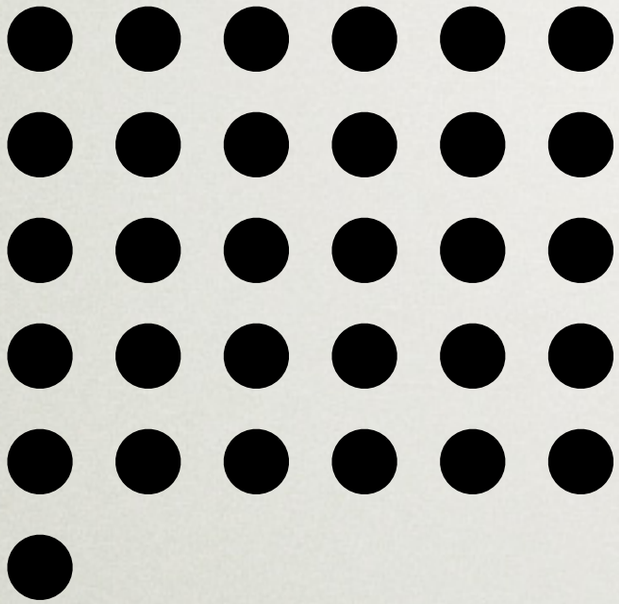
DIMM Memory



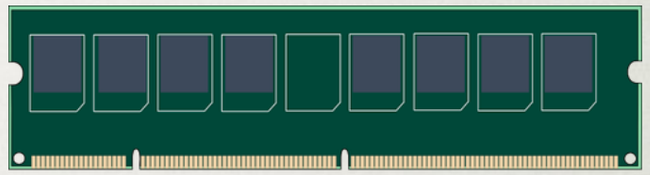
DIMM Memory

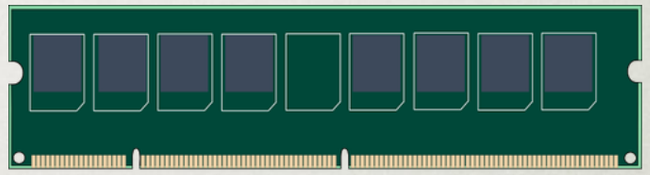
30 kubitov

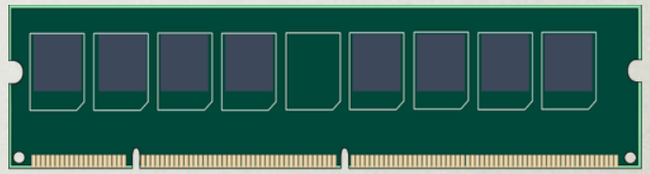
16 GB pomnilnika

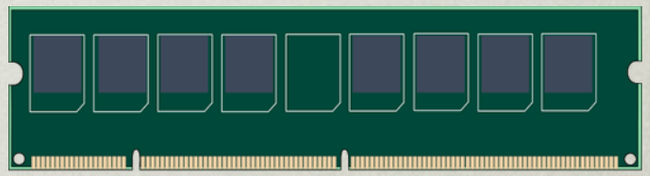


31 kubitov

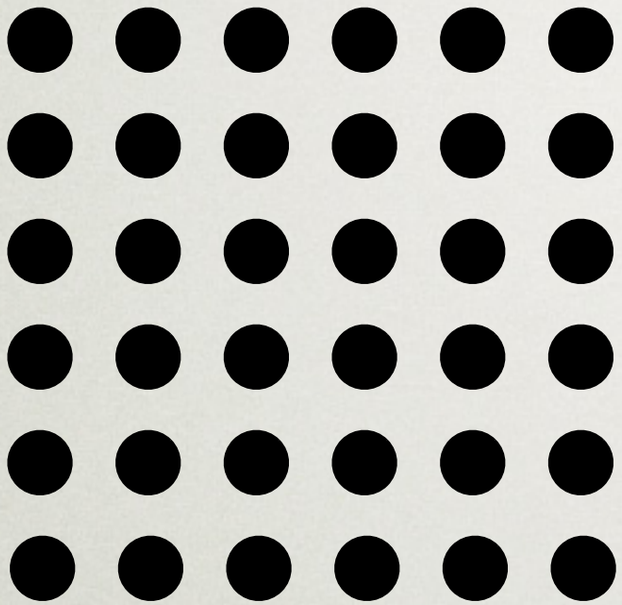




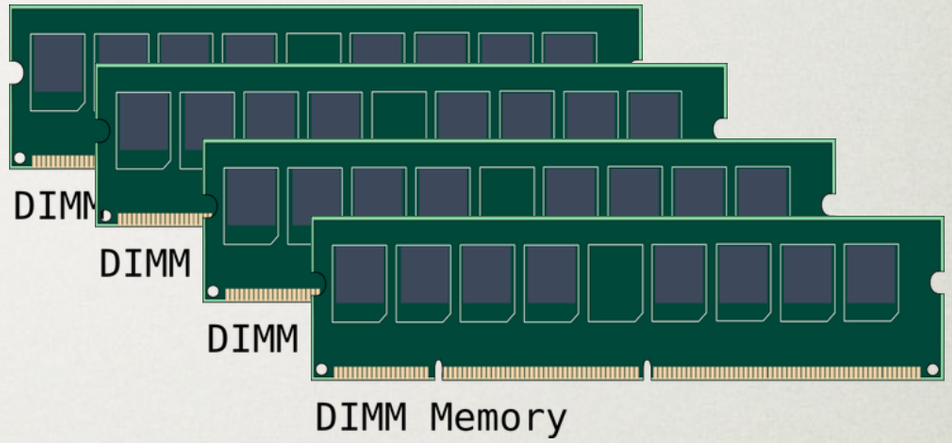




32 GB pomnilnika



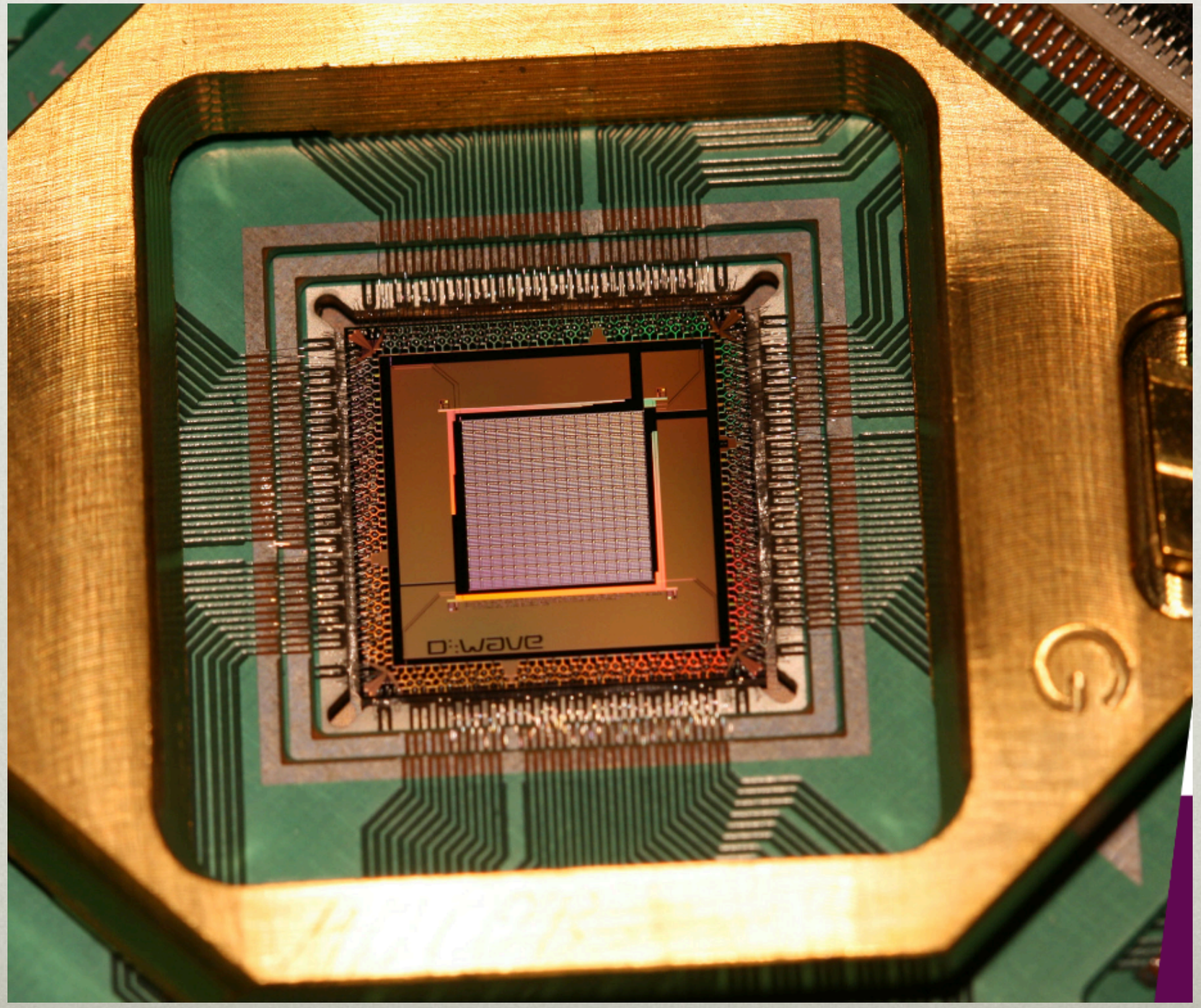
36 kubitov



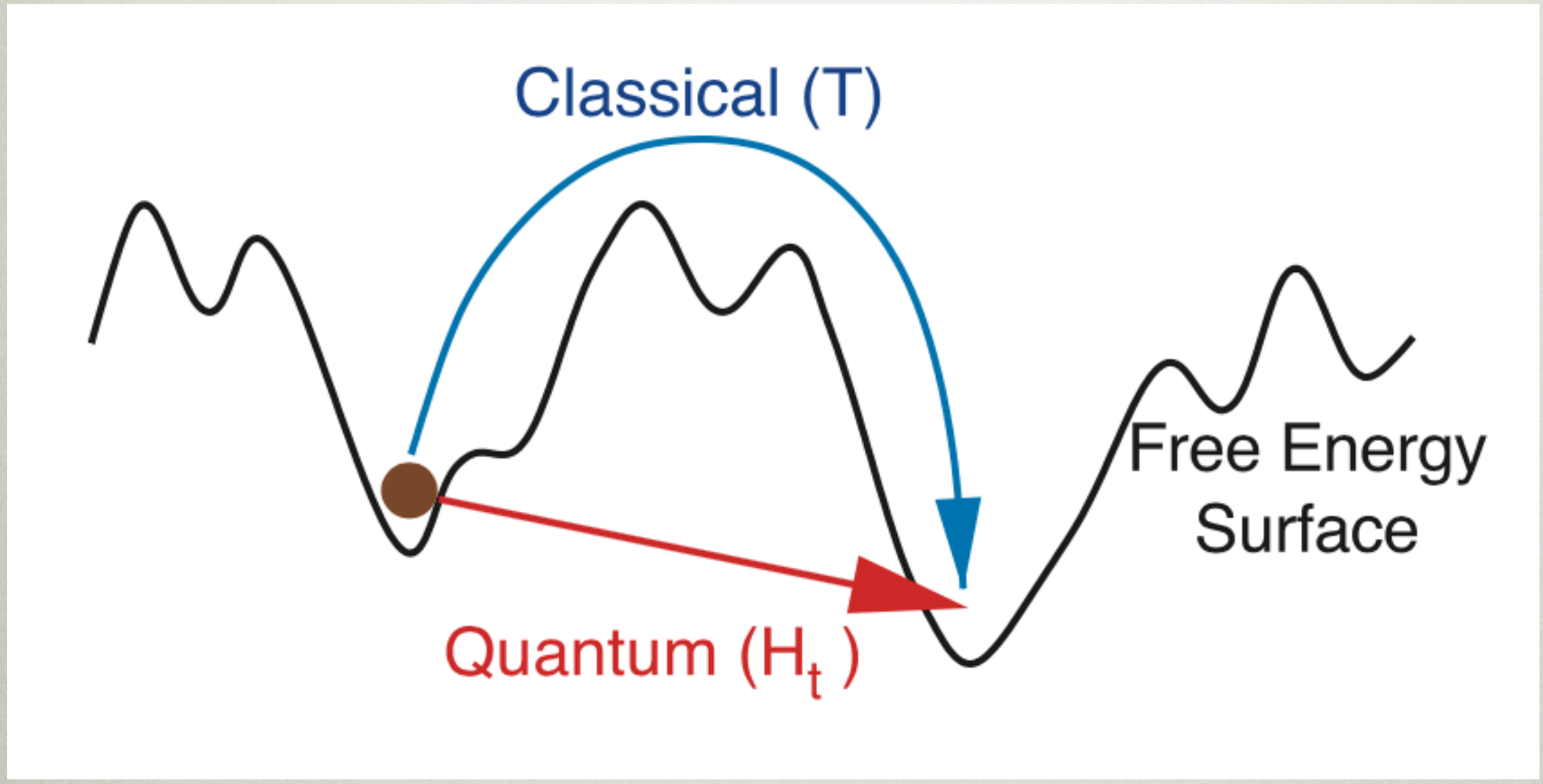
...

