Hrvoje Skenderović, Institut za fiziku, Zagreb

Kvantno računanje - budućnost informatike?

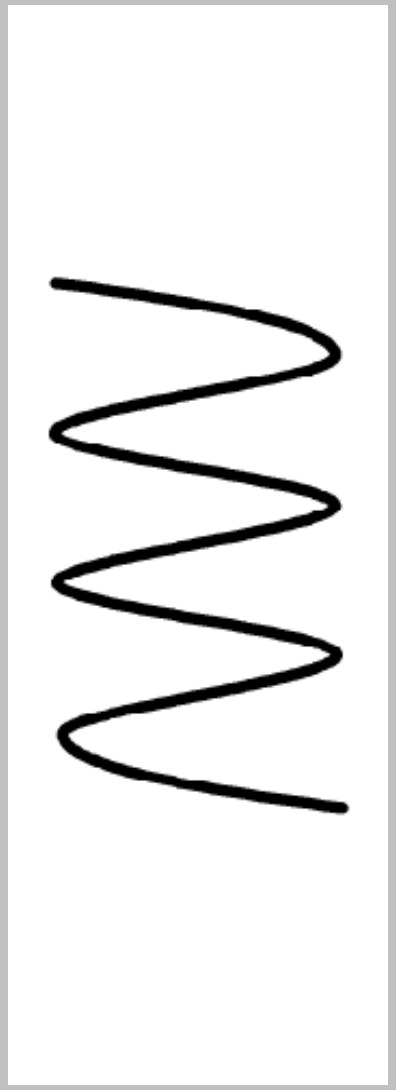
Superpozicija, Entanglement, Kvantna kriptografija, Kvantna teleportacija, ...
Kvatno računanje

Neke značajke kvantne fizike:

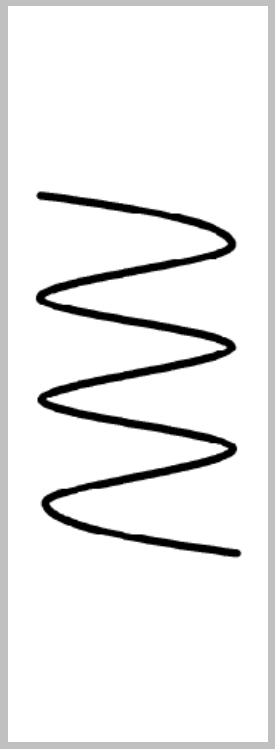
- valovi materije, valna funkcija
- ne može se izvršiti mjerenje a da se ne poremeti ono što se mjeri
- ne možemo apsolutno precizno znati poziciju i brzinu neke čestice
- ....

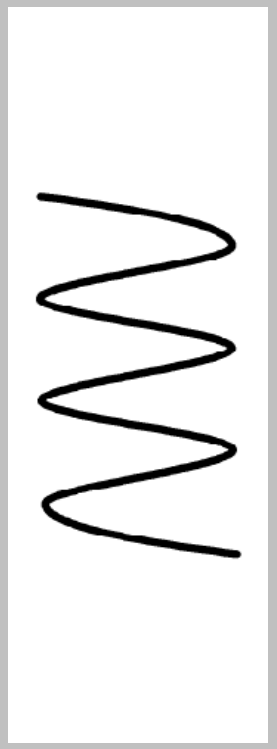
Kvantna fizika potpuno opisuje fizičku realnost. Međutim, u svakodnevnim pojavama u makroskopskom svijetu za opis realnosti je (gotovo uvijek) dovoljna klasična fizika.

Zašto se kvantni fenomeni ne iskazuju na makroskopskom nivou?



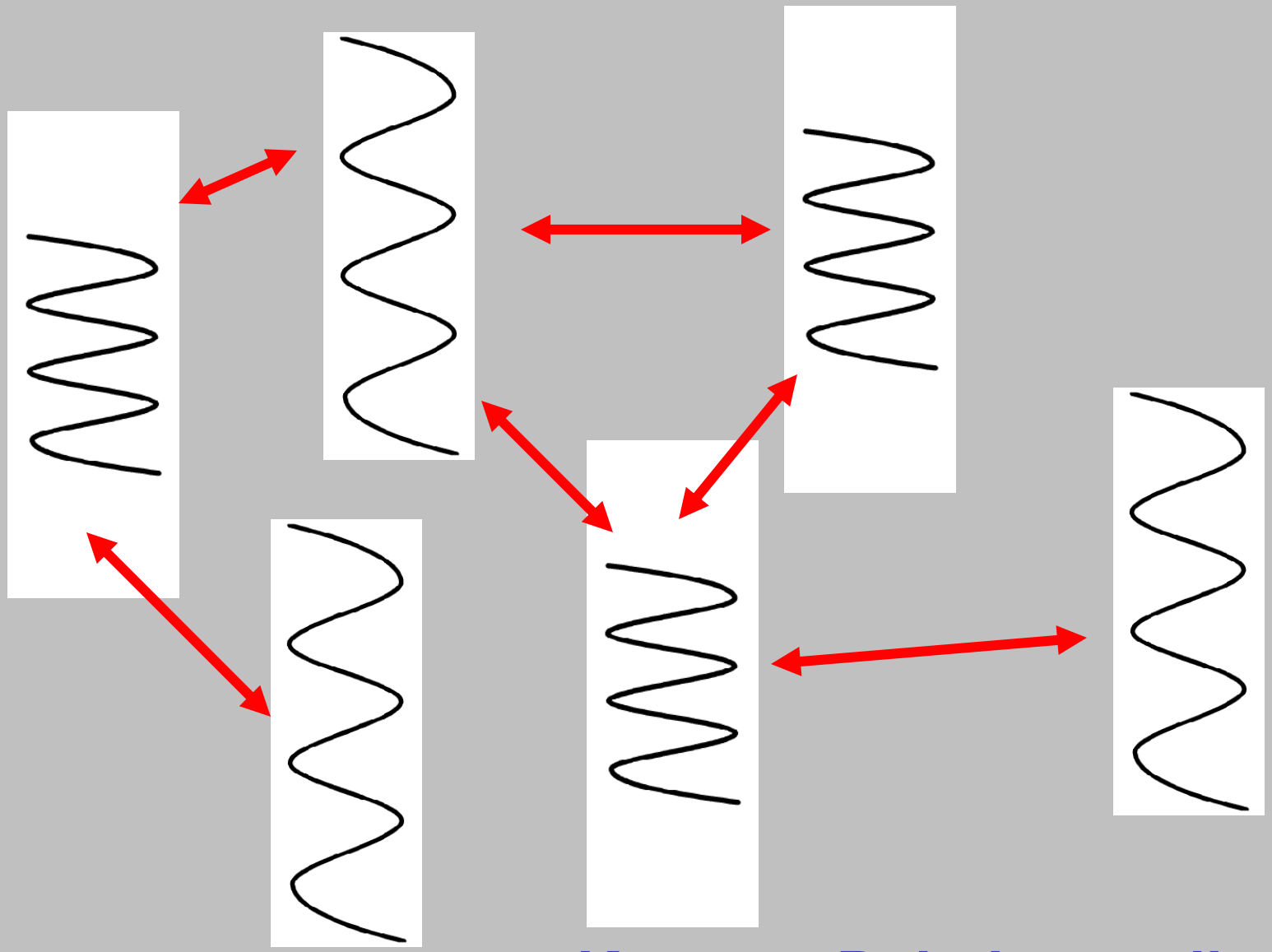
Valna funkcija subatomske čestice titra vlastitom frekvencijom





