Osnovni pojmovi komunikacija temeljenih na kvantno-mehaničkim efektima

Samardžija, Kristijan

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

ELEKTROTEHNIČKI FAKULTET OSIJEK

SVEUČILIŠNI DIPLOMSKI STUDIJ

OSNOVNI POJMOVI KOMUNIKACIJA TEMELJENIH NA KVANTNO-MEHANIČKIM EFEKTIMA

DIPLOMSKI RAD

SAMARDŽIJA KRISTIJAN

OSIJEK,2014

ETFOS
ELEKTROTEHNIČKI FAKULTET OSIJEK
Sveučilište Josipa Jurja Strossmayera u Osijeku

Obrazac D1: Obrazac za imenovanje Povjerenstva za obranu diplomskog rada

Osijek, 08.09.2014.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za obranu diplomskog rada

Ime i prezime studenta:	Kristijan Samardžija
Studij, smjer:	Diplomski studij, Komunikacije i informatika
Mat. br. studenta, godina upisa:	D-581, 2012
Mentor:	Prof.dr.sc. Tomislav Švedek dipl.ing.
Sumentor:	
Predsjednik Povjerenstva:	Doc.dr.sc. Marijan Herceg dipl.ing
Član Povjerenstva:	Doc.dr.sc. Tomislav Matić dipl.ing
Naslov diplomskog rada:	Osnovni pojmovi komunikacija temeljenih na kvantno-mehaničkim efektima
Primarna znanstvena grana rada:	**Elektrotehnika**
Sekundarna znanstvena grana (ili polje) rada:	**Radiokomunikacije**
Zadatak diplomskog rada:	Sa stanovišta inženjera komunikacija opisati teoriju kvantnih komunikacija koja uvodi kvantno-mehanička svojstva polarizacije i sprezanja (engl. entanglement) koja nemaju analogije u klasičnoj teoriji komunikacija. Na jednostavnim primjerima pokazati kako se ta kvantna svojstva mogu iskoristiti za realizaciju kanala bez šuma i za poboljšanje iskorištenja kanala kod raspodijeljenih MAC protokola. Također je potrebno opisati i kako se sprezanje može iskoristiti za poboljšanje zaštite i povećanje učinkovitosti distribucije šifre kod kriptografskih sustava zaštite sa simetričnom šifrom koji koriste kvantne kriptografske mreže.
Prijedlog ocjene pismenog dijela ispita (diplomskog rada):	izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu:3 Postignuti rezultati u odnosu na složenost zadatka:3 Jasnoća pismenog izražavanja:3 Razina samostalnosti:II

Potpis sumentora:	Potpis mentora:

Dostaviti:

1. Studentska služba

U Osijeku, godine Potpis predsjednika Odbora:

IZJAVA O ORIGINALNOSTI RADA

Osijek, 09.09.2014.

Ime i prezime studenta:	Kristijan Samardžija
Studij :	Diplomski studij, Komunikacije i informatika
Mat. br. studenta, godina upisa:	D-581, 2012.

Ovom izjavom izjavljujem da je rad pod nazivom**:**

Osnovni pojmovi komunikacija temeljenih na kvantno-mehaničkim efektima

izrađen pod vodstvom mentora

Prof.dr.sc. Tomislav Švedek dipl.ing.

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

Sadržaj:

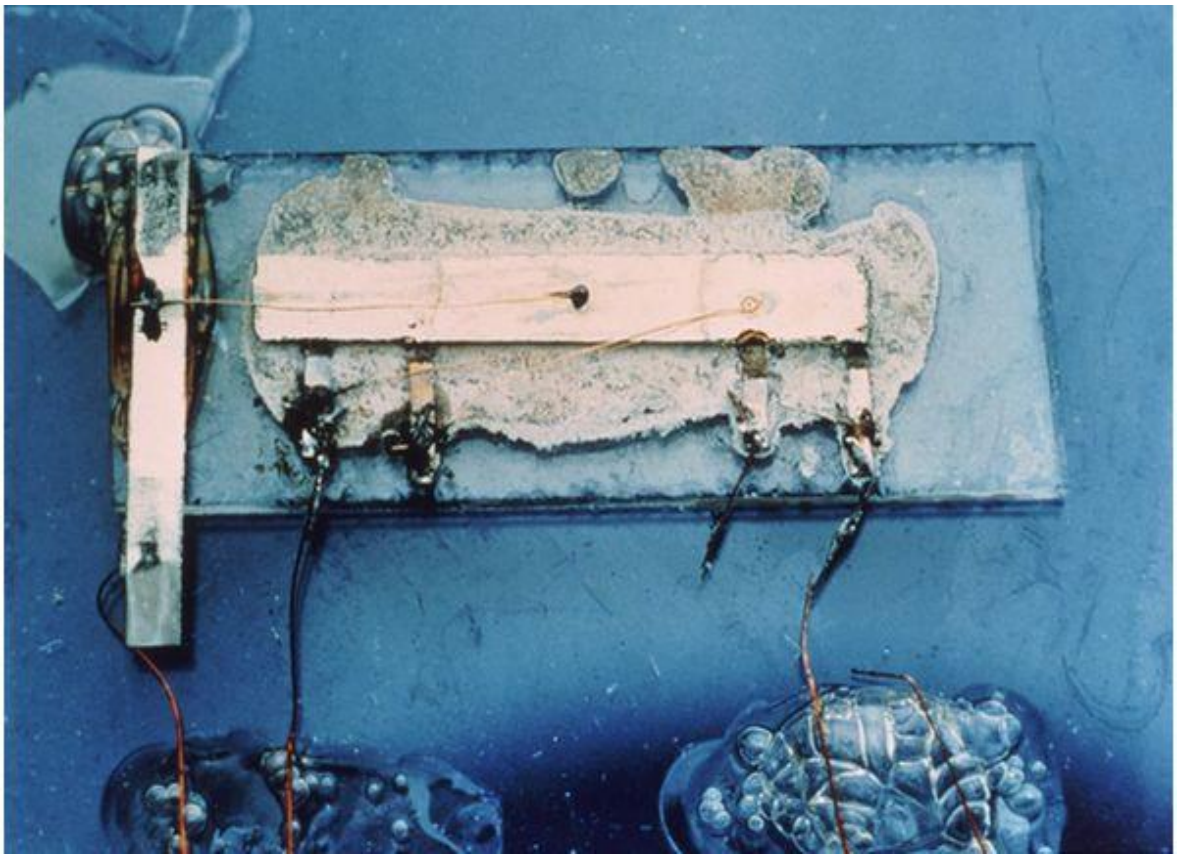
1. UVOD

Gordon E. Moore, suosnivač tvrtke Intel Corporation je 19. travnja 1965. godine u svom radu „Cramming More Components onto Integrated Circuits“ objavljenom u *Electronics magazine* predvidio da će se broj tranzistora po čipu udvostručavati svakih 18-24 mjeseci. Njegova predviđanja su se pokazala točnim, dijelom i zbog toga što poluvodička industrija koristi njegov zakon kako bi upravljala dugoročnim planovima i postavila ciljeve za istraživanje i razvoj. S jedne strane to rezultira sve bržim i bržim procesorima ispunjavajući snove i očekivanja akademske zajednice, industrije i korisnika. S druge strane dolazi do ključnog kompromisa, jer je potrebno gravirati sve tanje i tanje linije na površini poluvodiča, što dovodi do sve manjih i manjih tranzistora. U konačnici je dosegnut nano-svijet (10^{-9}), kojim vladaju pravila i zakoni nazvani kvantna-mehanika te se značajno razlikuje od mikro-svijeta klasične fizike s kojom je čovjek upoznat kroz svoju percepciju i tradicionalni sustav obrazovanja. Neka od ovih novih načela su slična klasičnim mikroskopskim načelima, dok druga nemaju analogije. U svakom slučaju moraju biti prihvaćena kao novi okvir rada računalnih znanosti i komunikacija te je potrebno shvatiti kako ih je moguće iskoristiti za usavršavanje komunikacijske tehnologije. Usklađivanje telekomunikacija i računalnih znanosti rezultira digitalnom obradom informacija na svim razinama stog protokola. Telekomunikacijski čvorovi poput usmjerivača (router) i mobilnih baznih stanica sadrže veliki broj procesora. Stoga, kontinuirani napredak u komunikacijama zahtjeva povećanje propusnosti na fizičkom sloju, ali također i sofisticiranije i brže algoritme. Richard Feynman je opazio među prvima da ako se binarna informacija može prikazati fizički, na primjer eksplozijom fotona ili nagomilanih elektrona, tada se kvantno-mehanička svojstva poput polarizacije fotona ili spina elektrona mogu iskoristiti za šifriranje i prijenos informacija. Ako bi bili sposobni iskoristiti kvantnu-mehaniku u svrhu komunikacija i računalnih znanosti, bilo bi moguće napraviti algoritme efikasnije od onih napravljenih klasičnim načinom zahvaljujući fizičkoj pojavi koja je moguća samo u kvantnom svijetu. Na taj se način otvara put za prekoračenje klasičnog kapaciteta komunikacijskih kanala te postoji mogućnost poboljšanja komunikacijskih protokola, na primjer moguće je eliminirati pitanja i rizike vezane uz sigurnost kriptografije s javnim ključem u globalnoj mreži. Klasična ili kvantna, računalna znanost i komunikacije imaju puno područja preklapanja. Na primjer, obrada signala je kritična za uspješnu visoko-kvalitetnu komunikaciju između dijelova, ali se također može svrstati i kao predmet računalnih znanosti. Kvantne računalne znanosti se mogu

iskoristiti kako bi omogućile puno efikasnija rješenja klasičnih problema obrade signala. [1] Ovaj rad je organiziran na sljedeći način. U uvodnom dijelu su uvedeni pojmovi Mooreovog zakona, kvantne-mehanike i kvantno-mehaničkih svojstava. U nastavku je objašnjen Mooreov zakon te kvantna-mehanika. Nakon toga prelazi se granica između klasičnog i kvantnog i pokazuju se jednostavni primjeri kvantne komunikacije i opisuje se kvantna kriptologija. Zatim slijedi objašnjene sprezanja, čudne, ali vrlo obećavajuće pojave i potencijalno revolucionarnog rješenja za komunikacije. Nakon toga su predstavljene trenutno dostupne primjene kvantne komunikacije, sigurne kvantne komunikacije koje povezuju kvantno-mehaničku teoriju sa svakodnevnom praksom te na kraju dolazi zaključak.

2. Mooreov zakon

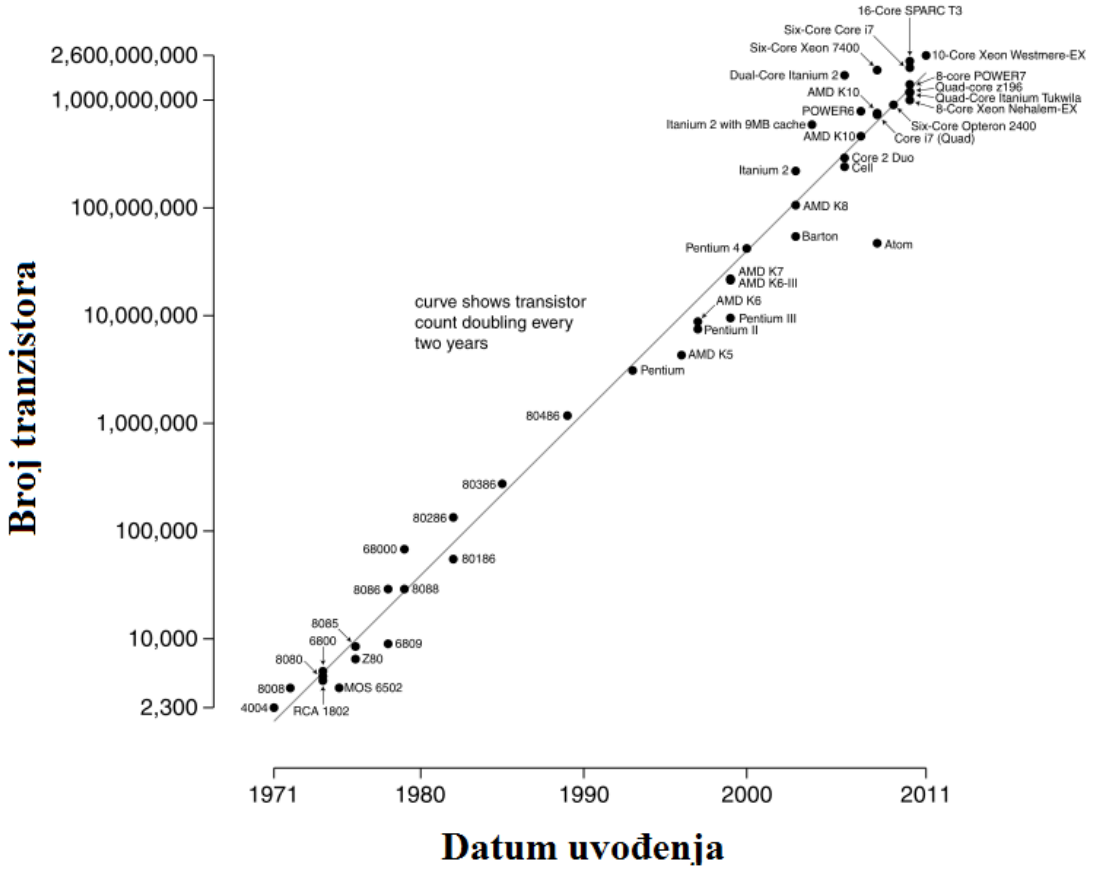
Njemački inženjer Werner Jacobi koji je radio u tvrtki Siemens AG je 1949. godine dobio ideju o razvoju integriranih krugova. Kroz slijedećih 9 godina ta je tehnologija istraživana i razvijana, a tada je Jack Kilby 12. rujna 1958. godine predstavio prvi integrirani krug koji radi. Robert Noyce je pola godine kasnije došao sa svojom idejom integriranih krugova te je njegov silikonski čip sa izoliranim p-n spojem rješavao mnoge probleme koje nije mogao riješiti germanijski čip Jacka Kilbyja.



Slika 2.1.: Fotografija integriranog kruga Jacka Kilbyja [3]

Najčešći poluvodički materijal u upotrebi je silicij (Si) koji se koristi na nižim frekvencijama, a ima ga u izobilju te je tehnologija razvijena oko njega i njegovih oksida, zatim germanij (Ge), dok se za posebne slučajeve (elektroluminescentne i telekomunikacijske elemente) koristi galij-arsenid (GaAs).

Gordon E. Moore je proučavao integrirane krugove od njihovog izuma 1958. godine do 1965. godine kada je objavio svoj rad te je tada došao do zaključka: „Za minimalne troškove, broj komponenti po čipu godišnje će se povećati približno dva puta te je izvjestan nastavak kroz kraći period, ako ne i povećanje. Kroz duži period povećanje je neizvjesno, iako ne postoji razlog vjerovati kako neće ostati konstantan najmanje 10 godina, a to znači kako će 1975. godine za minimalnu cijenu broj komponenti po čipu iznositi 65 000“. Nakon nekog vremena Moore je promijenio svoju formulaciju te je 1975. godine promijenio svoje predviđanje na svakih 2 godine. [2]



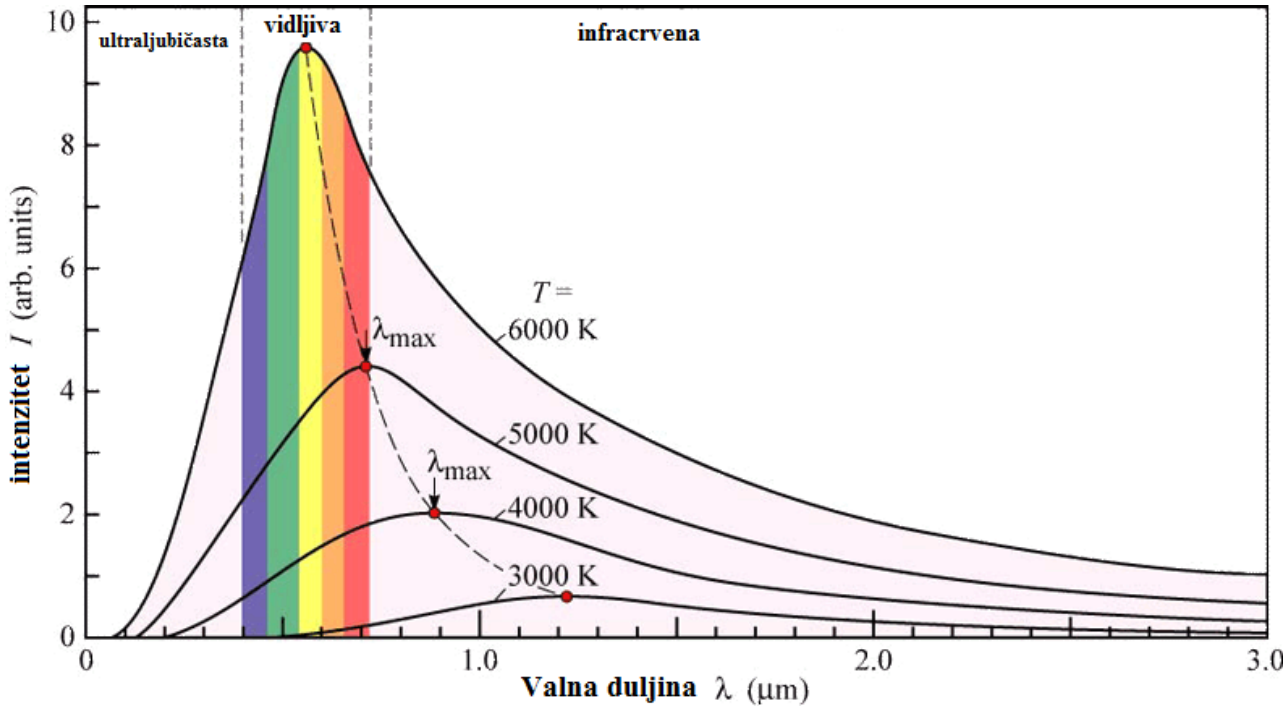
Slika 2.2.: Broj tranzistora i Mooreov zakon [4]

Na slici je prikazan razvoj integriranih krugova kroz godine te se vidi da je Mooreov zakon točno predvidio rast broja tranzistora po čipu (udvostručavanje svakih dvije godine).

Moore je također napisao kako je prednost integrirane elektronike to što će dovesti do razvoja i rasta elektronike te da će se ona proširiti u mnogo sfera, kao što su na primjer kućanski uređaji (hladnjaci, štednjaci), zatim u medicinske svrhe (ECG – *Electrocardiogram*, EEG – *Electroencephalogram*) i da najveći potencijal leži u proizvodnji velikih sustava i da će računala postati jača i brža. Predvidio je da će integrirana elektronika dovesti do toga da svako kućanstvo ima računalo te će svatko imati prijenosni uređaj za komuniciranje (mobitel). Napisao je da najveći potencijal leži u proizvodnji velikih sustava. [2]

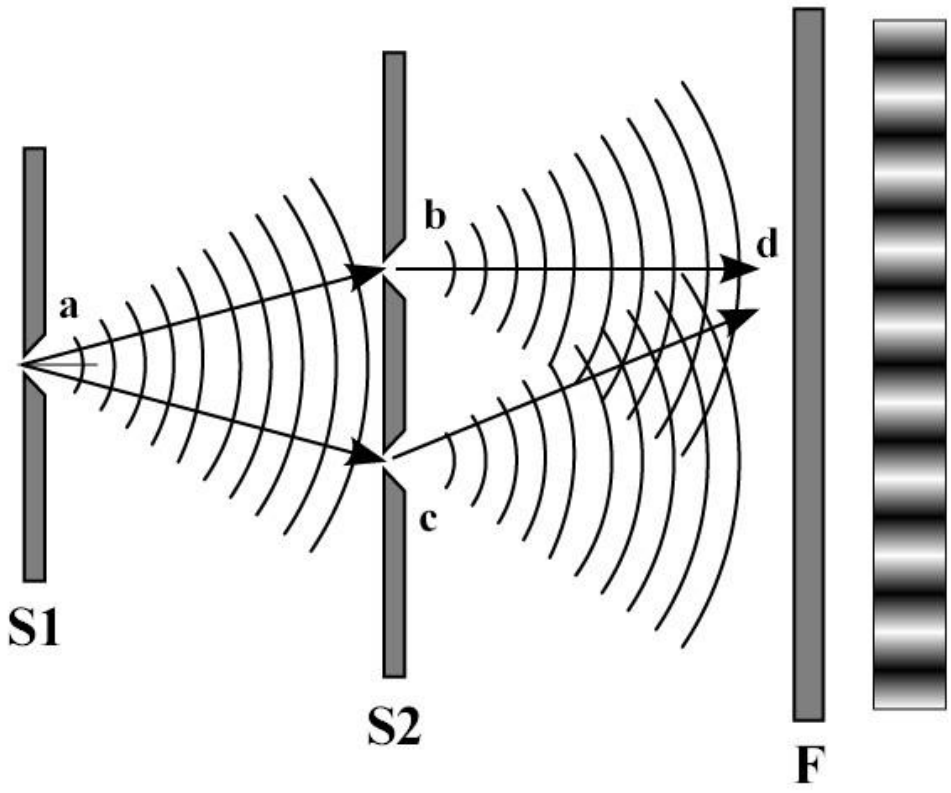
3. Kvantna-mehanika

Znanstveno istraživanje valne prirode svjetla je započelo u 17. i 18. stoljeću u kojima su se istaknuli znanstvenici poput Rooberta Hookea, Christiana Huygensa, Leonharda Eulera i Thomasa Younga. Gustav Kirchoff je 1859. godine iznio problem zračenja crnog tijela. Idealno crno tijelo je tijelo koje upija sve valne duljine elektromagnetskog zračenja koje padaju na njega. Budući da idealno crno tijelo upija sve valne duljine bez gubitaka, ono također emitira sve valne duljine bez gubitaka, ovisno samo o termodinamičkoj temperaturi tog tijela. Idealno crno tijelo ne postoji.



Slika 3.1.: Crno tijelo [5]

Na slici se vidi kako pada temperatura tijela, tako pada i intenzitet svjetlosti te ide prema većim valnim duljinama.



Slika 3.2.: Valna interferencija u pokusu Thomasa Younga [21]

Slika prikazuje prolazak svjetlosti kroz dvostruki razrez u pokusu Thomasa Younga te da svjetlost uzrokuje interferenciju, svojstvo karakteristično za valove, a on je bio u mogućnosti odrediti njenu valnu duljinu.