1 TB pomnilnika

Kvantni procesor podjetja DWave



Kvantno popuščanje (quantum annealing)



Kvantna prepletenost

kvantno stanje, pri katerem ne moremo opisati podsistem A neodvisno od podsistema B (tudi če sta ločena v prostoru)

Bellovo stanje: $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

močnejše korelacije kot v kateremkoli klasičnem stanju

eksperimentalno potrjeno leta 1972 (Alain Aspect),
dokočno in neizpodbitno pa leta 2015 (“loophole-free Bell tests”)

Računski model "kvantnega vezja"

$$|\psi\rangle \text{ ————}$$

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

OSNOVNA ENOKUBITNA VRATA

bit-flip

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$|0\rangle \to |1\rangle, |1\rangle \to |0\rangle$$

phase-flip

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|0\rangle \to |0\rangle, |1\rangle \to -|1\rangle$$

Hadamard

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

$$|0\rangle \to \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$
$$|1\rangle \to \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

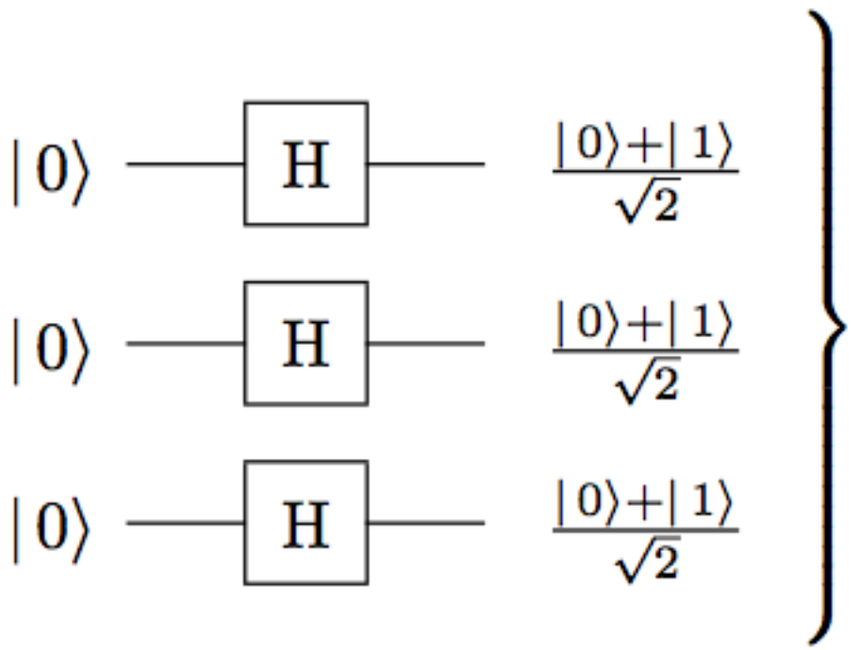
phase-gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

π/8 gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Hadamardova transformacija



IN BINARY

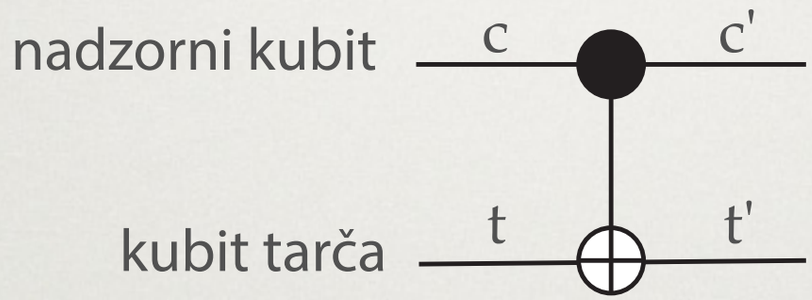
$$= \frac{1}{2^{3/2}} \left\{ \begin{array}{l} |000\rangle + |001\rangle + |010\rangle + |011\rangle + \\ + |100\rangle + |101\rangle + |110\rangle + |111\rangle \end{array} \right\}$$

$$= \frac{1}{2^{3/2}} \left\{ \begin{array}{l} |0\rangle + |1\rangle + |2\rangle + |3\rangle + \\ + |4\rangle + |5\rangle + |6\rangle + |7\rangle \end{array} \right\}$$

IN DECIMAL

Dvokubitna vrata

nadzorovani NE (controlled NOT = CNOT)

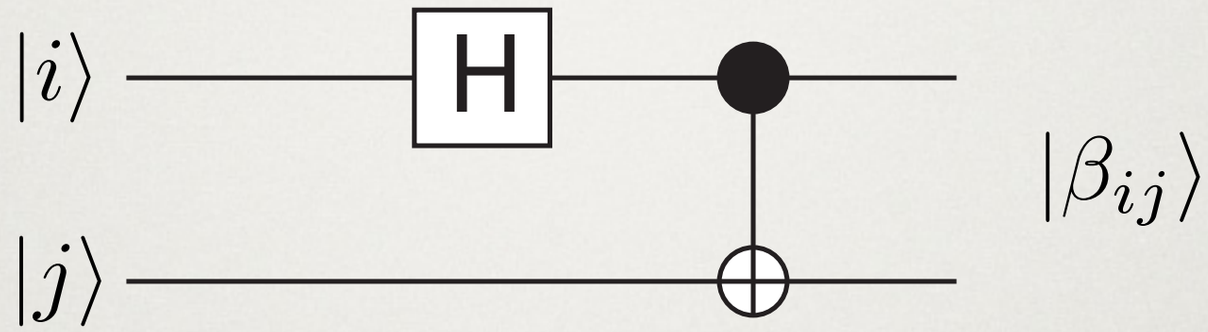


c	t	c′	t′
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

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

univerzalni nabor vrat: CNOT, H, S, T

Prepletane kubitov



Bellova prepletena stanja:

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

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

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

Katere probleme lahko rešujemo?

- vsi klasični algoritmi

- algebrajski problemi

(razcep na prafaktorje, izračun diskretnih logaritmov, razcep Abelovih grup,..)

- iskanje po neurejenih seznamih

(Groverjev algoritem)

- določanje topoloških invariant

(Jonesov polinom)

- reševanje linearnih sistemov enačb

(reševanje enačb, metoda najmanjših kvadratov, strojno učenje)

- simulacije kvantnih sistemov

http://math.nist.gov/quantum/zoo/

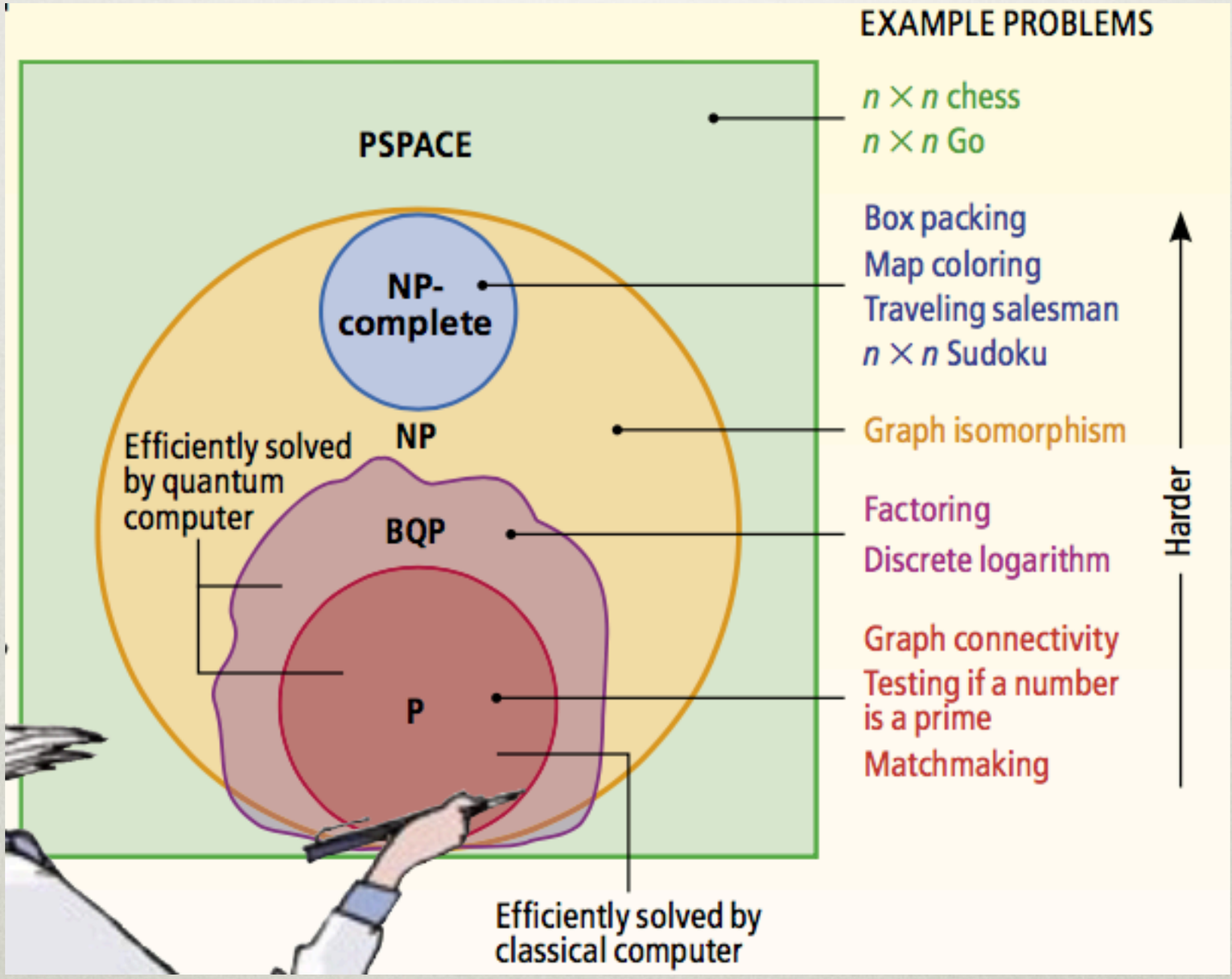
Kaj kvantni računlanik *ni*?

Kvantni računalnik ni klasični računalnik z visokim taktom.

Kvantni računalnik ne more vzporedno preizkusiti vseh možnosti in poiskati pravilne.

Verjetno ni učinkovitih kvantnih algoritmov za NP-polne probleme.

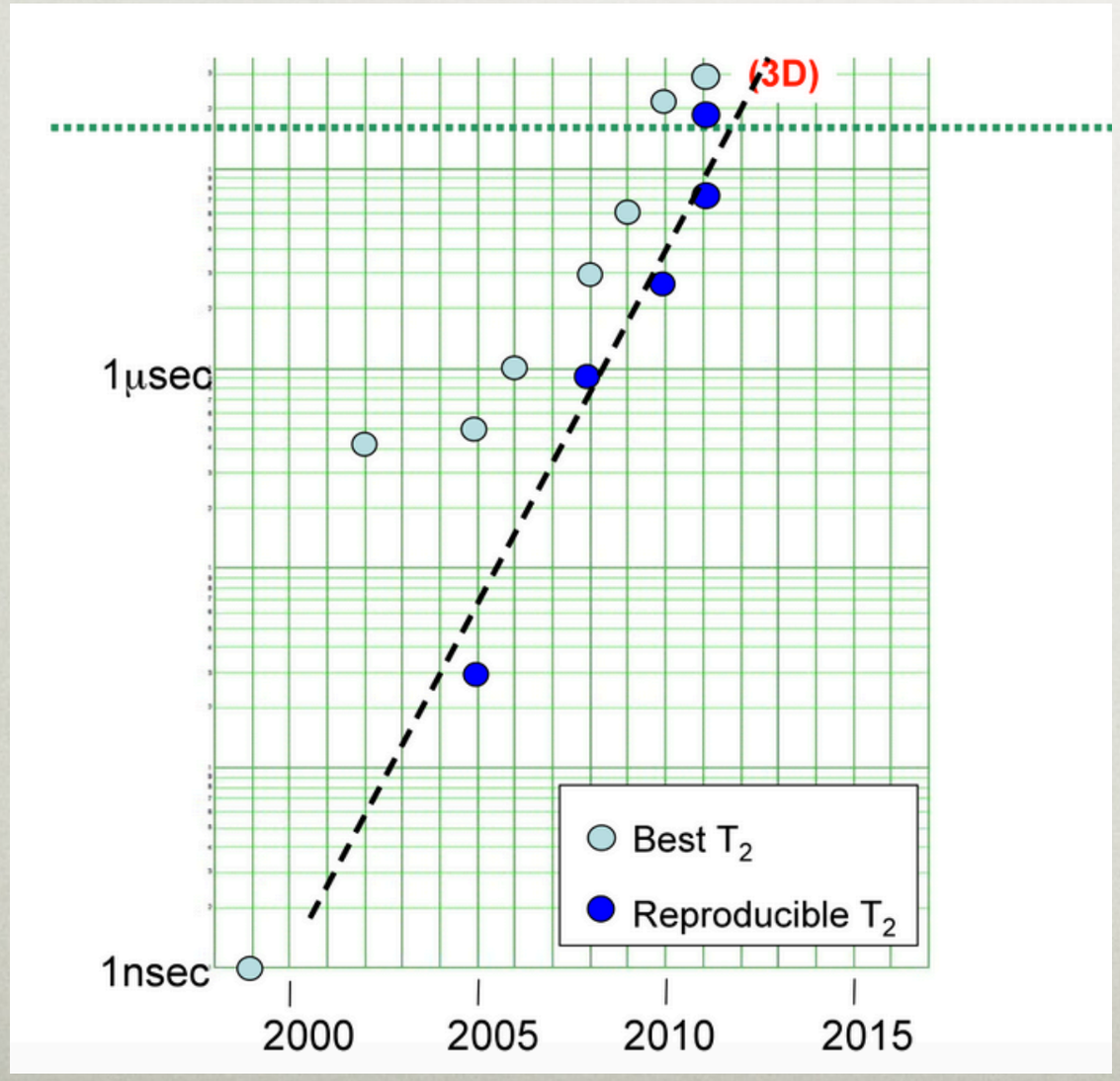
BQP = bounded-error, quantum, polynomial time



Scott Aaronson, Sci. Am. 62, marec 2008

Problem dekoherence

Motnje iz okolice (nehotena interakcija med računalnikom in okolico) kvarijo kvantno stanje.