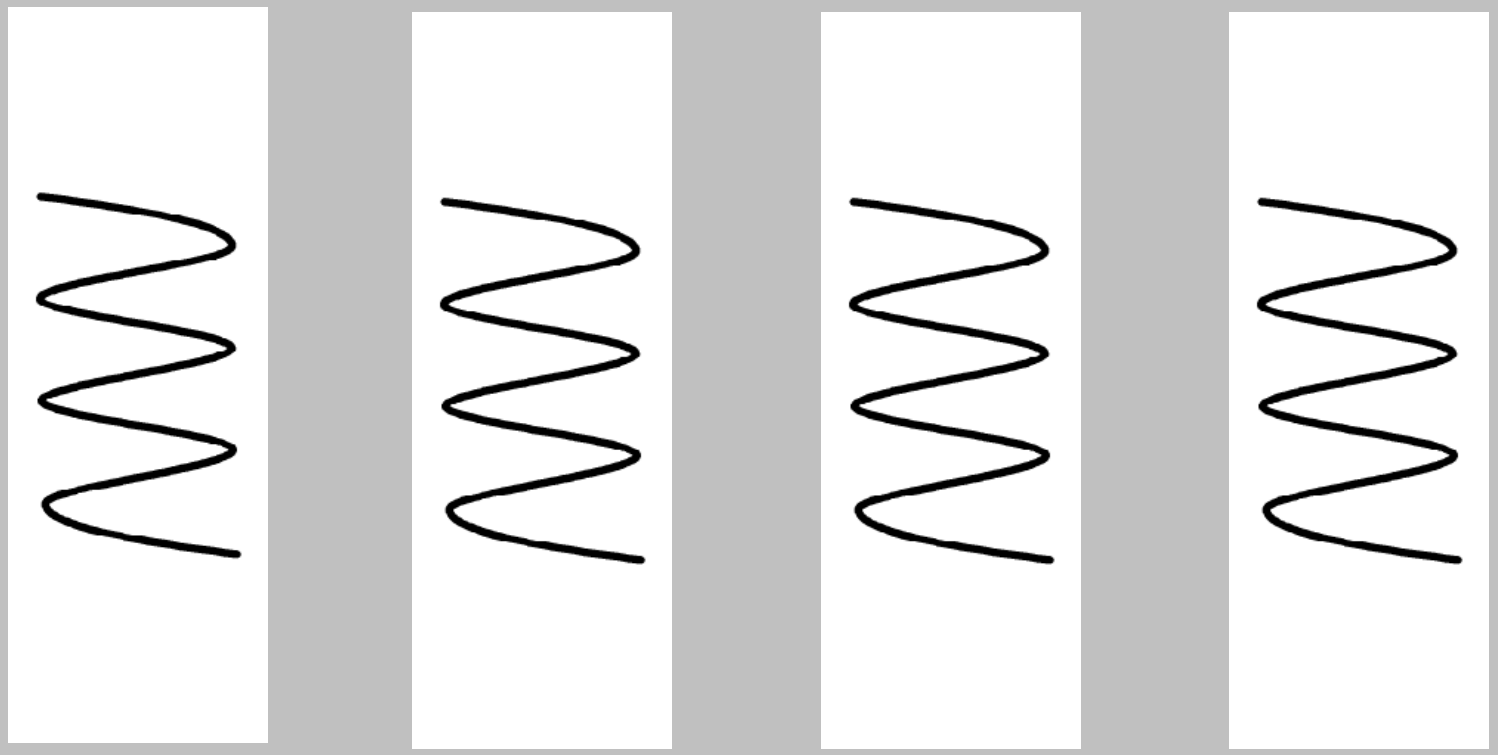
Kvantna Koherencija

Valne funkcije pojedinih čestica titraju u fazi



Kvantna Dekoherencija

Ansambl čestica ne titra u fazi



Makroskopska kvantna koherencija:

Laser Supravodljivost Quantum Hall effect

Princip superpozicije

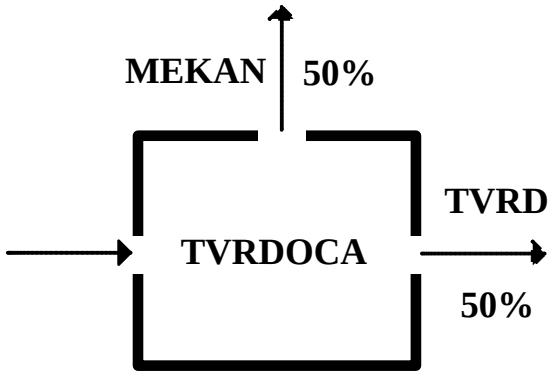
Neka elektron ima dvije osobine:

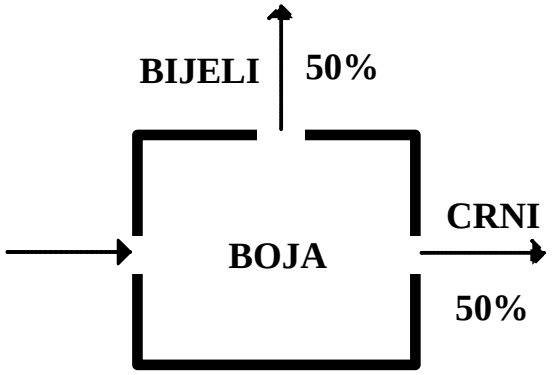
- tvrdoću

tvrd, mekan

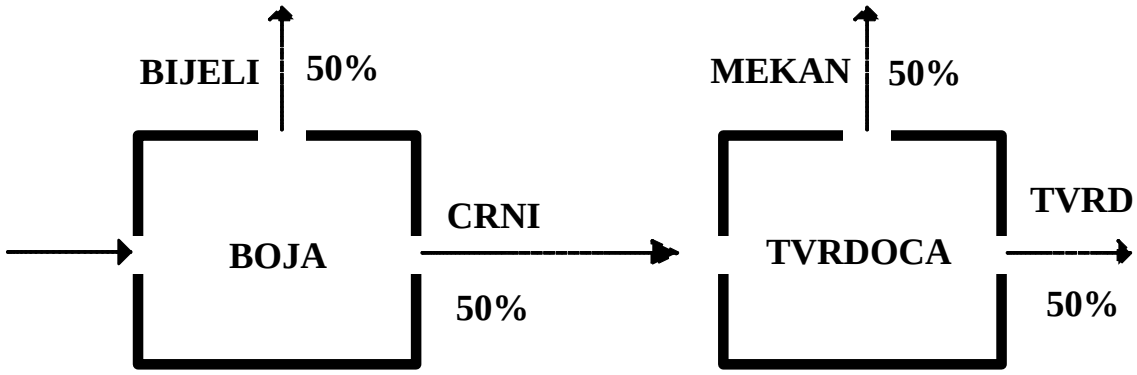
- boju

bijeli, crni

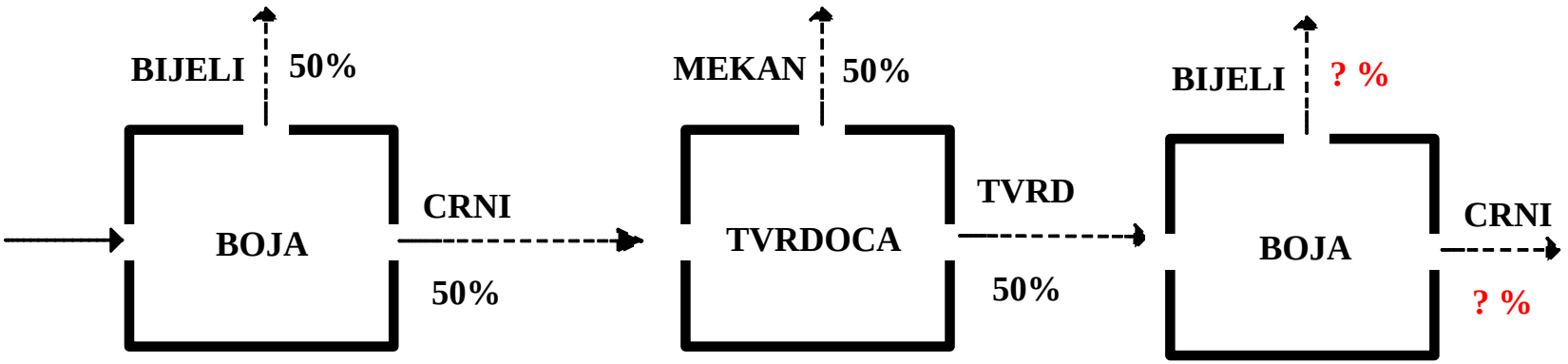




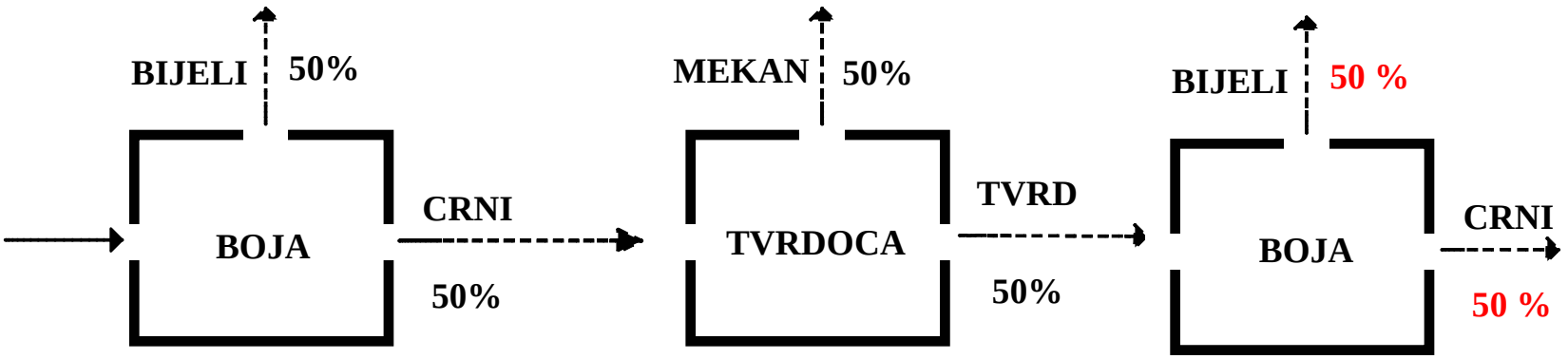
Osobine su međusobno nekorelirane



PRINCIP NEODREĐENOSTI

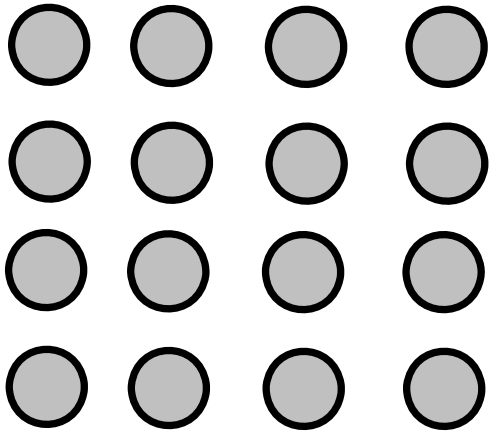


PRINCIP NEODREĐENOSTI

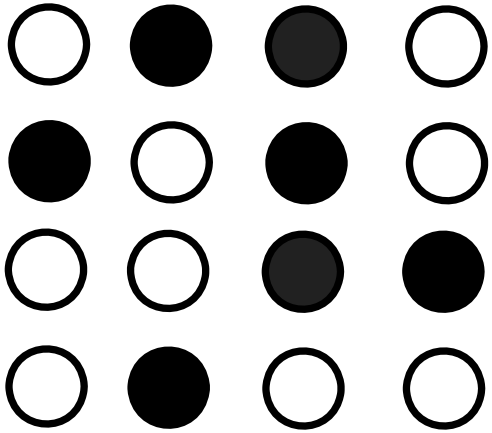


Mjerenje tvrdoće potpuno poremeti boju čestice.
Dvije inkompatibilne fizičke veličine ne mogu se istodobno izmjeriti !