Max Planck je 14. prosinca 1900. godine predstavio svoju kvantnu hipotezu kojom je objasnio zračenje crnog tijela. Definirao je kvant energije (h = 6,6260693·10^{-34} Js), kasnije nazvan Planckovom konstantom, kao najmanju količinu energije koju neko tijelo može primiti ili emitirati. U originalu je njegova hipoteza opisivala konstantnu proporcionalnost između energije (E) harmoničkog izolatora i frekvencije (f) titranja.

$$E = h \cdot f \quad , \tag{3-1}$$

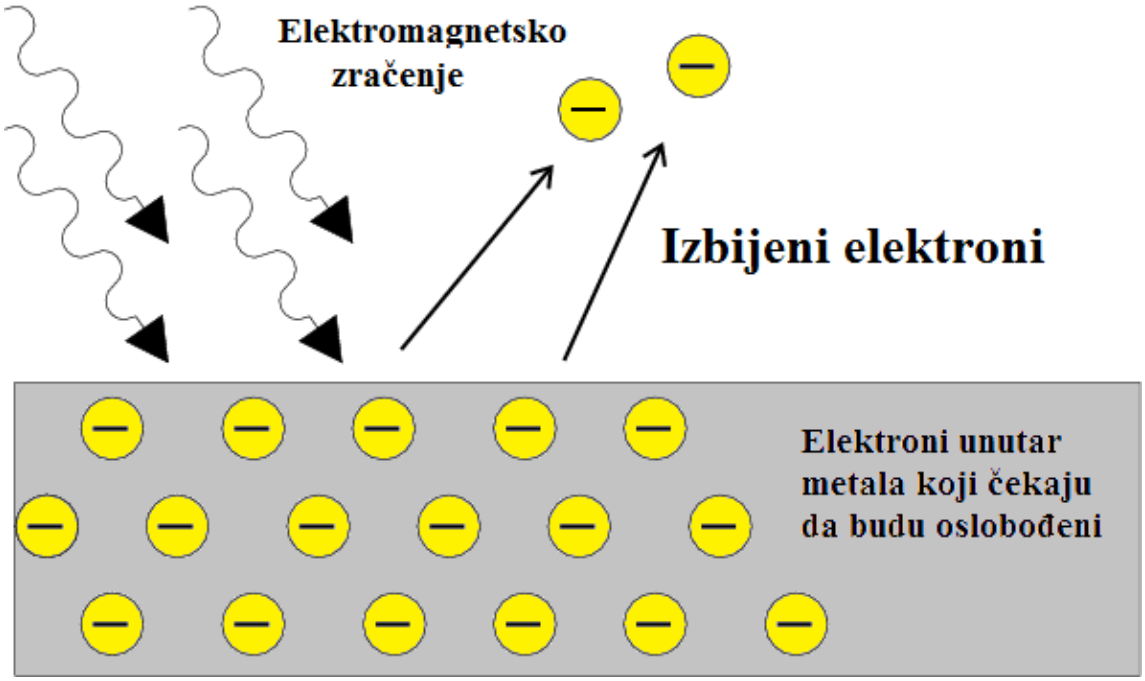
gdje je:

E energija harmoničkog izolatora

h = 6,6260693·10^{-34} Js Planckova konstanta

f frekvencija titranja.

Albert Einstein je 1905. godine iskoristio Planckovu kvantu hipotezu kako bi objasnio fotoelektrični efekt. Fotoelektrični efekt je fizikalna pojava kod koje djelovanjem elektromagnetskog zračenja dovoljno kratke valne duljine dolazi do izbijanja elektrona iz obasjanog materijala (najčešće metal).



Slika 3.3.: Fotoelektrični efekt [22]

Na slici se vidi elektromagnetsko zračenje koji dolazi s lijeva i udara elektrone unutar metala, koji apsorbiraju energiju te su izbijeni iz metala.

Daljnjim istraživanjem kvanta otkriveno je ponašanje povezano sa samostalnim jedinicama (česticama), koje su nazvani fotoni. Foton je elementarna čestica koja se u vakuumu giba brzinom svjetlosti (c = 299792458 m/s), nema masu i električni naboj te je stabilan. Zbog toga su znanstvenici došli do zaključka da svjetlost ima dvojnu narav, jer pokazuje svojstva i vala i čestice. Fotoelektrični efekt te Comptonovo raspršenje daju dokaze za čestičnu prirodu svjetla, a interferencija i difrakcija daju dokaze za valnu prirodu svjetla. Zahvaljujući Einsteinu i njegovu objašnjenju fotoelektričnog efekta te Planckovom objašnjenju zračenja crnog tijela ukazala se nužnost da se zrakama svjetlosti (elektromagnetsko zračenje) pridruže čestična svojstva. Za otkriće i

razvoj kvantne mehanike, ključan rad je bio Louisa V. P. R. de Brogliea. On je 1924. godine uveo hipotezu o elektronskim valovima, odnosno pretpostavio je da elektronima u pokretu treba pridružiti i valna svojstva, a tezu su potvrdili Lester Germer i Clinton J. Davisson 1927. godine u eksperimentu u kojemu je dokazana difrakcija elektrona na kristalima. Germer i Davisson su istraživali refleksiju elektrona na površini kristala nikla. Kada elektron pogodi kristal, atomi nikla u kristalu razbacaju elektrone u svim smjerovima. Njihovi normalni polikristalni uzorci su razbacivali elektrone u vrlo blagim kutovima. Početkom 1925. godine u nesreći koja se dogodila u njihovom laboratoriju došlo je do slučajne rekristalizacije uzorka koji je promijenio svoju strukturu u gotovo monokristalni oblik, što je rezultiralo oštrim vrhovima pri određenim kutovima. Ubrzo su Germer i Davisson shvatili da i ostali monokristali imaju anomalije u ponašanju, koje se razlikuju s kemijskim sastavom, kutom upada i orijentacijom uzorka. Njihova kasnija mjerenja su potvrdila kvantno-mehanička predviđanja valne duljine čestice kao funkcije impulsa *p*:

$$\lambda = \frac{h}{p} \quad , \tag{3-2}$$

gdje je:

λ valna duljina čestice

h = 6,6260693·10^{-34} Js Planckova konstanta

p impuls čestice.

Fenomen difrakcije elektrona je prilično općenit i može se objasniti valnom prirodom čestica atoma. [6][9] Ravnine atoma u kristalu (Braggova ravnina) su pravilno raspoređene i mogu proizvesti konstruktivni uzorak interferencije, ako je ispunjen Braggov zakon (zakon koji određuje Braggov kut difrakcijskog maksimuma nastalog rendgenskom, elektronskom ili neutronskom difrakcijom u kristalu):

$$n\lambda = 2\, d \sin\theta = D \sin\Phi \quad , \tag{3-3}$$

gdje je:

n cijeli broj (višekratnik valne duljine)

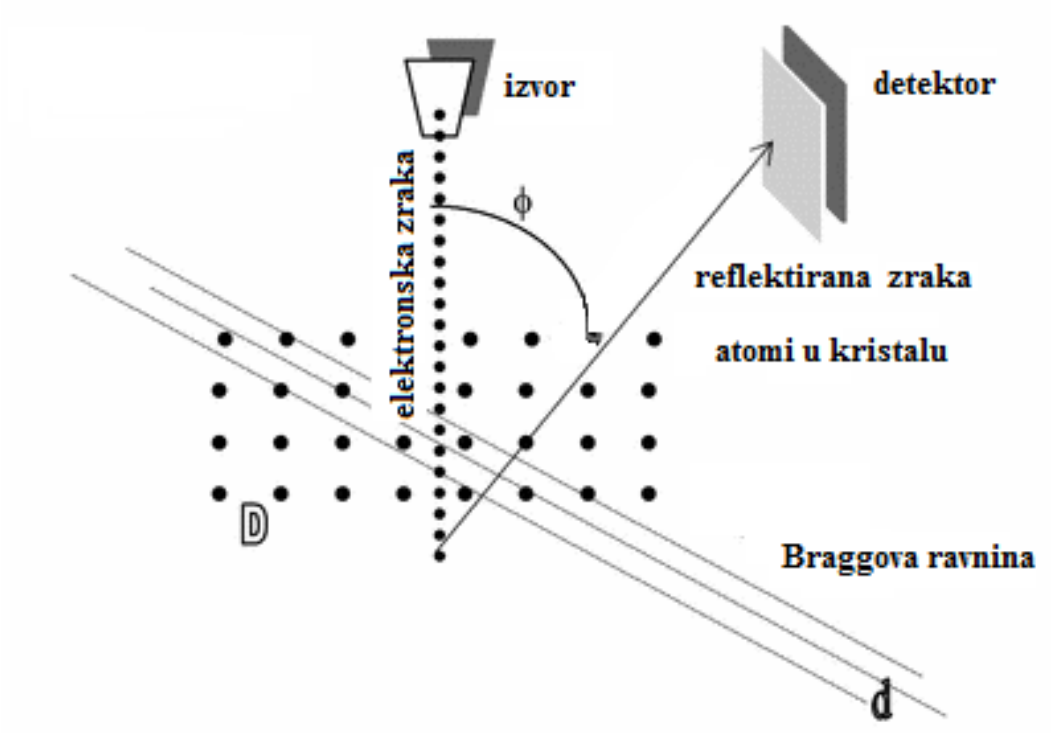
λ valna duljina upadnog vala

d razmak između ravnina atoma

θ kut između upadne i reflektirane zrake

D razmak između atoma u kristalu

Φ kut između upadne i reflektirane zrake.



Slika 3.4.: Pokus Germera i Davissona [9]

Na slici je prikazan pokus Germera i Davissona. Kada upadna zraka udari u kristal, kojemu su ravnine atoma raspoređene pravilno (svi atomi međusobno jednako udaljeni), tada dolazi do refleksije zrake, odnosno do difrakcije elektrona. Difrakcijska slika je bila dokaz valne prirode elektrona.

Jedna od primjena otkrića Louisa V. P. R. de Broglieva je elektronski mikroskop, koji ima veću rezoluciju od optičkih mikroskopa. U siječnju 1926. godine Erwin R. J. A. Schrödinger je u časopisu *Annalen der Physic* objavio članak „Quantisierung als Eigenwertproblem“. Taj rad je poznat kao Schrödingerova jednadžba, a ona predstavlja jedan od temelja kvantne mehanike. U članku je dao „derivaciju“ valne jednadžbe za vremenski neovisne sustave i pokazalo se da je dao

točnu energetsku vlastitu vrijednost za atom sličan vodiku. Ovaj članak slavljen je kao jedan od najvažnijih znanstvenih radova 20. stoljeća, a napravio je i revoluciju u kvantnoj mehanici te općenito u cijeloj fizici i kemiji. Četiri tjedna kasnije, Schrödinger izdaje još jedan članak koji je riješio kvantni harmonijski oscilator, kruti rotor i dvo-atomne molekule, a dao je i novu derivaciju njegovoj jednadžbi. Treći članak, iz svibnja, prikazao je ekvivalentnost pristupa sličnog onom koji je primjenjivao Werner Heisenberg, a dao je i obradu Starkovog učinka. Četvrti članak, iz ove impresivne serije, dao je način rješavanja problema u kojima se sustav mijenja s vremenom. Schrödingerova jednadžba prikazuje prostorno i vremensko ponašanje čestice u okviru kvantne mehanike. U svojoj prvobitnoj formulaciji, bez notacije koju je uveo P. A. M. Dirac, jednadžba glasi: [23]

$$i\hbar \frac{\partial}{\partial t}\psi(r,t) = -\frac{\hbar^2}{2m}\nabla^2 \psi(r,t) + V(r)\psi(r,t) \quad , \qquad (3\text{-}4)$$

gdje je:

$\hbar$ = 1,054571726 · 10^{-34} Js reducirana Planckova konstanta

$i = \sqrt{-1}$ imaginarna jedinica

$\frac{\partial}{\partial t}$ parcijalna derivacija po vremenu

$\psi(r,t)$ valna funkcija

∇^2 nabla operator

$V(r)$ potencijalna energija

m masa čestice.

Za svjetlost vrijedi Heisenbergovo načelo neodređenosti koje govori kako je načelo gotovo nemoguće odrediti točan položaj i brzinu neke čestice. Kako bi se pomoću promatranja odredio položaj nekog tijela, treba ga osvijetliti i primiti svjetlost koja se od njega reflektira. Međutim, zbog ogiba svjetlosti položaj tijela može se odrediti najpreciznije uz pomoć valne duljine svjetlosti. Smanjenjem valne duljine korištene svjetlosti može se sve preciznije odrediti položaj tražene čestice, ali se u tom slučaju povećava energija zračenja (3-1), odnosno čestična svojstva svjetlosti (elektromagnetskog vala) čiji foton u tom slučaju ima veću količinu gibanja, pa tako u

„sudaru“ s promatranom česticom više mijenja njenu količinu gibanja (u odnosu na početnu) tako da je i nju nemoguće sasvim točno odrediti. Povećanjem čestičnih svojstava svjetlosti kojom se osvjetljava (smanjenje valne duljine) gubi se na preciznosti mjerenja brzine (količine gibanja), a povećanjem valnih svojstava (povećanje valne duljine) gubi se na preciznosti određivanja položaja. [20] Za elektrone u kvantnom sustavu vrijedi Paulijev princip isključenja, unatoč velikom uspjehu Bohrova modela i Schrödingerove kvantne-mehanike, objašnjavajući glavna obilježja vodikovog spektra i ostalih jedno-elektronskih atomskih sustava, nijedan (od spomenute dvojice) nije dao zadovoljavajuće objašnjenje kemijskih svojstava atoma. Prema prijedlogu ruskog kemičara Mendeljejeva, atomi su posloženi u periodni sustav, no razlog takve sistematizacije ostao je nejasan. Zapravo je austrijski fizičar Wolfgang Pauli ponudio rješenje problema. Predložio je nešto što je poznato kao Paulijev princip isključenja: „U bilo kojem kvantnom sustavu, dva elektrona ne mogu zauzeti isto kvantno stanje“. Ustvari, princip isključenja ne vrijedi samo za elektrone nego za sve čestice čiji je spinski kvantni broj polovica cijelog neparnog broja (na primjer $\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}$ i tako dalje). [24] Princip isključenja zadaje važan uvjet simetrije za valnu funkciju više-elektronskih sustava. Engleski teorijski fizičar Paul A. M. Dirac je 1928. godine otkrio postojanje para čestice i antičestice. Čestica i antičestica imaju nekoliko identičnih svojstava, kao što su: masa, vrijeme raspada i tako dalje, ali imaju suprotan naboj. U prirodi svaka čestica ima svoju antičesticu. Primjerice, atom antivodika je sastavljen od negativno nabijenog antiprotona oko kojeg "kruži" pozitivno nabijeni elektron - pozitron. Ako se dogodi da se čestice tvari i antitvari (antitvar je struktura sastavljena od antičestica) sudare ili na neki drugi način dođu u međusobni kontakt, međusobno će se poništiti uz oslobađanje elektromagnetskih valova koji nose energiju. Diracova teorija uvodi i nova shvaćanja o praznom prostoru. On odbacuje zamisao o vakuumu kao teorijskom ništavilu. Prazan prostor koji ne sadrži nikakve čestice još uvijek nije „ništa“ već ima fizikalna svojstva. On se može polarizirati tako da se iz njega istrgnu elektroni, a „rupe“ koje pri tome izbijanju elektrona nastaju jesu pozitroni. Vakuum je nabijen mnoštvom virtualnih čestica i antičestica koje se mogu pojaviti praktično ni iz čega i potom se u najmanjem djeliću vremena natrag poništiti (što su čestice teže to će se prije poništiti). [25] Ovakav proces je moguć zbog Heisenbergovog načela neodređenosti.

3.1 Fizikalna svojstva valova

Val je poremećaj sredstva koji se određenom brzinom širi kroz prostor.

Postoje tri vrste valova:

a) Mehanički valovi (ponašaju se prema Newtonovim zakonima i mogu postojati samo unutar nekog sredstva, na primjer u vodi (vodeni valovi), u stijenama (seizmički valovi)).
b) Elektromagnetski valovi (ne zahtijevaju medij za prenošenje, jer se šire i u vakuumu i to brzinom svjetlosti, na primjer svjetlost, radio i TV valovi).
c) Valovi materije (valovi pridruženi elektronima, protonima, atomima,…).

Valovi se dijele na:

a) Transverzalne valove → čestice sredstva titraju okomito na smjer širenja vala
b) Longitudinalne valove → čestice sredstva titraju u smjeru širenja vala

I) Refleksija

Proces koji se zbiva kada zraka svjetlosti padne na granicu dvaju optičkih sredstava te se odbije i pod jednakim kutom vrati u isto sredstvo, pri čemu obje zrake i okomica na graničnu plohu leže u istoj ravnini.

II) Refrakcija

Promjena smjera svjetlosne zrake pri prijelazu iz jednog optičkog sredstva u drugo sredstvo, pri čemu upadna zraka, lomljena zraka i okomica na granicu sredstava leže u istoj ravnini.

III) Ogib ili difrakcija

Valna pojava pri kojoj se svjetlosni val ogiba iza ruba prepreke i ulazi u područje geometrijske sjene.

IV) Interferencija

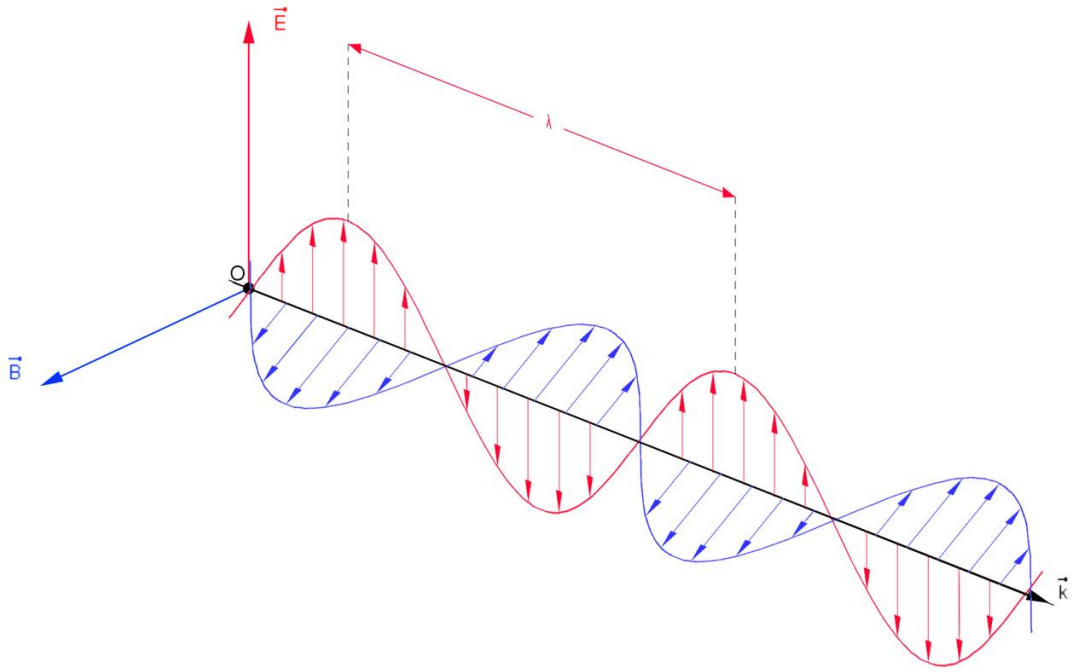
Pojava u kojoj se, ovisno o razlici optičkih putova, svjetlosni valovi koji u neku točku dolaze iz dvaju koherentnih izvora mogu pojačati, djelomično poništiti ili potpuno poništiti.

V) Disperzija

Razlaganje bijele svjetlosti na boje zbog ovisnosti indeksa loma o valnoj duljini.

VI) Polarizacija

Polarizacija (valova) je orijentacija oscilacija u ravnini okomitoj na transverzalan smjer širenja vala. Razlikuju se linearna, kružna i eliptična polarizacija.



Slika 3.1.1.: Polarizacija elektromagnetskog vala [26]

Na slici je prikazana linearna polarizacija elektromagnetskog vala, plavom bojom je predstavljena polarizacija magnetskog polja *B*, a crvenom bojom je predstavljena polarizacija električnog polja *E*.

3.2 Fizikalna svojstva čestica

Čestica je djelić tvari vrlo malih dimenzija koju je moguće opisati uz pomoć nekih fizikalnih ili kemijskih svojstava kao što su masa i volumen. Kada se proučava u kontekstu vrlo malih dimenzija, kvantna mehanika postaje bitna i pojačava nekoliko fenomena koji su demonstrirani u modelu čestice u kutiji (model koji opisuje česticu koja se slobodno kreće u malom prostoru, a okružena je neprobojnim preprekama, a služi kao hipotetski primjer objašnjenja razlike između klasičnih i kvantnih sustava), uključujući model dualnosti te teoretskih razmatranja.

I) Veličina

Izraz čestica se koristi u tri različita slučaja. Prvi je kada se govori o makroskopskim česticama, obično se radi o česticama mnogo većima od atoma i molekula ili čak i o objektima veličine

zvijezda ili čak galaksija. Primjeri makroskopskih čestica su prašina, pijesak te krhotine nakon automobilskih nesreća. Drugi tip je mikroskopska čestica i ona se obično odnosi na čestice u rasponu veličine od atoma molekule, kao što je to na primjer ugljični dioksid, pa sve do nanočestica i koloidnih čestica. Najmanje čestice su subatomske čestice, koje se odnose na čestice manje od atoma, uključujući čestice koje tvore atom – proton, elektron i neutron.

II) Sastav

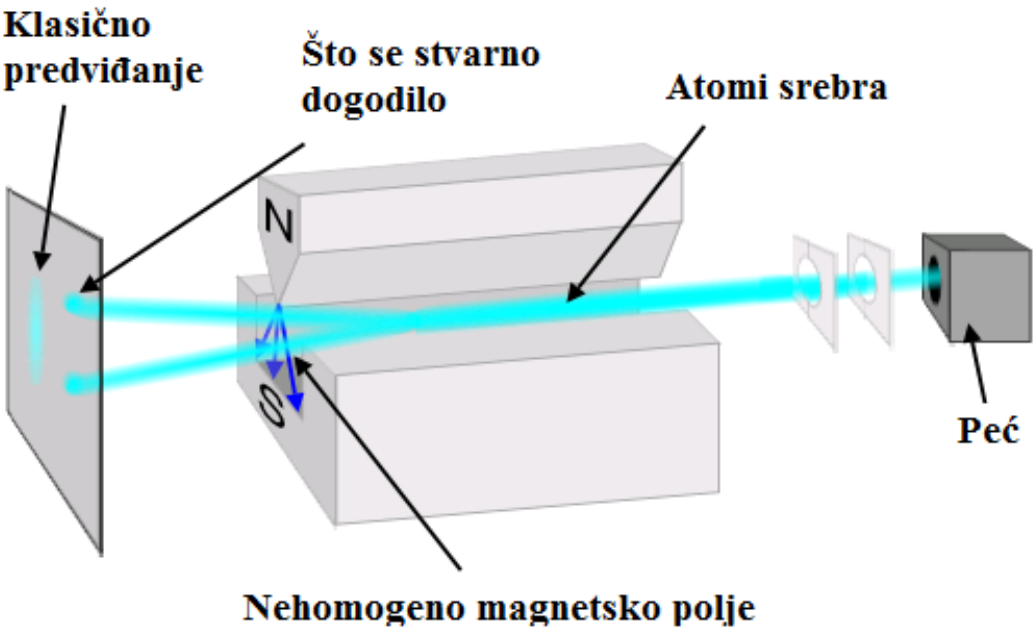
Čestice se također mogu podijeliti po sastavu. Sastavne čestice se odnose na čestice koje imaju sastav – na čestice koje su sastavljene od drugih čestica. Na primjer atom ugljik-14 (radioaktivni ugljik) se sastoji od 6 protona, 8 neutrona i 6 elektrona. Druga vrsta čestica podijeljenih po sastavu su elementarne čestice - čestice koje nisu sastavljene od drugih čestica. Prema trenutnom znanju takvih čestica je vrlo malo, kao što su Lepton, Kvark i Gluon.

