Pregled stanja kvantne komunikacijske mreže u državama EU

Mihovljanec, Goran

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

Pregled stanja kvantne komunikacijske mreže u državama EU

Kolegij: Sigurnost i zaštita informacijsko komunikacijskog prometa

Mentor: prof. dr. sc. Dragan Peraković

Student: Goran Mihovljanec

JMBAG: 0135249822

Zagreb, rujan 2022.

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 7. lipnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**

Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 6983

Pristupnik: Goran Mihovljanec (0135249822)

Studij: Promet

Smjer: Informacijsko-komunikacijski promet

Zadatak: **Pregled stanja kvantne komunikacijske mreže u državama EU**

Opis zadatka:

U radu je potrebno opisati osnovne principe kvantne komunikacije i osnoven moguće arhitekture kvantnih komunikacijska mreža. Analizirate principe i izazove razmjena kvantnih ključeva. Prikaz razvijenost / rasprostranjenost kvantne komunikacije u Europi.

Mentor:

prof. dr. sc. Dragan Peraković

Predsjednik povjerenstva za diplomski ispit:

SAŽETAK

Sve većom digitalizacijom u svakodnevnom životu, raste i rizik od „curenja“ informacija do neovlaštenih korisnika. Razvijaju se različiti protokoli i principi kako bi te informacije, podatke zaštili u samom prijenosu od izvorišta do odredišta. Jedna od tih tehnologija je i kvantna komunikacija koja leži na temeljima kvantne fizike, odnosno mehanike i predviđa joj se blistava budućnost baš zbog činjenice da je nemoguće od strane neovlaštenog korisnika presresti informaciju u samom prijenosu.

Kvantna komunikacija je polje primijenjene kvantne fizike koje je usko povezano s kvantnom teleportacijom i kvantnom obradom informacija. Najzanimljivija primjena je zaštita informacijskih kanala od prisluškivanja neovlaštenog korisnika, a to se ostvaruje primjenom kvantne kriptografije. Najrazvijenija i najpoznatija primjena kvantne kriptografije je kvantna distribucija ključeva (QKD). Za obavljanje kriptografskih zadataka ili za razbijanje kriptografskih sustava QKD opisuje korištenje kvantno mehaničkih učinaka. Načelo rada QKD sustava prilično je jednostavno: dvije strane, odnosno pošiljatelj (Alice) i primatelj (Bob) koriste pojedinačne fotone koji su nasumično polarizirani u stanja koja predstavljaju bitove 0 i 1 za prijenos niza slučajnih brojeva koji se zatim koriste kao ključevi u kriptografskoj komunikaciji. Obje strane su međusobno povezane i klasičnim i kvantnim kanalom. Alice generira nasumični tok kubita koji se šalju preko kvantnog kanala. Kada se međusobno povežu kvantnim kanalom Bob i Alice — koristeći klasični kanal — izvode klasične operacije kako bi provjerili je li prisluškivač pokušao izvući informacije o prijenosu kubita. Prisutnost prisluškivača otkriva se nesavršenom međusobnom povezanošću između dvije liste bitova dobivenih nakon prijenosa kubita između pošiljatelja i primatelja. Jedna važna komponenta praktički svih ispravnih shema šifriranja je prava slučajnost koja se može bez ikakvih problema generirati pomoću kvantne optike. Područja primjene kvantne komunikacije nalaze se u bankarstvu, vladi, industriji, vojsci i sl.

Ključne riječi: foton, kvantna komunikacija, kvantna isprepletenost, kvantni protokol, QKD, EPR parovi, kvantna kriptografija, kvantna isprepletenost

SUMMARY

With increasing digitization in everyday life, the risk of information "leaking" to an unauthorized user also increases. Various protocols and principles are being developed in order to protect this information and data during the actual transfer from source to destination. One of these technologies is quantum communication, which is based on the foundations of quantum physics, that is, mechanics, and is predicted to have a bright future precisely because of the fact that it is impossible for an unauthorized user to intercept the information in the transmission itself.

Quantum communication is a field of applied quantum physics closely related to quantum teleportation and quantum information processing. The most interesting application is the protection of information channels from eavesdropping by an unauthorized user, and this is achieved by applying quantum cryptography. The most developed and well-known application of quantum cryptography is quantum key distribution (QKD). To perform cryptographic tasks or to break cryptographic systems, QKD describes the use of quantum mechanical effects. The working principle of the QKD system is quite simple: two parties, the sender (Alice) and the receiver (Bob) use individual photons that are randomly polarized in a state representing bits 0 and 1 to transmit a series of random numbers that are then used as keys in cryptographic communication. . Both parties are connected to each other by both classical and quantum channels. Alice generates a random stream of qubits that are sent over the quantum channel. When Bob and Alice communicate with each other over the quantum channel — using the classical channel — classical operations are performed to check whether the listener has tried to extract information about the qubit transfer. The presence of an eavesdropper is detected by the imperfect correlation between the two lists of bits obtained after the transmission of the qubit between the sender and the receiver. One important component of practical all-correct encryption schemes is true randomness, which can be easily generated using quantum optics. Applications of quantum communications are in banking, government, industry, military, etc.

Keywords: photon, quantum communication, quantum entanglement, quantum protocol, QKD, EPR pairs, quantum cryptography, quantum teleportation

SADRŽAJ

1. UVOD

Današnji Internet povezuje nas globalno. Šalje pakete informacija koje prenose našu komunikaciju u klasičnim signalima - šalju se bljeskovima svjetlosti kroz optička vlakna, električnim putem kroz bakrenu žicu ili mikrovalovima radi uspostavljanja bežičnih veza.

Prijetnja kibernetičkih napada tjera vlade, vojske i tvrtke da istraže sigurnije načine prijenosa informacija. Danas se osjetljivi podaci obično šifriraju i zatim šalju preko optičkih kabela i drugih kanala zajedno s digitalnim "ključevima" potrebnim za dekodiranje informacija. Podaci i ključevi šalju se kao klasični bitovi — tok električnih ili optičkih impulsa koji predstavljaju 1 i 0 i to ih čini ranjivima.

Obradom ove teme predstavlja se kvantna komunikacija kojom se danas garantira potpunosti siguran prijenos informacija putem kvantne komunikacijske mreže, a korištenjem određenih protokola i QKD tehnologije.