koherenčni čas (T_2) superprevodnih kubitov

izrek o nezmožnosti kopiranja kvantne informacije

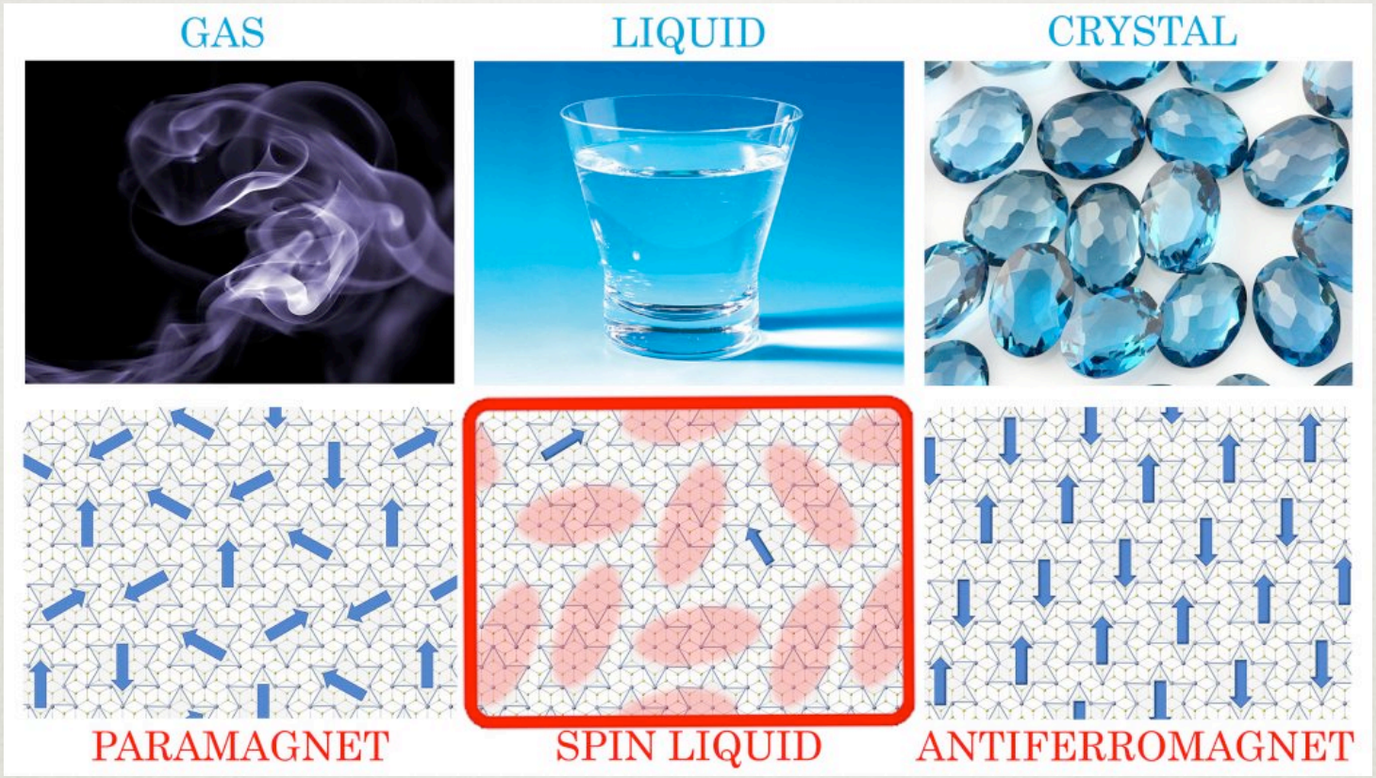
Wooters, Zurek, Dieks (1982)

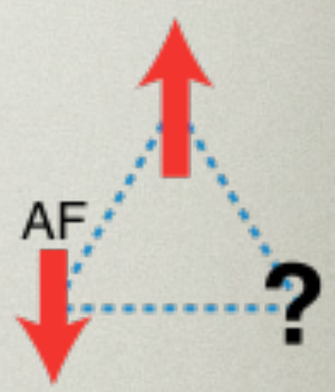
Topološka stanja

https://www.youtube.com/watch?v=9NlqYr6-TpA

- informacijo zapišemo nelokalno v razsežnem sistemu z N enakovrednimi osnovnimi stanji
- stanje je neobčutljivo na lokalne motnje
- opravljamo lahko unitarne transformacije nad N-krat degeneriranim osnovnim stanjem - ekvivalentno računanju!

Kvantne spinske tekočine



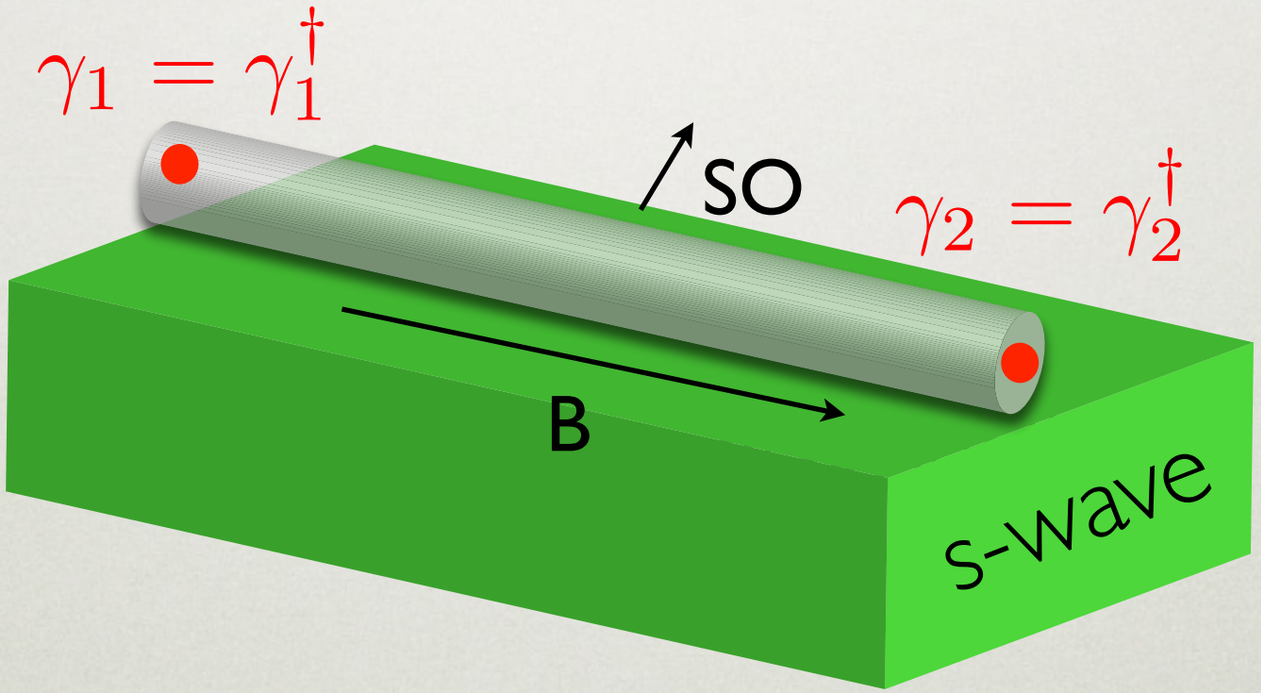


odsotnost ureditve zaradi kvantnih fluktuacij in/ali magnetne frustracije

nekatere spinske tekočine so močno kvantno prepletene in so topološko urejene

M. Klanjšek et al., Nature Physics 13, 1130 (2017)
N. Janša et al., Nature Physics 14, 786 (2018)

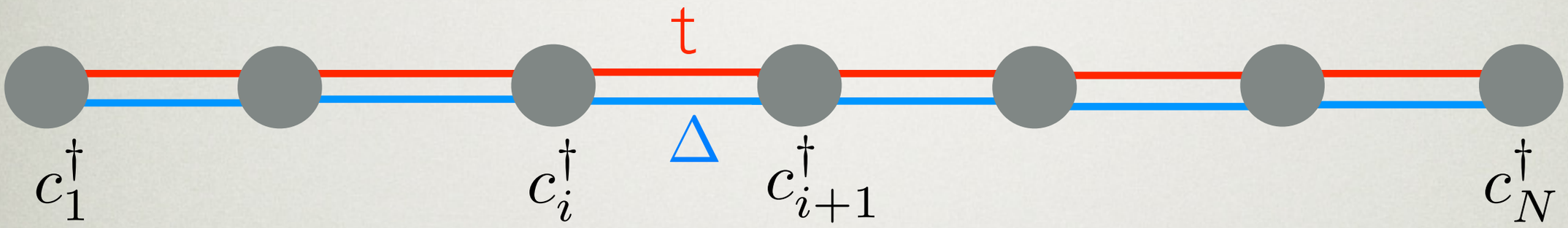
Majoranova stanja v nanožicah



Model Kitaeva

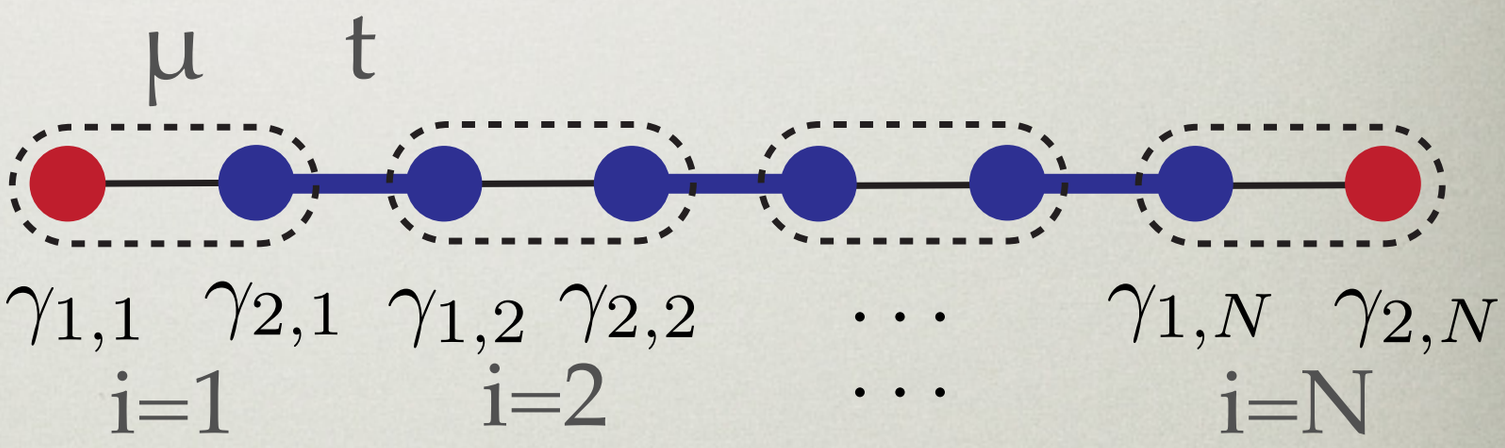
Kitaev (2000)

$$H = \sum_i t\left(c_i^\dagger c_{i+1} + c_{i+1}^\dagger c_i\right) - \mu c_i^\dagger c_i + \Delta\left(c_i c_{i+1} + c_{i+1}^\dagger c_i^\dagger\right)$$



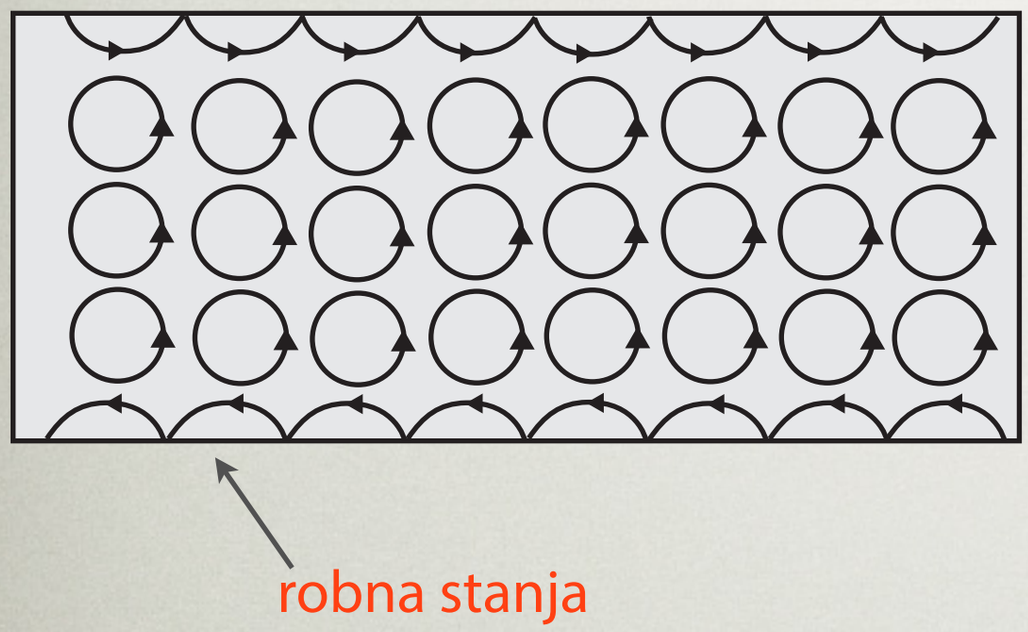
$$c_i \rightarrow \gamma_{1i} + i\gamma_{2i}$$