Kvantno računalo koristi qubite umjesto bitova



Mali broj čestica u stanju superpozicije može nositi veliku količinu informacija. Npr. 1000 čestica može predstavljati svaki broj od 1 do 10^{300} i računalo bi manipuliralo tim brojevima u paraleli, šaljući jedan laserski puls na čestice.



Na kraju računanja kad se izmjere stanja svih čestice ostaje samo jedan broj. Pogodnom manipulacijom qubitima moguće vrlo brzo rješavati nekae probleme popt faktorizacije velikih brojeva

Množenje dva broja je lagani zadatak:
87 x 1007 = 87609.
Faktorizacija je puno teži:
87609 = ☐ x ☐ ?

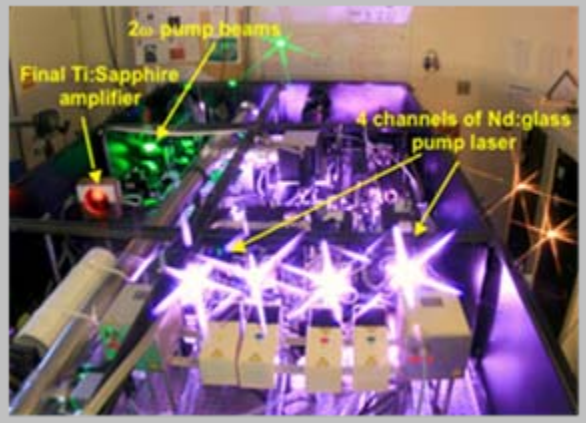
Kompleksnost nekog računskog zadatka se mjeri po tome koliko se vrijeme rješavanja zadatka poveća s povećavanjem veličine zadatka.

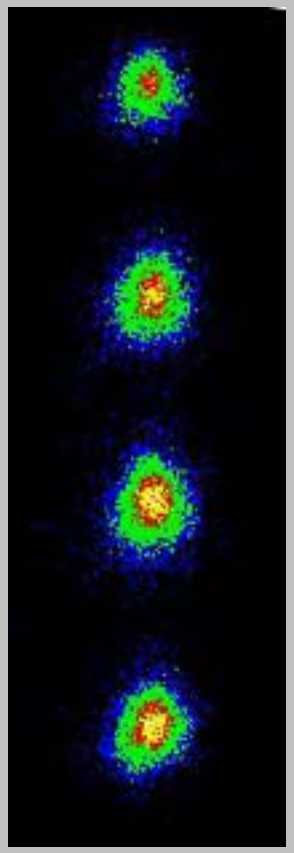
Broj koraka za množenje dva N-znamenkasta broja povećava se kao N^2. (Polinomno s N).
Faktorizacija N-znamenkastog broja ima složenost koja raste eksponencijalno s N.

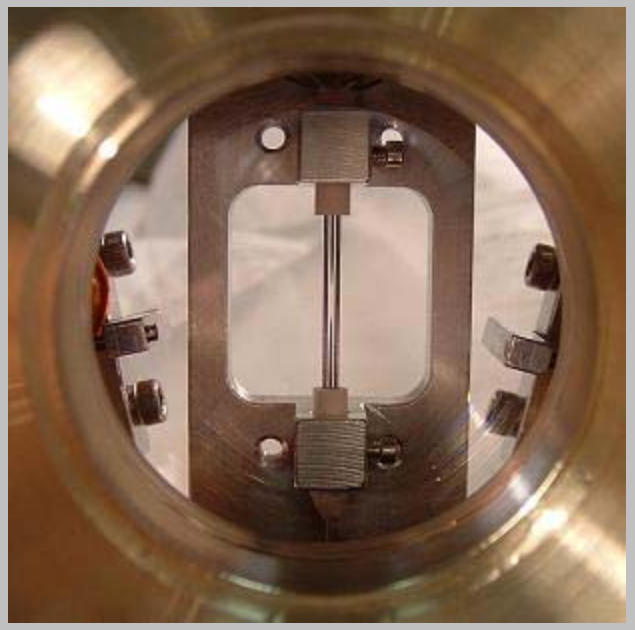
Zašto kvantno računalo?

Faktorizirati broj od 300 znamenki:
Klasičan algoritam daje rješenje u 5 x 10^{24} koraka što na terahercnoj brzini traje 150 000 godina. Kvantni algoritam nudi rješenje u 5 x 10^{10} koraka što na istoj brzini traje manje od sekunde!

Kvantno računalo na bazi iona u stupici



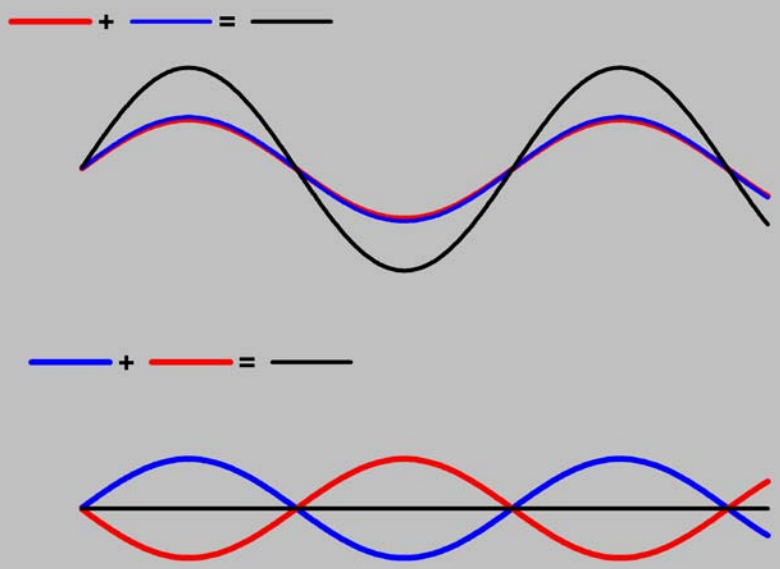




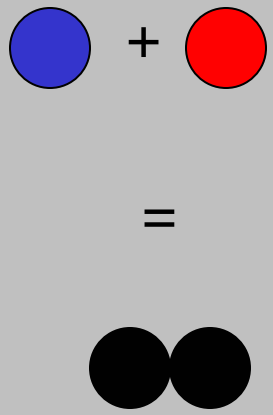
University of Maryland

Val ili čestica ?