Naslov teme diplomskog rada je „Pregled stanja kvantne komunikacijske mreže u državama EU“, a cilj rada je prikazati funkcionalnosti i način rada kvantne komunikacijske mreže, prikazati njezinu arhitekturu i upoznati se s nekim praktičnim implementacijama ovog područja. Također, upoznaje se s osnovama kvantne komunikacije, uređajima i protokolima koji služe kako bi se ona ostvarila. Rad je podijeljen u 6 poglavlja:

1. Uvod
2. Osnove kvantne komunikacije
3. Kvantna komunikacijska mreža
4. Kvantna razmjena ključeva
5. Prikaz razvijenosti/ rasprostranjenosti kvantne komunikacije u Europi
6. Zaključak

U poglavlju „Osnove kvantne komunikacije“ objašnjeni su temeljni pojmovi na kojima kvantna komunikacija počiva. Kvantna teorija informacija, kvantni kanal kojem se odvija kvantna komunikacija, isprepletenost koja je jedan od najbitnijih faktora za sigurnost kvantnog sustava. Tijekom kodiranja i dekodiranja ključa za prijenos informacija koriste se Bellova stanja ili EPR parovi kojih se također dotiče

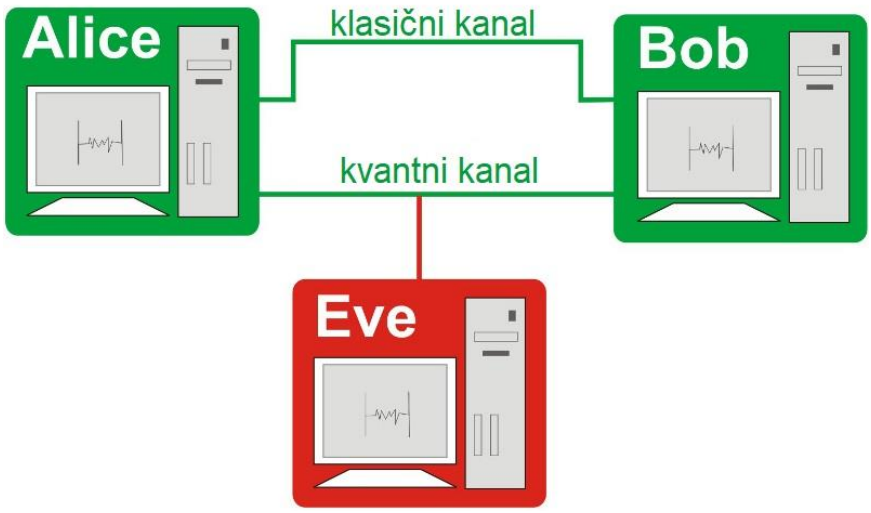
u ovom poglavlju. U sljedećem dijelu rada spominje se kvantna kriptografija i na koji način ona radi. Postoje određene bitne razlike u odnosu na klasičnu kriptografiju, a uz to naravno da postoje i određene prednosti i nedostaci sustava koji koriste kvantnu kriptografiju. Također su spomenuti neki od glavnih uređaja zaslužni za ostvarivanje komunikacije poput generatora kvantnih slučajnih brojeva, repetitora i jednofotonskog detektora, a uz njih je prikazan i primjer arhitekture kvantnog sustava na već postojeću infrastrukturu. Četvrto poglavlje donosi najvažniji dio kvantne komunikacije i njezine mreže, a to je kvantna razmjena ključeva (QKD). Koriste se dvije vrste sustava. Sustav s kontinuiranom i sustav s diskretnom varijablom. Postoje protokoli koji omogućuju prijenos informacija i podijeljeni su u dvije grupe koje su prikazane također ovim poglavljem. Sljedeće poglavlje prikazuje stanje kvantne mreže u Europi, odnosno njezinu rasprostranjenost i razvijenost. Dotiče se nekih od najvažnijih projekata i demonstracija i daje se uvid u blisku budućnost kvantne mreže u Europi.

2. OSNOVE KVANTNE KOMUNIKACIJE

Kvantna komunikacija je polje primijenjene kvantne fizike usko povezano s kvantnom obradom informacija i kvantnom teleportacijom. Njegova najzanimljivija primjena je zaštita informacijskih kanala od prisluškivanja pomoću kvantne kriptografije. Najpoznatija i najrazvijenija primjena kvantne kriptografije je kvantna distribucija ključeva (engl. QKD- Quantum Key Distribution). [1]

Kvantna komunikacija iskorištava zakone kvantne fizike za zaštitu informacija i podataka. Takvi zakoni dopuštaju česticama (obično fotonima[1]) svjetlosti koje služe za prijenos podataka duž optičkih kablova- da preuzmu stanje superpozicije[2], što znači da mogu predstavljati više kombinacija 1 i 0 istovremeno. Čestice su poznate kao kvantni bitovi ili kubiti. [2]

Kod kvantne komunikacije pošiljatelj i primatelj (u daljnjem tekstu Alice i Bob) povezani su i klasičnim i kvantnim kanalom kako je prikazano na slici 1.



Slika 1. Općeniti prikaz kvantne komunikacije između pošiljatelja i primatelja

Izvor: [1]

[1] svjetlosni kvant, kvant svjetlosti ili kvant elektromagnetskoga zračenja je osnovni djelić energije elektromagnetskoga zračenja, elementarna čestica koja je posrednik u prenošenju elektromagnetskoga međudjelovanja

[2] sposobnost kvantnog sustava da bude u više stanja u isto vrijeme dok se ne izmjeri

Izvrsnost kvantne komunikacije iz perspektive kibernetičke sigurnosti je u tome što neovlaštena strana (u daljnjem tekstu Eve) promatra kubite kojima se prenosi informacija, podatak samom prijenosu, gdje je njihovo kvantno stanje super-krhko te kolaborira na 1 ili 0. To znači da Eve ne može dirati u kubite a da za sobom ne ostaviti znak aktivnosti. Zbog takvih činjenica kvantna komunikacija je iznimno zanimljiva znanstvenicima za proučavanje i istraživanje.

2.1. Kvantna teorija informacija

Kvantna teorija informacija spaja ideje iz klasične teorije informacija, kvantne mehanike i računalne znanosti. Teoremi i tehnike raznih grana matematike i matematičke fizike, posebice teorije grupa, teorije vjerojatnosti i kvantne statističke fizike nalaze primjenu u ovom fascinantnom i brzorastućem području. [3]

U posljednje vrijeme povijesna je veza između informacija i fizike obnovljena, budući da su metode teorija informacija i računanja proširene na tretiranje prijenosa i obrade nepromijenjenih kvantnih stanja i interakcije takvih „kvantnih informacija“ s tradicionalnim „klasičnim“ informacijama. Iako su mnogi kvantni rezultati slični svojim klasičnim analogima, postoje značajne razlike. [4]

Kvantna teorija informacija, slično svom klasičnom dvojniku, proučava značenje i ograničenja komunikacije klasičnih i kvantnih informacija putem kvantnih kanala. U posljednjih nekoliko desetljeća klasična teorija informacija pružila je temelj za razvoj svoje kvantne analogije. Kvantna teorija informacija otkrila je posljedice za kvantni svijet koje se ne mogu predvidjeti njezinom klasičnom teorijom informacija. Unatoč tome, klasična teorija informacija pruža logičku strukturu za usklađeno uvođenje ideja kvantne teorije informacija. [3]

Kvantna informacija je informacija pohranjena u vrlo malim strukturama koje se nazivaju kubiti. Kubiti se mogu napraviti iz bilo kojeg kvantnog sustava koji ima dva stanja.