$$\gamma = \gamma^\dagger$$

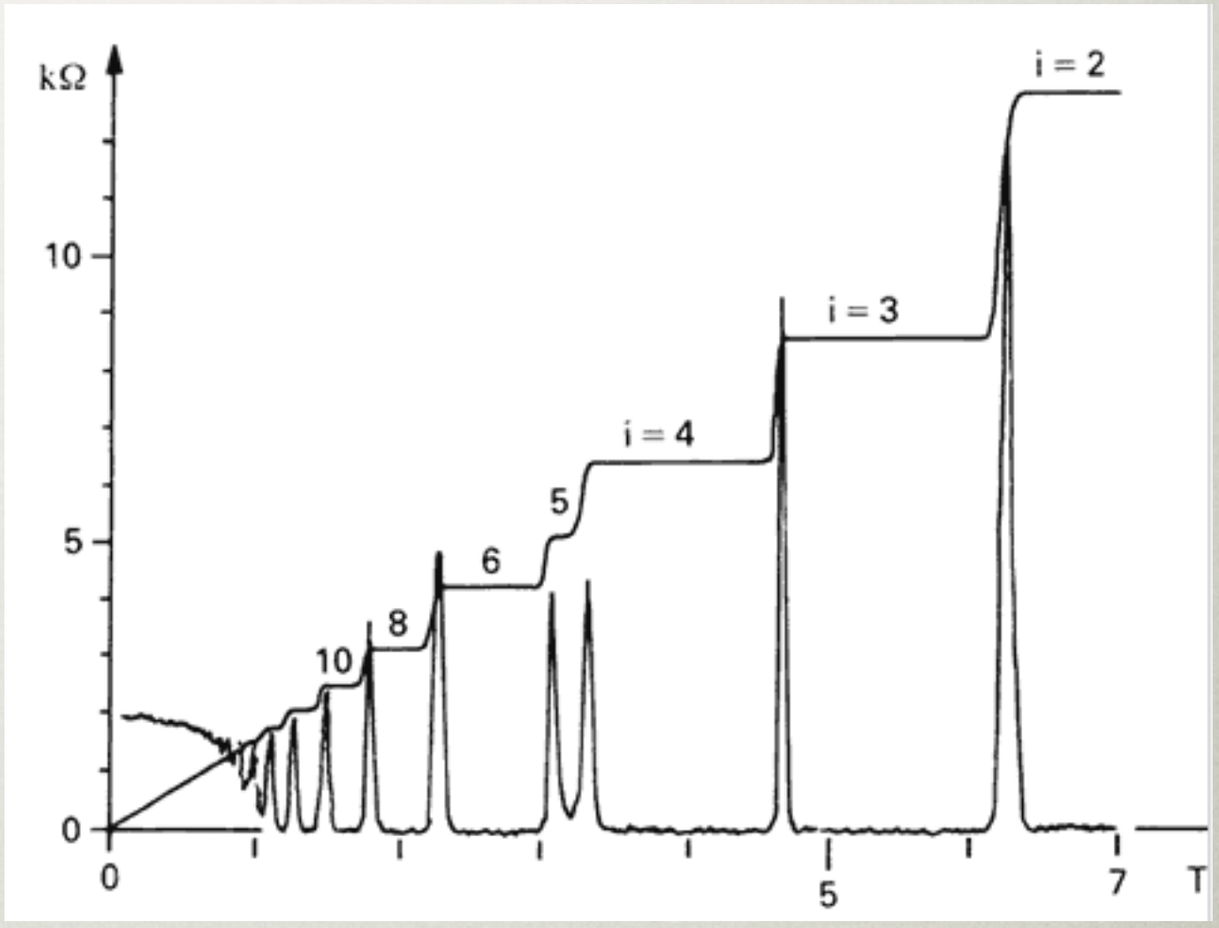


Celoštevilski kvantni Hallov pojav

dvodimenzionalni elektronski plih
v močnem magnetnem polju



robna stanja



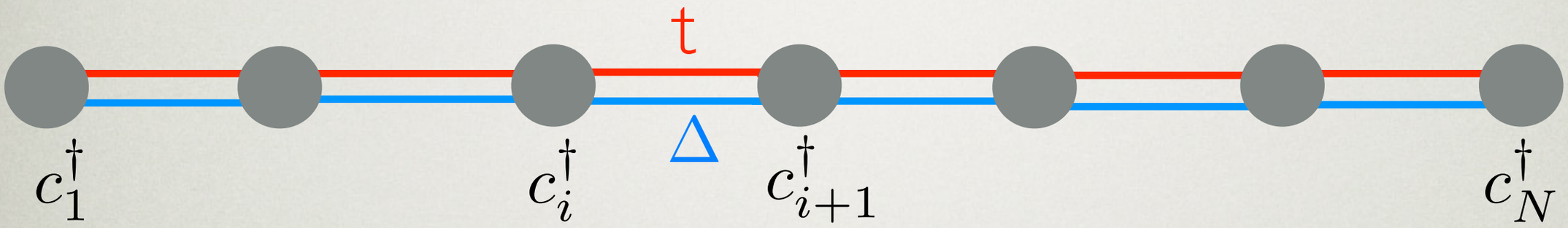
$$\rho_{xy} = \frac{h}{e^2}\frac{1}{N}$$

Nobelova nagrada leta 1985: von Klitzing

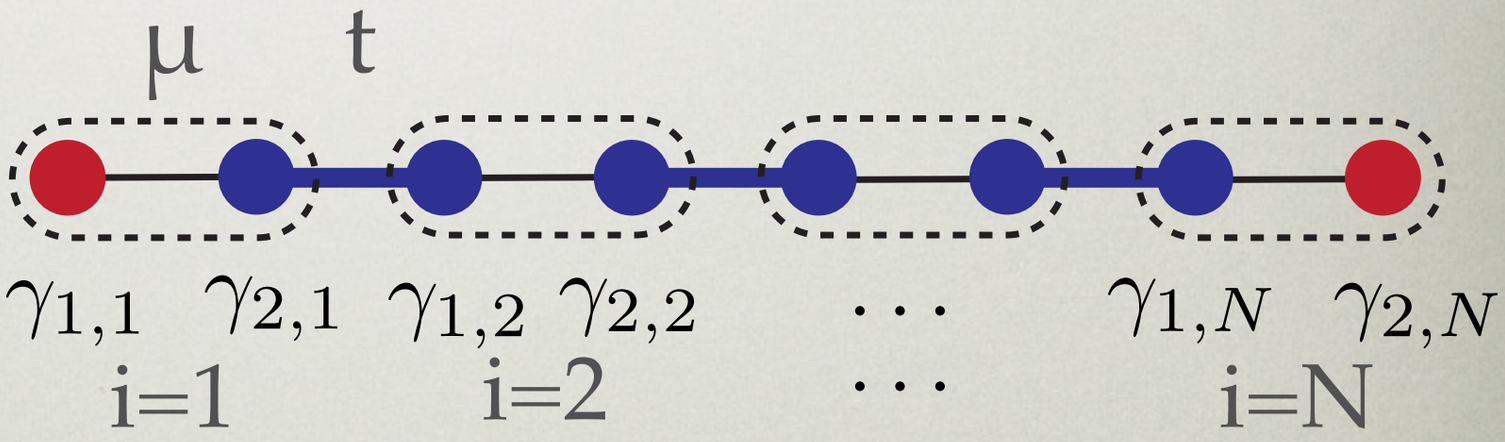
Model Kitaeva

Kitaev (2000)

$$H = \sum_i t\left(c_i^\dagger c_{i+1} + c_{i+1}^\dagger c_i\right) - \mu c_i^\dagger c_i + \Delta\left(c_i c_{i+1} + c_{i+1}^\dagger c_i^\dagger\right)$$



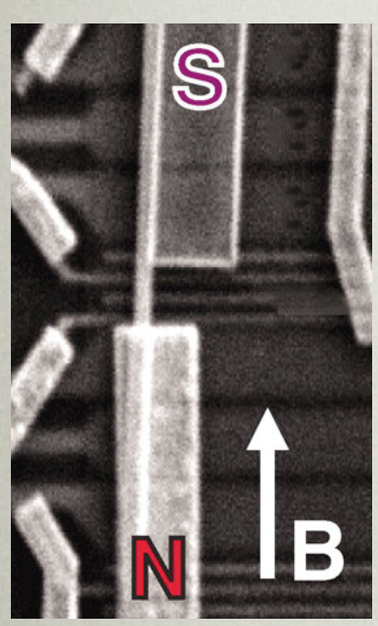
$$c_i \to \gamma_{1i} + i\gamma_{2i}$$

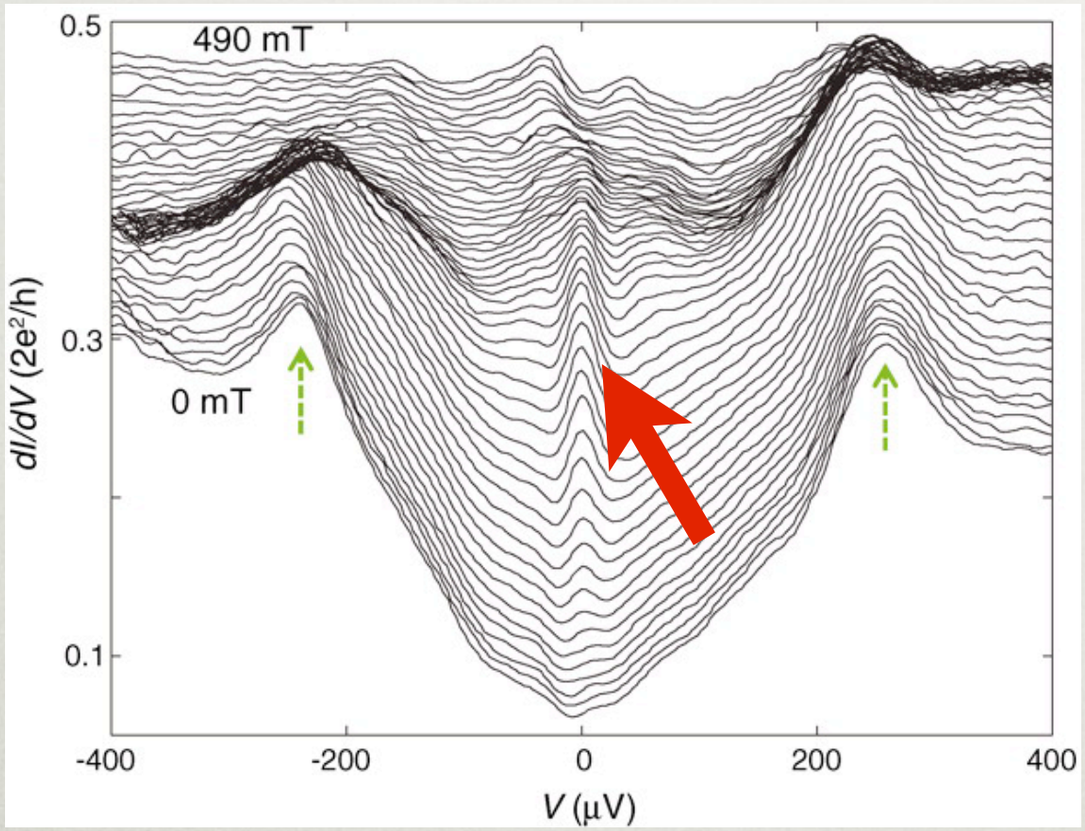


$$d = \gamma_{1,1} + i\gamma_{2,N}$$

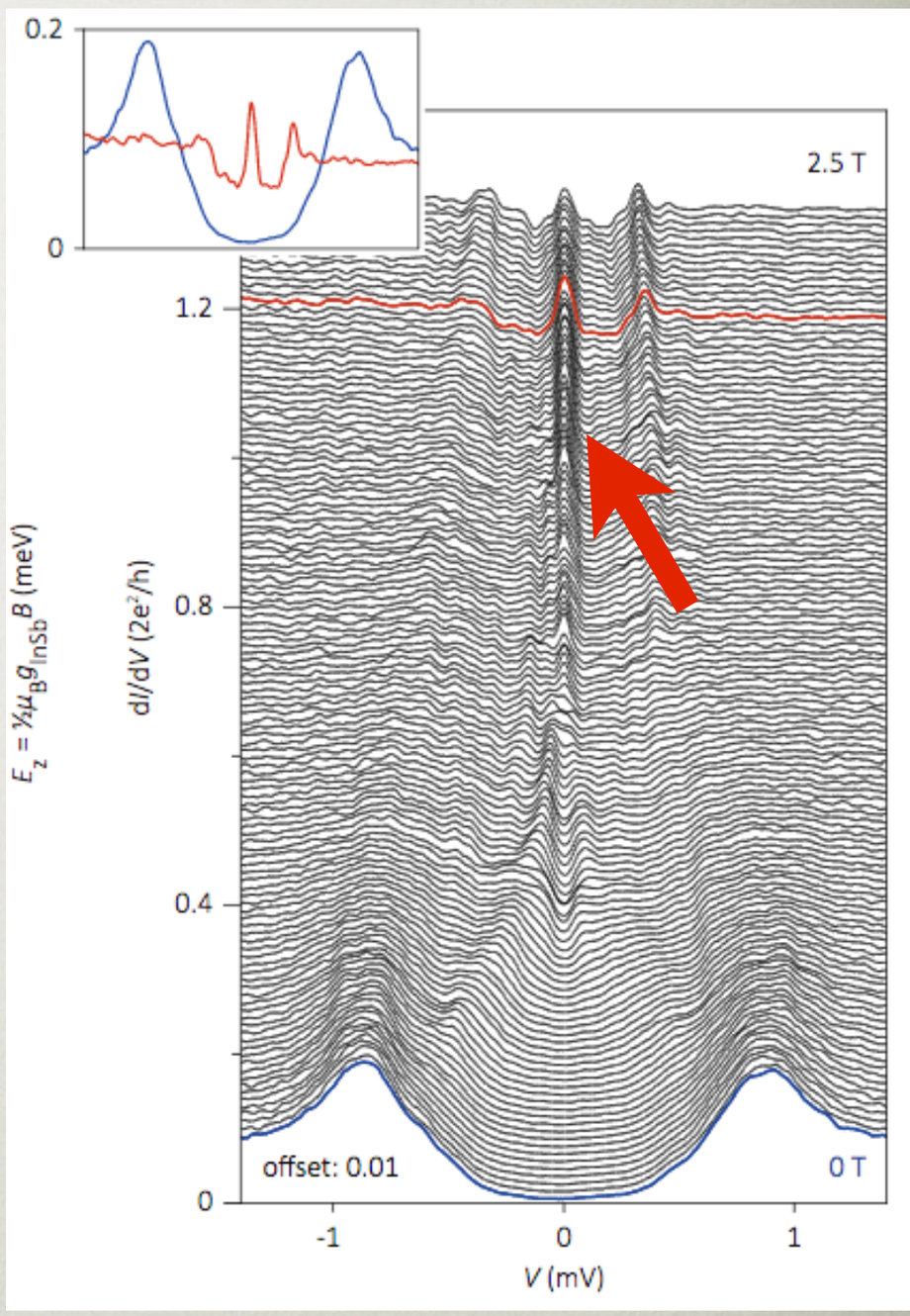
degenerirano osnovno stanje: $|\mathrm{GS}, 0\rangle$ & $|\mathrm{GS}, 1\rangle = d^\dagger |\mathrm{GS}, 0\rangle$

Topološka stanja: Majoranovi fermioni v nanožičkah



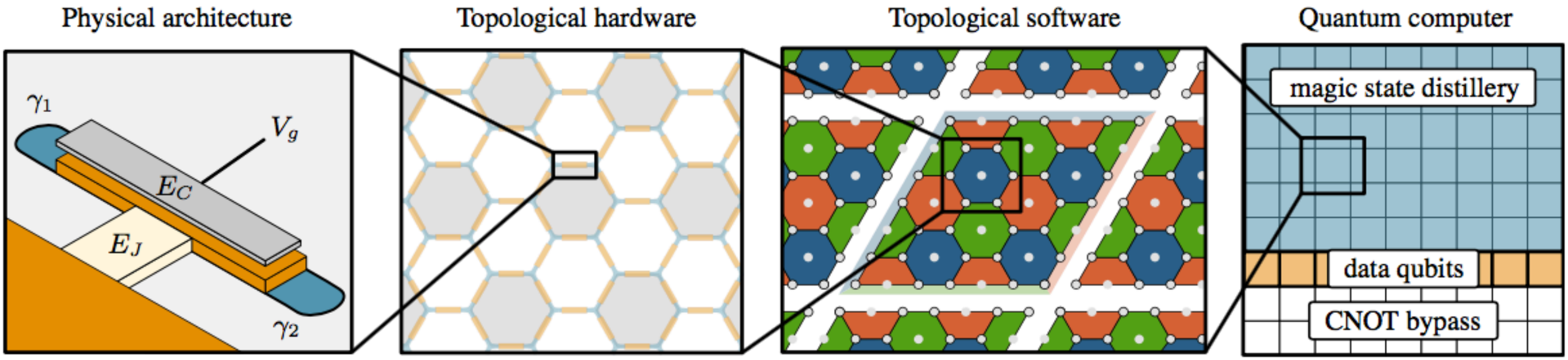


V Mourik, K Zuo, SM Frolov, SR Plissard, EPAM Bakkers, LP Kouwenhoven, Science 336, 1003 (2012)



O. Gul et al., Nature Nanotechnology, 13, 192 (2018)

Topološko kvantno računalništvo



Cliffordova grupa: Hadamard, CNOT, π/4 fazna vrata S (topološko zaščiteno na strojnem nivoju)

π/8 fazna vrata T niso zaščitena, potrebno je energijsko razcepiti stanja (fine tuning!).