Zbrajanje valova

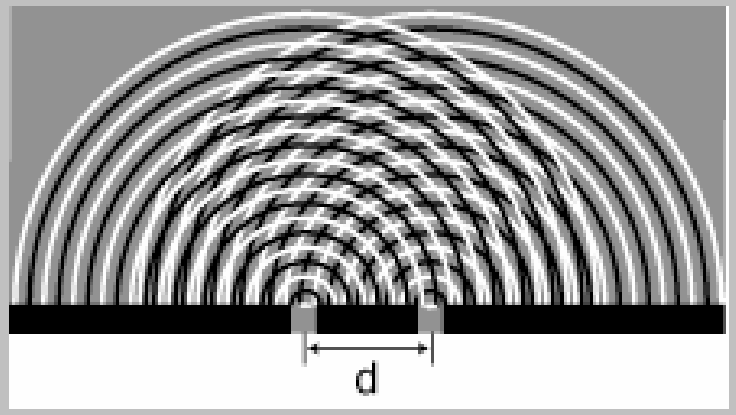


Zbrajanje čestica



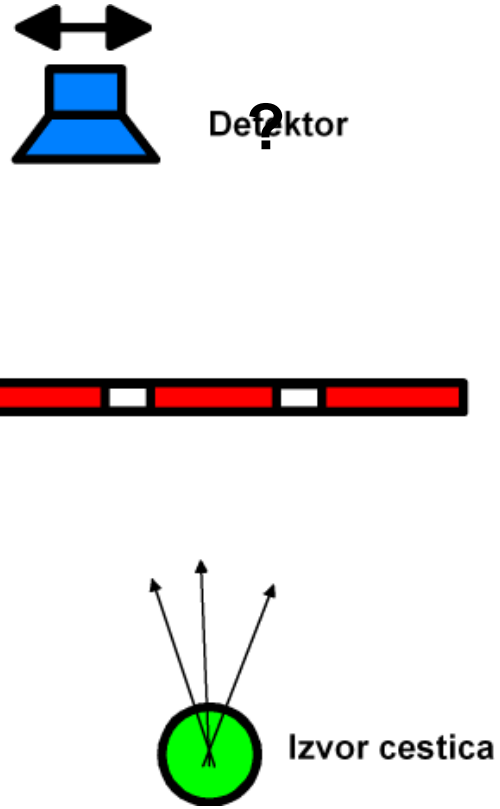
Ogib valova na dvije pukotine

Ogib svjetlosti kroz dvije pukotine dovodi do difrakcijske slike zbog valne prirode svjetlosti.



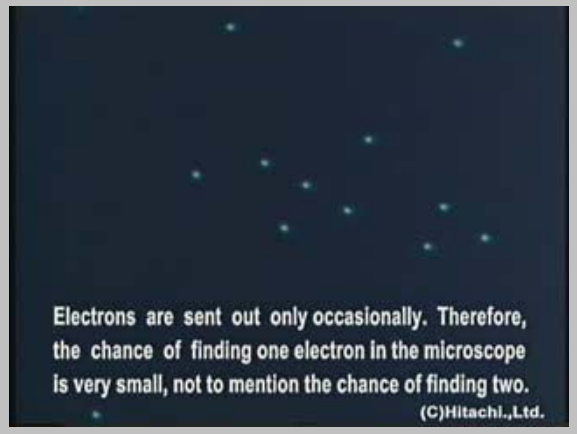
Kakva će slika nastati iza zaslona s pukotinama kada pucamo čestice prema zaslonu?

Ogib čestica na dvije pukotine



Zbog valne prirode čestica (de Broglie), i prolazak čestica kroz metu koja se sastoji od dvije pukotine može dovesti do ogibne slike.

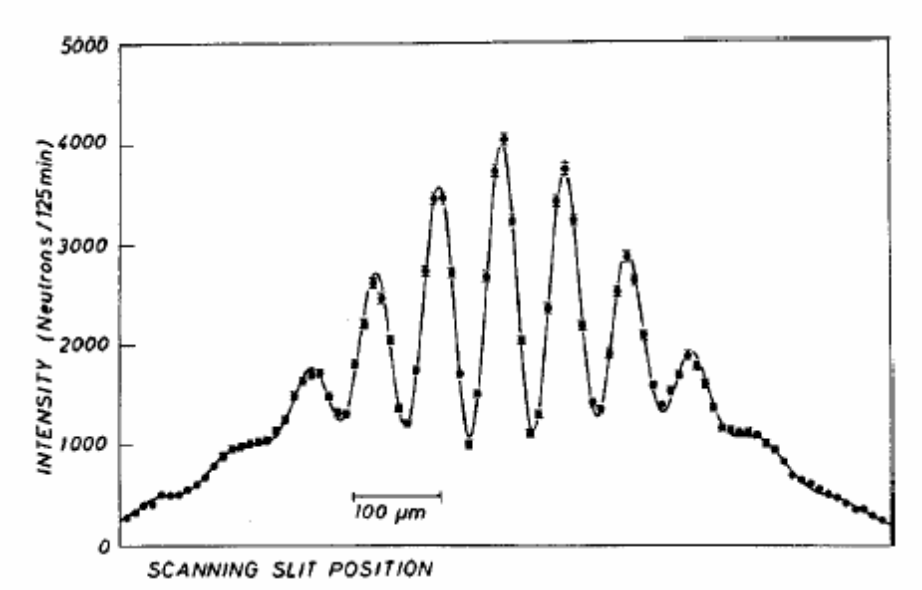
Ogib s elektronima, Tonomura



Akira Tonomura i suradnici u Hitachiju su 1989. napravili eksperiment sa slabim elektronskim snopom elektronskom biprizmom što odgovara ogibu na dvostrukoj pukotini. Opazili su ogibnu sliku kao rezultat (i) valne prirode čestica.