Središnja ideja je zamijeniti klasični bit, koji može poprimiti jednu od dvije vrijednosti, 0 ili 1, kvantnim dvorazinskim sustavom, opisanim u terminima dvaju ortonormiranih vektora stanja, $|0>$ i $|1>$ koji obuhvaćaju dvodimenzionalni Hilbertov

prostor[3] koji sadrži sve moguće linearne kombinacije, $a|0+b|1>$, gdje je $a, b\ \varepsilon\ C\ i\ |a|^2+b^2=1$. [5]

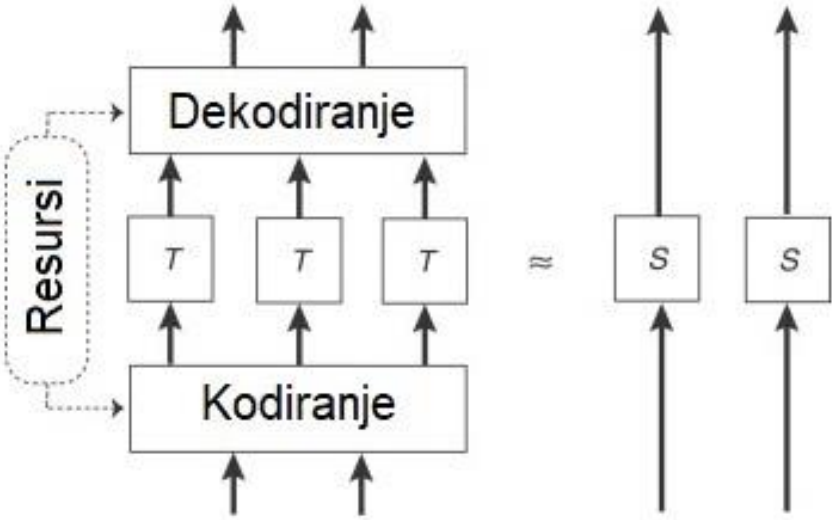
2.2. Kvantni kanal

Svaka obrada kvantnih informacija, bilo da se radi o pohranjivanju ili prijenosu, može se predstaviti kao kvantni kanal: potpuno pozitivan put koji čuva tragove koji pretvaraju stanja (matrice gustoće) na kraju kanala pošiljatelja, a u stanja na kraju primatelja. Vrlo često kanal „S“ koji bi pošiljatelj i primatelj (Alice i Bob) željeli implementirati nije lako dostupan, obično zbog štetnih učinaka šuma, ograničene tehnologije ili nedovoljnih novčanih sredstava . Oni tada mogu pokušati simulirati kanal „S“ s nekim drugim kanalom „T“, koji slučajno imaju na raspolaganju.

Kapacitet kvantnog kanala možemo prikazati kao Q(T, S). „T“ kanal u odnosu na „S“ kanal kvantificira koliko dobro se ova simulacija može izvesti, u ograničenju dugih ulaznih nizova, tako da Alice i Bob mogu iskoristiti zajedničku prednost prije i nakon obrade (slika 2.). Veći kapaciteti mogu rezultirati ako se Alice i Bobu dopusti korištenje dodatnih resursa u procesu, kao što su klasični sporedni kanali ili hrpa maksimalno isprepletenih parova koje dijele između sebe. [6]

Slika 2. prikazuje n=3 instance kanala „T“ koje simuliraju m=2 instance kanala „S“ opremljene zajedničkim operacijama kodiranja i dekodiranja (a možda i nekim pomoćnim resursima). Brzina prijenosa gornje sheme je 2/3. Kapacitet je najveća takva brzina, u granicama dugih poruka i optimalnog kodiranja i dekodiranja.

[3] unitarni prostor koji je potpuni metrički prostor s obzirom na metriku danu skalarnim kvadratom razlike vektora



Slika 2. Primjer prikaza principa funkcioniranja kapaciteta kvantnog kanala

Izvor: [6]

Kvantni kanal transformira ulazne sustave opisane Hilbertovim prostorom H_1 u izlazne sustave opisane Hilbertovim prostorom H_2. Za H_2 Hilbertov prostor se najčešće pretpostavlja da je identičan H_1. Matematički je predstavljen potpuno pozitivnom, unitarnom varijablom „T“ koja djeluje na faktor gustoće ρ kao:

$$T(\rho) = \sum_{j=1}^{n} E_j \, \rho \, E_j^{\dagger}$$

Ovdje E_j predstavljaju takozvane Krausovi operatore koji ispunjavaju:

$$\sum_{j} E_j^{\dagger} E_j < II$$

Kapacitet kanala kvantificira broj kubita koji se mogu vjerno prenijeti. Za idealan kanal imamo T = I, operacija identiteta.

Kanalni kapaciteti kvantnih kanala u potpunosti su razumljivi samo za posebne slučajeve. Na primjer, teorem Holevo-Schumacher-Westmoreland (HSW)[4] daje kapacitet kanala ako se koriste samo ulazna stanja proizvoda. [7]

2.3. Kvantna isprepletenost

U središtu kvantne komunikacije su informacije pohranjene u kubitima — kvantnom ekvivalentu bitova u običnim računalima — koji se mogu programirati da budu u superpoziciji '0' i '1'. Glavna svrha kvantne mreže je omogućiti da se kubiti na korisnikovom uređaju upletu s onima na tuđem. Ta isprepletenost ima mnoge potencijalne upotrebe, počevši od enkripcije: budući da su mjerenja na zapetljanim objektima uvijek međusobno povezana, učestalim čitanjem stanja njihovih kubita, korisnici mogu generirati tajni kod koji samo oni znaju. [8]

Osnovna usluga koju pružaju klasične mreže je prijenos podataka od pošiljatelja do primatelja. Temeljna usluga koju pružaju kvantne mreže, s druge strane, jest generiranje kvantne isprepletenosti između krajnjih točaka, koju zatim mogu koristiti aplikacije. U većini protokola i algoritama kvantnog umrežavanja ovo se isprepletanje generira korištenjem Bellovih stanja. [9]

Moguće je da se dvije čestice isprepleću tako da kada se određeno svojstvo izmjeri u jednoj čestici, trenutno će se uočiti suprotno stanje na isprepletenoj čestici. To vrijedi bez obzira na udaljenost između zapetljanih čestica. Nemoguće je, međutim, predvidjeti prije mjerenja kakvo će se stanje promatrati, stoga nije moguće komunicirati putem isprepletenih čestica bez rasprave o promatranju preko klasičnog kanala. Proces komuniciranja pomoću isprepletenih stanja, potpomognut klasičnim informacijskim kanalom, poznat je kao kvantna teleportacija i temelj je Ekertovog (E91) protokola. [10]

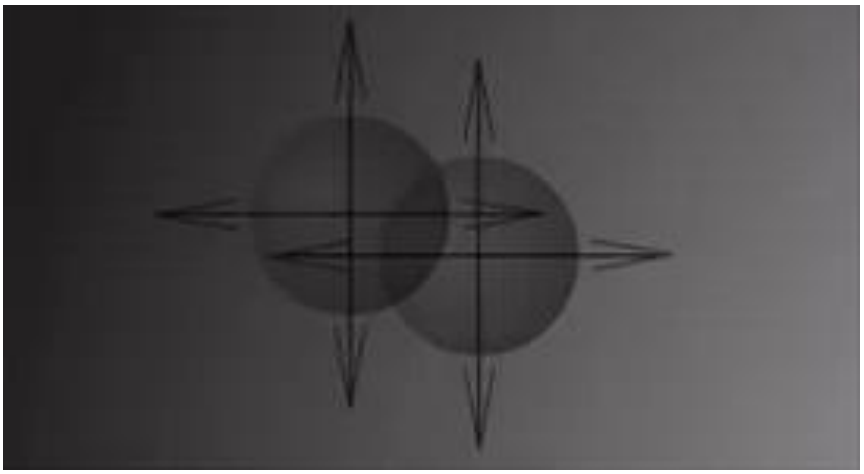
Kvantna isprepletenost je fenomen koji objašnjava kako dvije subatomske čestice mogu biti blisko povezane jedna s drugom čak i ako su odvojene milijardama