III) Stabilnost

Za sastavne i elementarne čestice se zna da prolaze kroz proces propadanja. One koje ne propadaju nazivaju se stabilnim česticama, kao što je na primjer elektron. Životni vijek stabilnih čestica može biti ili beskonačan ili dovoljno dugačak da sakrije proces raspadanja.

3.3 Spin elektrona

Elektroni su čestice koje imaju električni naboj. Kadgod se električni naboj kreće, stvara se magnetsko polje. Elektron se kreće orbitom oko jezgre te stvara magnetsko polje. Spin elektrona čini drugo magnetsko polje. Dakle atomi se ponašaju poput malih magneta. Magneti mogu djelovati međusobno, što znači da atomi mogu biti pod utjecajem vanjskog magnetskog polja. Otto Stern i Walther Gerlach su 1921. godine napravili zanimljiv pokus. Uzeli su snop električki neutralnih atoma srebra i pustili ga kroz nehomogeno magnetsko polje. Magnetsko polje je skrenulo atome srebra, baš kao što bi polje skrenulo male dvopolne magnete. Nakon prolaska kroz polje, atomi su udarali u foto-ploče i ostavljali vidljive točkaste tragove. Rezultat pokusa bio je totalno neočekivan te su Stern i Gerlach ostali vrlo iznenađeni.



Slika 3.3.1.: Sternov i Gerlachov pokus [11]

Slika prikazuje Sternov i Gerlachov pokus. Oni su puštali snop električki neutralnih atoma srebra kroz nehomogeno magnetsko polje te su očitavali rezultat sa foto-ploče. Očekivali su da će rezultat biti jednoliko pravocrtno raspoređeni atomi, a ne dvije „točke“ udaljene jedna od druge.

Postojalo je jedno moguće objašnjenje za takvo ponašanje atoma koji su prošli kroz nehomogeno magnetsko polje, magnetski moment i spin imaju samo dva određena smjera u prostoru. Stern i Gerlach su koristili atom srebra koji je imao 47 elektrona od kojih je 23 imalo jednu vrstu spina, a preostalih 24 suprotnu vrstu spina. Iz razloga što se suprotni spinovi poništavaju, onaj jedan neupareni spin je odredio spin atoma te je prolaskom kroz magnetsko polje došlo do razdvajanja zrake na dva dijela. Spin elektrona je intrinzično svojstvo čestice koje se ne može protumačiti kao smjer okretanja nekakve strukture unutar čestice, na primjer ako se elektron zamisli kao lopta električnog naboja koja se rotira oke neke osi, uz pretpostavku da taj rotirajući naboj proizvodi magnetski moment. Iz visokoenergetskih pokusa raspršenja je poznato da je gornja granica ovog područja manja od 10^{-19} m te je gornja granica brzine rotacije, brzina svjetlosti (c = 299.792.458 m/s), jer nije dozvoljeno da bilo što ima veću brzinu od brzine svjetlosti. Čak i uz pretpostavku da se sav naboj nalazi unutar tankog prstena oko središta lopte, moment količine gibanja bi bio premali za eksperimentalno objašnjenje promatranog spina elektrona. Bilo koja druga

raspodjela bi dala još niže vrijednosti. Na spin se može gledati i na drugačiji način, jer on može ukazivati i na simetriju koju ima čestica. Čestica kojoj je spin 0, ponaša se kao točka, izgleda identično s koje god strane ju pogledali, dok na primjer karte za belot je potrebno zarotirati za 360° kako bi one ponovno izgledale jednako. Spin elektrona iznosi ± $\frac{1}{2}$ te mu je potrebna dvostruka potpuna rotacija (2 x 360° = 720°) kako bi se vratio u početno stanje. Ne postoji ništa u makroskopskom svijetu što ima takvu simetriju, a zdrav razum govori kako nešto takvo ne može postojati i da je to jednostavno nemoguće, ali je to ipak tako i postoji. Zapravo je vrlo lako napraviti laboratorijski pokus koji će demonstrirati da se elektroni ponašaju na ovaj čudan način: ako ih se okrene za 360°, oni neće biti u istom stanju u kojemu su bili nego u takozvanom negativnom (-) stanju i tek nakon još jedne rotacije od 360°, elektroni se vraćaju u početno stanje. Iako ljudski rod ne može niti zamisliti ovakvo ponašanje, to ne znači da ga ne može izračunati. [10][11]

$$S = \hbar\sqrt{s\,(s+\,1)} = \frac{\sqrt{3}}{2}\,\hbar \qquad , \qquad (3\text{-}5)$$

gdje je:

S ukupni moment količine gibanja spina

s kvantni broj koji određuje moment količine gibanja čestice, za elektron je $s = \pm \frac{1}{2}$ (ovisno o vrsti spina)

$\hbar = 1{,}054571726 \cdot 10^{-34}$ Js reducirana Planckova konstanta

U današnje vrijeme spin ima važnu ulogu i u teorijskim i u praktičnim primjenama. Dobro uspostavljena praktična upotreba spina uključuje:

-spektroskopiju nuklearne magnetske rezonance u kemiji

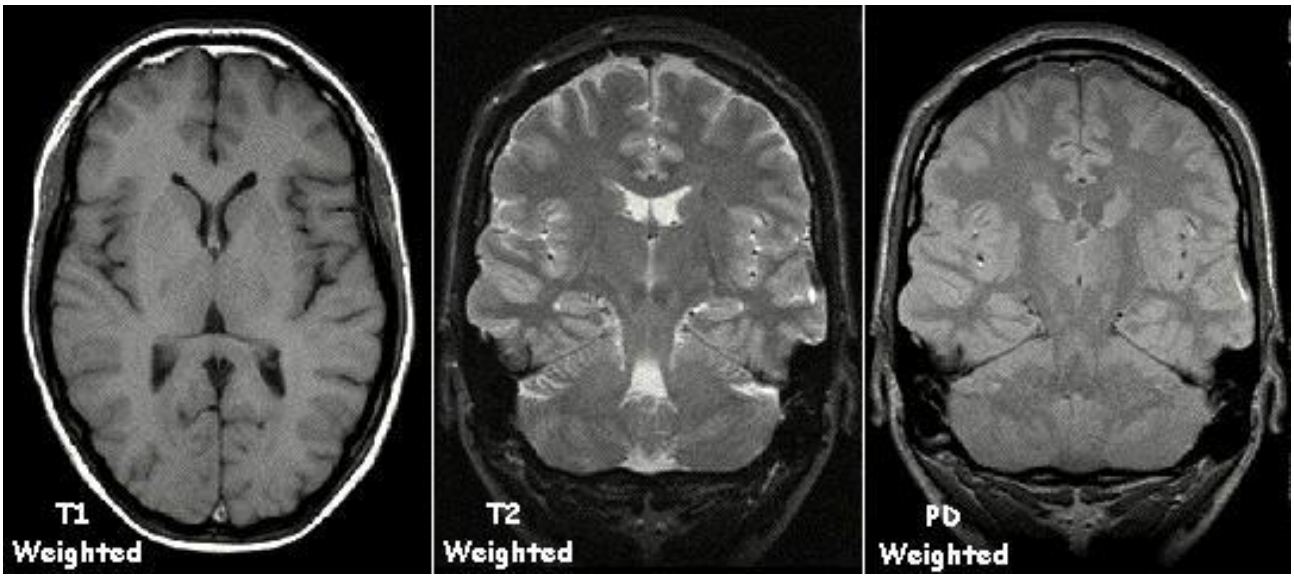
- spektroskopiju elektronske rezonance spina u kemiji i fizici

-magnetsku rezonancu u medicini, temelji se na gustoći protonskog spina

-ogromne magneto-otpore (GMR – *Giant magnetoresistance*) u tvrdim diskovima.

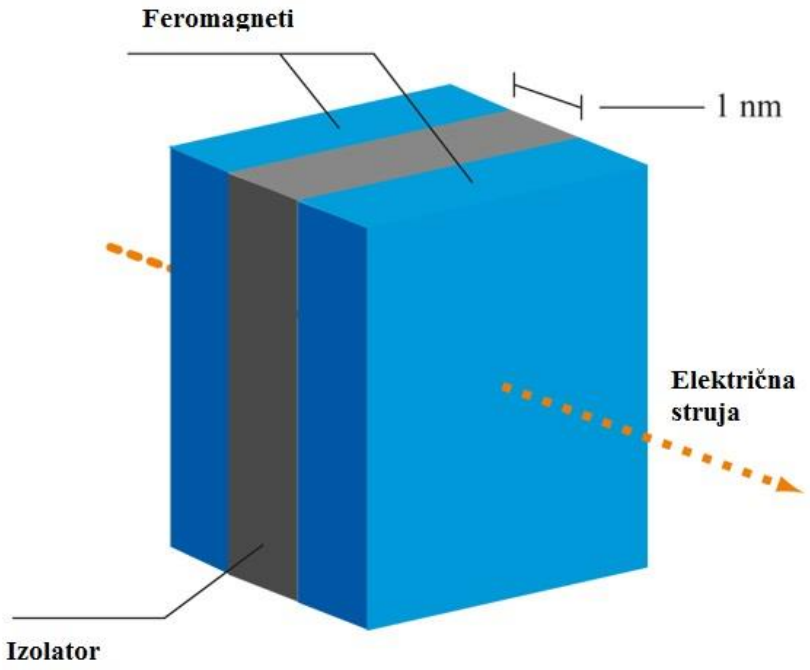
Nuklearna magnetska rezonanca je fizička pojava u kojoj jezgre u magnetskom polju apsorbiraju i ponovno isijavaju elektromagnetsko zračenje. Ta energija je na određenoj rezonantnoj

frekvenciji koja ovisi o jakosti magnetskog polja i o magnetskim svojstvima izotopa atoma, a u praktičnoj primjeni je ta frekvencija najsličnija televizijskim VHF (Very High Frequency) i UHF (Ultra High Frequency) frekvencijama emitiranja. VHF emitira na frekvencijama od 30 MHz do 300 MHz, a UHF emitira na frekvencijama od 300 MHz do 3 GHz. Spektroskopija elektronske rezonancije spina je tehnika proučavanja materijala sa neuparenim elektronima. Magnetska rezonanca je medicinska vizualizacijska tehnika koju koriste u radiologiji kako bi istražili anatomiju i fiziologiju tijela (zdravih i bolesnih ljudi). Uređaji za magnetsku rezonancu koriste jako magnetsko polje i radiovalove kako bi stvorili sliku tijela i organa. Koristi se u bolnicama za dijagnozu, prikaz i praćenje bolesti bez izlaganja ionizirajućem zračenju.



Slika 3.3.2.: Fotografija magnetske rezonance [27]

Slika prikazuje magnetsku rezonancu mozga koja je snimljena s tri strane.



Slika 3.3.3.: Ogromni magnetootpor (GMR – *Giant magnetoresistance*) [28]

Slika prikazuje magneto-otpor koji se koristi u računalima za tvrde diskove te je vrlo malih dimenzija (u nanometrima).

Magneto-otpori su kvantno-mehanički učinci primijećeni u strukturama tankih slojeva koje su sastavljene na način da se izmjenjuju feromagnetski i izolatorski slojevi. Spektroskopija je proučavanje međudjelovanja materije i izračene energije. Spoj spin – orbita (međudjelovanje spina čestice i njezinog kretanja) dovodi do dobro strukturiranog atomskog spektra koji se koristi u atomskim satovima i modernoj definiciji sekunde. [28]

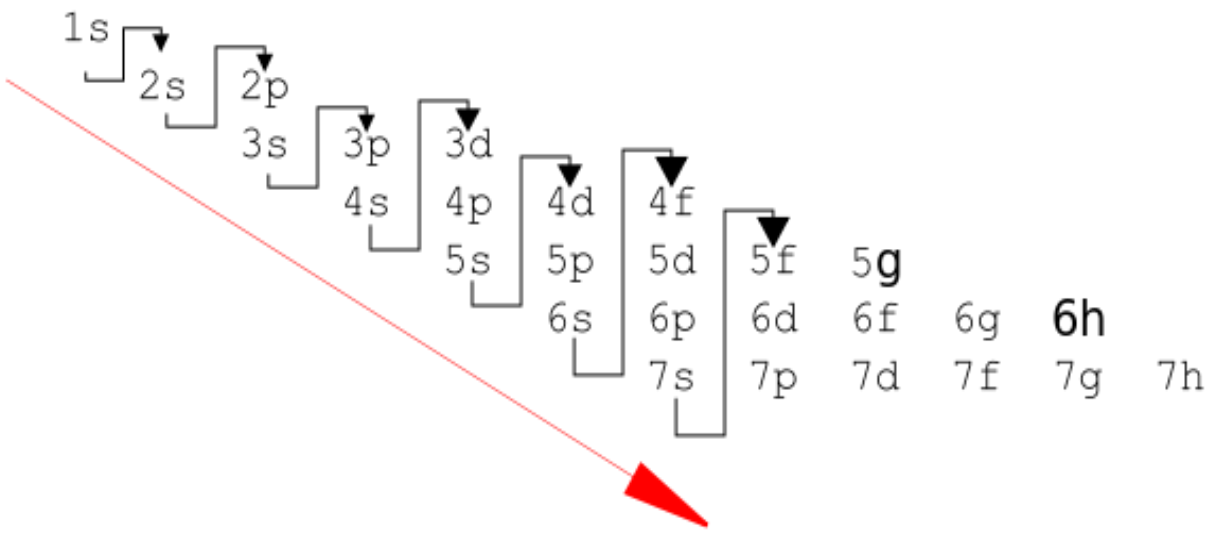
3.4 Kvantni brojevi

Kvantni broj opisuje specifično kvantno stanje bilo kojeg sustava u kvantnoj mehanici. Možda najvažniji aspekt kvantne mehanike je kvantizacija vidljivih količina, jer su kvantni brojevi diskretni skupovi cijelih brojeva ili polovice cijelih brojeva, a mogli bi dosegnuti i beskonačnost u nekim slučajevima, što se razlikuje od klasične mehanike, gdje se vrijednosti kreću kontinuirano. Kvantni brojevi često opisuju specifične razine energije elektrona u atomima, ali druge mogućnosti uključuju moment količine gibanja, spin, i tako dalje. Bilo koji kvantni sustav može imati jedan ili više kvantnih brojeva te je teško nabrojati sve moguće kvantne brojeve. Kvantni brojevi određuju

elektronsku konfiguraciju atoma. Elektronska konfiguracija atoma je raspored elektrona u atomu. Kvantni brojevi koji određuju elektronsku konfiguraciju su:

I) Glavni kvantni broj
II) Orbitalni kvantni broj
III) Magnetni kvantni orbitalni broj
IV) Spinski kvantni broj

Glavni kvantni broj opisuje elektronske ljuske ili razinu energije atoma. Može poprimiti vrijednosti n = 1, 2, 3, 4, 5, 6 i 7, a označava se s K, L, M, N, O, P i Q. Elektroni u vanjskoj ljuski imaju veću prosječnu energiju i udaljeniji su od jezgre od onih u unutarnjim ljuskama. Svaka ljuska se sastoji od jedne ili više podljuski, koje se i same sastoje od atomskih orbitala. Popunjavanje atomskih orbitala se vrši na način da se prvo popunjavaju energetski niži nivoi energije.



Slika 3.4.1.: Princip popunjavanja atomskih orbitala [28]

Slika prikazuje princip popunjavanja atomskih orbitala, počevši od najnižeg energetskog nivoa 1s pa nadalje.

Orbitalni kvantni broj opisuje moment količine gibanja u atomskim orbitalama i određuje njihov oblik te se označava s ℓ. Moment količine gibanja elektrona L je povezana s kvantnim brojem ℓ sljedećom jednadžbom:

$$L^2 \psi = \hbar^2 \ell (\ell + 1) \psi \quad , \quad (3\text{-}6)$$

gdje je:

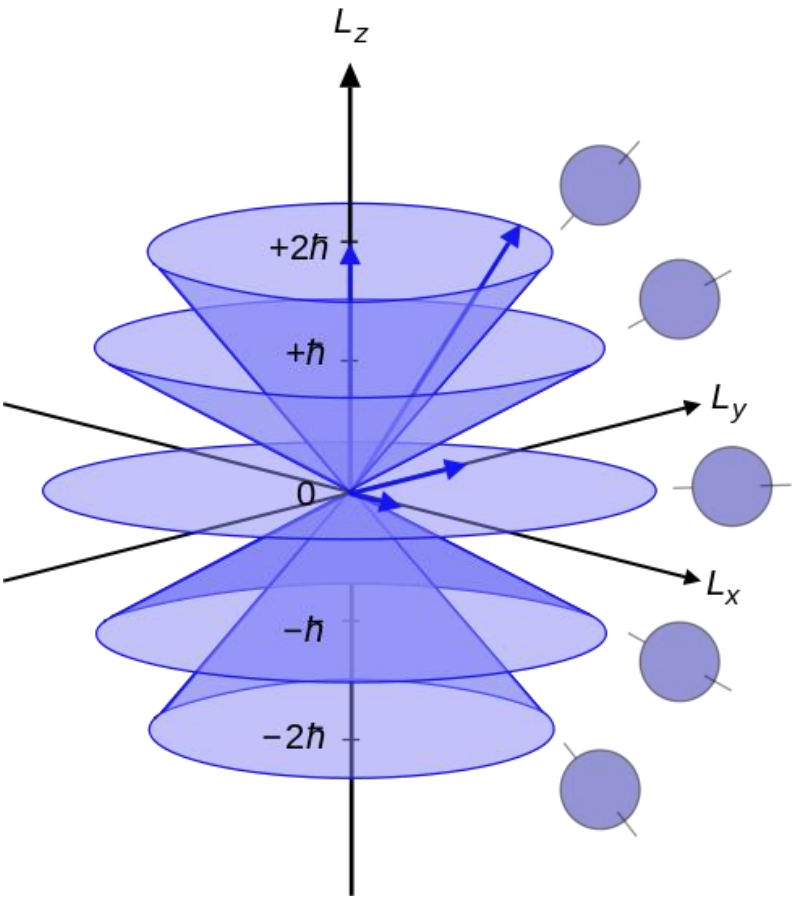
L^2 operator momenta količine gibanja orbitale

Ψ valna funkcija elektrona

$\hbar = 1{,}054571726 \cdot 10^{-34}$ Js reducirana Planckova konstanta

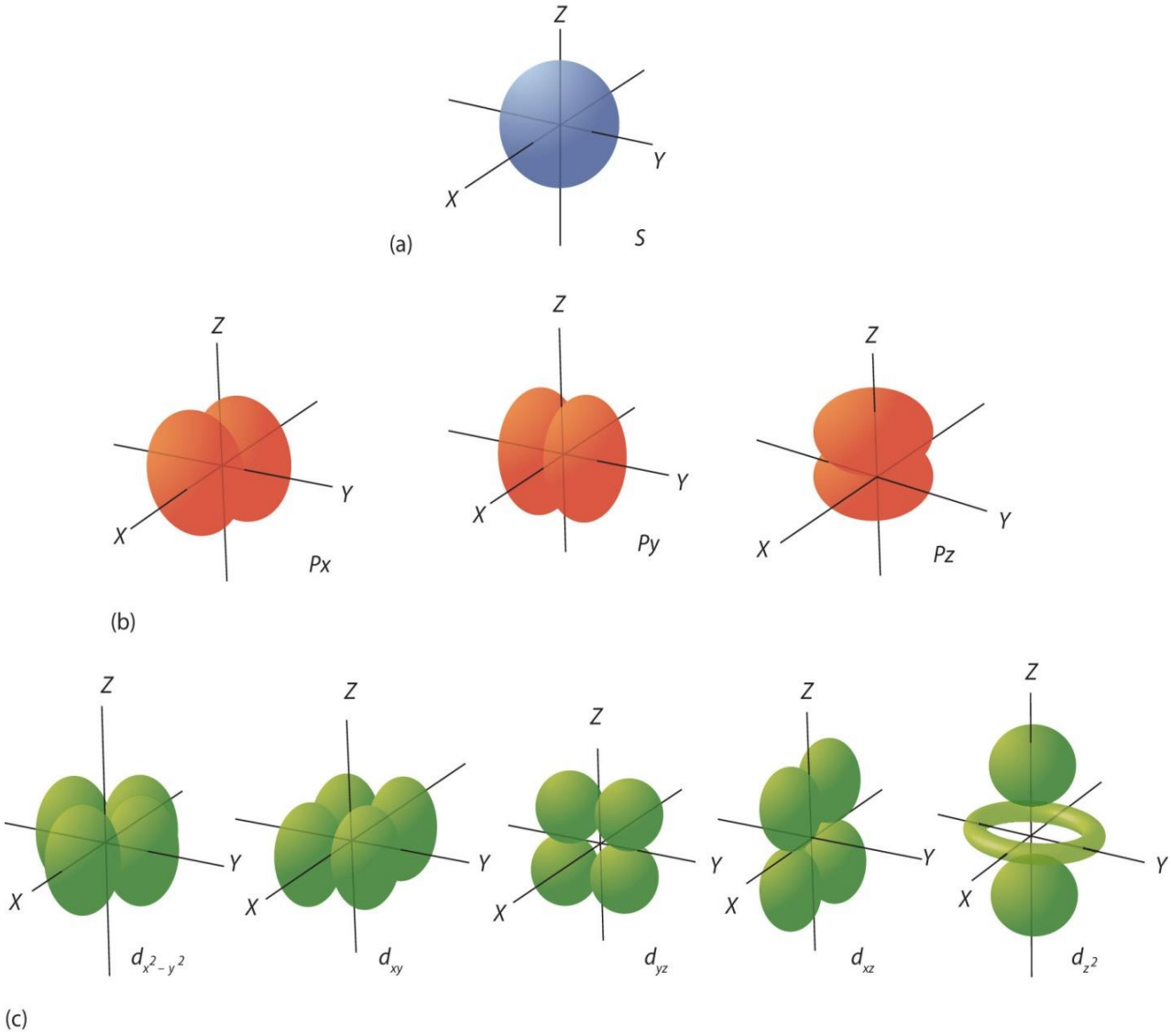
ℓ orbitalni kvantni broj.