http://www.hqrd.hitachi.co.jp/em/movie/doubleslite-n.wmv

Ogib sa sporim neutronima, Zeilinger

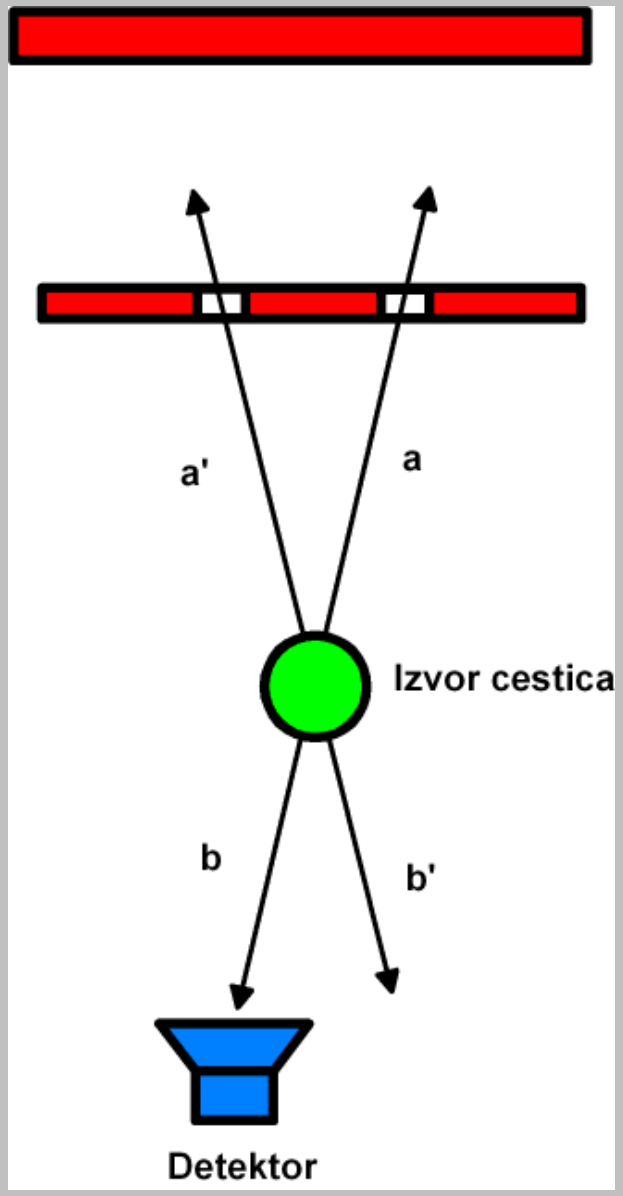


Difrakcijska slika iza dvije pukotine, mjerena s vrlo sporim neutronima čija je valna duljina 2 nm, odnosno brzine 200 m/s. Pukotine su bile 22 mm široke, razdvojene 104 nm. Pripadajući kutevi su reda veličine tek 10 miliradijana, tako da je opažačka ravnina morala biti udaljena 5 m od pukotine. Točkice predstavljaju eksperiment, puna crta je teorijski proračun. (Zeilinger *et al.*, 1988)

Čestice stižu jedna po jedna u detektor. Jedini način na koji one mogu stvarati interferometrijsku sliku je da je putanja svake čestice dana kao superpozicija putanje kroz jednu i kroz drugu pukotinu.

Po principima kvantne fizike, ovakva interferencijska slika je moguća samo zbog toga što mi ni na koji način ne možemo znati kroz koju je pukotinu prošla čestica.

Možemo li zamisliti eksperiment u kojemu ćemo točno znati kroz koju pukotinu prolazi čestica i što će se onda dogoditi s interferencijskom slikom?



Neka istodobno (nuklearnim raspadom) nastaju dvije čestice koje se gibaju po istom pravcu, suprotnim smjerovima. (Zakon sačuvanja gibanja!)

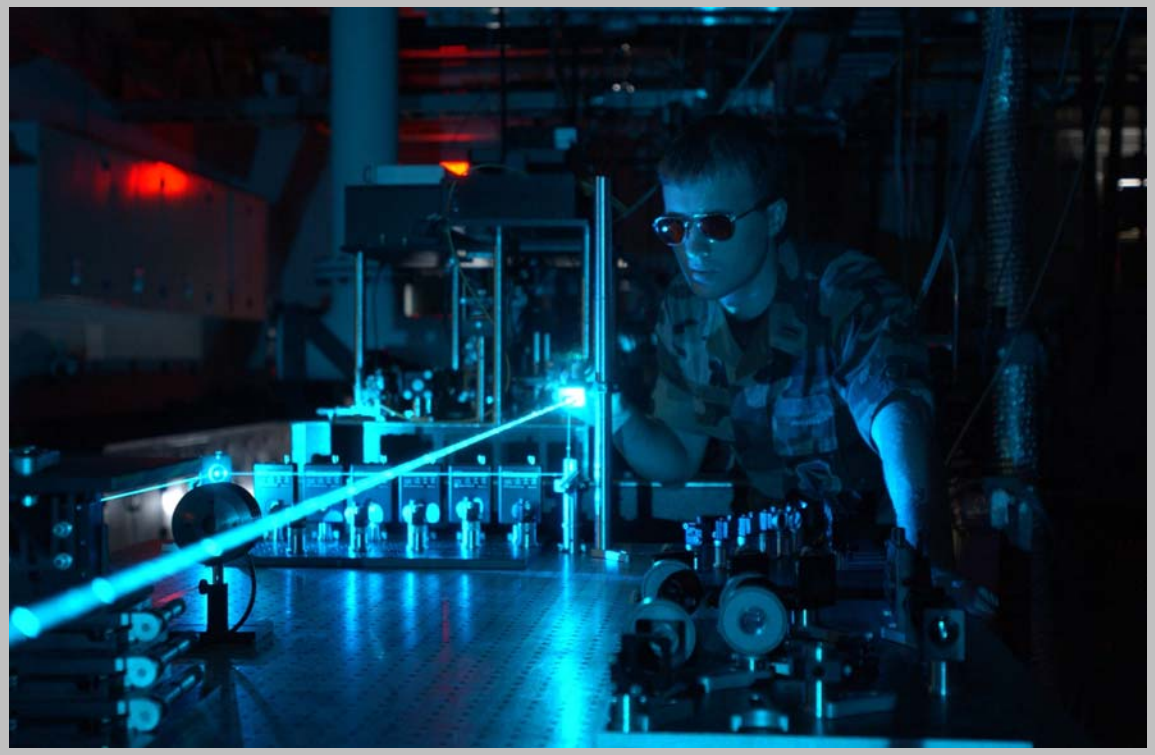
Tada ćemo postavljanjem detektora na pravac gibanja b čestice i detektiranjem te čestice točno znati da je u tom događaju ona druga čestica prošla kroz pukotinu a.