Combining Topological Hardware and Topological Software: Color Code Quantum Computing with Topological Superconductor Networks

Daniel Litinski, Markus S. Kesselring, Jens Eisert, and Felix von Oppen
Dahlem Center for Complex Quantum Systems and Fachbereich Physik, Freie Universität Berlin, Arnimallee 14, 14195 Berlin, Germany

Kopenhagen, Danska

Charles Marcus

MICROSOFT QUANTUM

Krysta Svore Leo Kouwenhoven Michael Freedman

Delft, Nizozemska

Microsoft Quantum Development Kit

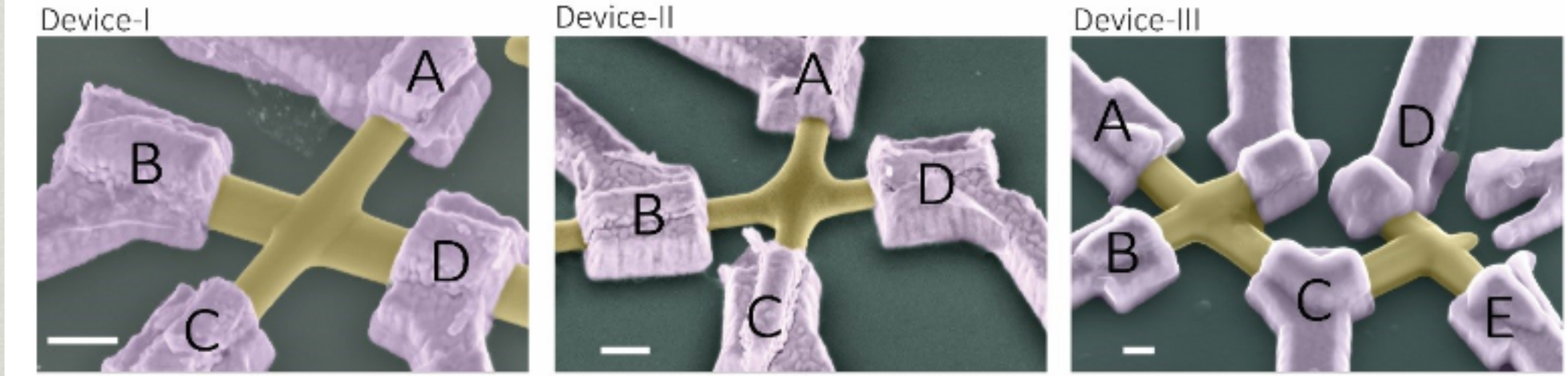
Server Explorer Toolbox

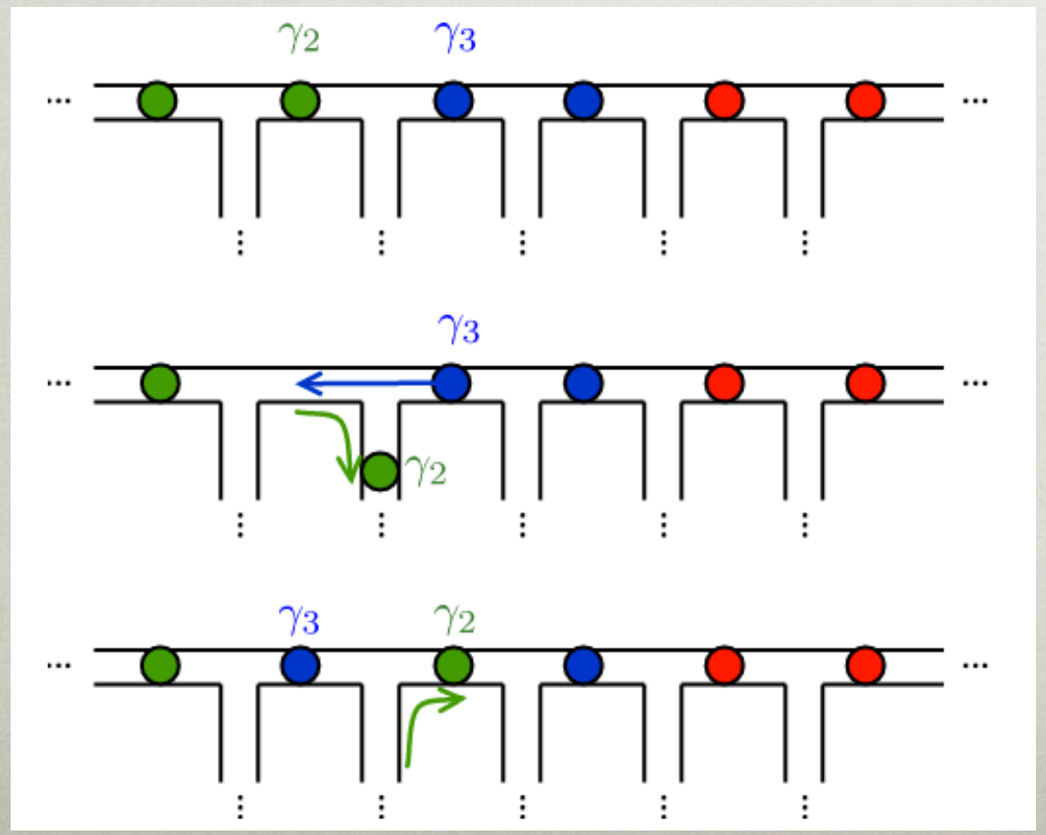
ExampleH2.qs | Program.fs | TeleportationSample.qs | Program.cs

```
40      /// ## there
41      /// A qubit intitially in the |0⟩ state that we want to send
42      /// the state of msg to.
43      operation Teleport(msg : Qubit, there : Qubit) : () {
44          body {
45
46              using (register = Qubit[1]) {
47                  // Ask for an auxillary qubit that we can use to prepare
48                  // for teleportation.
49                  let here = register[0];
50
51                  // Create some entanglement that we can use to send our message.
52                  H(here);
53                  CNOT(here, there);
54
55                  // Move our message into the entangled pair.
56                  CNOT(msg, here);
57                  H(msg);
58
59                  // Measure out the entanglement.
60                  if (M(msg) == One)  { Z(there); }
61                  if (M(here) == One) { X(there); }
62
63                  // Reset our "here" qubit before releasing it.
64                  Reset(here);
65              }
66
67          }
```

jezik Q#

Razvejane nanožice



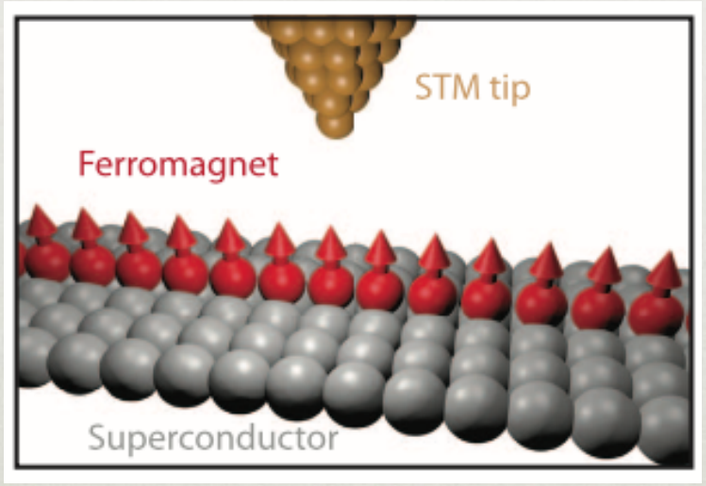


Kouwenhoven, Bakkers, 2017

Cilj: prepletanje v nanožičkah do konca tega desetletja?

Stanja znotraj superprevodniške energijske reže

Verige magnetnih atomov v stiku s superprevodnikom
imajo lahko na svojih krajiščih vzbuditve, ki so Majoranova stanja.



Nadj-Perge et al., Science **346**, 602 (2014)

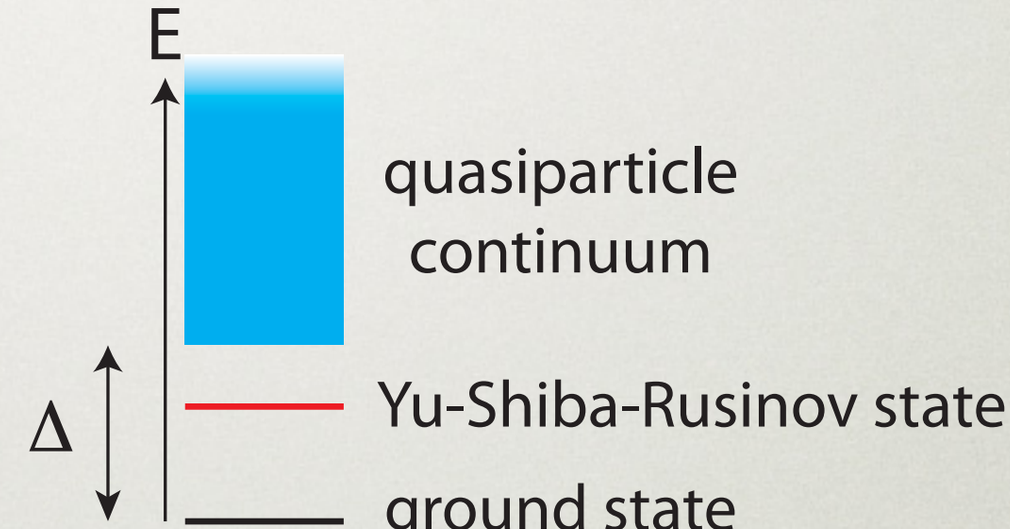
Osnovni gradniki, posamezni magnetni atomi, imajo vzbuditve,
ki jih imenujemo Shibova stanja.

Shibova stanja

Lokalni moment (magnetni atom) ustvari vezana stanja kvazidelcev Bogoljubova znotraj energijske reže superprevodnika.

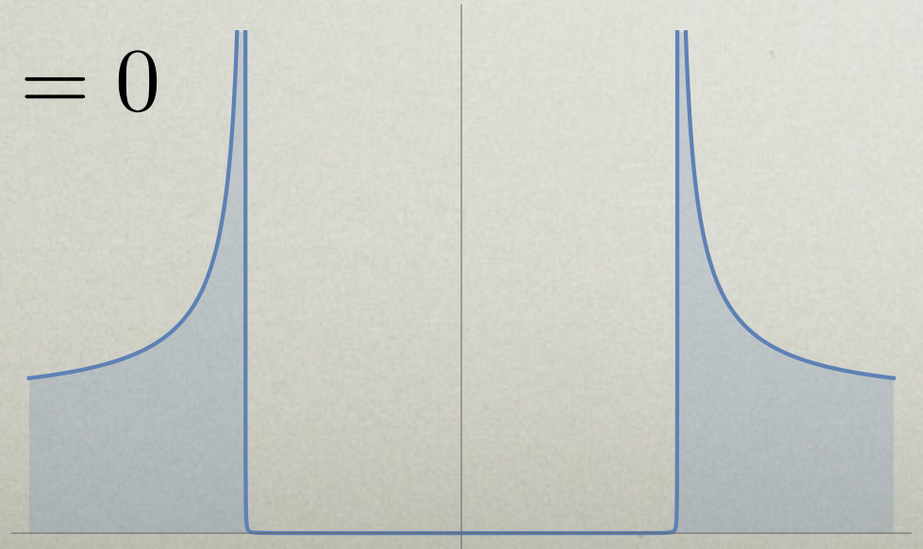
$$E_{\mathrm{YSR}} = \Delta \frac{1-\alpha^2}{1+\alpha^2}$$

$$\alpha = JS\pi\rho/2$$

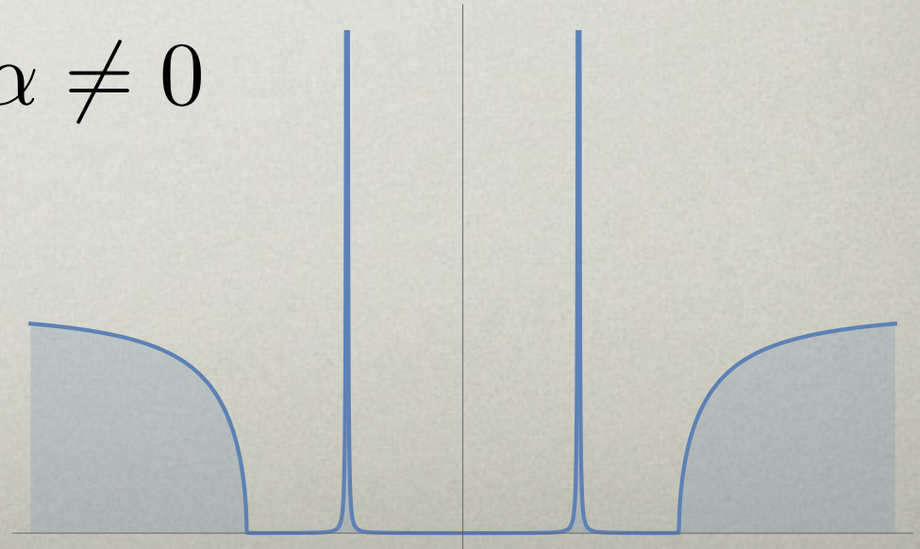


Yu Lu, Acta Physica Sinica (1965)
H. Shiba, Prog. Theor. Phys. (1968)
A. I. Rusinov, ZhETF Pis. Red (1969)