Orbitalni kvantni broj ℓ je uvijek nenegativan cijeli broj (0, 1, 2, 3 i tako dalje). U kemiji i spektroskopiji se $\ell = 0$ naziva orbitala *s*, $\ell = 1$ orbitala p, $\ell = 2$ orbitala *d* i tako dalje.



Slika 3.4.2.: Orbitalni moment količine gibanja [30]

Slika prikazuje orbitalni moment količine gibanja u prvoj orbitali (orbitala *s*).



Slika 3.4.3.: Elektronske orbitale [31]

Slika prikazuje procjenu raspodjele elektrona u prostoru. Pod a) se radi o jednoj *s* orbitali i o sfernoj raspodjeli elektrona, pod b) se radi o tri *p* orbitale koje imaju raspodjelu poput bućice (utezi za vježbanje) i svaki je usmjeren u drugom smjeru i pod c) se radi o pet *d* orbitala u obliku koji podsjeća na ružu osim oblika d_z^2 koji je kombinacija oblika bućice i torusa i svaki od njih je usmjeren u drugom smjeru.

Magnetni kvantni orbitalni broj opisuje jedinstveno kvantno stanje elektrona i označava se slovom m. Magnetni kvantni orbitalni broj označava razinu energije koju sadrži podljuska i daje projekciju momenta količine gibanja duž određene osi.

$$L_Z = m_\ell \hbar \quad , \tag{3-7}$$

gdje je:

L_Z komponenta momenta količine gibanja u smjeru z osi

m_ℓ magnetni kvantni orbitalni broj

$\hbar = 1{,}054571726 \cdot 10^{-34}$ Js reducirana Planckova konstanta.

Magnetni kvantni orbitalni broj je svojstvena vrijednost i može poprimiti vrijednosti: $m_\ell = -\ell, -\ell + 1, \ldots, 0, \ell - 1, \ell$.

Tablica 3.4.1.: Veza između orbitalnog kvantnog broja ℓ i magnetskog kvantnog orbitalnog broja [32]

Veza između kvantnih brojeva		
Orbitala	Vrijednost	Broj vrijednosti za m_ℓ
s	$\ell = 0,\ m_\ell = 0$	1
p	$\ell = 1,\ m_\ell = -1, 0, 1$	3
d	$\ell = 2,\ m_\ell = -2, -1, 0, 1, 2$	5
f	$\ell = 3,\ m_\ell = -3, -2, -1, 0, 1, 2, 3$	7
g	$\ell = 4,\ m_\ell = -4, -3, -2, -1, 0, 1, 2, 3, 4$	9

Spinski kvantni broj opisuje spin (intrinzični moment količine gibanja) elektrona unutar orbitala i daje projekciju momenta količine gibanja spina duž određene osi:

$$S_Z = m_S \hbar \quad , \tag{3-8}$$

gdje je:

S_Z - ukupni moment količine gibanja spina u smjeru osi z

m_S - projekcija spinskog kvantnog broja i može poprimiti vrijednosti: $m_S = -s, -s + 1, -s + 2, \ldots, s-2, s - 1, s$.

s - spinski kvantni broj koji određuje moment količine gibanja čestice te je intrinzično svojstvo čestice.

$\hbar = 1{,}054571726 \cdot 10^{-34}$ Js reducirana Planckova konstanta.

Elektron ima spin $s = \pm \frac{1}{2}$ (ovisno o vrsti spina), pa slijedom toga će i m_S imati vrijednost $\pm \frac{1}{2}$. Svaki elektron u bilo kojoj pojedinačnoj orbitali mora imati drugačiji spin zbog Paulijevog principa isključenja. [33]

3.5 Postulati kvantne-mehanike

Postulat 1:

Stanje kvantnog sustava je u potpunosti određeno funkcijom ψ (r, t) koja ovisi o koordinatama čestice, r i vremenu t. Ta funkcija se naziva valnom funkcijom ili funkcijom stanja i ima svojstvo da je $\psi^*(r, t)\psi(r, t)d\tau$ vjerojatnost da se čestica nalazi u elementu volumena $d\tau$ nalazi u r u vremenu t. To je probabilistička interpretacija valne funkcije. Rezultat valne funkcije mora zadovoljiti uvjet da je vjerojatnost jednaka 1 da se čestica nalazi u prostoru te to daje uvjet normiranosti:

$$\int_{-\infty}^{+\infty} \psi^*(r,t)\,\psi(r,t)d\tau = 1 \quad (3\text{-}9)$$

Postulat 2:

Svakoj (opazivoj) dinamičkoj varijabli – opservabli – pripada odgovarajući linearni operator, hermitski operator.

Tablica 3.5.1.: Primjeri hermitskih operatora [7]

Opservabla	Klasična oznaka	Kvantni operator	Operacija
Položaj	r	$\hat{r}$	Množenje sa r
Impuls	p	$\hat{p}$	$-i\,\hbar\,(\hat{\imath}\,\frac{\partial}{\partial x} + \hat{\jmath}\,\frac{\partial}{\partial y} + \hat{k}\,\frac{\partial}{\partial z})$
Kinetička energija	T	$\hat{T}$	$\frac{-\hbar^2}{2m}(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2})$
Potencijalna energija	$V(r)$	$\hat{V}(r)$	Množenje s $V(r)$
Ukupna energija	E	$\mathcal{H}$	$\frac{-\hbar^2}{2m}(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}) + V(r)$

Moment količine gibanja	l_x	$\hat{l}_x$	$-i\,\hbar\,(y\,\frac{\partial}{\partial z} - z\,\frac{\partial}{\partial y})$
	l_y	$\hat{l}_y$	$-i\,\hbar\,(z\,\frac{\partial}{\partial x} - x\,\frac{\partial}{\partial z})$
	l_z	$\hat{l}_z$	$-i\,\hbar\,(x\,\frac{\partial}{\partial y} - \hat{\jmath}\,\frac{\partial}{\partial x})$

Postulat 3:

U bilo kojem mjerenju opservable povezane s operatorom $\hat{A}$, jedina vrijednost koja će se dobiti je svojstvena vrijednost, a, koja zadovoljava svojstvenu jednadžbu:

$$\hat{A}\,\psi = a\,\psi \qquad (3\text{-}10)$$

Ovo je postulat koji vrijednosti dinamičkih varijabli kvantizira u kvantnoj-mehanici (iako je moguće imati beskonačno mnogo svojstvenih vrijednosti u slučaju nevezanih stanja). Ako se sustav nalazi u svojstvenom stanju $\hat{A}$, sa svojstvenom vrijednošću a, tada bilo koje mjerenje A će dati svojstvenu vrijednost a. Iako će mjerenja uvijek dati svojstvenu vrijednost a, početno stanje ne mora biti početno stanje od $\hat{A}$. Proizvoljno stanje se može proširiti u potpuni skup svojstvenih vektora $\hat{A}$, iz $\hat{A}\,\psi_i = a_i\,\psi_i$, kao:

$$\psi = \sum_i^n c_i\,\psi_i \quad (3\text{-}11)$$

gdje n može ići do beskonačnosti. U tom slučaju će mjerenje A, dati jednu od svojstvenih vrijednosti a_i, ali se neće znati koju. Vjerojatnost promatranja svojstvene vrijednosti a je dana kvadratom apsolutne vrijednosti koeficijenta $|c_i|^2$. Treći postulat također podrazumijeva da će se nakon mjerenja ψ, opet dobiti neka vrijednost a_i, pa će valna funkcija prijeći u svojstveno stanje ψ_i koje odgovara a_i. Ako se a_i nalazi u stanju opadanja, tada će ψ prijeći u degenerirani podprostor.

Postulat 4:

Ako se sustav nalazi u stanju opisanom normiranom valnom funkcijom ψ, tada će prosječna vrijednost opservable odgovarati $\hat{A}$ prema:

$$\langle\hat{A}\rangle = \int_{-\infty}^{+\infty} \psi^*\,\hat{A}\,\psi\,d\tau \qquad (3\text{-}12)$$

Postulat 5:

Vremenski razvoj kvantnog stanja dan je Schrödingerovom jednadžbom prema (3-4).

Postulat 6:

Ukupna valna funkcija mora biti antisimetrična s obzirom na razmjenu svih koordinata jednog fermiona s onima od drugog. Elektronski spin mora biti uključen u tu skupinu koordinata. Paulijev princip isključenja je rezultat ovog antisimetričnog postulata. [7]

4. Pretvaranje komunikacija iz klasičnih u kvantne

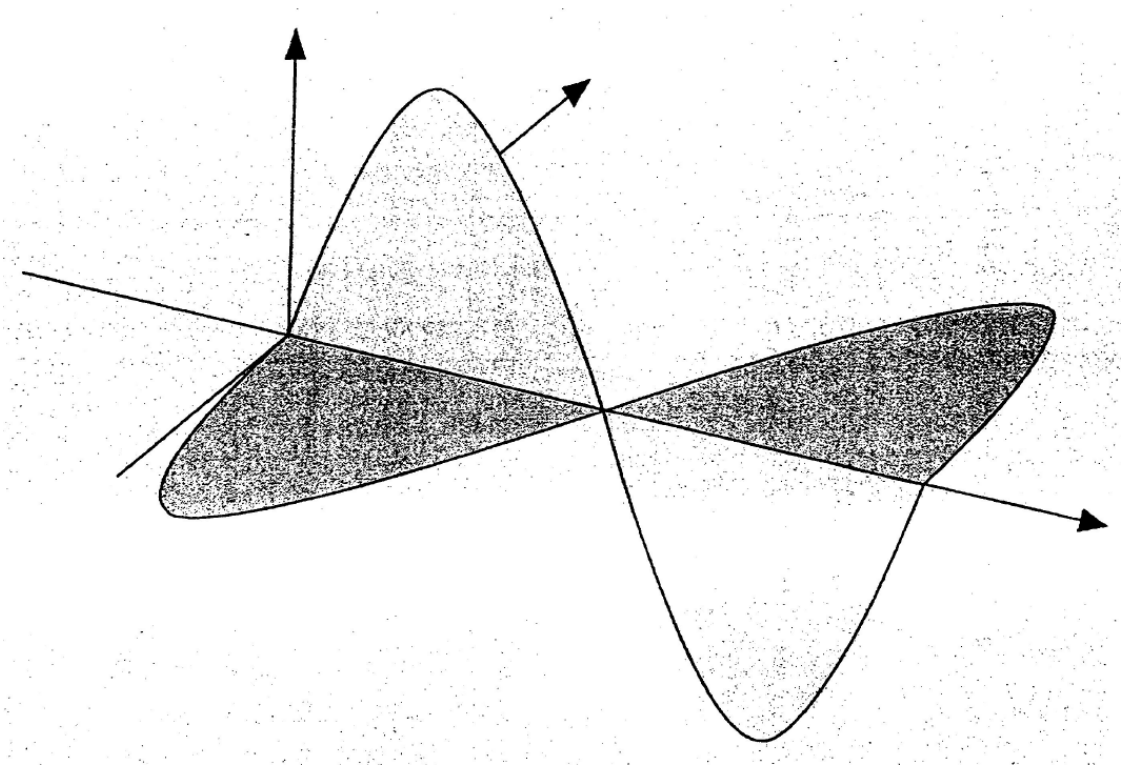
Ponašanje elementarnih čestica, a prema tome i svakog komunikacijskog ili računalnog uređaja napravljenog od njih podliježe specijalnim pravilima, postulatima kvantne-mehanike. U kvantnom svijetu, postulati imaju analogiju sa Euklidovom geometrijom. Umjesto korištenja teoretske fizike za objašnjavanje postulata, ovdje će biti objašnjeni uz pomoć imaginarnih primjera, koji bi mogli biti korisniji za razumijevanje kvantnih komunikacija sa inženjerskog gledišta. Za početak će biti uvedena tri lika: Ana, Branko i Iva. Oni će slati, primati i prisluškivati informacije prema trenutnom scenariju. Započet će se s razlikama između klasične i kvantne prirode svjetlosti. Klasična svjetlost pripada lozi elektromagnetskih valova koja ima posebno svojstvo karakterizirano s polarizacijom. Polarizacija je orijentacija oscilacija u ravnini okomitoj na smjer širenja vala. Premda se kvantno-mehanička svjetlost ponaša kao grupa elementarnih čestica (nazvanih fotoni), to održava svojstvo polarizacije, ali se polarizacija pokorava postulatima kvantne-mehanike, kao što će se vidjeti u nastavku.

Prvi korak: najjednostavnije klasično rješenje:

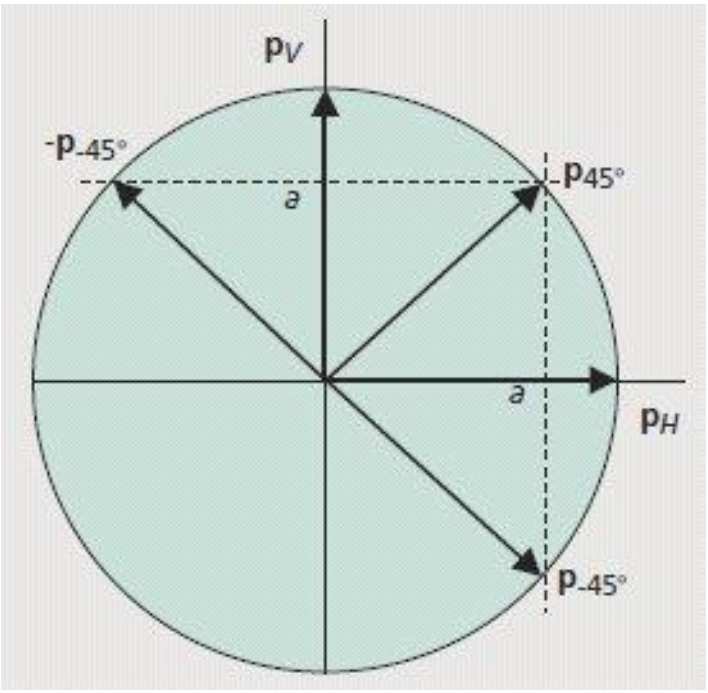
Započet će se s najjednostavnijim primjerom komunikacije koji prelazi granicu između klasične i kvantne metode komunikacije. Ana želi poslati nekoliko bita informacija Branku preko optičkog vlakna. U klasičnom slučaju ona može lako šifrirati informacije: za logičku jedinicu, ona emitira svjetlost na određenoj valnoj duljini (to jest u određenom vremenskom periodu šalje eksploziju fotona), dok za logičku nulu ne šalje ništa. U današnje vrijeme postoji mogućnosti proizvesti i detektirati jedan jedini foton; dakle Ana može iskoristiti jedan foton za dostavljanje jednog bita informacija.

Drugi korak: prelazak klasično/kvantne granice

Ana je iskoristila svojstvo položaja u prvom koraku (to jest je li ili nije određeni foton smješten u određenom vremenskom periodu). Sada koristi drugo svojstvo, polarizaciju, za šifriranje podataka.



Slika 4.1.: Horizontalna i vertikalna polarizacija svjetla [1]



Slika 4.2.: Polarizacija fotona [1]

Na slici 4.1. prikazana je horizontalna i vertikalna polarizacija svjetla, a na slici 4.2. je dan odgovarajući vektorski prikaz fotona, gdje je vertikalna polarizacija označena sa $\boldsymbol{p}_V$, a horizontalna polarizacija sa vektorom $\boldsymbol{p}_H$ u ravnini okomitoj na smjer širenja.

Ana je odabrala da će logička jedinica biti prikazana vertikalno polariziranim fotonima, a logička nula sa horizontalno polariziranim fotonima. Koristeći detektor polarizacije fotona, Ana šalje informacije Branku. Prijemnik na Brankovoj strani može lako dešifrirati logičke vrijednosti fotona koje prima na način da odredi njihovu polarizaciju. Ana i Branko još uvijek komuniciraju na klasičan način.

Treći korak: potpuno kvantno djelovanje

Ana zna da svjetlost može biti polarizirana ne samo na 0° i 90°, nego na bilo kojem kutu. Ona priprema foton sa polarizacijom od 45°, prikazan na slici 4.2., kao $\boldsymbol{p}_{45^\circ}$ i onda ga šalje Branku. Brankov detektor fotona je u mogućnosti odlučiti je li Ana poslala horizontalno ili vertikalno polarizirani foton (to jest jedino su ortogonalni kutovi dopušteni, nije moguće detektirati bilo koji kut između njih). Zato što je vektor $\boldsymbol{p}_{45^\circ}$ jednako udaljen i od $\boldsymbol{p}_H$ i od $\boldsymbol{p}_V$, tada projekcija vektora $\boldsymbol{p}_{45^\circ}$ na osi $\boldsymbol{p}_H$ i $\boldsymbol{p}_V$ ima istu veličinu a (slika 4.2.), pa se tada može opisati kao linearna kombinacija $\boldsymbol{p}_H$ i $\boldsymbol{p}_V$:

$$\boldsymbol{p}_{45^\circ} = a\boldsymbol{p}_V + a\boldsymbol{p}_H \quad , \tag{4-1}$$

gdje je:

$\boldsymbol{p}_{45^\circ}$ foton sa polarizacijom od 45°

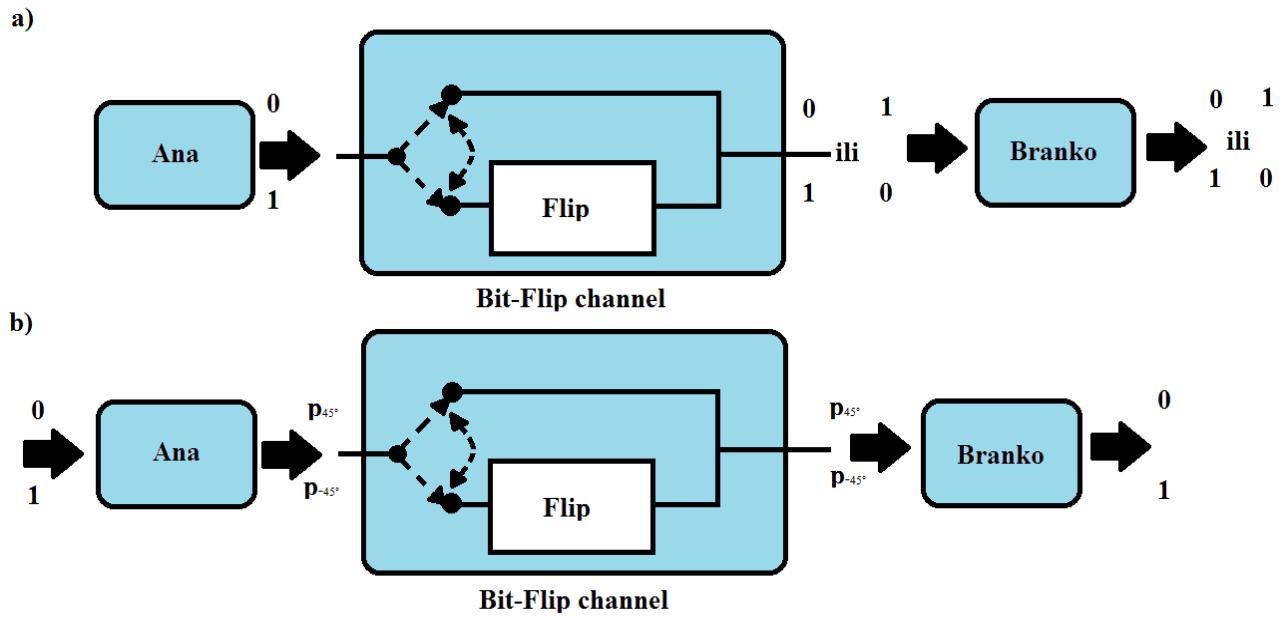
$\boldsymbol{p}_V$ vertikalna polarizacija

$\boldsymbol{p}_H$ horizontalna polarizacija

a udaljenost $\boldsymbol{p}_{45^\circ}$ od $\boldsymbol{p}_V$ i $\boldsymbol{p}_H$.

Ako Ana pošalje nekoliko fotona, sve njih s polarizacijom $\boldsymbol{p}_{45^\circ}$, Brankov prijemnik će odgovoriti logičkom nulom u pola slučajeva, a logičkom jedinicom u drugoj polovici slučajeva i to će učiniti slučajno. Dakle u klasičnom smislu, niti jedna informacija nije poslana od Ane za Branka. Ova slučajnost je unikatna kvantna odlika koja naglašava neodređenost kvantne-mehanike. Foton koji

ima polarizaciju $\boldsymbol{p}_{45^\circ}$ nosi obje moguće logičke vrijednosti, 0 i 1 u isto vrijeme. Sada je ta pojava potpuno kvantna. Potrebno je uočiti: iako su prikazi jednog qubita stanja i *M*-terostruke modulacije na slici 4.2. isti, među njima postoje značajne razlike. *M*-terostruka modulacija je prikazana pomoću kompleksnog koordinatnog sustava, gdje je svaka konstelacijska točka prikazana uz pomoć jednog kompleksnog broja: osi prikazuju realni i imaginarni dio (u fazi i kvadraturnoj fazi). Udaljenost konstelacijske točke od koordinatnog ishodišta (duljina vektora) može biti proizvoljna jer je povezana sa snagom signala. Prema tome klasični prikaz *M*-terostruke modulacije ima dva parametra (realni i imaginarni dio) sa proizvoljnim veličinama. U suprotnom, kvantna konstelacijska točka na slici 4.2. se sastoji od dva kompleksna broja, to jest tada postoji 2 x 2 = 4 parametara. (Dva imaginarna dijela na slici 4.2. imaju iznos nula, kako bi se lakše prikazalo vektore). Štoviše, postoji uvjet da su dozvoljeni samo jedinični vektori. Na kraju, ako se poveća broj bita/qubita, *M*-terostruki oblik ostaje dvodimenzionalan, dok svaki novi qubit udvostručava broj parametara. Ovaj slučajno-generirani protokol može biti koristan za komunikacije, ali je prvo potrebno uvesti svakodnevnu analogiju ovog komunikacijskog sustava - novčić – kako bi se pojednostavio opis ponašanja ovog protokola u kvantnoj domeni. Na taj si način i laik može modelirati i prikazati eksperimente.