[4] Formula kapaciteta za isprepletena ulazna stanja i zajedničko mjerenje. Holevo granica postavlja gornju granicu koliko informacija može biti sadržano u kvantnom sustavu, koristeći određeni skup. Ustvari kaže da jedan kubit može sadržavati najviše jedan bit informacije.

svjetlosnih godina. Unatoč njihovoj velikoj razdvojenosti, promjena izazvana u jednom utjecat će na drugo.

Godine 1964. fizičar John Bell je pretpostavio da se takve promjene mogu inducirati i dogoditi trenutno, čak i ako su čestice jako udaljene. Bellov teorem smatra se važnom idejom u modernoj fizici, ali je u sukobu s drugim dobro utvrđenim principima fizike. Na primjer, Albert Einstein pokazao je godinama prije nego što je Bell iznio svoj teorem da informacije ne mogu putovati brže od brzine svjetlosti. Einstein je slavno opisao ovaj fenomen isprepletenosti kao "jezivu akciju na daljinu". [11]

Isprepleteni fotonski parovi važni su za realizaciju kvantne komunikacije i kvantnog računanja [12]. Na slici 3. je grafički prikazan foton koji je razdvojen na dva međusobno isprepletena fotona.



Slika 3. Foton razdvojen na dva međusobno isprepletena fotona, [13]

Pravila kvantne fizike kažu da neopaženi foton postoji u svim mogućim stanjima istovremeno, ali kada se promatra ili mjeri, pokazuje samo jedno stanje. Spin je ovdje prikazan kao os rotacije, ali stvarne čestice ne rotiraju. Isprepletanje se događa kada par čestica, poput fotona, fizički međusobno djeluju. Laserska zraka ispaljena kroz određenu vrstu kristala može uzrokovati razdvajanje pojedinačnih fotona u parove isprepletenih fotona. Fotoni mogu biti razdvojeni velikom udaljenošću (kako je predočeno slikom 4.), stotinama milja ili čak i više.

Slika 4. Prikaz fotona na velikoj udaljenosti, [13]

Kako je prikazan slikom 5., kada se promatra, foton A poprima stanje uzlazne vrtnje. Isprepleteni foton B, iako sada daleko, zauzima stanje u odnosu na foton A (u ovom slučaju, stanje vrtnje prema dolje). Prijenos stanja između fotona A i fotona B odvija se brzinom od najmanje 10 000 puta većom od brzine svjetlosti, moguće čak i trenutno, bez obzira na udaljenost.

Slika 5. Promatranje stanja dva fotona ovisna jedna o drugome, [13]

Još jedna od važnijih stvari povezanih s kvantom isprepletenošću je tzv. EPR paradoks. Godine 1935. Einstein i još dva fizičara u Sjedinjenim Državama, Boris Podolsky i Nathan Rosen, analizirali su misaoni eksperiment za mjerenje položaja i momenta u paru sustava koji međusobno djeluju. Koristeći konvencionalnu kvantnu mehaniku, dobili su neke zapanjujuće rezultate, koji su ih doveli do zaključka da teorija ne daje potpuni opis fizičke stvarnosti. Zajedno sa svojim kolegama Borisom Podolskim i Nathanom Rosenom, Einstein je razvio EPR paradoks kao način da pokaže da teorija nije u skladu s drugim poznatim zakonima fizike.

Cilj ovoj eksperimenta bilo je demonstrirati inherentni paradoks u ranim formulacijama kvantne teorije. To je jedan od najpoznatijih primjera kvantne isprepletenosti. Paradoks uključuje dvije čestice koje su isprepletene jedna s drugom prema kvantnoj mehanici. Prema kopenhaškoj interpretaciji kvantne mehanike, svaka je čestica pojedinačno u neizvjesnom stanju dok se ne izmjeri, a tada stanje te čestice postaje izvjesno. U tom točno istom trenutku stanje druge čestice također postaje sigurno. Razlog zašto je ovo klasificirano kao paradoks je taj što naizgled uključuje

komunikaciju između dviju čestica brzinama većim od brzine svjetlosti, što je u sukobu s teorijom relativnosti. Paradoks Einsteina, Podolskog i Rosena bio je istaknut kao argument da kvantna mehanika ne može biti potpuna teorija, već da je treba nadopuniti dodatnim varijablama.

2.4. Bellova stanja (EPR parovi)

Izraz „Bellova stanja“ ili „EPR parovi“ zapravo opisuje jedno od četiri isprepletena kvantna stanja para kubita, poznata pod zajedničkim nazivom četiri "Bell stanja".

Dva Bellova stanja daju jednaku superpoziciju tako da oba kubita završe u istom stanju kada se mjere, s 50% šanse da će oba biti ili u $|0\rangle$ ili u $|1\rangle$ stanju. Druga dva Bellova para daju jednaku superpoziciju tako da oba kubita završavaju u suprotnim stanjima kada se mjere. To znači da ako se prvi kubit mjeri u $|0\rangle$ tada će se drugi kubit mjeriti u $|1\rangle$ i obrnuto.

Simbol Bellovom stanja	**Matematički prikaz**
$\|\Phi^+\rangle$	$\frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$
$\|\Phi^-\rangle$	$\frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$
$\|\Psi^+\rangle$	$\frac{\|01\rangle + \|10\rangle}{\sqrt{2}}$
$\|\Psi^-\rangle$	$\frac{\|01\rangle - \|10\rangle}{\sqrt{2}}$

Tablica 1. Prikaz simbola Bellovog stanja i pridruženog matematičkog prikaza

Izvor: [14]