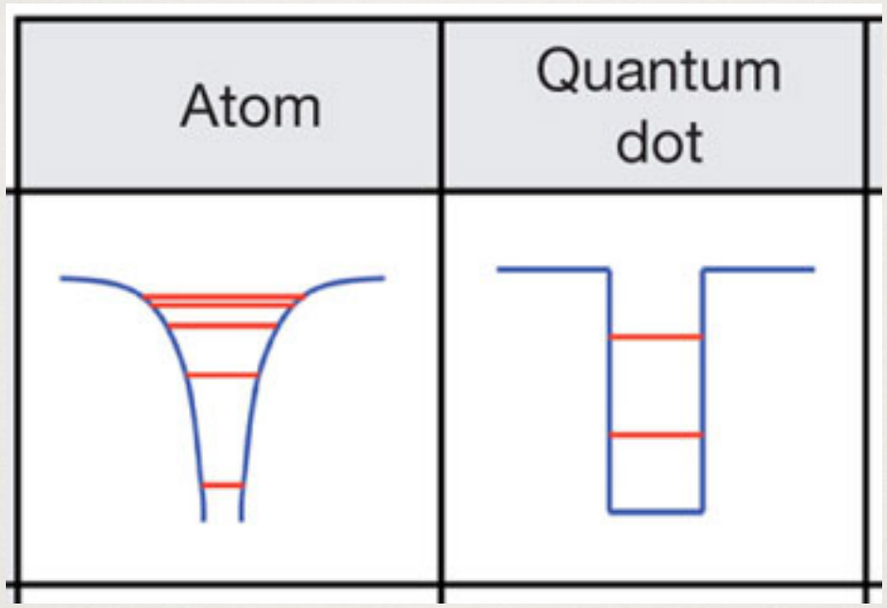
$\alpha = 0$

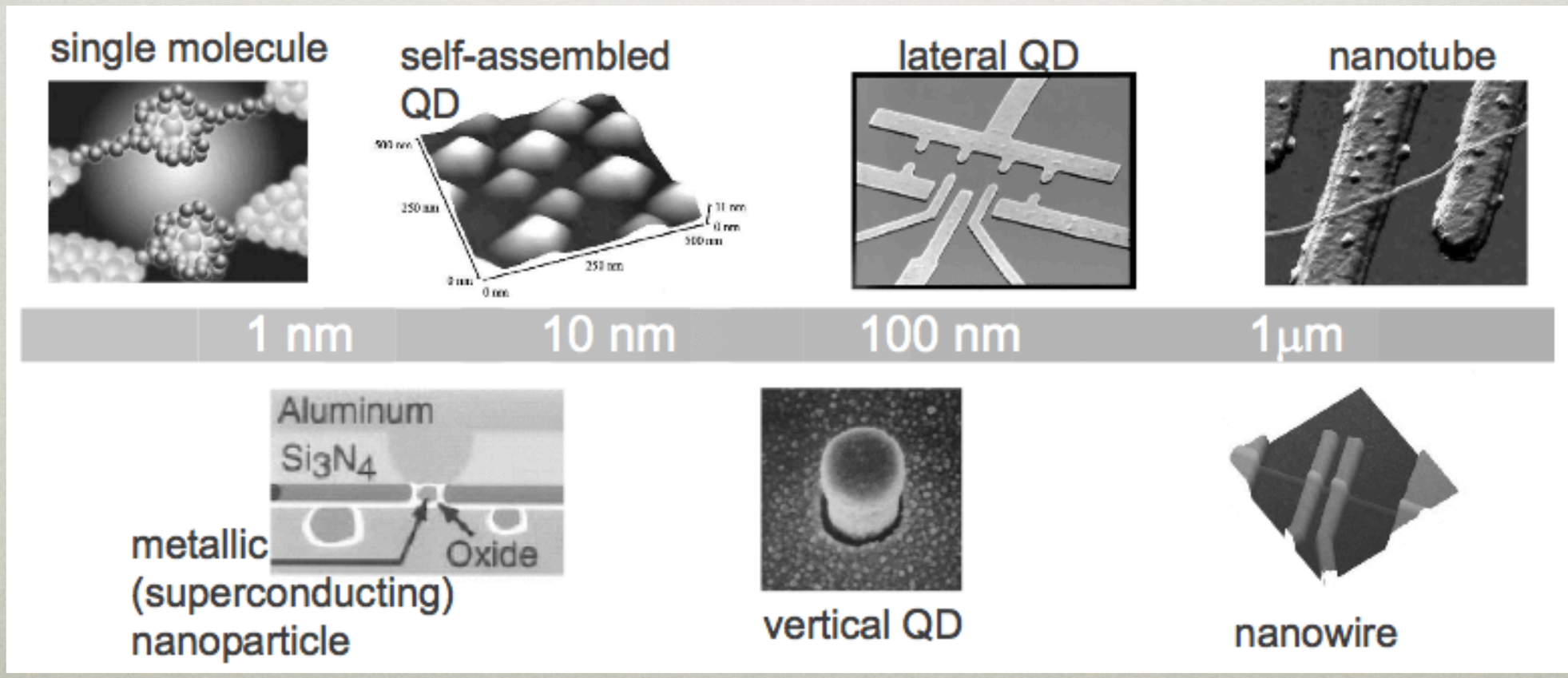


$\alpha \neq 0$

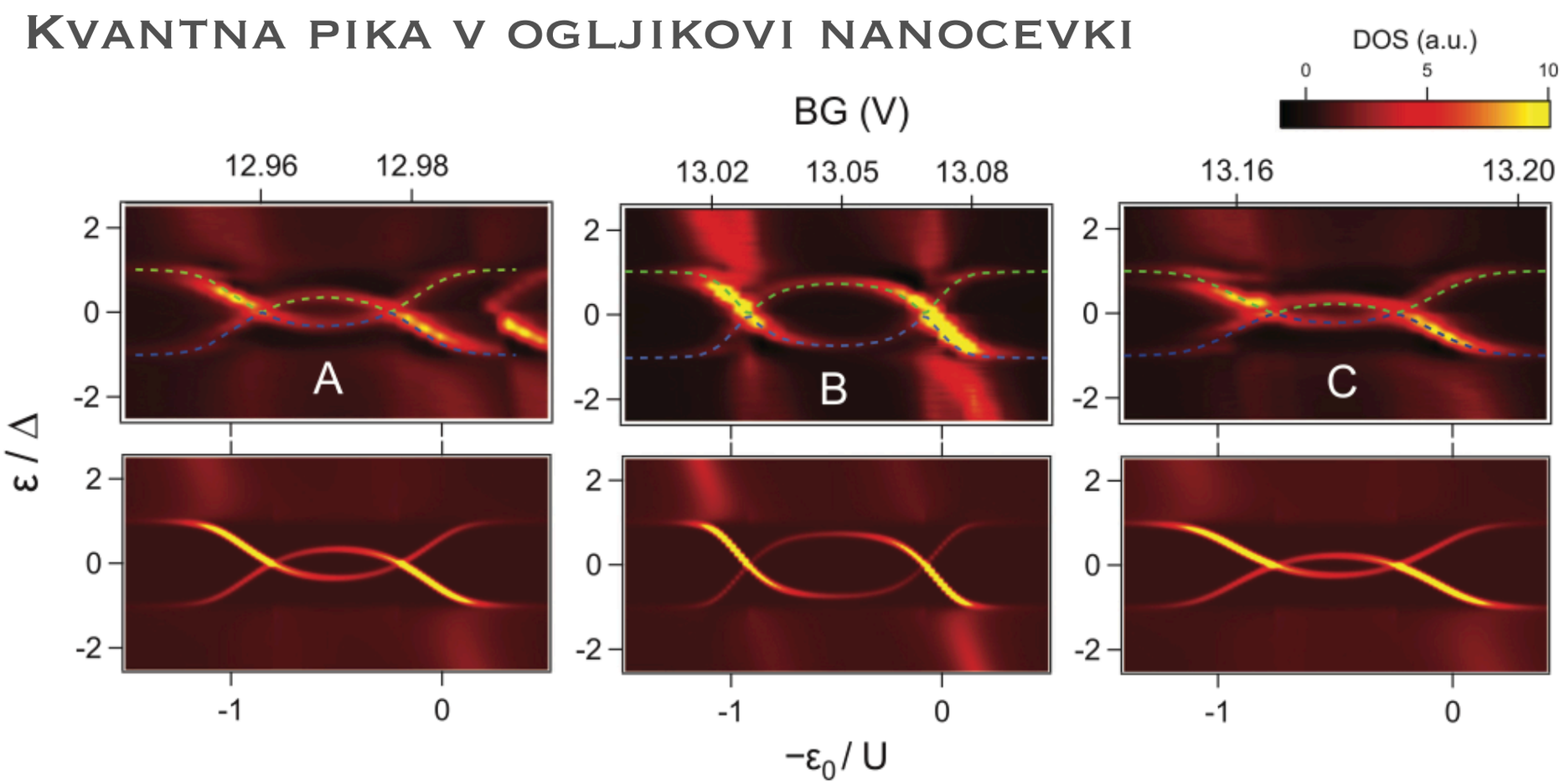


Kvantna pika = umetni atom





Kvantna pika v ogljikovi nanocevki

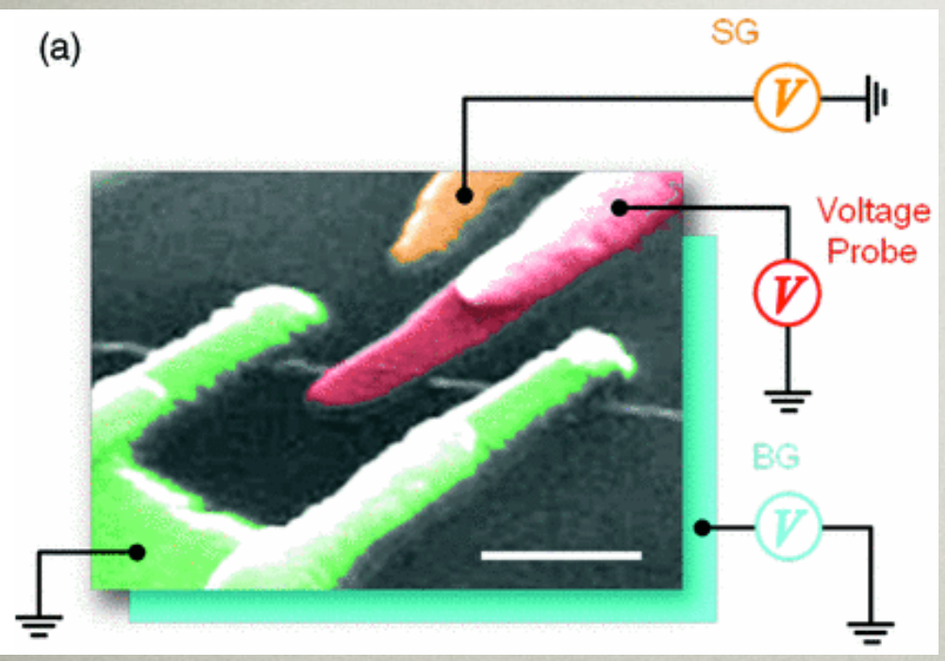


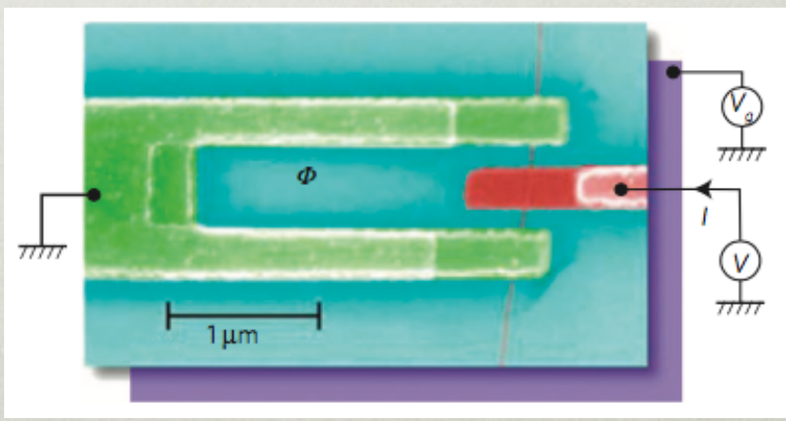
eksperiment

teorija

račun z metodo NRG

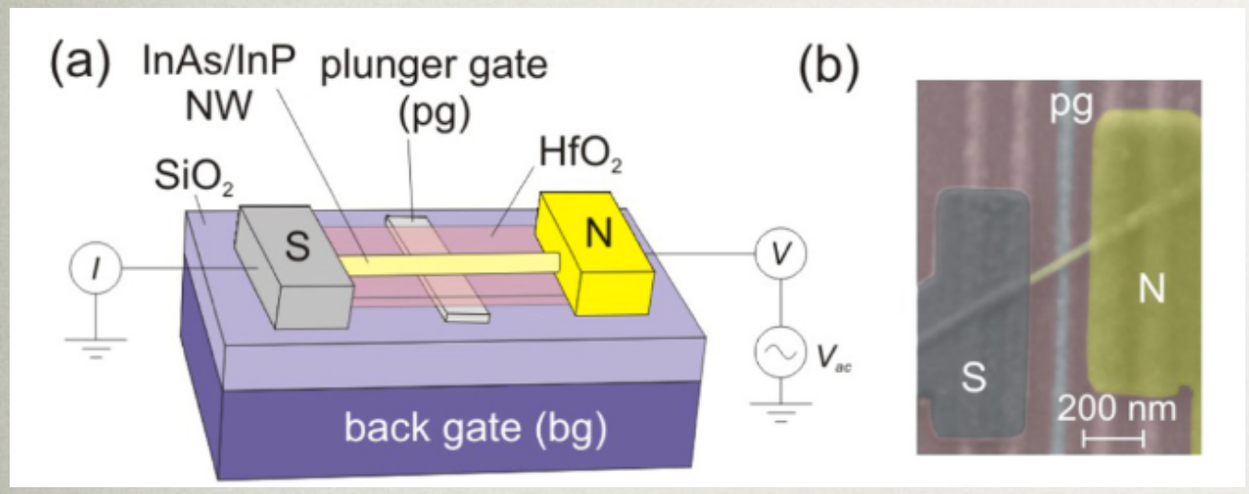
(NRG = numerična renormalizacijska grupa)