Slika 4.3.: Bit-Flip kanal [1]

Slika 4.3. prikazuje dvije vrste komunikacije, u prvom slučaju (pod a) se radi o klasičnoj komunikaciji, a u drugom slučaju (pod b) o kvantnoj komunikaciji između Ane i Branka uz pomoć prekidača koji bira model kanala. Prekidač može odabrati gornji put koji je „prečica“ ili „žica“ koja prenosi nepromijenjene ulazne podatke; dok donji put negira (obrće) ulazne podatke: 0 → 1.

Koristeći analogiju novčića, opisani komunikacijski protokol tada se ponaša na sljedeći način:

Prvi korak: Najjednostavnije klasično rješenje: Ako Ana želi poslati jedinicu, daje novčić Branku u određenom vremenskom periodu, a u drugom slučaju, kako bi poslala nulu, ona ne daje Branku ništa.

Drugi korak: Prelazak klasično/kvantne granice: Dvostrani novčić, koji ima pismo i glavu koji predstavljaju logičku jedinicu i logičku nulu, može se smatrati klasičnim imitatorom bita. Ako je okrenuta glava, tada je postavljena vrijednost bita 0, a ako je okrenuto pismo, tada je vrijednost bita 1. Ana okreće stranu novčića kako bi komunicirala željeni bit. Tada ga ona predaje Branku, koji odlučuje koji je bit poslan, tako što promatra je li okrenuta glava ili pismo sa svojim prijemnikom (prijemnik su njegove oči).

Treći korak: Potpuno kvantno djelovanje: Potrebno je promotriti slučaj u kojemu su Ana i Branko povezani jednostavnim kanalom, ali kanalom koji ima šum, prikazan u sredini na slici 4.3. pod a. Model kanala koji ima šum se sastoji od prekidača koji povezuje ulaz kanala na gornji ili donji put modela kanala. Gornji put je „prečica“ ili „žica“ koja prenosi nepromijenjene ulazne podatke; dok donji put negira (obrće) ulazne podatke: 0 → 1. Oba puta, gornji i donji su sami po sebi deterministički. Ako je prekidač trajno postavljen na gornji put (žicu), Branko ne bi morao učiniti ništa kako bi primio poslane podatke ispravno. U suprotnom, ako bi prekidač trajno bio postavljen na donji put, tada bi Branko morao koristiti još jednom negiranje podataka, kako bi mogao primiti ispravno poslane podatke. Kako god, u ovom modelu kanala koji ima šum, prekidač bi slučajnim odabirom (sa vjerojatnošću $\frac{1}{2}$) prebacivao između gornjeg i donjeg puta (to jest, tako se uvodi šum). Zbog ovog slučajnog odabira, Branko ne zna koji je put odabran za određeni bit; stoga Branko ne može napraviti klasični prijemnik koji će biti u mogućnosti istovremeno primljene bitove identificirati i obrtati (0 → 1 i obrnuto). Zbog toga Branko promatra slučajni šum i ne može odrediti što je Ana zapravo poslala.

U nastavku je objašnjeno kako se kvantne operacije mogu iskoristiti za kanale bez šuma. Za početak je potrebno vratiti se objašnjenju pomoću novčića. Iva se nalazi između Ane i Branka te je njena uloga biti model kanala sa šumom. Slično kao u drugom koraku, Ana priprema njezin novčić na način da prema gore okrene glavu (0) ili pismo (1) i predaje ga Ivi. Slučajnim odabirom sa vjerojatnošću $\frac{1}{2}$, Iva ili ostavlja novčić netaknut, ili ga okreće (mijenja stranu koja je okrenuta prema gore) i predaje novčić Branku. Kao i prije, Branko ne može biti siguran koji je podatak (0 ili 1) poslala Ana, zbog Ivine slučajne operacije okretanja novčića. Kako bi popravili komunikaciju, Ana diže novčić u zrak te ga okreće u smjeru kazaljke na satu ako šalje nulu (0), a u smjeru obrnutom od smjera kazaljke na satu ako šalje jedinicu (1). Iva - kanal - prihvaća novčić te ga ponovno uz slučajan odabir ostavlja netaknutim ili ga okreće. Međutim, Iva neće promijeniti smjer rotacije te novčić diže u zrak i zakreće ga u istom smjeru u kojem je novčić i dobila od Ane. Kako bi detektirao informaciju koja je šifrirana u novčiću koji je podignut u zrak, Branko kreira prijemnik koji razlikuje dva moguća smjera rotacije koji šifriraju nulu (0) i jedinicu (1), (na primjer web kameru koja može usporiti snimljeni video novčića, kako bi Branko mogao razlikovati smjer rotacije). Pošto Ivina slučajna operacija okretanja novčića ne mijenja smjer vrtnje, Branko će primiti informaciju od Ane bez greške. Osim toga, Ana i Branko nisu primijenili nikakvu redundanciju te je provedeno ispravljanje pogreške bez dodatnih novčića (bita). Prije spomenuta kvantno-mehanička svojstva, koja nemaju analogije u klasičnoj teoriji komunikacija, su iskorištena na slici 4.3.. Ne postoji klasičan kod za ispravljanje grešaka koji može nadvladati p = 0,5 modela kanala sa šumom. Redundancija ne pomaže. Koristeći kvantno šifriranje moguće je prilagoditi ulazne vrijednosti na način da će biti nepromjenjivi u smislu kanala. Sada se prelazi na originalni treći korak gdje Ana i Branko komuniciraju koristeći polarizirane fotone. U tom slučaju se došlo do zaključka da će slanje fotona $\boldsymbol{p}_{45^\circ}$ rezultirati različitim slučajnim rješenjima kod Branka. Uz pretpostavku da je Ana povezana s Brankom preko kvantnog bit-flip kanala koji slučajnim odabirom ili ostavlja polarizaciju fotona netaknutu ili promijeni koeficijente svake komponente polarizacije fotona koje predstavljaju logičke vrijednosti (0 → 1). Ako je originalni foton:

$$\boldsymbol{p} = a\boldsymbol{p}_V + b\boldsymbol{p}_H \quad , \tag{4-2}$$

gdje je:

$\boldsymbol{p}$ foton sa nekom polarizacijom

$\boldsymbol{p}_V$ vertikalna polarizacija

$\boldsymbol{p}_H$ horizontalna polarizacija

a udaljenost $\boldsymbol{p}$ od $\boldsymbol{p}_V$

b udaljenost $\boldsymbol{p}$ od $\boldsymbol{p}_H$.

Bit-flip kanal originalni foton ili ostavlja netaknutim, ili zamijeni koeficijente a i b:

$$\boldsymbol{p} = b\boldsymbol{p}_V + a\boldsymbol{p}_H \tag{4-3}$$

Matematički se to može zapisati i na drugačiji način, koristeći Paulijev-*X* operator:

$$exch(\boldsymbol{p})\ b\boldsymbol{p}_V + a\boldsymbol{p}_H \quad , \tag{4-4}$$

gdje je:

exch(·) operator zamjene.

Prema primjeru s novčićem, Ana šifrira klasične vrijednosti 0 i 1 u fotone $\boldsymbol{p}_{45^\circ}$ i $\boldsymbol{p}_{-45^\circ}$. Novčić bačen u zrak svojom rotacijom oponaša kvantni bit (kasnije će se vidjeti koja je razlika između rotirajućeg novčića i fotona $\boldsymbol{p}_{45^\circ}$). Novčić sadrži i pismo i glavu pri rotaciji, slično kao i $\boldsymbol{p}_{45^\circ}$ koji sadrži polarizaciju $\boldsymbol{p}_V$ i $\boldsymbol{p}_H$ u jednakoj linearnoj kombinaciji:

$$\boldsymbol{p}_{45^\circ} = a\boldsymbol{p}_V + b\boldsymbol{p}_H \quad , \tag{4-5}$$

gdje je:

$\boldsymbol{p}_{45^\circ}$ foton sa polarizacijom od 45°

$\boldsymbol{p}_V$ vertikalna polarizacija

$\boldsymbol{p}_H$ horizontalna polarizacija

a udaljenost $\boldsymbol{p}_{45^\circ}$ od $\boldsymbol{p}_V$

b udaljenost $\boldsymbol{p}_{45^\circ}$ od $\boldsymbol{p}_H$.

Sljedeće što je potrebno istražiti je utjecaj kvantnog bit-flip kanala na poslane fotone pomoću slike 4.3.. Kanal može napraviti dvije stvari, prva je da pusti ulazni foton $\boldsymbol{p}_{in} = \boldsymbol{p}_{45^\circ}$ bez ikakvih izmjena

$\boldsymbol{p}_{out} = \boldsymbol{p}_{in} = \boldsymbol{p}_{45°}$, a druga mogućnost je da zamjeni koeficijente od $\boldsymbol{p}_V$ i $\boldsymbol{p}_H$: $a\boldsymbol{p}_V + a\boldsymbol{p}_H \rightarrow a\boldsymbol{p}_H + a\boldsymbol{p}_V \equiv a\boldsymbol{p}_H + a\boldsymbol{p}_V$. Zbog toga što su težinski koeficijent jednaki, polarizacija fotona ostaje nepromijenjena: $\boldsymbol{p}_{out} = a\boldsymbol{p}_H + a\boldsymbol{p}_V = \boldsymbol{p}_{45°}$.

U slučaju kada je foton $\boldsymbol{p}_{in} = \boldsymbol{p}_{-45°} = -a\boldsymbol{p}_V + a\boldsymbol{p}_H$, kanal opet radi identičnu transformaciju:

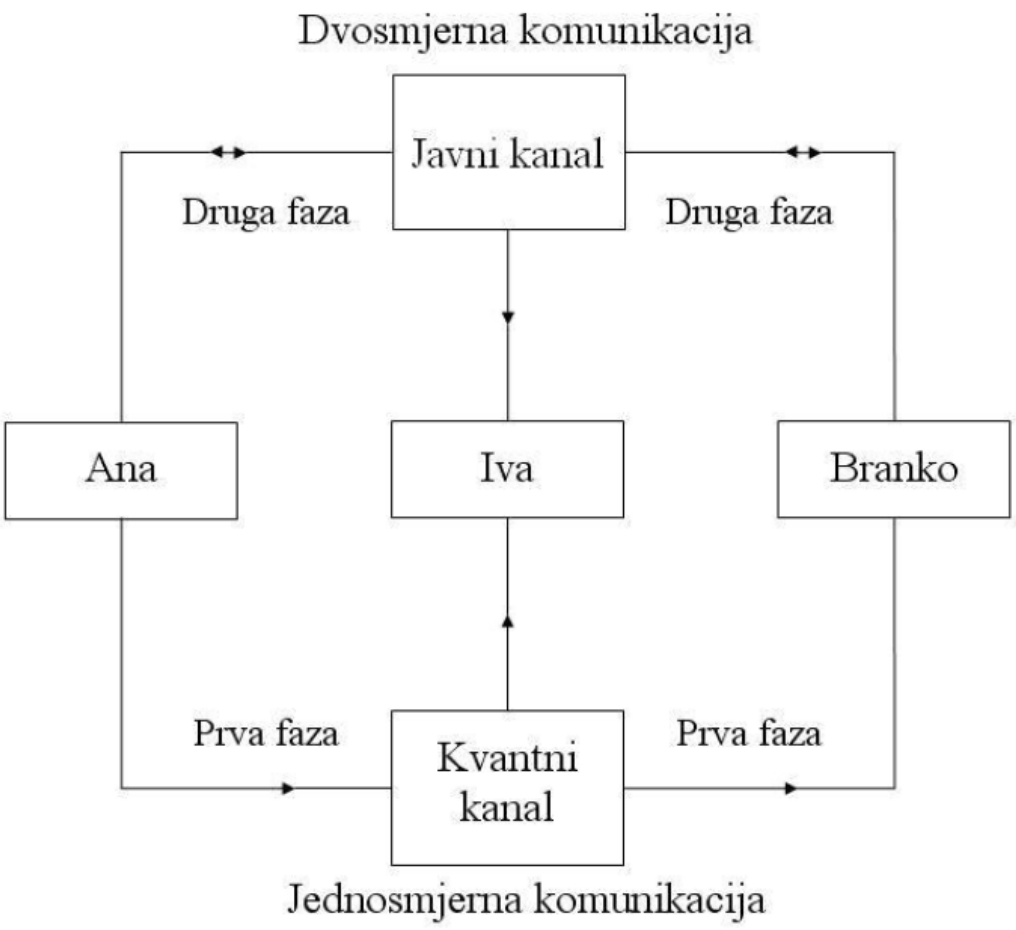
$\boldsymbol{p}_{out} = \boldsymbol{p}_{in} = \boldsymbol{p}_{-45°}$ ili modificira foton: $\boldsymbol{p}_{out} = -a\boldsymbol{p}_H + a\boldsymbol{p}_V = -(-a\boldsymbol{p}_V + a\boldsymbol{p}_H) = -\boldsymbol{p}_{-45°}$.

Sada Branko primjenjuje detektor polarizacije prilagođen na $\pm\boldsymbol{p}_{45°}$. Ovaj uređaj razlikuje fotone prema njihovim kutovima polarizacije te ignorira znak vektora polarizacije. Dakle, detektor će pokazati 0 Branku, ako je primljen foton $\boldsymbol{p}_{45°}$ te 1 za svaki foton $\pm\boldsymbol{p}_{-45°}$. S obzirom da kanal sada ne radi promjene polarizacijskog kuta poslanog fotona, Branko dešifrira informaciju bez pogreške; ova klasično-kvantna metoda šifriranja omogućava realizaciju kanala bez šuma. [1]

4.1 Kvantna kriptografija

Svrha kriptografije je prijenos informacija na način da su one dostupne samo osobi kojoj su i poslane. Na početku je sigurnost šifriranog teksta ovisila isključivo o tajnosti cijelog procesa šifriranja i dešifriranja, a danas se koriste šifre čiji su algoritmi javno poznati, a da to ne ugrožava sigurnost šifrirane poruke. U takvim sustavima tajni ključ poruke i jasni tekst se unose kao parametri u algoritam. Ako se želi koristiti savršeno siguran kriptografski sustav, onda je odgovor Vernamova šifra, poznatija pod imenom jednokratna bilježnica. Jednokratna bilježnica koristi slučajno generirani ključ $\boldsymbol{K}$ jednake duljine kao i poruka koja se želi šifrirati. Glavni problem kod takvog sustava je potreba za razmjenom tajnog ključa između pošiljatelja i primatelja poruke (Ana i Branko). U većini slučajeva, ključ $\boldsymbol{K}$ je predugačak i time ga je nepraktično i preskupo slati sigurnim kanalom. Danas se u većini praktičnih kripto-sustava, koristi ključ $\boldsymbol{K}$ koji je konstantne veličine i obično je puno kraći od duljine jasnog teksta te je rezultat toga da kripto-sustavi više nisu savršeno sigurni. Praktično siguran kripto-sustav znači da napadač (Iva) može teoretski dešifrirati poruku bez znanja ključa, ali ona to vjerojatno neće uspjeti, iz razloga što ona nema dovoljno veliku procesorsku snagu, ali ni vrijeme potrebno za napad. Slaba točka klasičnih kriptografskih sustava je ta da se sigurna komunikacija može odvijati tek od trenutka kada je ključ sigurno razmijenjen komunikacijskim kanalom. Taj problem se naziva „kvaka 22“ kriptografije. Osim toga, ako Ana i Branko nekako i uspiju razmijeniti ključ preko sigurnog komunikacijskog kanala, ne postoji mehanizam u klasičnoj kriptografiji koji može garantirati da je ključ poslan sigurno, to jest da ga Iva

nije uspjela prisluškivanjem komunikacijskog kanala saznati. Klasična kriptografija nema rješenja za taj problem, ali kvantna kriptografija ima. Kvantna kriptografija vrši kvantnu razmjenu ključeva, koja omogućuje i Ani i Branku komunikaciju koja je u potpunosti sigurna. Kvantna kriptografija koristi prirodnu neodređenost kvantnog svijeta. Pomoću nje se može uspostaviti komunikacijski kanal koji nije moguće prisluškivati bez ometanja prijenosa, to jest dva korisnika koja međusobno komuniciraju mogu otkriti prisustvo treće strane koja pokušava saznati ključ. Također, osoba koja prisluškuje ne može kopirati nepoznate kvantne bitove - qubite, to jest nepoznata kvantna stanja, zbog teorema o nekloniranju koji su prvi iskazali Wooters i Zureck. Kvantna kriptografija služi samo za dobivanje i distribuciju ključa, a ne za prijenos poruka. Tako generirani ključ može poslužiti u nekom kripto-sustavu za šifriranje i dešifriranje poruke. Kvantna mehanika kaže da se čestice ne nalaze na samo jednom mjestu. One se nalaze na nekoliko mjesta odjednom, s određenim vjerojatnostima da postoje na različitim mjestima. Kad se čestica i uhvati njoj nije moguće istovremeno izmjeriti sve njene fizikalne veličine. Mjerenjem neke od veličina čestice, uništava se svaka mogućnost mjerenja nekog drugog njenog svojstva. Ta neodređenost se može iskoristiti za generiranje tajnog ključa. Dok putuju, fotoni titraju pod nekim kutom. Kada velika grupa fotona titra u istom smjeru tada su oni polarizirani. Polarizacijski filtri propuštaju samo one fotone koji su polarizirani u određenom smjeru dok su ostali blokirani. Kvantna komunikacija uključuje kodiranje informacija u kvantna stanja, ili qubite, nasuprot klasičnoj kriptografiji koja koristi bitove. Korištenjem kvantne superpozicije ili kvantnog sprezanja te šaljući informacije u kvantnim stanjima može se implementirati komunikacijski sustav koji otkriva napadača. Kvantna kriptografija iskorištava svojstva kvantnih stanja kako bi osigurala sigurnost sustava. Postoji nekoliko pristupa u distribuciji kvantnih ključeva, ali se općenito mogu podijeliti u dvije skupine, u ovisnosti jesu li qubitovi nezavisni jedni o drugima ili nisu. [14][34][35][36]



Slika 4.1.1: Prikaz kvantnog komunikacijskog kanala [34]

Slika 4.1.1. prikazuje kvantni komunikacijski kanal. Ana i Branko prvo komuniciraju preko kvantnog kanala i razmjenjuju ključ ***K***, a zatim komuniciraju preko javnog kanala i razmjenjuju informacije koje Iva ne može prisluškivati, jer na taj način ometa komunikaciju i biva otkrivena.

4.1.1 Kvantni protokoli

i) Protokol „pripremi i izmjeri“

Čin mjerenja je sastavni dio kvantne mehanike. Generalno govoreći, mjerenje nepoznatog kvantnog stanja će promijeniti to stanje. To je poznato pod imenom kvantna neodređenost i počiva na rezultatima Heisebergovog principa neodređenosti te teorema o nekloniranju. To se može iskoristiti kako bi se detektirali pokušaji prisluškivanja komunikacijskog kanala te, važnije, da bi se izračunala količina informacija koja je presretnuta. [14][34]

ii) Protokoli zasnovani na sprezanju

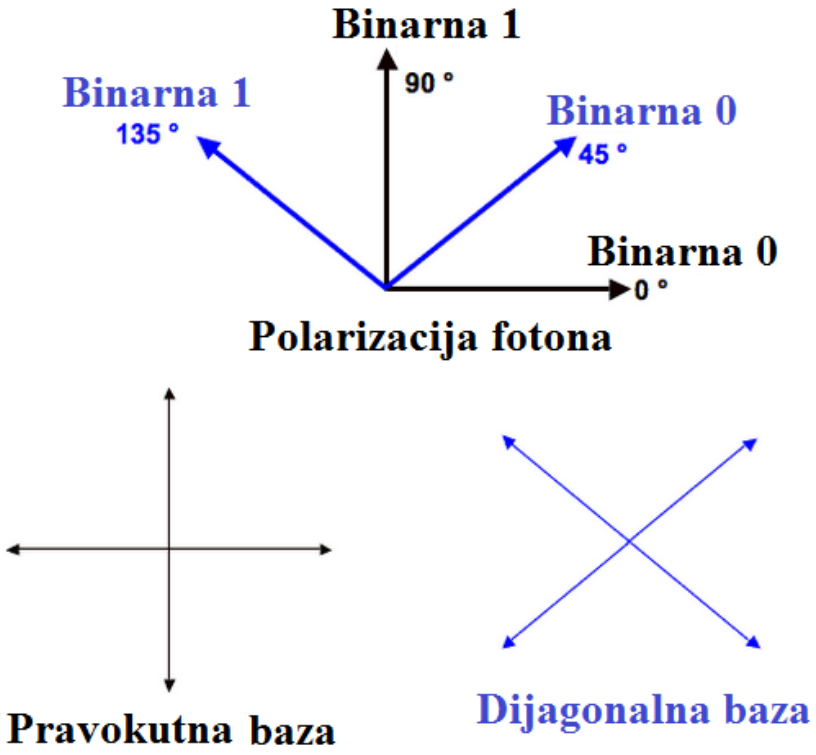
Kvantna stanja dva ili više odvojena objekta mogu postati povezana tako da se opišu kombiniranim kvantnim stanjem, a ne kao individualni objekti. To znači da će provođenje mjerenja na jednom objektu utjecati na drugi objekt. Ako se spregnuti par objekata pošalje komunikacijskim kanalom, pokušaj presretanja bilo koje čestice će uzrokovati promjenu cjelokupnog sustava, što će dovesti do otkrića treće strane, to jest napadača u komunikacijskom kanalu. Ova dva pristupa se nadalje mogu podijeliti u tri skupine protokola:

- diskretne varijable,
- kontinuirane varijable i
- distribuirano fazno referentno kodiranje.

Protokoli zasnovani na diskretnim varijablama su kronološki nastali prvi i danas su najrasprostranjeniji. Protokoli ostalih dviju skupina su uglavnom orijentirani ka prevladavanju praktičnih ograničenja u eksperimentima. [14]

iii) Protokol BB84

Prvi kvantni protokol koji su napravili Charles Bennett i Gilles Brassard 1984. godine je opisan na način da se informacije prenose uz pomoć polariziranih stanja fotona. Međutim bilo koja dva para konjugiranih stanja mogu se koristiti za protokol. Ana i Branko su povezani kvantnim komunikacijskim kanalom koji omogućuje prijenos kvantnih stanja. U slučaju fotona, taj komunikacijski kanal je ili optičko vlakno ili slobodan prostor. Također, Ana i Branko su povezani nekim javnim klasičnim komunikacijskim kanalom (primjerice Internetom). Niti jedan od tih kanala ne mora biti siguran, protokol je dizajniran s pretpostavkom da treća strana može prisluškivati. Sigurnost protokola dolazi iz kodiranja informacija u neortogonalnim stanjima. BB84 koristi dva para stanja, gdje je svaki par konjugiran u odnosu na drugi par, a dva stanja unutar jednog para su ortogonalna jedan prema drugom.