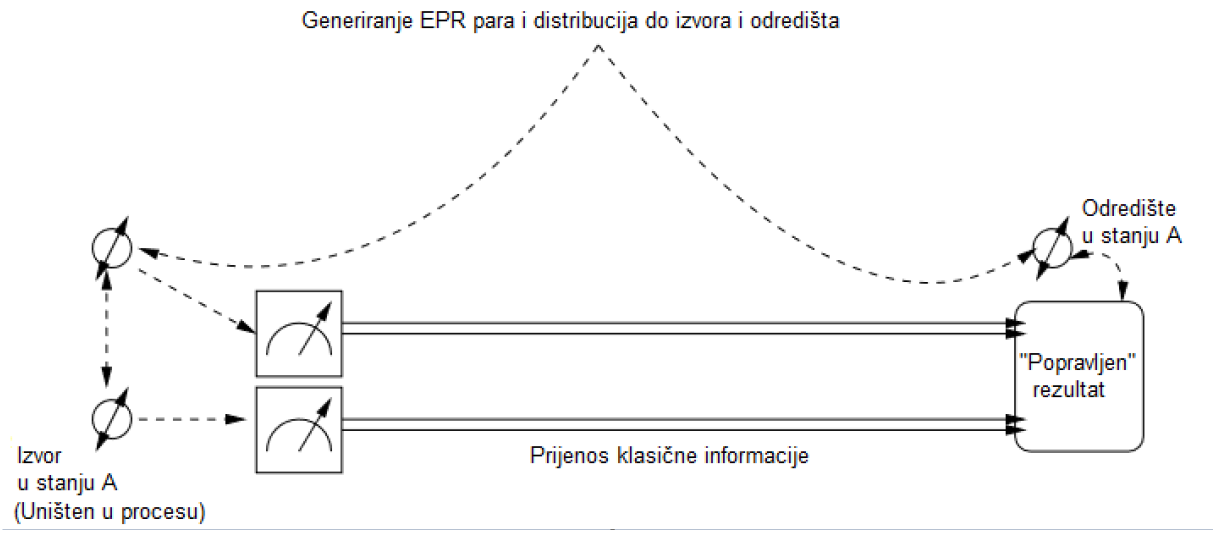
U svakom od Bellovih parova, ako se izmjeri jedan od dva kubita, tada točno znamo što će biti drugi kubit kada se izmjeri. Ako se razmotri jedan od $|\Phi^+\rangle$ ili $|\Phi^-\rangle$ stanja kao što je prikazano tablicom 1. može se zaključiti da su to dva Bellova para kod kojih oba kubita moraju završiti u istom stanju kada se mjere. Ako se mjeri prvi kubit u stanju $|0\rangle$ znamo da i drugi kubit mora biti u istom stanju bez obzira ako su kubiti na beskonačnoj udaljenosti ili ako ih mjerimo odmah tik jedan nakon drugog, oba kubita moraju biti u stanju $|0\rangle$. [14]

Bellova stanja prilično su jednostavan primjer isprepletenosti, ali se usprkos tome široko koriste i u teoretskom i u eksperimentalnom radu. Za brojne primjene korisno je razmotriti moguće generalizacije Bellovih stanja. Značajna količina rada u ovom smjeru koncentrirana je na istraživanje isprepletenosti između nekoliko kubita, jer je ovaj pristup vrlo prirodan za određene primjene kao što je kvantno računanje. [15]

2.5. Kvantna teleportacija

Kvantna teleportacija, kao jedno od važnih polja u istraživanju kvantne komunikacije, igra važnu ulogu u području kvantnog računanja i kvantne komunikacije. Kvantna teleportacija je tehnika za prijenos kvantnih informacija od izvora do odredišta korištenjem isprepletenih stanja. [16]

Kvantna teleportacija je način da se stanje jednog kubita zamijeni stanjem drugog. Ime izvan ovog svijeta dobio je po činjenici da se stanje "prenosi" postavljanjem isprepletenog prostora stanja od tri kubita i zatim uklanjanjem dva kubita iz isprepletenosti (putem mjerenja). Budući da su informacije izvornog kubita sačuvane ovim mjerenjima, te "informacije" (tj. stanje) završavaju u posljednjem trećem, odredišnom kubitu. To se, međutim, događa bez izravne interakcije izvornog (prvog) i odredišnog (trećeg) kubita. Interakcija se događa putem ispreplitanja. Slika 6. prikazuje postavku za kvantnu teleportaciju.



Slika 6. Postavka za kvantnu teleportaciju

Izvor: [17]

Teleportacija na početku zahtijeva slanje EPR para do izvora i do odredišta. Kubit koji sadrži stanje koje treba "teleportirati" tada stupa u interakciju s jednom polovicom EPR para, stvarajući zajednički prostor stanja. Jedinice se izvode u ovom zajedničkom prostoru stanja, a zatim se mjere ta dva kubita. Rezultirajuća klasična informacija o ishodu mjerenja prenosi se na odredište. Ove klasične informacije koriste se za "popravljanje" odredišnog kubita s pojedinačnim kubitima. [17]

Teleportacija i kvantna komunikacija koju ona omogućuje jedna je od temeljnih primjena mreža „Entanglement as a Service (EaaS). Dok je cilj klasičnih mreža distribucija informacija, cilj kvantnih mreža je distribucija isprepletenosti. Kvantna teleportacija je protokol koji omogućuje korištenje te isprepletenosti za prijenos kvantnih stanja. [14]

Pretpostavimo da je jedan promatrač, Alice, dobio kvantni sustav kao što je foton ili čestica spina 1/2, pripremljen u njoj nepoznatom stanju |Ø>, i ona želi komunicirati s drugim promatraču, Bobom, s dovoljnim brojem informacija o kvantnom sustavu da bi mogla napraviti njegovu točnu kopiju. Poznavanje samog vektora stanja |Ø> bila bi dovoljna informacija, ali općenito ne postoji način da se to može učiniti tako. Samo ako Alice unaprijed zna da |Ø> pripada danom ortonormiranom skupu, može napraviti mjerenje čiji će joj rezultat omogućiti da napravi točnu kopiju |Ø>. Nasuprot

tome, ako mogućnosti za |Ø> uključuju dva ili više neortogonalnih stanja, tada nijedno mjerenje neće dati dovoljno informacija za pripremu savršeno točne kopije.

Trivijalan način da Alice pruži Bobu sve informacije u |Ø> bio bi da pošalje samu česticu. Ako želi izbjeći prijenos izvorne čestice, može je učiniti jedinstvenom interakcijom s drugim sustavom „ancilla“, koji je u početku u poznatom stanju $|\alpha_0>$, na takav način da nakon interakcije izvorna čestica ostane u standardnom stanju $|Ø_0>$ a ancilla je u nepoznatom stanju |α> koji sadrži potpune podatke o |Ø>. Ako Alice sada pošalje Bobu ancillu (možda tehnički lakše od slanja izvorne čestice), Bob može poništiti njezine radnje kako bi pripremio repliku njezinog izvornog stanja |Ø>. Ovo "mjerenje izmjene spina" ilustrira bitnu značajku kvantne informacije: ona se može mijenjati iz jednog sustava u drugi, ali se ne može duplicirati ili "klonirati". U tom smislu je prilično različita od klasičnih informacija, koje se mogu duplicirati po želji.