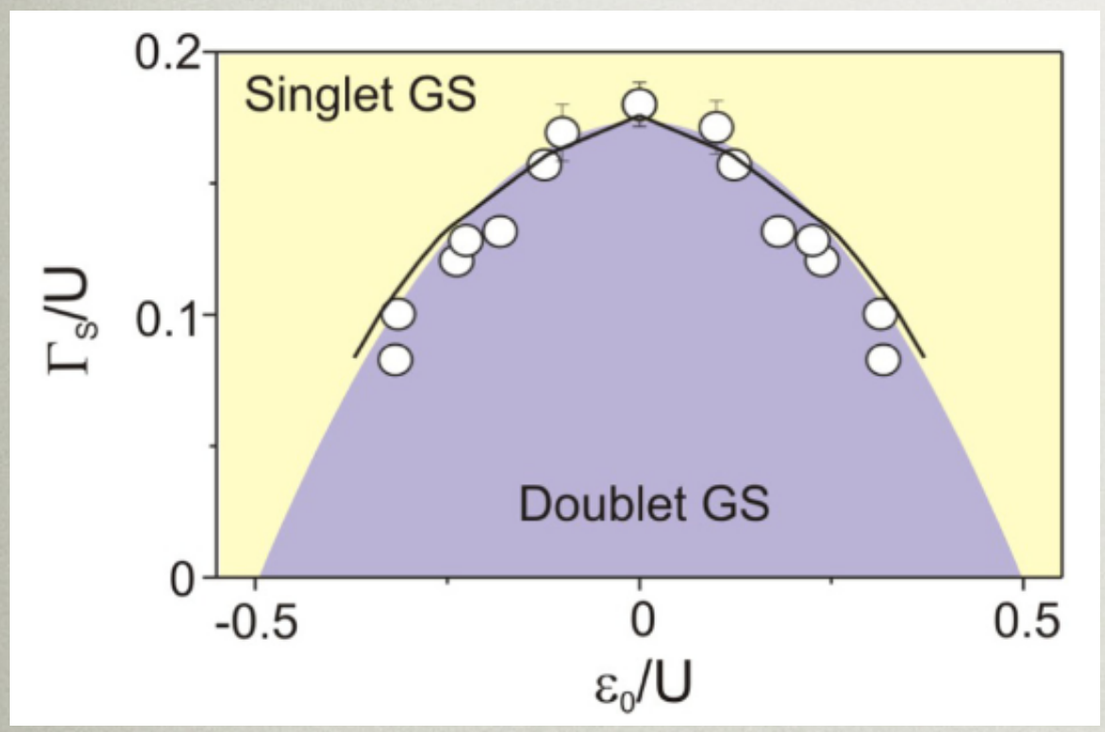


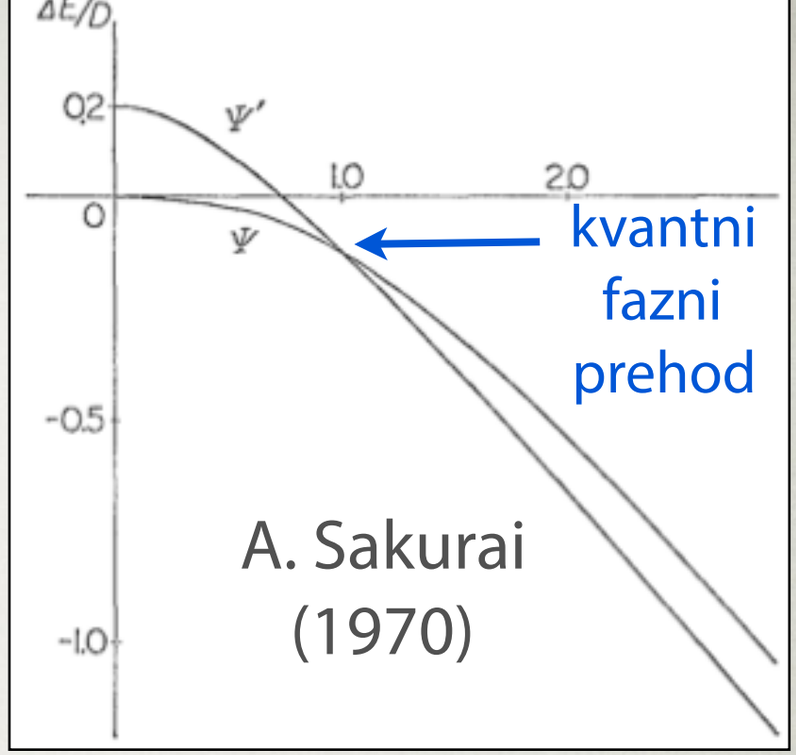


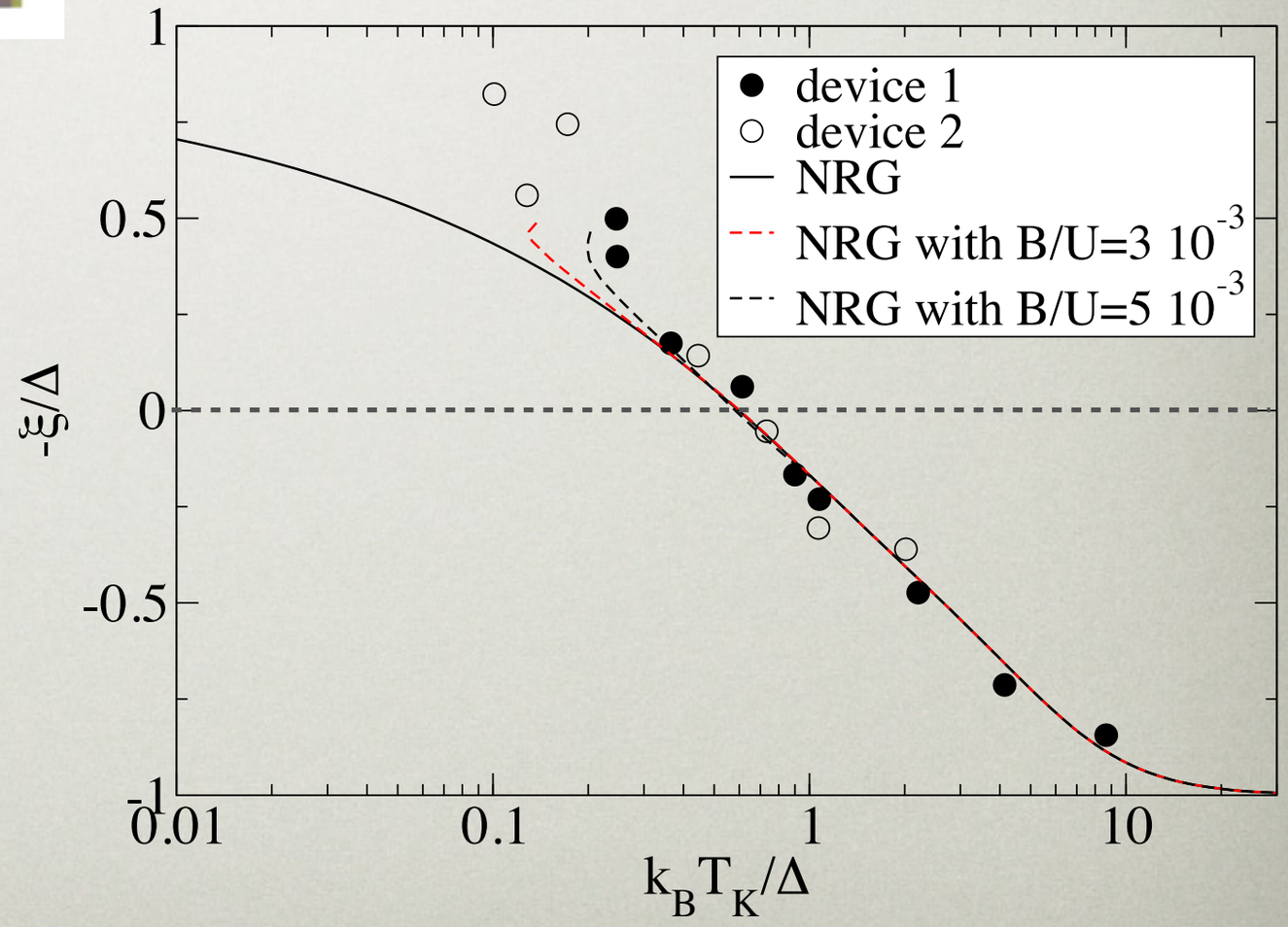
JD Pillet, P Joyez, R Žitko, MF Goffman, PRB (2013)