Slika 4.1.1.1.: BB84 šifriranje bita [38]

Slika 4.1.1.1 prikazuje šifriranje bita u polarizacijska stanja fotona te parove ortogonalnih stanja, pravokutnu i dijagonalnu bazu.

Parovi ortogonalnih stanja zovu se baze. Uobičajena polarizacija stanja je: linearna horizontalna – linearna vertikalna, linearna pod 45 stupnjeva – linearna pod 135 stupnjeva, cirkularna lijeva – cirkularna desna polarizacija. Bilo koje dvije polarizacije iz različitih baza su međusobno konjugirane. Za BB84 se odabiru dvije baze polarizacije i svakom od stanja u bazama se dodjeljuju vrijednost 0 ili 1 čime se tvori kvantna abeceda. U prvoj fazi komunikacije Ana šalje Branku tajni ključ preko kvantnog kanala. Za svaki od impulsa slučajno izabire jednu od dviju baza polarizacije. Branko ima detektor polarizacije. On ga može postaviti tako da mjeri ili jednu ili drugu polarizaciju. Kvantna mehanika mu brani da mjeri obje polarizacije odjednom. Mjerenje jedne polarizacije uništava svaku mogućnost mjerenja druge polarizacije. Ako Branko ispravno postavi detektor, on će registrirati ispravnu polarizaciju, inače će registrirati neko slučajno stanje s jednakom vjerojatnošću. Branko ne može odrediti razliku između ta dva slučaja. U sljedećem koraku Branko uspostavlja vezu s Anom preko javnog kanala i obavještava ju koje je orijentacije polarizatora koristio za

detekciju. Ana odgovara Branku koja su podešavanja bila ispravna. Ana i Branko zadržavaju samo one polarizacije koje su bile ispravno postavljene. Tako dobiveni bitovi čine tajni ključ. Prosječno će Branko pogoditi ispravnu polarizaciju u 50% slučajeva. Prisluškivanjem Iva pogađa polarizacije kao i Branko. Također, može se pretpostaviti da će pogoditi u 50% slučajeva. Budući da pogrešne pretpostavke mijenjaju polarizaciju impulsa, ona bi na taj način unijela pogreške u sustav. Unošenje grešaka u impulse tijekom prisluškivanja će pokvariti zajednički tajni ključ jer će i Ana i Branko na kraju dobiti različite nizove bitova. Tada Ana i Branko završavaju protokol tako da usporede nekoliko bitova svojih nizova. Ako postoje neusuglašenosti, oni znaju da su bili prisluškivani. U suprotnom, odbacuju bitove koje su koristili za usporedbu i zadržavaju ostale. [14][34][35][36][37]

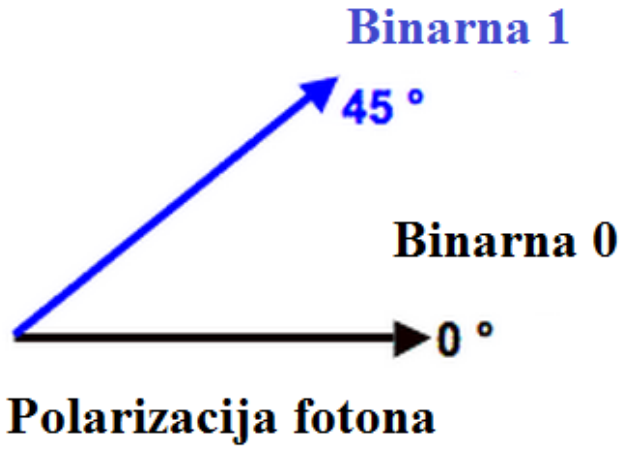
Anini bitovi	0	1	1	0	1	0	0	1
Anine baze	+	+	X	+	X	X	X	+
Anina polarizacija	↑	→	↖	↑	↖	↗	↗	→
Brankove baze	+	X	X	X	+	X	+	+
Brankova mjerenja	↑	↗	↖	↗	→	↗	→	→
Javna rasprava								
Dijeljeni tajni ključ	0		1			0		1

Slika 4.1.1.2.: Princip dobivanja zajedničkog tajnog ključa [38]

Slika 4.1.1.2 prikazuje princip dobivanja zajedničkog tajnog ključa. Ana šalje Branku tajni ključ preko kvantnog kanala, a ona je za svaki impuls odabrala jednu od dviju baza polarizacije. Branko ima detektor te postavlja polarizaciju koju će mjeriti. Ako Branko ispravno postavi detektor, on će registrirati ispravnu polarizaciju, inače će registrirati neko slučajno stanje. U sljedećem koraku Branko uspostavlja vezu s Anom preko javnog kanala i obavještava ju koje je orijentacije polarizatora koristio za detekciju. Ana odgovara Branku koja su podešavanja bila ispravna. Ana i Branko zadržavaju samo one polarizacije koje su bile ispravno postavljene. Tako dobiveni bitovi čine tajni ključ.

iv) Protokol B92

Za razliku od protokola BB84 koji zahtijeva dvije ortogonalne kvantne abecede (baze), protokol B92 zahtijeva samo jednu neortogonalnu abecedu.



Slika 4.1.1.3.: B92 šifriranje bita [38]

Slika 4.1.1.3 prikazuje samo jednu neortogonalnu bazu koju koristi protokol B92

Neka se sa θ označi foton koji je polariziran pod kutom φ u odnosu na vertikalu, gdje je $0 < \varphi < 45°$, a sa θ' označimo foton polariziran pod kutom $-\varphi$ u odnosu na vertikalu. Tada im se pridruže vrijednosti 0 i 1. Kao i kod protokola BB84,Ana i Branko komuniciraju u dvije faze, prvo preko jednosmjernog kvantnog kanala, a zatim preko dvosmjernog javnog kanala. Kako Ana koristi neortogonalni sustav ne postoji način koji bi jednoznačno razlučio ta dva stanja polarizacije. Branko može točno detektirati poslani bit ili primiti dvosmisleni rezultat. Prilikom komunikacije javnim kanalom Branko obavještava Anu o rednim brojevima bitova koje je primio nedvosmisleno, a ostali bitovi se odbacuju. Bitovi koji su primljeni nedvosmisleno postaju ključ. Ostatak se odvija kao i u protokolu BB84. Prisutnost Ive se može otkriti velikim brojem grešaka u sustavu. Ovaj protokol je puno jednostavnije implementirati nego BB84 protokol, ali je njegova sigurnost upitna. [14][34][35][36][37]

v) Protokol E91

Protokol je dobio ime po Arthuru Ekertu koji ga je 1991. godine izmislio. Ekertova shema koristi spregnuti par fotona. Oni mogu biti kreirani od strane Ane, Branka ili nekog izvora neovisnog o

njima, uključujući i Ivu. Fotoni se distribuiraju tako da Ana i Branko dobiju po jedan foton iz svakog para. Ova se shema zasniva na dva svojstva spregnutih fotona:

- spregnuta stanja su savršeno povezana
- bilo koji pokušaj prisluškivanja uništava korelaciju između fotona na način koji Ana i Branko mogu detektirati.

Ana i Branko neovisno biraju bazu u kojoj će mjeriti primljeni foton, s tim da Ana bilježi izmjereni bit, a Branko bilježi komplement izmjerenog bita, jer je njegov foton ortogonalan onome koji je primila Ana. U komunikaciji javnim kanalom Ana i Branko uspoređuju korištene baze detekcije i izdvajaju bitove u kojima su koristili jednake operacije mjerenja. Oni bitovi na kojima su koristili različite operacije mjerenja ne odbacuju već koriste za otkrivanje prisutnosti Ive u komunikaciji korištenjem Bellove nejednadžbe. Ona se upotrebljava za određivanje postojanja lokalno skrivenih varijabli. Ukoliko je nejednadžba zadovoljena, Iva je prisluškivala. Ostatak protokola je isti kao i u BB84. [14][34]

vi) Protokol SARG04

Ovaj protokol je izveden iz protokola BB84. SARG04 su definirali Scarani i suradnici 2004. godine. SARG04 protokol je namijenjen za situacije gdje informacije šalje Poissonov izvor koji stvara slabe pulsove (gdje je srednja vrijednost poslanih fotona manja od 1) i informacije prima nesavršeni detektor. Prednost SARG04 nad BB84 protokolom je njegova robusnost kod nekoherentnih PNS napada. [34]

vii) Protokol šest stanja

Protokol koristi tri para ortogonalnih polarizacijskih stanja da bi predstavio stanja 0 ili 1. Protokol se pokazao manje učinkovit u prijenosu ključa, ali je pokazao veću otpornost na greške nego protokoli BB84 i B92. [34]

4.1.2 Kvantna distribucija ključa (QKD)

Svrha kvantne distribucije ključa (*Quantum Key Distribution* – QKD) je omogućavanje dvjema stranama koje komuniciraju, dogovor o slučajnom kriptografskom ključu u situacijama gdje je moguće prisluškivanje. Međutim, u komunikaciji između Ane i Branka dio točno izmjerenih fotona može biti detektiran pogrešno. Također, ako Iva pokuša izmjeriti fotone koje je Ana poslala prije

nego stignu do Branka, greške će nastati zbog činjenice da Iva pokušava izmjeriti podatke o polarizaciji fotona. Ove dvije situacije se ne mogu razlikovati: prirodan ili umjetan šum izgledaju jednako. Procjena o razini šuma vodi do procjene o količini informacija koje je Iva dobila. Posljedično, protokol u tri faze dozvoljava Ani i Branku da dobiju i da se slože oko manjeg, tajnog kriptografskog ključa na temelju njihovog toka podataka sa šumom koji je prisluškivan. Te tri faze se nazivaju procjena greške, poravnanje informacija i pojačanje privatnosti. [14][34][37]

i) Procjena greške

Provodi se na način da Ana ili Branko odaberu slučajan broj $\boldsymbol{t}$ od prethodno poslanih bitova koji su točno izmjereni i javi ih drugoj strani. Druga strana tada uspoređuje bitove s onima koje ona ima i javlja broj grešaka $\boldsymbol{e}$. Za dovoljno velike uzorke, omjer $\frac{\boldsymbol{e}}{\boldsymbol{t}}$ bi trebao biti razumna procjena broja grešaka koje su ostale u neobjavljenom dijelu ključa. [34]

ii) Poravnanje informacija

Predstavlja način ispravke grešaka koji se provodi između ključeva Ane i Branka, u pokušaju osiguravanja identičnosti oba ključa. Postupak se provodi javnim kanalom te je tako od najveće važnosti minimizirati poslane informacije o ključevima, jer ih Iva može pročitati. Uobičajeni protokol je kaskadni protokol. On se odvija u nekoliko faza, gdje se oba ključa dijele u blokove u svakoj fazi i uspoređuje se paritet tih blokova. Ako se pronađe razlika u paritetu provodi se binarna pretraga da bi se našla i ispravila greška. Ovaj se proces provodi rekurzivno i nakon što se svi blokovi usporede te sve faze završe Ana i Branko će imati iste ključeve sa velikom vjerojatnošću. Međutim, Iva će također dobiti dodatne informacije o ključu iz ovog procesa. [14][34]

iii) Pojačanje privatnosti

Predstavlja metodu za uklanjanje djelomičnih informacija koje Iva ima o ključu Ane i Branka. Te djelomične informacije mogu biti rezultat prisluškivanja kvantnog kanala tijekom prijenosa ključa ili javnog kanala tijekom poravnanja informacija. Pojačanje privatnosti koristi Anin i Brankov ključ za stvaranje novog, kraćeg ključa na način da Iva ima samo zanemarive informacije o novom ključu. To se može postići korištenjem funkcija sažimanja, koje kao ulazni parametar primaju binarni niz dužine ključa i kao izlaz daju binarni niz kraće dužine. Novi ključ se sažima na temelju količine informacija koje je Iva mogla saznati o starom ključu što se zna iz količine grešaka koje postoje. Na

taj način se smanjuje vjerojatnost da Iva ima bilo kakve informacije o novom ključu na vrlo male vrijednosti. [14][34]

4.1.3 Mogući napadi i dokazi sigurnosti

Kako bi kvantni kriptografski sustav bio potpuno siguran neki uvjeti moraju biti zadovoljeni:

- Iva ne može pristupiti uređajima za šifriranje i dešifriranje u Aninom i Brankovom vlasništvu.
- Slučajni generator brojeva koji koriste Ana i Branko mora uistinu davati slučajne brojeve.
- Klasični komunikacijski kanal mora biti autentificiran korištenjem potpuno sigurne sheme autentifikacije.

U nastavku su opisani najpoznatiji napadi na kvantne kriptografske sustave. [14][34]

I) Napad „osoba u sredini“

Kvantna kriptografija je osjetljiva na ovaj napad kada nema autentifikacije kao i klasična kriptografija. Ana i Branko ne mogu autentificirati jedno drugo i uspostaviti sigurnu vezu bez nekog načina provjere identiteta kao na primjer bez tajne poznate objema stranama. Ako Ana i Branko imaju takvu tajnu onda mogu koristiti shemu savršeno sigurne autentifikacije (kao na primjer Carter-Wegman shema) zajedno sa kvantnom distribucijom ključa da bi eksponencijalno proširili ključ te koristeći mali dio novog ključa da bi autentificirali novo razdoblje razmjene podataka. [14][34]

II) Napad razdvajanjem broja fotona (PNS napad)

U protokolu BB84 Ana šalje kvantna stanja Branku koristeći pojedinačne fotone. U praksi se koriste oslabljeni laserski pulsovi za slanje kvantnih stanja. Ti pulsovi sadržavaju malu količinu fotona raspodijeljenih po Poissonovoj razdiobi. To znači da neki pulsovi ne sadržavaju niti jedan foton, neki jedan, a neki dva ili više fotona. Ako puls sadrži više od jednog fotona tada Iva može razdijeliti dodatne fotone i poslati jedan foton Branku. Tada Iva može spremiti dodatne fotone u kvantnu memoriju, dok Ana ne otkrije koje su kodirajuće baze. Iva može izmjeriti fotone u ispravnoj bazi i time dobiti podatke o ključu bez uvođenja grešaka koje se mogu detektirati. [14][34]

III) DoS (Denial of Service)

Budući da se za kvantnu kriptografiju koriste optički kablovi ili zrak kao medij prijenosa informacija, napad se može pokušati prekidajući ili blokirajući liniju, te prisluškujući liniju. [14][34]

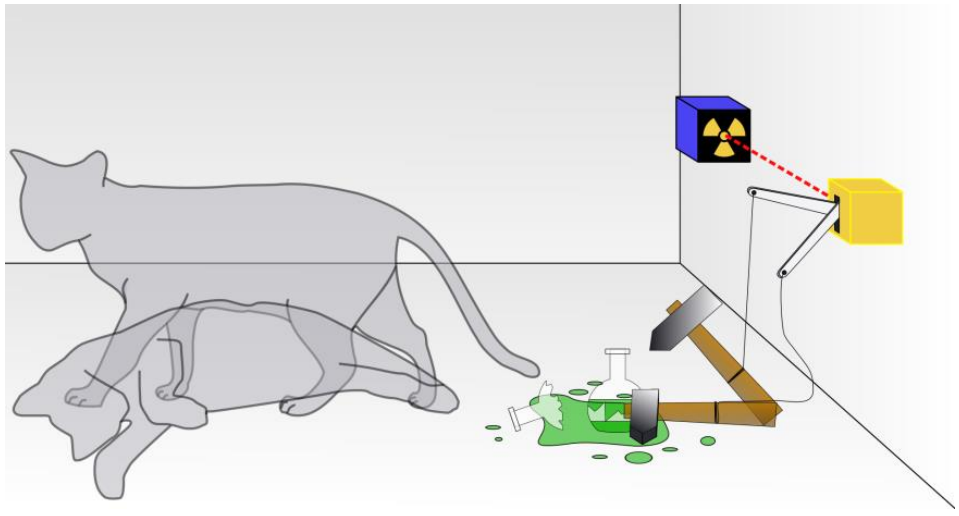
IV) Dokaz sigurnosti

Ako se pretpostavi da Iva ima neograničene resurse, na primjer i klasično i kvantno veliku procesorsku snagu računala, tada postoji još puno mogućih napada. Protokol BB84 je dokazano siguran protiv bilo kojeg napada kojeg dopušta kvantna mehanika, ali također i za slanje informacija koristeći idealni izvor fotona koji istovremeno emitira samo jedan foton ili koristeći praktične izvore fotona koji emitiraju više fotona istovremeno. Ovi dokazi su bezuvjetno sigurni u smislu da ne nameću nikakve uvjete na resurse koji su dostupni onome tko želi prisluškivati, ali osim toga postoje još neki uvjeti kako bi sigurnost bila maksimalna: [14][34]

1. Iva ne može fizički pristupiti Aninim i Brankovim uređajima za šifriranje i dešifriranje.
2. Slučajno generirani broj kojeg koriste Ana i Branko mora biti pouzdan i stvarno slučajan (na primjer kvantni generator slučajnih brojeva)
3. Klasični komunikacijski kanal mora biti autentificiran koristeći bezuvjetno sigurne autentifikacijske sheme
4. Poruka mora biti šifrirana koristeći shemu jednokratne bilježnice (Vernamova šifra)

5. Sprezanje

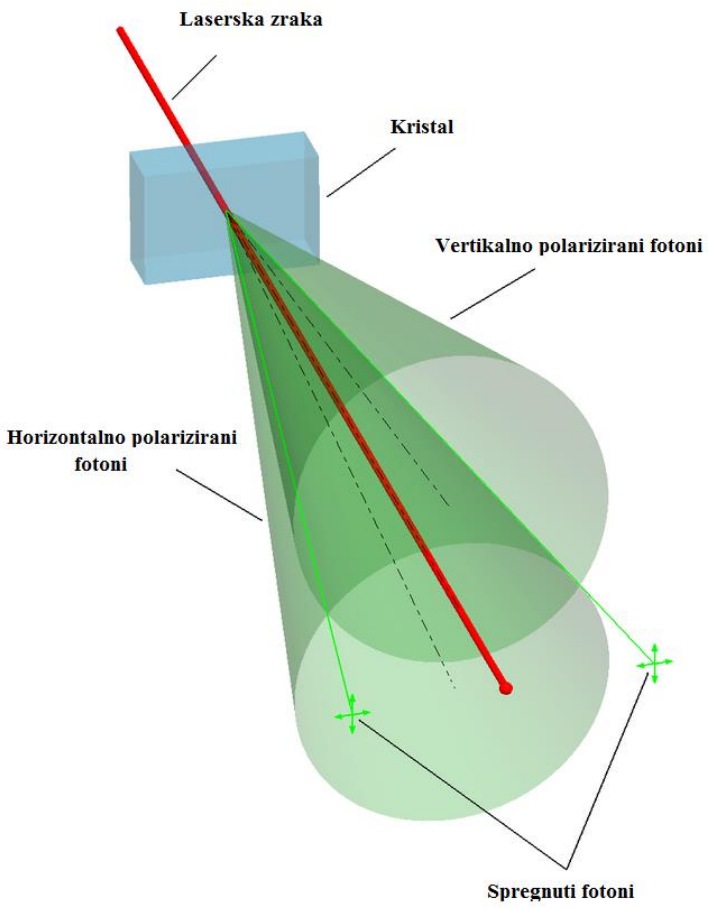
Sprezanje je fizička pojava koja se događa kada su parovi ili grupe čestica u međusobnoj interakciji na način da se kvantno stanje svake čestice ne može opisati samostalno već se kvantno stanje može dati samo za sustav u cjelini. Mjerenje fizikalnih svojstava kao što su pozicija, moment količine gibanja, spin, polarizacija i slično na česticama koje su spregnute, nalaze se u korelaciji. Na primjer ako se generira par čestica kojima je ukupni spin 0, a pronađe se jedna čestica čiji spin je u smjeru kazaljke na satu duž neke osi, tada će se naći i druga čestica koja duž te iste osi ima spin u smjeru suprotnom od smjera kazaljke na satu. Međutim, zbog kvantne prirode mjerenja takvo ponašanje izaziva učinke koji se pojavljuju paradoksalno: mjerenjem bilo kojeg svojstva čestice vidi se kako to mjerenje utječe na samu česticu te u slučaju spregnutih čestica djeluje na sustav u cjelini. Taj fenomen je bio tema članka kojeg su 1935. godine napisali Albert Einstein, Boris Podolsky i Nathan Rosen, a poznat je pod nazivom „*ERP paradox*“. Članak je rana i utjecajna kritika usmjerena protiv Kopenhagenske interpretacije kvantne-mehanike. Napravili su misaoni pokus u kojemu su otkrili da prihvaćanje tadašnje formulacije kvantne-mehanike ima za posljedicu koju dotad nisu primjećivali, a i nije im imala smisla. Njihov scenarij je uključivao fenomen koji je poznat kao kvantno sprezanje (*quantum entanglement*). Misaoni pokus promatra nekakve hipoteze, teorije ili principe kroz njihove posljedice, a najbolji primjer misaonog pokusa je Schrödingerova mačka. To je pokus u kojemu se promatra mačka koja može biti ili živa ili mrtva ovisno o ranijem slučajnom događaju i objašnjava problem Kopenhagenske interpretacije kvantne mehanike.



Slika 5.1.: Schrödingerova mačka [23]

Slika 5.1. prikazuje Schrödingerov misaoni pokus u kojemu se promatra mačka koja se nalazi u hermetički zatvorenoj kutiji s radioaktivnim izvorom i ampulom otrova. Ako se u kutiji detektira radioaktivnost, odnosno propadanje jednog atoma, otrovna ampula se razbija i ubija mačku. Kopenhagenska interpretacija kvantne-mehanike implicira da je nakon nekog vremena mačka i živa i mrtva, ali ako netko pogleda u kutiju vidjet će da je mačka ili živa ili mrtva.