Najopipljivija manifestacija neklasičnosti kvantne informacije je kršenje Bellovih nejednakosti opaženo u eksperimentima na EPR stanjima. Druge manifestacije uključuju mogućnost kvantne kriptografije kvantno paralelno računanje, te superiornost interaktivnih mjerenja za izvlačenje informacija iz para identično pripremljenih čestica. [18]

2.6. Kvantna memorija

Baš kao što su klasična računala nezamisliva bez memorije, kvantna memorija će biti bitni elementi za buduće kvantne informacijske procesore. Kvantna memorija za svjetlost proučavaju se osobito aktivno u kontekstu kvantne komunikacije za implementaciju kvantnih repetitora. Područje kvantne memorije nedavno je doživjelo velik napredak, s npr. postignuća vrlo dugih vremena pohranjivanja, visoke učinkovitosti, različiti eksperimenti koji uključuju isprepletenost i realizacija vrlo multimodnih memorija. [19]

Kvantne memorije su uređaji koji mogu pohraniti kvantno stanje fotona, bez uništavanja nepostojane kvantne informacije koju nosi foton. Kvantna memorija trebala bi moći otpustiti foton s istim kvantnim stanjem kao i pohranjeni foton, nakon vremena koje je postavio korisnik. Kvantna sjećanja zahtijevaju koherentne sustave materije, inače će kvantne informacije pohranjene unutar medija biti izgubljene zbog dekoherencije. Također vjerujemo da bi se svaki praktični uređaj trebao temeljiti na materijalima u čvrstom stanju. [20]

Kvantna memorija ključna je za razvoj mnogih uređaja u kvantnoj obradi informacija, uključujući alat za sinkronizaciju koji povezuje različite procese unutar kvantnog računala, kvantna vrata identiteta koja ostavljaju nepromijenjena bilo koje stanje i mehanizam za pretvaranje najavljenih fotona u fotone na zahtjev . Uz kvantno računalstvo, kvantna memorija bit će instrumentalna za implementaciju kvantne komunikacije na velike udaljenosti pomoću kvantnih repetitora. Važnost ovih osnovnih kvantnih vrata ilustrirana je mnoštvom mehanizama optičke kvantne memorije koji se proučavaju, kao što su optičke linije kašnjenja, šupljine i elektromagnetski inducirana prozirnost. [21]

3. KVANTNA KOMUNIKACIJSKA MREŽA

Kvantne mreže prenose kvantne podatke, obično pohranjene u obliku pojedinačnih fotona [14]. Koriste kvantna svojstva fotona za kodiranje informacija. Na primjer, fotoni polarizirani u jednom smjeru (npr. u smjeru koji bi im omogućio prolaz kroz polarizirane sunčane naočale) povezani su s vrijednošću „1“, a fotoni polarizirani u suprotnom smjeru (tako da ne prolaze kroz sunčane naočale) povezani su s vrijednošću „0“. Istraživači razvijaju kvantne komunikacijske protokole kako bi formalizirali te asocijacije, dopuštajući kvantnom stanju fotona da prenosi informacije od pošiljatelja do primatelja kroz kvantnu mrežu.

Kvantne mreže iskorištavaju snagu kvantne mehanike, čudna fizička svojstva koja se pojavljuju samo na vrlo malim razinama - poput pojedinačnih čestica. Koristeći pojedinačne fotone, kvantne mreže mogu stvoriti isprepletena kvantna stanja diljem svijeta. [22]

Kvantne mreže koriste jedinstvene kvantne fenomene, poput superpozicije, zabrane kloniranja i isprepletenosti koji nisu dostupni klasičnim mrežama. Prije nego što se foton izmjeri, on postoji u superpoziciji svih svojih mogućih kvantnih stanja, od kojih svako ima odgovarajuću vjerojatnost. Mjerenje odabire jedno od tih stanja.

Zapravo, kvantno stanje fotona ne može se izmjeriti bez izazivanja poremećaja koji uzrokuje pokušaj. Niti se može kopirati proizvoljno, nepoznato kvantno stanje – teorem o zabrani kloniranja. Pravilno projektirana i korištena kvantna mreža izvlači inherentnu sigurnost iz ovog ponašanja. [23]

Kubiti, isprepletenost i kvantni repetitori čine neke od sastavnih dijelova funkcioniranja kvantnih mreža. Kvantne mreže mogu omogućiti ultrasigurnu komunikaciju temeljenu na fizici, snažnija kvantna računala i bolje kvantne senzore. [22]

3.1. Kvantna kriptografija

Kriptografija je proces šifriranja i zaštite podataka tako da ih samo osoba koja ima pravi tajni ključ može dešifrirati. Kvantna kriptografija razlikuje se od tradicionalnih kriptografskih sustava po tome što se oslanja na fiziku, a ne na matematiku, kao ključni aspekt svog sigurnosnog modela. Kvantna kriptografija temelji se na fenomenu kvantne fizike koji omogućuje siguran prijenos podataka između pošiljatelja i primatelja. Predstavlja revoluciju u području mrežne sigurnosti. Najnovija je i napredna grana kriptografije čija osnova leži u dvama uvjerenjima kvantnih tehnikalija: Heisenbergovom načelu neodređenosti i principu polarizacije fotona. [25] [26]

Kvantna kriptografija vjerojatno je najbrže rastuće područje u kvantnoj informacijskoj znanosti. Redovito se osmišljavaju novi teorijski protokoli, sigurnosni dokazi se neprestano poboljšavaju, a eksperimenti se postupno kreću od laboratorijskih demonstracija novih mogućnosti do implementacija na terenu i tehnoloških prototipa. [27]

Kvantna kriptografija je metoda enkripcije koja koristi prirodna svojstva kvantne mehanike za osiguranje i prijenos podataka koji se ne može hakirati. To je sustav koji je potpuno siguran protiv kompromitiranja bez znanja pošiljatelja ili primatelja poruke. To jest, nemoguće je kopirati ili vidjeti podatke kodirane u kvantnom stanju bez da se pošiljatelj ili primatelj ne upozore. Kvantna kriptografija također bi trebala ostati sigurna od onih koji koriste kvantno računalstvo.

Kvantna kriptografija koristi pojedinačne čestice svjetlosti ili fotone za prijenos podataka putem optičke žice. Fotoni predstavljaju binarne bitove. Sigurnost sustava oslanja se na kvantnu mehaniku. Ova sigurna svojstva uključuju sljedeće:

- čestice mogu postojati na više od jednog mjesta ili stanja u isto vrijeme,
- kvantno svojstvo ne može se promatrati a da se ono ne promijeni ili ne poremeti i
- cijele se čestice ne mogu kopirati

Ova svojstva onemogućuju mjerenje kvantnog stanja bilo kojeg sustava bez ometanja tog sustava.

Fotoni se koriste za kvantnu kriptografiju jer nude sve potrebne kvalitete: njihovo ponašanje je dobro poznato i oni su prijenosnici informacija u kabelima s optičkim vlaknima. Jedan od trenutno najpoznatijih primjera kvantne kriptografije je kvantna distribucija ključeva (QKD), koja pruža sigurnu metodu za razmjenu ključeva, a detaljno je interpretirana u sljedećem poglavlju. [24]

Kvantna kriptografija također se može pokazati korisnom za zaštitu privatnih informacija dok se koristi za donošenje javnih odluka. Klasičan primjer takvog diskretnog donošenja odluka je "problem spojeva", u kojem dvoje samaca traže način da izađu na spoj samo ako se jedan sviđa drugome, bez otkrivanja ikakvih daljnjih informacija. Na primjer, ako se Bobu sviđa Alice, ali se Alice ne sviđa Bob, spoj treba otkazati a da Alice ne sazna da se ona sviđa Bobu (s druge strane, logično je da će Bob saznati da se on ne sviđa Alice jer spoja na kraju neće biti. [27]

3.1.1. Razlika između klasične i kvantne kriptografije

Glavna razlika između kvantne kriptografije i klasične kriptografije je u tome što kvantni protokoli za distribuciju ključeva (QKDPs) koriste kvantnu mehaniku za distribuciju ključeva sesije i javne rasprave za provjeru prisluškivača i provjeru ispravnosti ključa sesije. U slučaju javne rasprave potrebni su dodatni krugovi komunikacije između pošiljatelja i primatelja, dok klasični kriptografski pristup ima učinkovitije tehnike za provjeru ključa i autentifikaciju korisnika.