U ovom eksperimentu se NE opaža interferencijska struktura na zaslonu.

Kažemo da je par čestica ab spregnut (entangled).

Spregnuta stanja najupečatljivije pokazuju osobine nelokalnosti i nerazdvojivosti u kvantnoj fizici.

Kvantna kriptografija pomoću lasera



Laser: izvor koherentne svjetlosti.

Snop koherentnih fotona.

Klasična kriptografija

Izazov kriptografije se sastoji u tome da pošiljatelj i primatelj dijele isti ključ za kojeg su sigurni da ga nitko drugi nema. Pomoću ključa pošiljatelj šifrira poruku, a isti ključ služi primatelju za dešifriranje poruke.

Vernam, 1917.

A	B	C	D	E	F	G	H	I	J	K	,	.....	....	X	Y	Z	?		,	.
00	01	02	03	04	05	06	07	08	09	10				23	24	25	26	27	28	29

Poruka za Jamesa Bonda:

	S	H	A	K	E	N		N	O	T		S	T	I	R	R	E	D
Tekst	18	07	00	10	04	13	26	13	26	19	26	18	19	08	17	17	04	03
Ključ	15	04	28	13	14	06	21	11	23	18	09	11	14	01	19	05	22	07
Kodirana poruka	03	11	28	23	18	19	17	24	07	07	05	29	03	09	06	22	26	10

← zbrajanje modulo 30

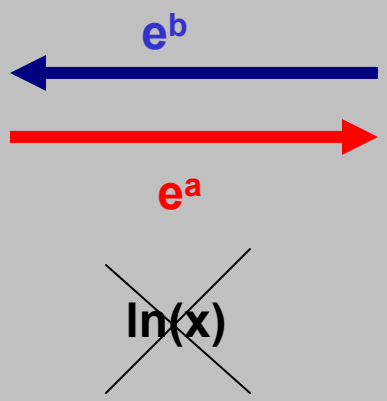
Ključ se može distribuirati tajnim kanalom ili javnim (public key)

Moderna klasična Public-key kriptografija se zasniva na upotrebi one-way funkcija, tj funkcija koje nemaju inverznu funkciju.

RSA algoritam:

Alice odabire slučajni broj a, izračuna veliki broj e^a

Iz dobivenog e^b, Alice računa $(e^b)^a$



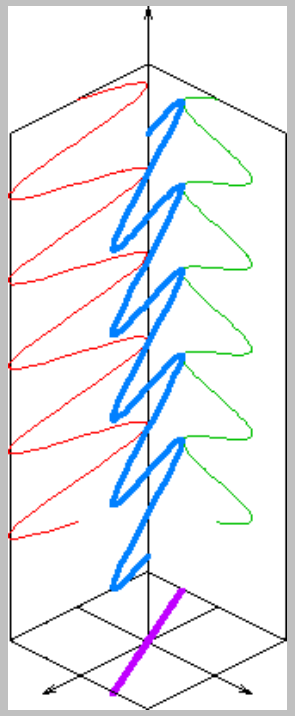
Bob odabire slučajni broj b, izračuna veliki broj e^b

Iz dobivenog e^a, Bob računa $(e^a)^b$

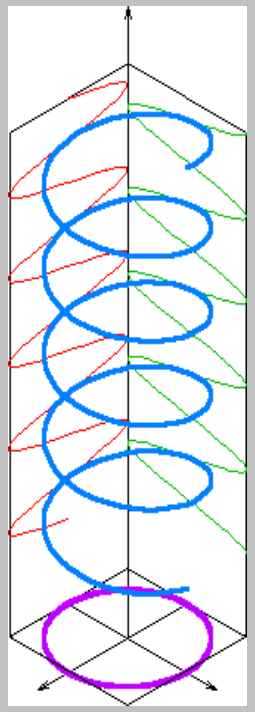
Funkcija e je komutativna, pa je $(e^b)^a = (e^a)^b$ i taj veliki broj je zajednički ključ.

Bitna osobina svjetlosti: polarizacija

Opisuje usmjerenost električnog polja u elektromagnetskom valu.



Linearna polarizacija: x, y



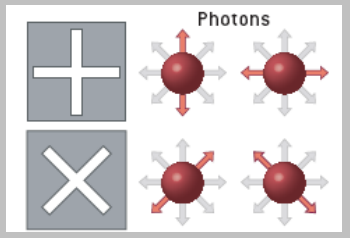
Cirkularna polarizacija: lijeva, desna

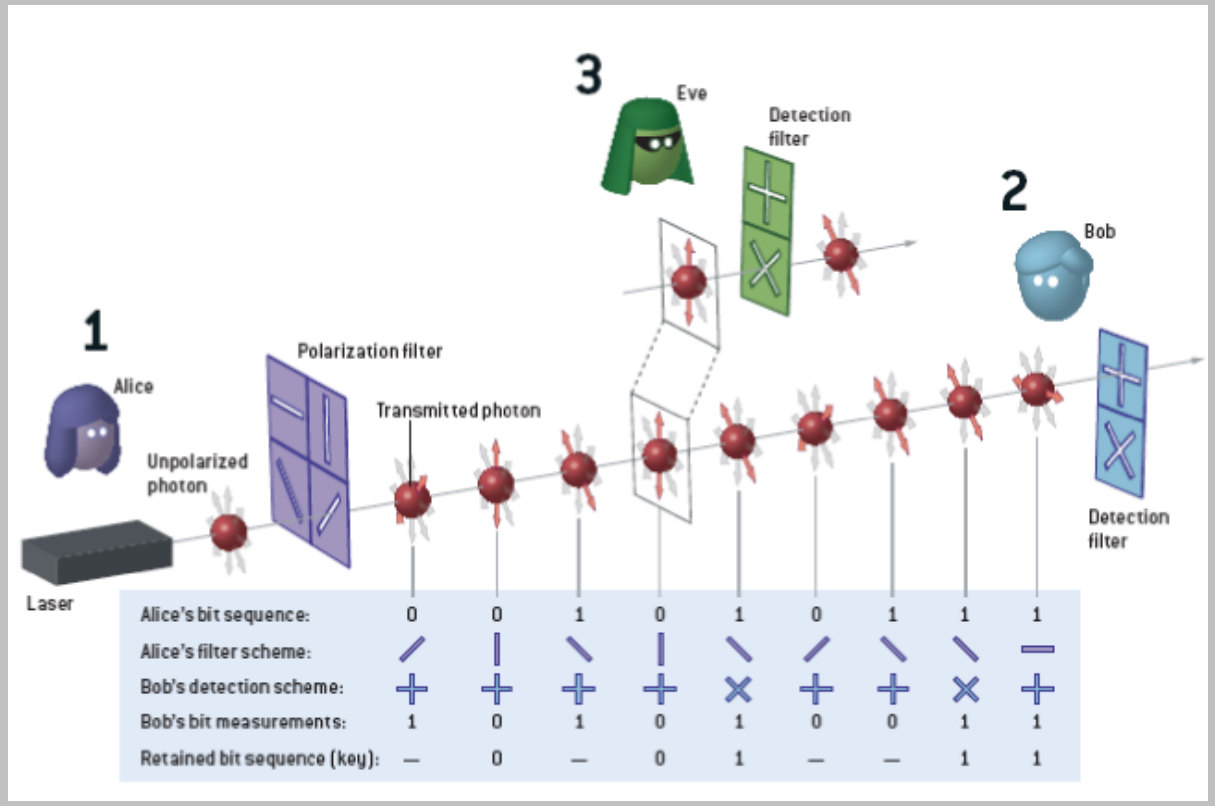
Laserska svjetlost može se dobro polarizirati zbog svoje koherencije.