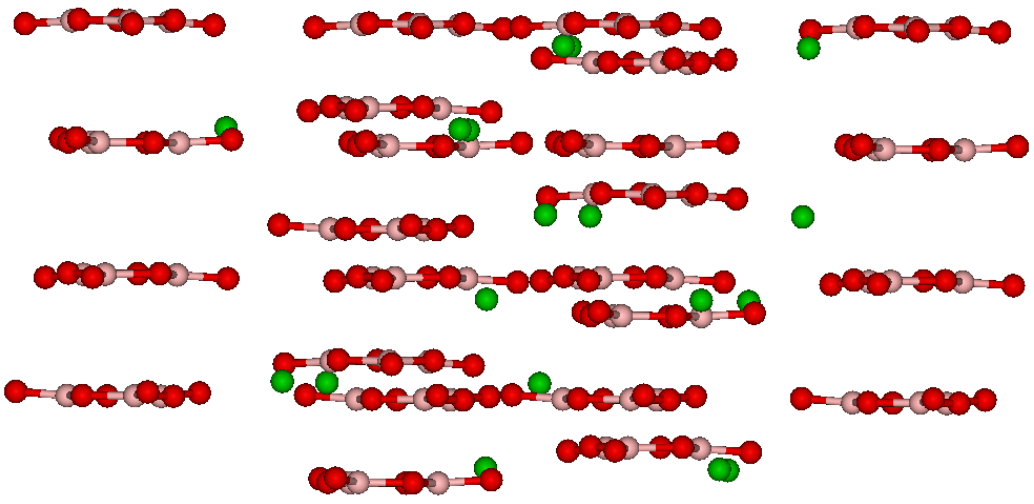
Prema kvantnoj mehanici u određenim uvjetima par kvantnih sustava se može opisati jednom valnom funkcijom, koja kodira vjerojatnosti ishoda pokusa koji se može izvesti na dva sustava, pojedinačno ili zajedno. U ERP članku je napisano kako se rezultati nekih pokusa ne mogu jedinstveno predvidjeti. Primjer takve neodređenosti je vidljiv kada se snop svjetlosti usmjeri na polu-srebrno zrcalo. Polovica zrake će se reflektirati, a druga polovica će proći, ali ako se intenzitet svjetlosnog snopa smanji na samo jedan foton, tada je nemoguće kvantno-mehanički predvidjeti rezultat, odnosno hoće li se foton reflektirati ili će pak proći.



Slika 5.2.: Sprezanje fotona [13]

Slika 5.2. prikazuje primjer sprezanja fotona kada se snop svjetlosti propušta kroz neku kristalnu strukturu. Pronalazi se jedan foton koji ima vertikalnu polarizaciju duž neke osi, a odmah tada se pronalazi i drugi foton koji ima horizontalnu polarizaciju duž neke osi (spregnuti fotoni).

Kako bi se sprezanje lakše shvatilo, ponovno će se koristi analogija novčića, ali ovoga puta će Ana koristiti dva novčića. Ona baca novčiće u zrak, jedan za drugim i govori Branku da ih uhvati. Branko će primiti jednu od kombinacija bitova: 00, 01, 10 ili 11, ovisno koju kombinaciju novčića uhvati (glava je 0, a pismo je 1). Zatim Ana uzima šibicu i lijepi jedan kraj za prvi novčić, a drugi kraj šibice za drugi novčić tako da novčićima glava bude okrenuta prema gore. Rezultat toga je sinkronizirano rotiranje dva novčića kada su bačeni u zrak. Ako Ana uhvati jedan novčić, drugi novčić će se također prestati rotirati zbog šibice koja striktno povezuje dva novčića. Dakle, Ana će primiti ili 00 ili 11 kombinaciju bita. Moguće je napraviti pokus sa dva fotona koji će predstavljati glavu (0) i pismo (1) s vertikalnom i horizontalnom polarizacijom fotona. Bačeni novčić koji se rotira u zraku istovremeno predstavlja i glavu i pismo, baš kao i foton polariziran pod 45°. Njegova polarizacija je linearna kombinacija $\boldsymbol{p}_V$ i $\boldsymbol{p}_H$ kao što je prikazano na slici 4.2. Kada Branko mjeri taj foton $\boldsymbol{p}_{45°}$ sa mjernim uređajem $\boldsymbol{p}_{V\text{-}H}$, on će slučajnim odabirom dobiti $\boldsymbol{p}_V$ ili $\boldsymbol{p}_H$ (0 ili 1). Ako Ana pripremi dva fotona s polarizacijom od 45° i jedan za drugim pošalje Branku, Branko će detektirati kombinaciju: 00, 01, 10 ili 11. Ana sada uvodi analogiju šibice koja povezuje dva novčića. Ona proizvodi dva fotona nelinearnog kristala Beta-Barij Borata (Beta-Barium Borate BBO) kako bi njihove polarizacije bile povezane, iako ta veza ostaje nevidljiva.



Slika 5.3.: Struktura BBO [39]

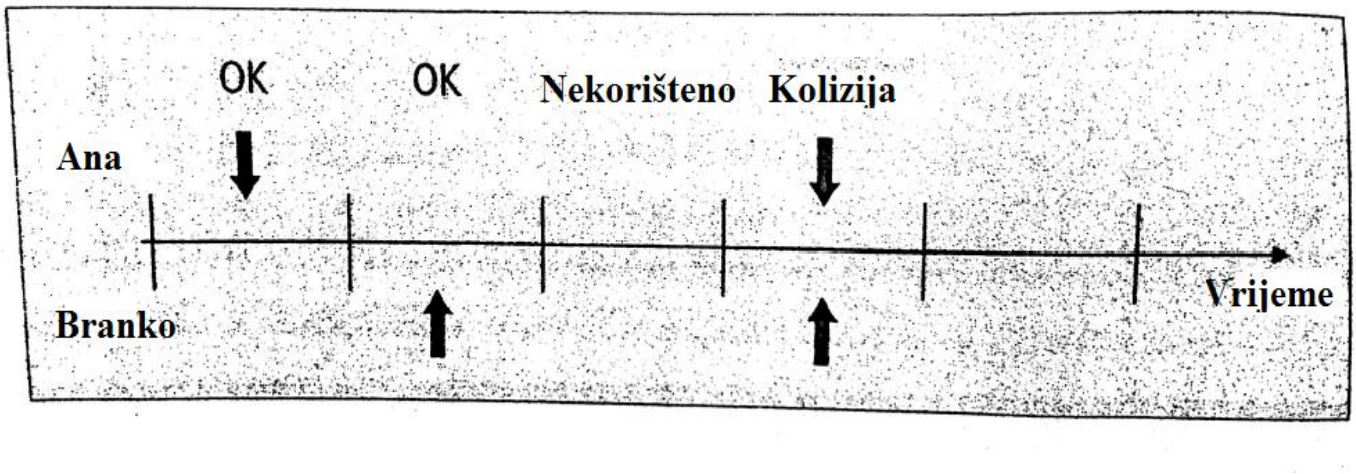
Slika 5.3. prikazuje strukturu kristala BBO koja se koristi za objašnjenje sprezanja.

Ana zadržava prvi foton,a drugi šalje Branku. Zatim Ana mjeri njezin foton s detektorom. Ponaša se poput fotona (Ana slučajnim odabirom promatra 0 ili 1). Kada Branko mjeri svoj foton u bilo kojem trenutku nakon što Ana izmjeri svoj foton, Branko će promatrati istu vrijednost kao i Ana, jer Anino mjerenje postavlja istu vrijednost Brankovom fotonu. Dakle rezultati dva mjerenja će biti ili 00 ili 11. Ovaj nevidljivi efekt povezanosti se naziva sprezanje, a odnosi se na činjenicu da dva fotona imaju posebnu vezu: djelovanje na jednog utječe na stanje drugog. Einstein je ovu pojavu nazvao „zastrašujuće djelovanje na udaljenosti“. Nitko ne bi trebao biti iznenađen s ovom pojavom, jer u svijetu klasične fizike, zbog djelovanja nevidljivog elektromagnetskog zračenja udaljeni uređaji utječu jedan na drugog. Za razliku od elektromagnetizma, međudjelovanje spregnutih fotona događa se trenutačno, bez obzira na udaljenost fotona, dok je elektromagnetski utjecaj ograničen brzinom svjetlosti.

Prije predstavljanja primjera primjene sprezanja u komunikacijama, napravit će se kratka pauza za objašnjenje jedne razlike između fotona i novčića. Trenutno postoji mogućnost sprezanja samo osnovnih čestica (fotoni, elektroni i tako dalje) i nekih većih struktura, koje su manje od nano-svijeta. Trenutno ne postoji mogućnost sprezanja makroskopskih objekata, kao što su na primjer novčić ili svemirski brodovi. Nadalje, rezultat bacanja novčića u zrak čini se slučajnim, ali je moguće korištenjem odgovarajućih formula klasične fizike deterministički izračunati rezultat. Za razliku od novčića i klasične fizike, prema trenutnom znanju o kvantnoj-mehanici, rezultati mjerenja fotona $\boldsymbol{p}_{45^\circ}$ sa mjernim uređajem $\boldsymbol{p}_{V\text{-}H}$ će biti u potpunosti slučajna (nitko ne može predvidjeti rezultat mjerenja). Iz tog razloga je prije spomenuto kako je bacanje novčića samo imitacija onoga što se događa u kvantnom svijetu, ali vrlo uvjerljiva imitacija.

Sprezanje ima vrlo važnu ulogu u kvantnoj-mehanici, a samim time i u kvantnom računalstvu i komunikacijama. Šum u kvantnom komunikacijskom kanalu može se pratiti natrag sve do sprezanja između kanala i njegovog okoliša. Ako je foton koji putuje kroz optičko vlakno spregnut s nekim fotonom izvan vlakna i taj foton izvan vlakna bude pod utjecajem nekakvih efekata, tada će ti efekti utjecati i na stanje fotona unutar vlakna. Dakle ili će se fotoni čuvati od utjecaja sprezanja ili će snositi posljedice (šum kanala). Na sreću da bi dva fotona bila spregnuta, u nekom trenutku u vremenu moraju se nalaziti blizu jedan drugome, što znači da se sprezanje neće dogoditi između udaljenih čestica. Također, tamo gdje se prirodno javlja sprezanje koje uzrokuje

neželjeni šum u kvantnom komunikacijskom kanalu, može se umjetno stvoreno sprezanje iskoristiti za poboljšanje komunikacija i računalnih mogućnosti. Za kraj će se predstaviti jednostavan primjer komunikacije u kojemu se sprezanje može iskoristiti. U tekstu se spominjao problem fizičkog sloja: kako smanjiti ili u potpunosti ukloniti šum iz komunikacijskog kanala. Sada se pristupa MAC sloju (*Medium Access Control Layer*) i opisuje kako se sprezanje može iskoristiti za poboljšanje iskorištenja kanala kod raspodijeljenih MAC protokola. Kao uzorak ponašanja koristit će se ALOHA protokol, koji je pojednostavljena verzija raspodijeljenih MAC protokola koji se koriste u bežičnim mrežama (WiFi – *Wireless Fidelity*). U sustavima koji koriste ALOHA protokol, vremenska dimenzija je podijeljena na intervale (vremenske odsječke) s određenim (fiksnim) trajanjem, kao što je i pokazano na slici 5.4.



Slika 5.4.: Vremenski intervali ALOHA protokola [1]

Slika 5.4. prikazuje vremensku raspodjelu na fiksne intervale u ALOHA protokolu.

Na početku svakog vremenskog intervala Ana i Branko odlučuju hoće li ili neće slati pakete. Ako samo jedno od njih pošalje paket u kanal, paket će biti dostavljen. Ako oboje odluče ne poslati nikakav paket u kanal, interval će ostati prazan te će izgubiti priliku za prijenos paketa kanalom. U konačnici, ako oboje odluče poslati paket, doći će do kolizije i ponovno će se izgubiti prilika za prijenos paketa kanalom. U centraliziranim MAC rješenjima, postoji čvor (pristupna točka ili bazna stanica) koja vrši koordinaciju Ane i Branka kako ne bi došlo do kolizije. Međutim, postoji puno protokola koji koriste raspodijeljeni MAC (na primjer *ad hoc* mrežni protokoli). Prema teoriji

informacija, najbolja raspodijeljena rješenja (mjereno prema pravednosti i ukupnoj propusnost) imaju sljedeća svojstva:

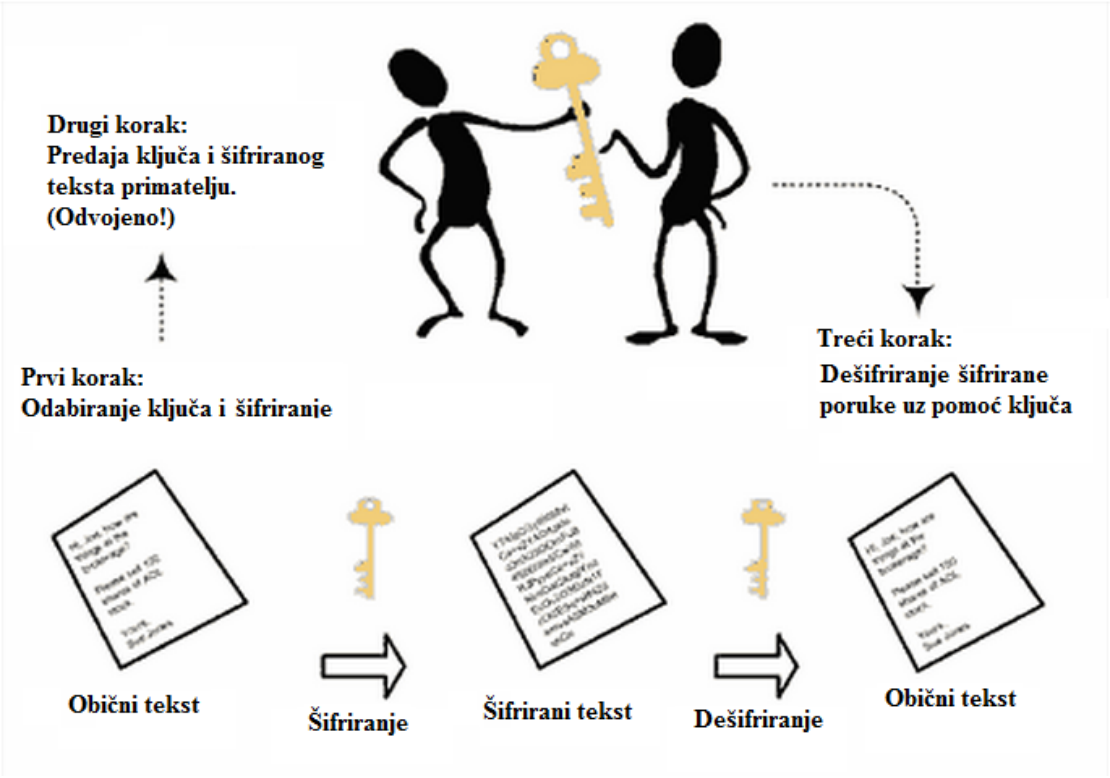
- Ana i Branko pristupaju kanalu metodom slučajnog odabira
- Vjerojatnost svakog korisnika da šalje paket u određenom vremenskom intervalu je $\frac{1}{N}$, gdje je N broj aktivnih korisnika.

Što znači da uzimajući u obzir četiri moguća rezultata u slučaju Ane i Branka (dva korisnika), samo dva intervala će biti iskorištena (kao što se i vidi na slici 5.4.), a to je neučinkovito. Centralizacija bi poboljšala učinkovitost, ali taj pristup ne bi bio moguć, iako je poželjan u mnogim situacijama. Međutim, treba se razmotriti svojstvo koordinacije između korisnika sustava za poboljšanje iskoristivosti kanala. Centralizacija omogućava koordinaciju, a već se došlo do zaključka kako taj pristup nije moguć, zato će se razmotriti je li moguće iskoristiti kvantne komunikacije kako bi se ostvarila koordinacija između raspodijeljenih korisnika. Potrebno je razmotriti par spregnutih fotona koji se ponašaju poput dva novčića povezanih šibicom. Ponovno se koristi analogija dva novčića povezana šibicom, ali uz jednu izmjenu, a to je da je jedan novčić (foton) negiran, odnosno da je kod jednog novčića prema gore okrenuta glava, a kod drugoga pismo. Na taj način se šifrira logička kombinacija 01 ili 10. Za početak, Ana i Branko pripremaju takav par i podijele ga. Kada budu htjeli komunicirati, moraju izmjeriti fotone. Kako bi izbjegli koliziju, i Anin i Brankov mjerni uređaj na slučajan način odabiru rezultat mjerenja između logičke kombinacije 01 i 10. Tko god dobije 1 može poslati paket, dok drugi mora ostati tih, odnosno ne smije poslati ništa. Ovaj protokol je pravedan, raspodijeljen i daje slučajne rezultate što osigurava savršenu koordinaciju između korisnika. Na prvi pogled se čini kako se ovdje ne može učiniti ništa više nego što se može učiniti sa generatorom dijeljenog pseudo-slučajnog broja (ako je sljedeći bit 0, Ana će poslati paket, u suprotnom, ako je sljedeći bit 1, Branko će poslati paket). Međutim, ovo neće raditi u raspodijeljenom okruženju, jer je potrebna centralna jedinica koja će proizvoditi slučajne šifre i raspodjeljivati ih korisnicima. Nasuprot tome, kvantni pristup ne treba centralnu jedinicu, jer se sprezanje može proizvesti na raspodijeljeni način te zbog toga centralna jedinica nije potrebna za proizvodnju i distribuciju slučajnih šifri. Druga razlika je ta što kvantna-mehanika stvarno osigurava slučajne brojeve umjesto pseudo-slučajnih brojeva u klasičnom slučaju. Što znači da sprezanje omogućava koordinaciju između raspodijeljenih korisnika te osigurava poboljšanje iskoristivosti kanala bez uvođenja centralizacije. Sprezanje se često koristi u novim kvantnim

komunikacijskim (i računalnim) sustavima. Jedna od najvažnijih primjena sprezanja je povećanje kapaciteta kanala sprezanjem uzastopno poslanih bitova. Značaj komunikacijskih protokola koji iskorištavaju sprezanje očituje se definicijom nove mjere kapaciteta: kapacitet ostvaren uz pomoć sprezanja (*entanglement-assisted capacity*). Postoje kvantni kanali koji individualno imaju informacijski kapacitet kanala nula, ali primjenom sprezanja mogu biti super-aktivirani: kombinacijom takva dva kanala može se dostaviti ne-nulta informacija prijemniku i to se smatra najekstremnijom primjenom sprezanja. Sprezanje često naziva resursom u literaturi kvantnih komunikacija i računalstva.[1][13][37]

6. Sigurne kvantne komunikacije

Sigurnost – autentifikacija, kriptografija, privatnost i tako dalje – sve su to zahtjevi za komunikacijske mreže. Međutim danas je obrana od napada nedovoljna i ne efikasna protiv trenutnih *cyber* prijetnji. Mnogi *cyber* napadi nisu otkriveni ili ne budu otkriveni do trenutka kada već nanesu ozbiljnu tehničku i financijsku štetu. Kvantna rješenja bazirana na optici nude nove efikasne metode obrane. Ovdje će se fokusirati na kriptografiju koja je odgovorna za sigurnost komunikacije u prisustvu treće osobe. Ana želi poslati informaciju – običan tekst ili običnu poruku – sigurno do Branka. Iva je zainteresirana za prisluškivanje ove informacije. U kontekstu komunikacija, zanimljive su dvije vrste kriptografije: simetrični (tajni) ključ i javni ključ. Kriptografija simetričnim ključem je sustav šifriranja u kojemu pošiljatelj (Ana) i primatelj (Branko) dijele jedan zajednički ključ za šifriranje i dešifriranje poruke. To je brži i jednostavniji sustav šifriranja, ali ima veliku manu, Ana i Branko moraju nekako razmijeniti ključ na siguran način. Kriptografija simetričnim ključem se često naziva i kriptografija tajnim ključem. Najpopularnija kriptografija simetričnim ključem je DES (*Data Encryption Standard*).



Slika 6.1.: Kriptografija simetričnim ključem [40]

Slika 6.1. prikazuje kriptografiju simetričnim ključem u kojoj pošiljatelj prvo odabire ključ kojim će šifrirati poruku, odnosno običan tekst, zatim razmjenjuje ključ s primateljem poruke preko sigurne linije te mu šalje poruku koju zatim primatelj dešifrira pomoću ključa kojeg je razmijenio s pošiljateljem preko sigurne linije.

Savršeni kriptografski sustav simetričnim ključem je Vernamova šifra ili jednokratna bilježnica. U Vernamovoj šifri ključ je:

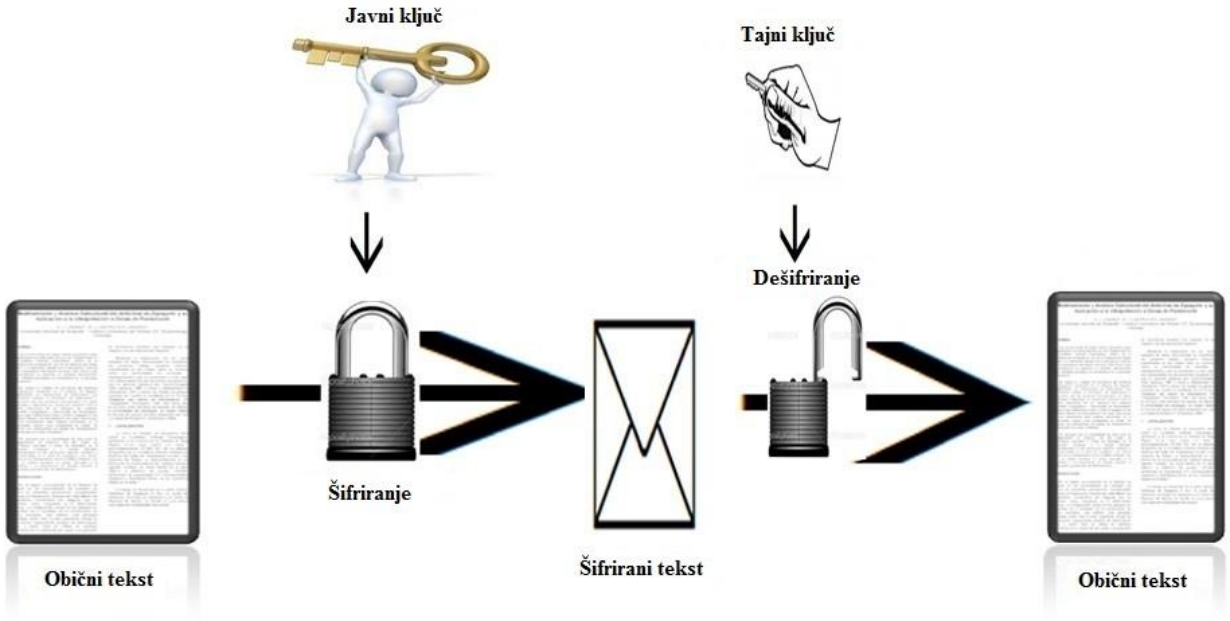
a) Jednake duljine kao i običan tekst
b) Stvarno slučajan
c) Nikada se ponovno ne koristi
d) Ostaje tajan

Iako su sva ova svojstva dostupna u praksi (s različitim stupnjevima težine) klasičnim metodama, svojstvo tajnosti (d) je praktički teško ostvariv u današnjem internetskom okruženju. U nastavku će se objasniti kako se uz pomoć kvantnih metoda može značajno smanjiti težina. Glavno pitanje sigurnosti je kako će Ana i Branko razmijeniti ključ prije nego započnu komunikaciju. Postoji efikasno, ali skupo rješenje ovog problema: centralizirana infrastruktura. Na primjer u slučaju celularne mobilne mreže za svakog korisnika (Ana i Branko), dvije kopije ključa se nalaze:

a) U korisnikovoj SIM (*Subscriber Identity Module*) kartici
b) U mrežnoj bazi podataka

Kako bi komunicirala s Brankom,Ana prvo uspostavlja komunikaciju simetričnim ključem s mrežom. Namjenski mrežni čvor ima funkciju posrednika između korisnika, jer prvo dešifrira poruku s kopijom Aninog ključa, šifrira poruku s Brankovim ključem te šalje poruku (šifriranu) Branku. Branko dešifrira poruku u običan tekst. Metoda dva koraka zadržava tajnost, ako se namjenski mrežni čvor održava sigurnim. Međutim ovo rješenje ne radi u praksi za distribuirane pružatelje mrežnih usluga, poput interneta. Povijesno gledano internetski korisnici nikada nisu koristili centraliziranu infrastrukturu i jednostavno ne žele koristiti usluge koje zahtijevaju centraliziranu registraciju. Kriptografija javnim ključem može pomoći u ovakvim situacijama. Branko generira slučajni ključ i čuva ga tajnim. Zatim generira javni ključ, dobiven iz tajnog ključa pomoću specijalne funkcije **f()**. Nakon toga objavljuje javni ključ na internetu kako bi bio dostupan svima koji žele komunicirati s njim. Ana želi komunicirati s Brankom, pa koristi Brankov javni

ključ kako bi šifrirala običan tekst poruke i poslala ju kao šifriranu poruku Branku. Branko dešifrira poruku pomoću svog tajnog ključa i čita tekst poruke.