Klasični oblik kriptografije je proces matematičkog kodiranja podataka, gdje ih samo jedna osoba koja ima pristup pravom ključu može pročitati. Cjelovitost podataka, autentifikacija, neporicanje i povjerljivost podataka neki su od osnovnih alata moderne kriptografije. Slučaj upotrebe moderne kriptografije ili klasične kriptografije je e-trgovina, automatizirani bankomati, računalne lozinke i mnoge druge važne aplikacije.

Tradicionalna kriptografija ima dvije različite vrste distribucije ključeva: simetrični ključ i asimetrični ključ. Algoritmi simetričnog ključa rade pomoću jednog ključa za šifriranje i dešifriranje informacija, dok asimetrična kriptografija koristi dva ključa -- javni ključ za šifriranje poruka i privatni ključ za njihovo dekodiranje.

Tradicionalnim kriptografskim metodama se vjeruje jer bi klasičnim računalima bio potreban neprihvatljiv vremenski okvir za generiranje potrebnih velikih brojeva koji čine javne i privatne ključeve.

Klasična kriptografija je u osnovi pretvaranje običnog teksta u neki kodirani tekst pomoću različitih algoritama strojnog učenja. Ključevi koji se koriste za dekodiranje podataka dijele se između pošiljatelja i primatelja kako bi mogli šifrirati ili dešifrirati poruku. [24] [25]

Klasična kriptografija	**Kvantna kriptografija**
koristi logiku temeljenu na digitalnoj logici	temelji se na kvantnoj teoriji
šalje digitalne signale pomoću bitova	šalje podatke pomoću čestica ili fotona
raspon ne ovisi o infrastrukturi	Raspon ovisi o infrastrukturi
šifriranje se temelji na matematičkim algoritmima	šifriranje se temelji na kvantnim svojstvima

Tablica 2. Usporedba klasične i kvantne kriptografije

Izvor: [24]

Kako je prikazano u tablici 2., za razliku od tradicionalne kriptografije koja se temelji na matematici, kvantna kriptografija temelji se na zakonima kvantne mehanike. I dok se tradicionalna kriptografija temelji na matematičkom izračunu, kvantnu kriptografiju je mnogo teže dešifrirati budući da i najsitniji čin promatranja uključenih fotona mijenja očekivani ishod istih, čineći i pošiljatelja i primatelja svjesnima prisutnosti prisluškivača. Kvantna kriptografija također obično ima povezanu infrastrukturu budući da proces zahtijeva optičke kabele i repetitore na određenim međusobnim razmacima kako bi pojačali signal. [24]

3.1.2. Način rada kvantne kriptografije

Kvantna kriptografija koristi seriju fotona (svjetlosnih čestica) za prijenos podataka s jedne lokacije na drugu preko optičkog kabela. Uspoređujući mjerenja svojstava frakcije tih fotona, dvije krajnje točke mogu prepoznati ključ i je li on siguran za upotrebu. [28]

Model pretpostavlja da postoje dvije osobe po imenu Alice i Bob koje žele sigurno razmijeniti poruku. Alice inicira poruku šaljući Bobu ključ. Ključ je tok fotona koji putuju u jednom smjeru. Svaki foton predstavlja jedan bit podataka -- bilo 0 ili 1. Međutim, osim svog linearnog putovanja, ti fotoni osciliraju ili vibriraju na određeni način. [26]

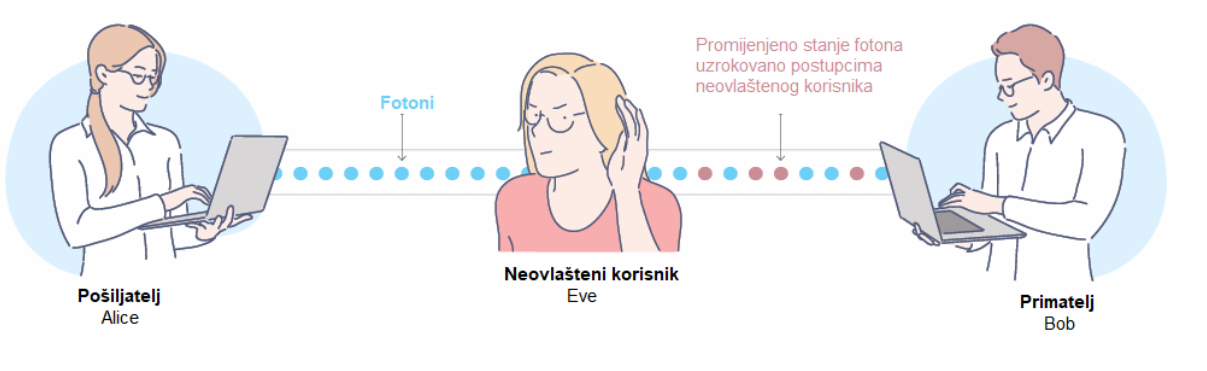
Alice šalje fotone kroz filter (ili polarizator) koji im nasumično daje jednu od četiri moguće polarizacije i bitne oznake:

a) okomito (1),
b) vodoravno (0),
c) 45 stupnjeva desno (1) ili
d) 45 stupnjeva lijevo (0)

Fotoni sada putuju optičkim vlaknom od polarizatora prema prijemniku, Bobu. Ovaj proces koristi razdjelnik snopa koji očitava polarizaciju svakog fotona. Prilikom primanja fotonskog ključa, Bob ne zna točnu polarizaciju fotona, pa se nasumično odabire jedna polarizacija. Alice sada uspoređuje što je Bob upotrijebio za polarizaciju ključa i zatim daje Bobu do znanja koji je polarizator koristila za slanje pojedinog fotona. Bob zatim potvrđuje je li upotrijebio ispravan polarizator. Fotoni očitani s pogrešnim razdjelnikom tada se odbacuju, a preostali niz se smatra ključem. [28]

Pretpostavimo da je prisutan neovlašteni korisnik po imenu Eve kao što je prikazano slikom 7. Eve pokušava dohvatiti komunikaciju između Alice i Bob i ima iste alate kao i Bob. Međutim, Bob ima prednost razgovora s Alice kako bi potvrdio koji je tip polarizatora korišten za svaki foton, a Eve nema tu mogućnost. Eve na kraju dohvaća neispravan konačni ključ. Alice i Bob bi također znali je li ih Eve prisluškivala

jer dok bi Eve promatrala tok fotona promijenila bi položaje fotona koje Alice i Bob očekuju vidjeti. [24]