Kodiranje Polarizacije:

Filter Linearne Polarizacije

Filter Cirkularne Polarizacija

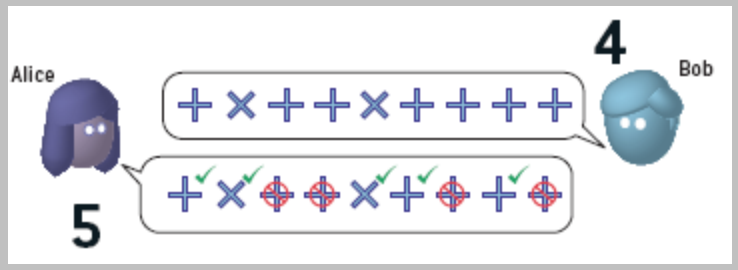




Alice šalje polarizirane fotone i pri tome zapisuje vrstu filtra i vrijednost.

Bob na slučajan način odabire vrstu filtra za svaki pristigli foton, mjeri vrijednost polarizacije i zapisuje vrstu filtra i vrijednosti.

[Scientific American]



Nakon završetka prijenosa, Bob preko klasičnog kanala priopćava Alice koje je filtre upotrebljavao. Alice mu priopćava kad je sve upotrijebio ispravan filter. Alice i Bob zadržavaju samo te, pogođene bitove i taj niz predstavlja njihov tajni ključ.

Teleportacija:

- skeniranje objekta
- “dematerijalizacija” objekta
- spremanje u “međuspremnik”
- slanje u obliku snopa materije na odredište

Tehnički priručnik Sljedeće generacije

10^{28} atoma = jedno ljudsko biće,

ogromna količina energije potrebna za razlaganje na nivo elementarnih čestica

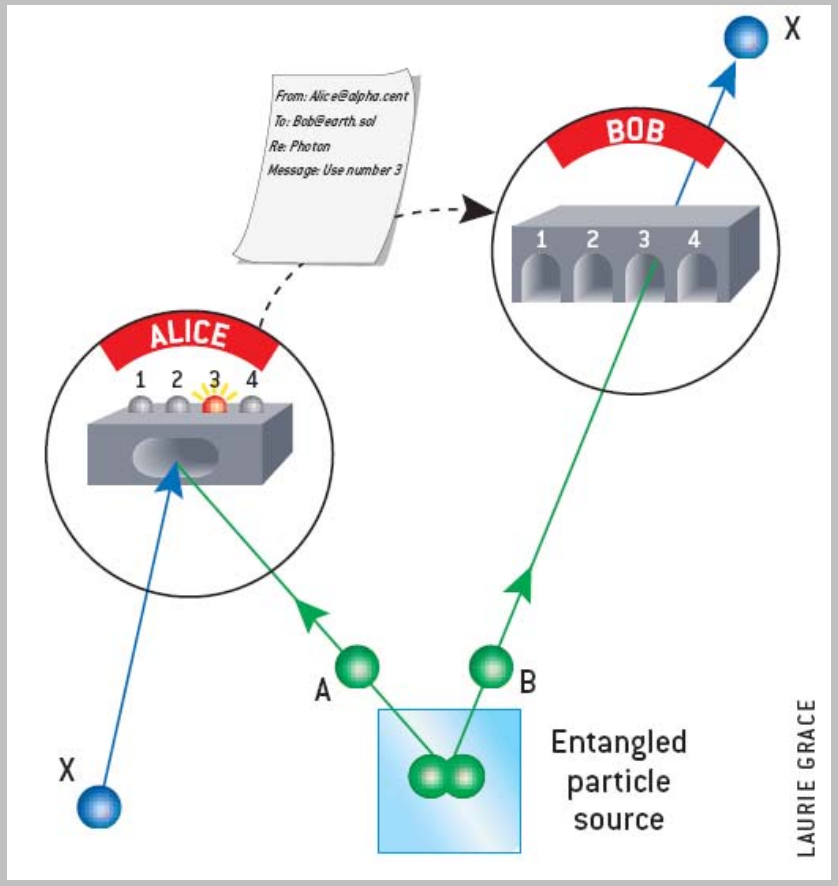
Kako ih ponovno složiti da tvore original?

NEPREMOSTIVE PREPREKE

Slati bitove umjesto atoma?

Kvantna teleportacija

Predstavlja prijenos nepoznatog kvantnog stanja s jednog mjesta na drugo.
Alice želi prenijeti nepoznato kvantno stanje X Bobu. To se postiže na sljedeći način: Alice i Bob dijele spregnuti fotonski par A i B, Alice izvrši skupno mjerenje A i X i time se spregnuti foton kod B postavlja u stanje koje korelira sa stanjem X i rezultatom mjerenja. Javlja Bobu rezultat mjerenja i on tada izvrši mjerenje na B koji sada prelazi u stanje X!



[Zeillinger, Scientific American]

Istraživanja *entanglementa* su bila motivirana u početku filozofskim razlozima. Međutim, razvojem tehnologije i dubljim spoznajama, ovaj intrinzično kvantni pojam dobija primjene u informacijskoj tehnologiji, točnije u kvantnoj informaciji.

Spregnute čestice (najčešće fotoni) imaju primjenu u kvantnoj kriptografiji, kvantnoj teleportaciji, a jednoga dana i u kvantnom računanju.