Slika 6.2.: Kriptografija javnim ključem [41]

Slika 6.2. prikazuje kriptografiju javnim ključem u kojoj pošiljatelj šifrira svoju poruku iz primateljevog javnog ključa i šalje ju primatelju. Primatelj prima šifriranu poruku i dešifrira ju pomoću svog tajnog ključa.

Pragmatičnost i sigurnost kriptografije javnim ključem ovisi o dva svojstva funkcije **f()**. Prvo, mora biti lak za izračunati kako bi ga Branko mogao lako generirati. I drugo, inverz funkcije **f()** treba biti teško izračunati, kako bi spriječilo Ivu od mogućnosti izračuna tajnog ključa iz javnog ključa. Na primjer, za RSA (*Rivest, Shamir and Adleman*) algoritam koji je u širokoj upotrebi, Branko uspješno množi dva velika (tajna) glavna broja kako bi generirao javni ključ. Tajni ključ također se generira iz dva velika glavna broja. Iva može dešifrirati bilo koju poruku koja je šifrirana Brankovim javnim ključem, pod uvjetom da može generirati tajni ključ dijeljenjem javnog ključa na dva glavna broja pomoću kojih je generiran. Međutim, ne postoji učinkovit klasični algoritam faktorizacije cijelih brojeva, a zbog veličine glavnih brojeva (obično 1024 bita ili preko 300 digitalnih znamenki) – resursi potrebni za izračun faktora javnog ključa su previsoki te je nemoguće izračunati faktore i tajni ključ. Sigurnost kriptografije asimetričnim ključem ovisi o drugom svojstvu

funkcije **f()**. Iako je kvantno računanje izvan opsega ovog rada, samo će se spomenuti da postoje određeni kvantni algoritmi koji djelotvorno rješavaju problem faktorizacije. Stoga, prva stolna kvantna računala će značajno utjecati na razvoj kriptografskih sustava s asimetričnim ključem koji ovise o računski teškoj i zahtjevnoj faktorizaciji. Kriptografski sustavi sa simetričnim ključem mogli bi istisnuti s tržišta kriptografski sustav s asimetričnim ključem,ako se riješi problem uskog grla u centraliziranoj infrastrukturi.

Na sreću, kvantna komunikacija i kvantna kriptografija može se nositi ne samo sa klasičnim prisluškivanjem, nego i sa hakerima koji koriste kvantna računala. Nadalje, dok će ljudski rod možda pričekati i desetljeća na praktičnu upotrebu, prvi prototipovi kvantnih kriptografskih mreža i proizvoda razvijaju se već jedno desetljeće i spremni su za tržište, kao što je i vidljivo u tablici 6.1.

Tablica 6.1.: Glavni pokusi komercijalne kvantne distribucije ključa [1]

Pokusi	Status
DARPA Quantum network	Mreža kvantne distribucije ključa s 10 čvorova u Sjedinjenim Američkim Državama od 2004. godine
SECOQC	200 km standardne svjetlovodne mreže koja povezuje 6 lokacija u Austriji, 2008. godine
SwissQuantum	Dvije godine testiranja pouzdanosti komercijalne kriptografske tehnologije u Ženevi, Švicarska, gradsko područje 2009-2011
Tokyo QKD Network	Testiranje 4 čvora duljine 45 km u Japanu pokrenuto 2010.

Postoji nekoliko vrsta kvantnih kriptografskih protokola, ali je osnovni koncept sličan. Ako je Ana u mogućnosti poslati kopiju njezinog ključa Branku, uz garanciju da će svaki pokušaj prisluškivanja biti otkriven, tada oni mogu koristiti kriptografiju sa simetričnim ključem, što je teorijski dokazano sigurno: kvantna kriptografija uklanja sigurnosne propuste („rupe“) u kriptografiji sa simetričnim ključem. Sprezanje se može iskoristiti za sigurnu razmjenu ključa za šifriranje. Ako Ana proizvede par spregnutih fotona koji sadrže logičku kombinaciju 00 ili 11 i pošalje jedan foton Branku, mjerenjem fotona s obje strane oboje će promatrati 00 ili 11 slučajnim odabirom. Gledanjem s kriptografske strane, oni generiraju prvi bit simetričnog para ključa za šifriranje, jer je vrijednost bita apsolutno slučajna i slaže se s obje strane (i s Anine i s Brankove strane). Kao što je i objašnjeno u petom poglavlju, nitko ne može utjecati na mjerenje fotona, jer

daje slučajne vrijednosti i iz tog razloga nitko ne može predvidjeti rezultate mjerenja, to jest Iva ne može izračunati bitove ključa. Ako oni ponove ove korake nekoliko puta, mogu proizvesti ključ za šifriranje odgovarajuće duljine. Svatko će se zapitati sljedeće: tko će generirati ključ? Odgovor bi mogao biti iznenađujući. Zbog toga što Ana i Branko istovremeno rade ista mjerenja, ključ generiraju njih dvoje. Što znači da ključ nije postojao prije mjerenja, pa Iva nema što prisluškivati. Dakle, kvantna distribucija ključa može se smatrati i kao raspodijeljeno stvaranje kvantnog ključa. U praktičnoj primjeni protokoli kvantne distribucije ključa su ranjivi na napad „osoba u sredini“, kada se zlonamjerna osoba koja prisluškuje predstavlja Ani kao Branko i Branku kao Ana. Kako bi se spriječio ovakav napad, potrebno je napraviti autentifikaciju stranaka (korisnika) što uključuje zajednički ključ. Jednom kada se autentifikacija obavi uspješno, moguće je s kvantnom distribucijom ključa proširiti ovaj ključ za autentifikaciju sljedeće sjednice (sesije). [1][34][35][36]

7. Zaključak

Zadatak diplomskog rada je opisati teoriju kvantnih komunikacija koja uvodi kvantno-mehanička svojstva polarizacije i sprezanja koja nemaju analogije u klasičnoj teoriji komunikacija. Gordon E. Moore je 19. travnja 1965. godine u svom radu predvidio da će se broj tranzistora po čipu udvostručavati svakih 18-24 mjeseci. S jedne strane je to rezultiralo sve bržim i bržim procesorima, a s druge strane je došlo do ključnog kompromisa, jer se počelo gravirati sve tanje i tanje linije na površini poluvodiča, što je dovelo do sve manjih i manjih tranzistora. U konačnici je dosegnut nano-svijet (10^{-9}), kojim vladaju pravila i zakoni kvantne-mehanike, a koji se značajno razlikuje od mikro-svijeta klasične fizike s kojom je čovjek upoznat kroz svoju percepciju i tradicionalni sustav obrazovanja. Znanstvena istraživanja valne prirode svjetla započela su u 17. i 18. stoljeću, a 1859. godine je Gustav Kirchoff iznio problem zračenja crnog tijela. Idealno crno tijelo je tijelo koje upija sve valne duljine elektromagnetskog zračenja koje padaju na njega, ali isto tako i emitira sve valne duljine. Max Planck je 14. prosinca 1900. godine predstavio svoju kvantnu hipotezu kojom je objasnio zračenje crnog tijela. Definirao je kvant energije, kao najmanju količinu energije koju neko tijelo može primiti ili emitirati. Albert Einstein je 1905. godine objasnio fotoelektrični efekt. Fotoelektrični efekt je fizikalna pojava kod koje djelovanjem elektromagnetskog zračenja dovoljno kratke valne duljine dolazi do izbijanja elektrona iz obasjanog materijala. Daljnjim istraživanjem kvanta otkriveno je ponašanje povezano sa samostalnim česticama, koje su nazvani fotoni. Foton je elementarna čestica koja se u vakuumu giba brzinom svjetlosti, nema masu i električni naboj te je stabilan. Zbog toga su znanstvenici došli do zaključka da svjetlost ima dvojnu narav, jer pokazuje svojstva i vala i čestice. U siječnju 1926. godine Schrödinger je u znanstvenom časopisu objavio članak, poznat kao Schrödingerova jednadžba, a ona predstavlja jedan od temelja kvantne mehanike. U članku je dao „derivaciju“ valne jednadžbe za vremenski neovisne sustave i pokazalo se da je dao točnu energetsku vlastitu vrijednost za atom sličan vodiku. Schrödingerova jednadžba prikazuje prostorno i vremensko ponašanje čestice u okviru kvantne mehanike.

Prednost prelaska komunikacija iz klasične u kvantnu domenu proizlazi iz povećanja stupnjeva slobode. Ako se klasični fizikalni mediji koji predstavljaju logičke vrijednosti 0 i 1 zamjene s onima iz nano-svijeta (na primjer fotoni, elektroni,…) kojima vladaju pravila i zakoni kvantne-mehanike, onda se linearna kombinacija može koristiti za logičke vrijednosti. Na primjer, za polarizirani foton $\boldsymbol{p} = a\boldsymbol{p}_V + b\boldsymbol{p}_H$, koeficijenti $\boldsymbol{a}$ i $\boldsymbol{b}$ se mogu prilagoditi za optimizaciju bilo kojeg komunikacijskog

protokola i prema tome oni predstavljaju nove stupnjeve slobode koji nemaju analogije u klasičnoj domeni. Kvantna informacija se može dostaviti preko raznih medija. Kroz jedan kanal optičkog vlakna se umjesto svjetlosnih impulsa šalju polarizirani fotoni, ali se tu nailazi na prepreku. Sadašnja infrastruktura optičkih vlakana se ne može koristiti u svrhu kvantnog prijenosa podataka jer su komercijalna vlakna projektirana da rade na drugačijim valnim duljinama nego što je optimalno za kvantni prijenos podataka. Rani pokusi su prelazili udaljenost od 200 km, a cilj pokusa je ostvariti komunikaciju Zemlja-satelit uz pomoć kvantnih komunikacija kroz slobodan prostor.

Sprezanje je fizička pojava koja se događa kada su parovi ili grupe čestica u međusobnoj interakciji na način da se kvantno stanje svake čestice ne može opisati samostalno već se kvantno stanje može dati samo za sustav u cjelini. Sprezanje ima vrlo važnu ulogu u kvantnoj-mehanici, a samim time i u kvantnom računalstvu i komunikacijama. Može se iskoristiti za poboljšanje iskorištenja kanala kod raspodijeljenih MAC protokola, na način da se pomoću spregnutih fotona vrši koordinacija između raspodijeljenih korisnika. Sprezanje se također može iskoristiti i za poboljšanje zaštite i povećanje učinkovitosti distribucije šifre kod kriptografskih sustava zaštite sa simetričnom šifrom koji koriste kvantne kriptografske mreže. To je moguće ostvariti na način da se koristi centralizirana infrastruktura što je vrlo efikasno, ali skupo rješenje. Tada bi dva korisnika (pošiljatelj (Ana) i primatelj (Branko)) komunicirali uz pomoć „posrednika“ koji ima kopije ključeva za šifriranje od Ane i Branka u svojoj bazi podataka. Ana prvo uspostavlja komunikaciju simetričnim ključem s mrežom. Namjenski mrežni čvor ima funkciju posrednika između korisnika, jer prvo dešifrira poruku s kopijom Aninog ključa, šifrira poruku s Brankovim ključem te šalje poruku (šifriranu) Branku. Branko dešifrira poruku u običan tekst. Metoda dva koraka zadržava tajnost, ako se namjenski mrežni čvor održava sigurnim. Međutim ovo rješenje ne radi u praksi za distribuirane pružatelje mrežnih usluga, poput interneta. Sprezanje se može iskoristiti i za sigurnu razmjenu ključa za šifriranje. Ako Ana proizvede par spregnutih fotona koji sadrže logičku kombinaciju 00 ili 11 i pošalje jedan foton Branku, mjerenjem fotona s obje strane oboje će promatrati 00 ili 11 slučajnim odabirom. Gledanjem s kriptografske strane, oni generiraju prvi bit simetričnog para ključa za šifriranje, jer je vrijednost bita apsolutno slučajna i slaže se s obje strane (i s Anine i s Brankove strane). Nitko ne može utjecati na mjerenje fotona, jer daje slučajne vrijednosti i iz tog razloga nitko ne može predvidjeti rezultate mjerenja, pa osoba koja prisluškuje (Iva) ne može izračunati bitove ključa. Ako oni ponove ove korake nekoliko puta, mogu proizvesti ključ za šifriranje odgovarajuće duljine. Zbog toga što Ana i Branko istovremeno rade ista mjerenja,

ključ generiraju njih dvoje. Što znači da ključ nije postojao prije mjerenja, pa Iva nema što prisluškivati.

S obzirom da mnogi fizički mediji mogu nositi kvantne informacije, otvaraju se novi smjerovi u komunikacijama. Najsuvremenija istraživanja su fokusirana s jedne strane na teoretska ograničenja kvantnih kanala i protokola, a s druge strane na praktičnu primjenu u već postojećoj klasičnoj mreži, čime se utire put za širenje kvantnih komunikacija.

Republika Kina je otkrila da će napraviti prvi pokus sa satelitskim komunikacijama temeljenim na kvantnoj-mehanici. Planiraju 2016. godine lansirati *Chinese Quantum Science Satellite*, a cilj im je postati prva nacija sa svemirskim programom i satelitima koja će koristiti kvantne komunikacije.

8. Literatura

[1] S. Imre, Quantum Communications: Explained for Communication Engineers, IEEE Communications Magazine, vol:51, issue:8, pages: 28-35

[2] G. E. Moore, Cramming More Components onto Integrated Circuits, http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf, (24. 04. 2014.)

Internet stranice:

[3] http://en.wikipedia.org/wiki/Integrated_circuit, (24. 04. 2014.)

[4] http://en.wikipedia.org/wiki/Moore's_law, (24. 04. 2014.)

[5] http://quantumfreak.com/introduction-to-blackbody-radiation/, (04. 08. 2014.)

[6] http://en.wikipedia.org/wiki/Quantum_mechanics, (09. 04. 2014.)

[7] http://sydney.edu.au/science/chemistry/~mjtj/CHEM3117/Resources/postulates.pdf, (24. 04. 2014.)

[8] http://en.wikipedia.org/wiki/Photon_polarization, (09. 04. 2014.)

[9] http://link.springer.com/chapter/10.1007%2F978-3-540-70626-7_45#page-1, (04. 08. 2014.)

[10] http://en.wikipedia.org/wiki/Spin_(physics), (09. 04. 2014.)

[11] http://en.wikipedia.org/wiki/Stern%E2%80%93Gerlach_experiment, (24. 04. 2014.)

[12] http://www.fizika.unios.hr/~ilukacevic/dokumenti/materijali_za_studente/qm1/Lecture_4_Osnovna_svojstva_valne_mehanike.pdf, (24. 04. 2014.)

[13] http://en.wikipedia.org/wiki/Quantum_entanglement, (09. 04. 2014.)

[14] http://en.wikipedia.org/wiki/Quantum_cryptography, (09. 04. 2014.)

[15] http://en.wikipedia.org/wiki/Quantum_key_distribution, (09. 04. 2014.)

[16] http://en.wikipedia.org/wiki/EPR_paradox, pristup ostvaren (09. 04. 2014.)

[17] http://spectrum.ieee.org/computing/networks/mother-of-all-quantum-networks-unveiled-in-vienna, (04. 08. 2014.)

[18] http://spectrum.ieee.org/tech-talk/computing/networks/quantum-cryptography-done-over-shared-data-line, (04.08. 2014.)

[19] http://spectrum.ieee.org/computing/networks/longdistance-quantum-cryptography, (04. 08. 2014.)

[20] http://en.wikipedia.org/wiki/Uncertainty_principle, (24. 04. 2014.)

[21] http://www.physicsoftheuniverse.com/topics_quantum_quanta.html, (04. 08. 2014.)

[22] http://cnx.org/content/m39551/1.1/?collection=col11244/latest, (04. 08. 2014.)

[23] http://en.wikipedia.org/wiki/Schr%C3%B6dinger_equation, (09. 04. 2014.)

[24]http://en.wikipedia.org/wiki/Pauli_exclusion_principle, (09.04.2014.)

[25] http://en.wikipedia.org/wiki/Dirac_equation, (09.04.2014)

[26] http://en.wikipedia.org/wiki/Wave, (07. 08. 2014.)

[27] http://en.wikipedia.org/wiki/Magnetic_resonance_imaging, (04. 08. 2014.)

[28] http://eng.thesaurus.rusnano.com/wiki/article1831, (04. 08. 2014.)

[29] http://en.wikipedia.org/wiki/Electron_configuration, (04. 08. 2014.)

[30] http://en.wikipedia.org/wiki/Azimuthal_quantum_number, (04. 08. 2014.)

[31] http://catalog.flatworldknowledge.com/bookhub/2273?e=ball-ch08_s02, (11. 08. 2014.)

[32] http://en.wikipedia.org/wiki/Magnetic_quantum_number, (11. 08. 2014.)

[33] http://en.wikipedia.org/wiki/Quantum_number, (11. 08. 2014.)

[34] S. Picek, M. Golub, Kvantna kriptografija: razvoj i protokoli, http://os2.zemris.fer.hr/ostalo/2009_picek/Kriptografija.htm, (09. 04. 2014.)

[35] R. D. Sharma, Quantum Cryptography: A New Approach to Information Security, http://www.interscience.in/IJPSOEM_Vol1Iss1/paper3.pdf, (09. 04. 2014.)

[36] M. M. I. Khan, M. Sher, Protocols for Secure Quantum Transmission: A Review of Recent Developments, http://www.researchgate.net/publication/45949338_Protocols_for_Secure_Quantum_Transmission_A_Review_of_Recent_Developments, (09. 04. 2014.)

[37] L. Bacsardi, On the Way to Quantum-Based Satellite Communication, IEEE Communications Magazine, vol:51, issue:8, pages: 50-55

[38] http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#bb84, (10. 08. 2014.)

[39] http://en.wikipedia.org/wiki/Barium_borate, (10. 08. 2014.)

[40] http://www.powayusd.com/pusdtbes/cs/class7.htm, (16. 08. 2014.)

[41] http://www.onlinebusiness.newstipstricks.com/cryptography-of-public-keys/, (16. 08. 2014.)

9. Sažetak

Zadatak diplomskog rada je opisati teoriju kvantnih komunikacija koja uvodi kvantno-mehanička svojstva polarizacije i sprezanja koja nemaju analogije u klasičnoj teoriji komunikacija. Prvo je opisan Mooreov zakon, a potom i pojam kvantne-mehanike i njezin razvoj kroz povijest. Opisana su fizikalna svojstva valova i čestica, objašnjen je spin elektrona i opisani su postulati kvantne-mehanike. Zatim su komunikacije pretvorene iz klasičnih u kvantne i na jednostavnim primjerima je pokazano kako se polarizacija i sprezanje mogu iskoristiti za realizaciju kanala bez šuma i za poboljšanje iskorištenja kanala kod raspodijeljenih MAC protokola. Opisan je i princip kvantne kriptografije, opisana je i kvantna distribucija ključa. Na samom kraju je opisano i kako se sprezanje može iskoristiti za poboljšanje zaštite i povećanje učinkovitosti distribucije šifre kod kriptografskih sustava zaštite sa simetričnom šifrom koji koriste kvantne kriptografske mreže.

Ključne riječi: Mooreov zakon, kvantna-mehanika, val, čestica, spin, postulati kvantne-mehanike, polarizacija, sprezanje, kvantna kriptografija, kvantna distribucija ključa

Communication based on quantum-mechanical properties

Abstract

The task of thesis is to describe the theory of quantum communications, which introduces the quantum mechanical properties of polarization and entanglement which do not have analogs in classical communications theory. At first, describes Moore's Law, and then the concept of quantum mechanics and its development throughout history. Describes the physical properties of waves and particles, explains electron spin and the postulates of quantum mechanics. Turns communication from classical to quantum and simple examples demonstrate how polarization and entanglement may be exploited to create noise-free channel and to improve channel utilization for distributed MAC protocols. It also describes the principle of quantum cryptography and describes quantum key distribution. Finally, describes how entanglement is used to enhance security and improve key distribution efficiency in symmetric-key cryptography systems used by operational quantum cryptographic networks.

Keywords: Moore's Law, quantum mechanics, wave, particle, spin, postulates of quantum mechanics, polarization, entanglement, quantum cryptography, quantum key distribution

10.Životopis

Kristijan Samardžija rođen je 16. Studenog 1990. godine u Slavonskom Brodu. Završio je osnovnu školu Josipa Kozarca u Kruševici. Nakon završetka petog razreda 28. lipnja 2002. godine je nagrađen za posebno zalaganje u prometnoj sekciji i odličan rezultat na prometnom natjecanju. Na kraju osnovne škole, 27. lipnja 2005. godine nagrađen je od strane Učiteljskog vijeća za odličan uspjeh tijekom osmogodišnjeg školovanja. Elektrotehničku i prometnu školu u Osijeku, smjer elektrotehničar upisuje 2005. godine. Elektrotehnički fakultet u Osijeku upisuje 2009. godine, smjer elektrotehnika. Na drugoj godini fakulteta, upisuje smjer Komunikacije i Informatika, a na trećoj godini piše završni rad pod nazivom „Pojačala snage s bipolarnim tranzistorima“. U rujnu 2012. godine postaje univ. bacc. ing. el. te upisuje diplomski studij Komunikacije i Informatika na Elektrotehničkom fakultetu u Osijeku.

Kristijan Samardžija

_____