Kvantna pika v nanožici



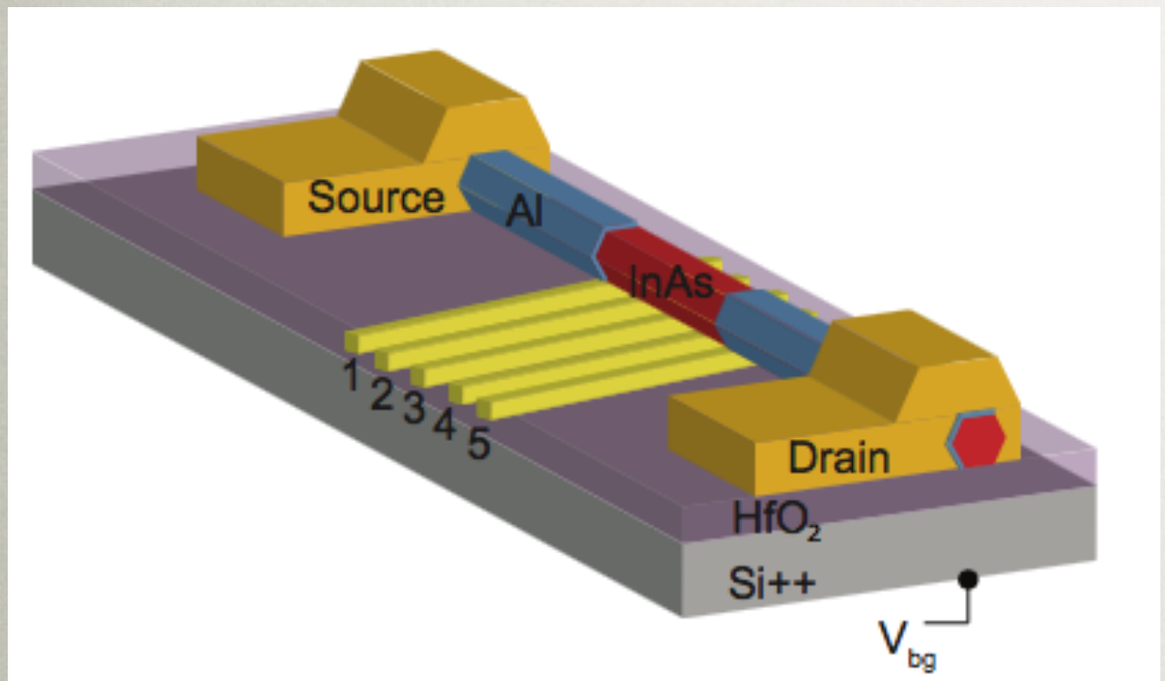


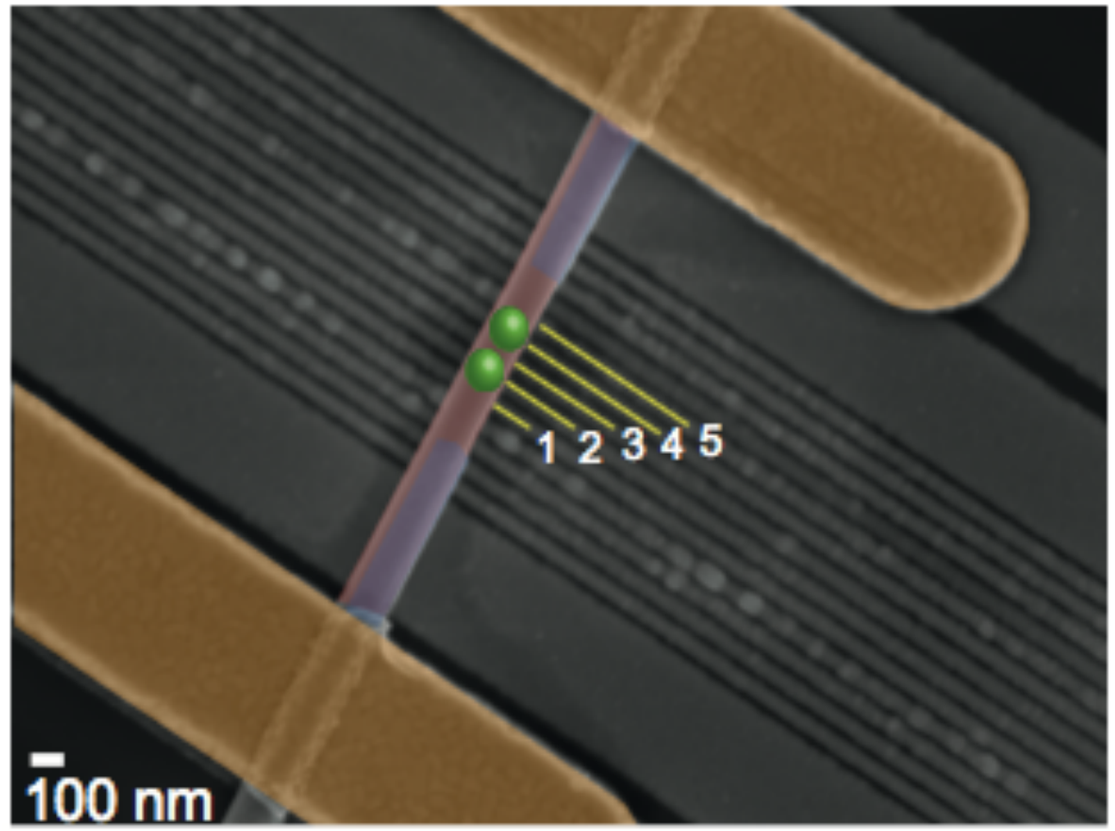




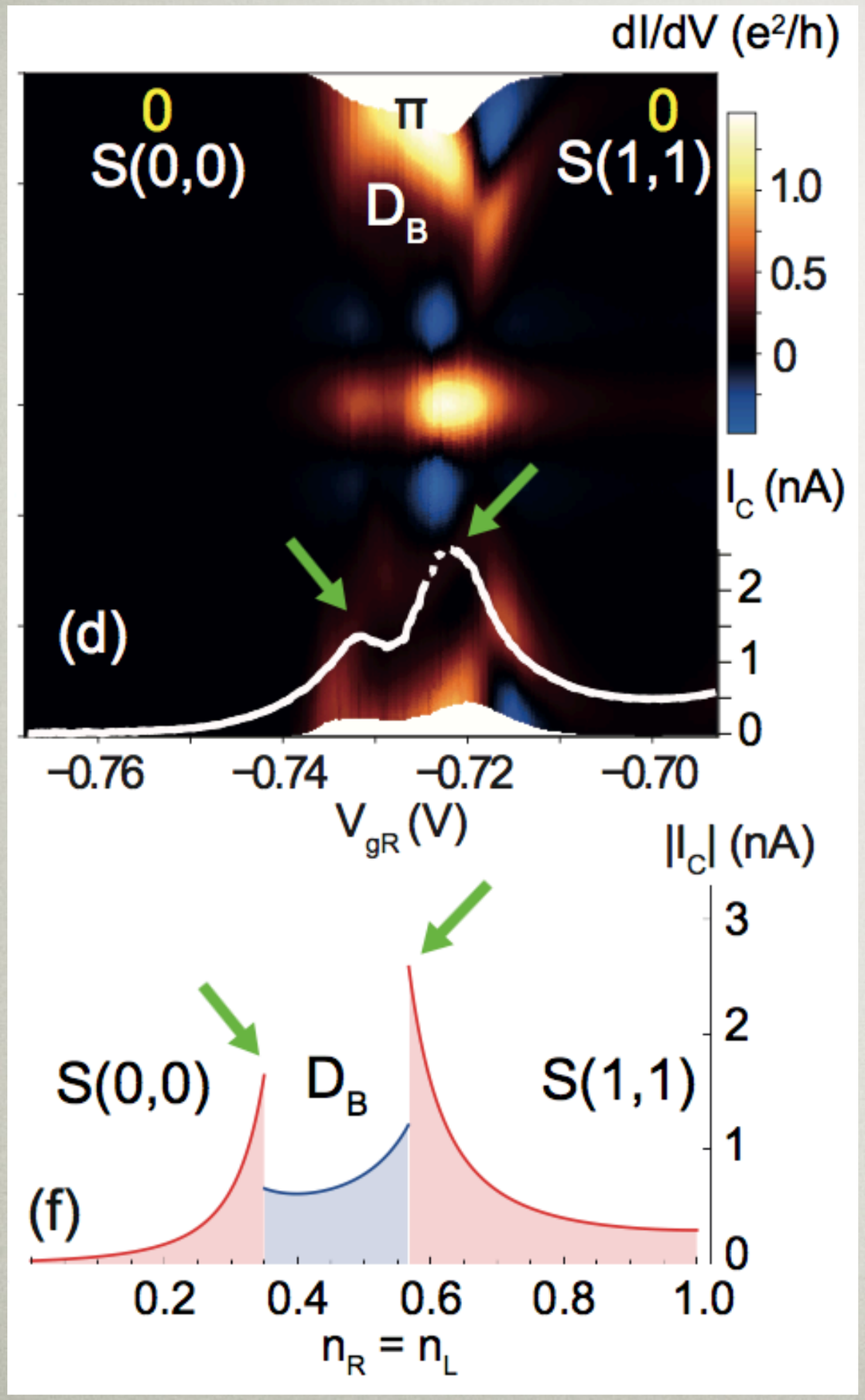
Lee, Jiang, Žitko, Aguado, Lieber, de Francesci, PRB (2017)

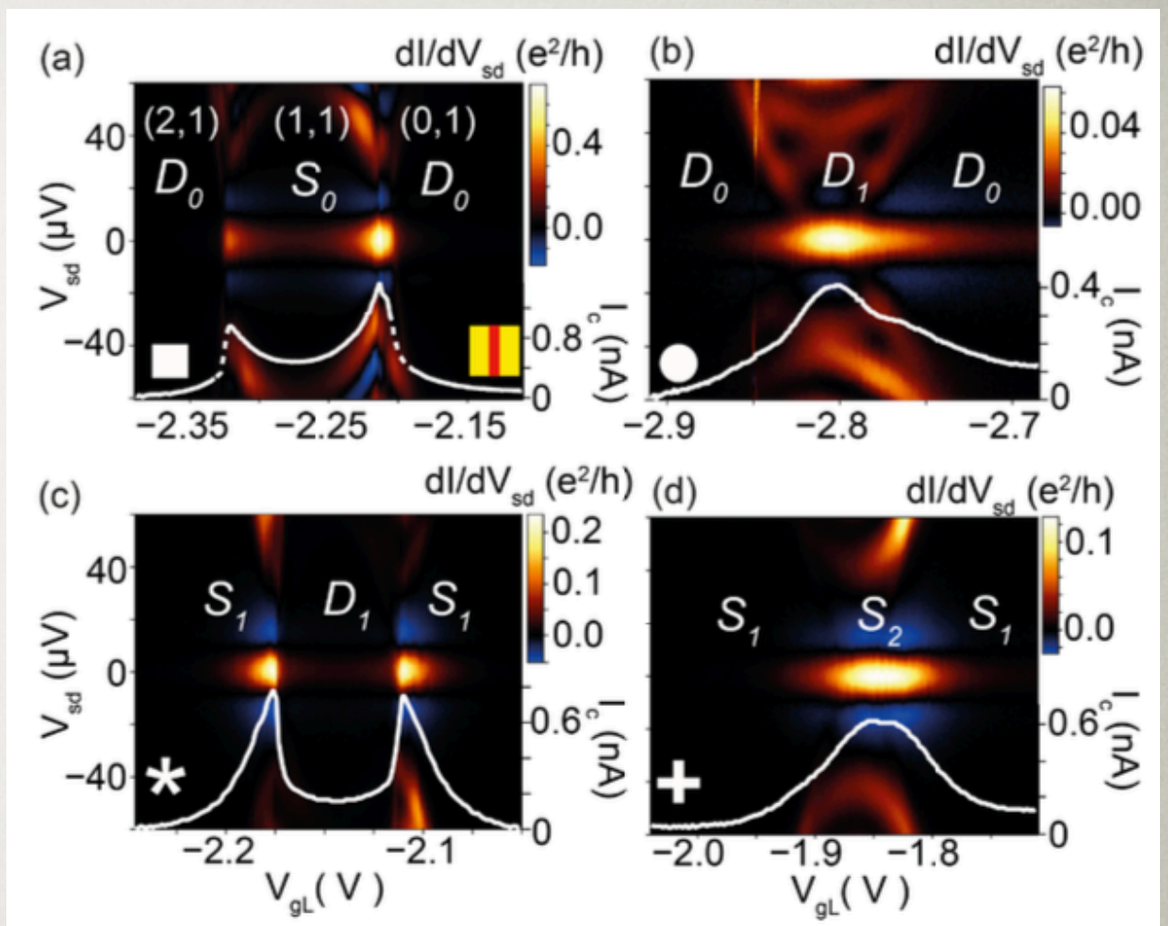
Skloplјene kvantne pike = umetne molekule

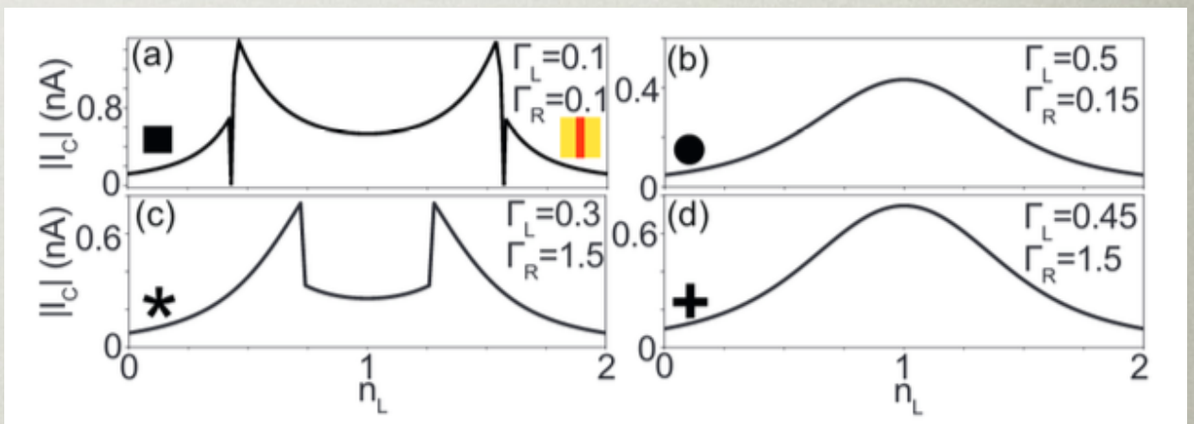




J. C. Estrada Saldaña, A. Vekris, G. Steffensen, R. Žitko,
P. Krogstrup, J. Paaske, K. Grove-Rasmussen, J. Nygård
PRL (2018) in arxiv (2018)


dI/dV (e²/h)
0
S(0,0)
π
D_B
0
S(1,1)
1.0
0.5
0
I_C (nA)
(d)
2
1
0
−0.76
−0.74
−0.72
−0.70
V_gR (V)
|I_C| (nA)
3
2
1
0
S(0,0)
D_B
S(1,1)
(f)
0.2
0.4
0.6
0.8
1.0
n_R = n_L


(a)
dI/dV_sd (e²/h)
(2,1)
(1,1)
(0,1)
D_0
S_0
D_0
40
0
−40
V_sd (μV)
0.4
0.0
0.8
0
I_c (nA)
−2.35
−2.25
−2.15
(b)
dI/dV_sd (e²/h)
D_0
D_1
D_0
0.04
0.00
0.4
0
I_c (nA)
−2.9
−2.8
−2.7
(c)
dI/dV_sd (e²/h)
S_1
D_1
S_1
40
0
−40
V_sd (μV)
0.2
0.1
0.0
0.6
0
I_c (nA)
−2.2
−2.1
V_gL (V)
(d)
dI/dV_sd (e²/h)
S_1
S_2
S_1
0.1
0.0
0.6
0
I_c (nA)
−2.0
−1.9
−1.8
V_gL (V)


(a)
Γ_L=0.1
Γ_R=0.1
(b)
Γ_L=0.5
Γ_R=0.15
(c)
Γ_L=0.3
Γ_R=1.5
(d)
Γ_L=0.45
Γ_R=1.5
|I_C| (nA)
0.8
0.4
0.6
0.6
0
1
2
n_L

Strateški projekt (flagship) Kvantne tehnologije

- krovni program financiranja Evropske Unije
- začetek jeseni 2018 v okviru Horizon 2020, nadaljeval se bo v okviru Horizon Europe
- 3 milijarde EUR celotnega financiranja
- tema: nadzor kvantnih sistemov brez izgube koherence
- nanotehnologije + atomska fizika + kvantna optika
- poudarek na inženirskih vidikih in fiziki naprav bolj kot na osnovnih raziskavah na področju kvantne mehanike

https://qt.eu

KVANTNE NAPRAVE

- <u>danes</u>:
  atomske ure
  generatorji naključnih števil
  kvantna distribucija ključev za šifriranje
  majhni kvantni računalniki
- <u>prihodnost</u>:
  še boljše atomske ure
  inercijska navigacija
  natančna gravimetrija
  simulacije kvantnih sistemov (molekul)
  globalni kvantni internet
  kvantni računalniki z veliko kubiti

PRILOŽNOSTI

- ustanavljajo se dobro opremljeni raziskovalno/razvojni centri
- konference, delavnice, poletne šole
- namenske poletne šole in doktorski študiji
- odpirajo se delovna mesta za raziskovalce (postdoc)

več informacij: poštni seznam QUROPE (~2-3 obvestila na dan)

Kvantne tehnologije v Sloveniji

- IJS F-1: teorija in računalniške simulacije
- IJS F-5: kvantne spinske tekočine, hladni atomi
- IJS F-7: kvantni materiali, dinamika
- FMF UL: teorija neravnovesnih kvantnih sistemov
- IJS E-8, FE UL, FRI UL

http://www.qutes.si

KVANTNE TEHNOLOGIJE
NASLEDNJA TEHNOLOŠKA REVOLUCIJA

KVANTNE KOMUNIKACIJE

VARNE KOMUNIKACIJE
- popolna varnost osebnih podatkov
- zagotavljanje zasebnosti
- nacionalna varnost

KVANTNI SENZORJI

NAVIGACIJA
- ultra-natančne ure za globalno sinhronizacijo
- natančna navigacija za avtonomna vozila
- inercijska navigacija, ki deluje tudi v stavbah in v tunelih

NOVE SNOVI
- simulacije kompleksnih molekul
- zdravila prirejena za posameznika
- lahke baterije
- prepoznavanje vzorcev v podatkih

KVANTNI SENZORJI

OPAZOVANJE ZEMLJE
- iskanje nahajališč naravnih bogastev
- napovedovanje nevarnosti potresov, plazov in poplav
- natančno spremljanje podnebja
- zgodnje prilagajanje spremembam

KVANTNE SIMULACIJE

ZDRAVJE
- visokoločljivo slikanje telesa
- spremljanje možganske aktivnosti
- zgodnje odkrivanje bolezenskih znakov

KVANTNI SENZORJI

KVANTNO RAČUNALNIŠTVO

VARNO POSLOVANJE
- preprečevanje zlorab pri splet nem nakupovanju
- varno bančništvo

KVANTNE KOMUNIKACIJE

RAČUNANJE
- reševanje optimizacijskih problemov v logistiki
- upravljanje cestnega prometa
- hitro iskanje in odločanje