Slika 7. Primjer promjene stanja fotona u slučaju prisluškivanja od strane neovlaštenog korisnika

Izvor: [24]

3.1.3. Prednosti kvantne kriptografije

Prednosti koje dolaze s kvantnom kriptografijom uključuju sljedeće:

- Omogućuje sigurnu komunikaciju- umjesto brojeva koje je teško probiti, kvantna kriptografija temelji se na zakonima fizike, što je sofisticiranija i sigurnija metoda šifriranja.
- Jednostavna za uporabu
- Performanse takvih kriptografskih sustava kontinuirano se poboljšavaju. To rezultira njegovim brzim usvajanjem u šifriranju najvrjednijih podataka vlade i industrije.
- Koristi se za otkrivanje prisluškivanja u QKD (engl. Quantum Key Distribution). To je zbog činjenice da nije moguće kopirati podatke kodirane u kvantnom stanju. Ako netko pokuša pročitati tako kodirane podatke, kvantno stanje mijenja postojeće stanje.
- Nudi više metoda za sigurnost- koriste se brojni protokoli kvantne kriptografije. Neki od njih mogu se kombinirati s klasičnim metodama šifriranja za povećanje sigurnosti. [24] [29]

3.1.4. Nedostaci kvantne kriptografije

Potencijalni nedostaci i ograničenja koja dolaze s kvantnom kriptografijom uključuju sljedeće:

- Tijekom putovanja kroz kanal (tj. optičko vlakno ili zrak), postoji mogućnost promjene polarizacije fotona zbog raznih uzroka.
- Raspon- maksimalni domet kvantne kriptografije obično je oko 400 do 500 km, s izuzetcima poput Terra Quantum- a
- Svjetska primjena može zauzeti mnogo radnih mjesta i stoga će se povećati nezaposlenost.
- Trošak- kvantna kriptografija obično zahtijeva vlastitu infrastrukturu, korištenjem optičkih linija i repetitora.
- Broj odredišta- nije moguće poslati ključeve na dvije ili više lokacija u kvantnom kanalu.
- Kvantnoj kriptografiji nedostaju mnoge vitalne značajke kao što su digitalni potpis, ovjerena elektronička pošta itd. [24] [29]

3.2. Generatori kvantnog slučajnog broja (QRNG)

Slučajni brojevi igraju ključnu ulogu u različitim primjenama, kao što su sigurne komunikacije, stohastičko modeliranje, kockanje, Monte Carlo simulacije i opsežna obrada podataka. Za razliku od pseudoslučajnih brojeva koji se generiraju računalnim algoritmima, pravi slučajni brojevi generiraju se fizičkim procesima. Slučajnost se smatra "istinitom" ako je dokaziva informacijskom teorijom. Fizički generatori slučajnih brojeva oslanjaju se na fizičke procese za koje se vjeruje da su slučajni, kao što su elektronički i toplinski šum, pojačana spontana emisija i kaotični poluvodički laseri. [30]

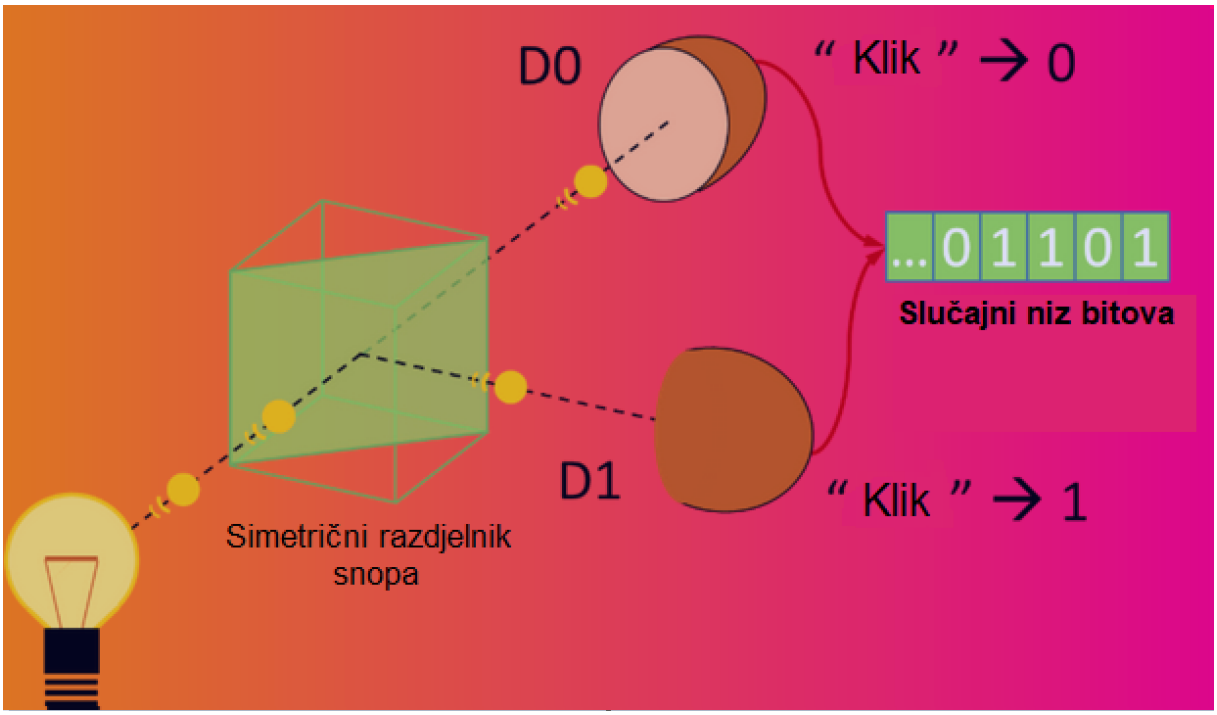
Kvantni generatori slučajnih brojeva (engl. Quantum Random Number Generators (QRNG)) su podskup fizičkih generatora slučajnih brojeva koji izvode slučajnost iz kvantno mehaničkih procesa i događaja. Probabilistička priroda kvantne mehanike čini QRNG preferiranim izvorom za generiranje pravih slučajnih brojeva. QRNG generiraju slučajnost mjerenjem kvantnih procesa, koji su po prirodi

nedeterministički. Prednosti su višestruke, uključujući temeljnu prednost u korištenju kvantne neodređenosti, obično brže performanse korištenjem fotonike i što je najvažnije, sposobnost razumijevanja i provjere podrijetla nepredvidivosti, što je ključno jamstvo za cijeli lanac kibernetičke sigurnosti.

Od QRNG-a se očekuje da proizvede nekorelirane i ravnomjerno distribuirane tokove nasumičnih podataka i obično se sastoji od izvornog bloka kvantne entropije i bloka za naknadnu obradu. Entropijski izvor je fizički sustav koji generira nasumične fizičke varijable, koje se nazivaju neobrađeni podaci, i očitava ih pomoću opreme za mjerenje i otkrivanje. U izvoru entropije priprema se kvantno stanje kako bi se osigurala prava slučajnost i mjeri kako bi se generirali neobrađeni slučajni podaci. U fazi naknadne obrade vrši se procjena stupnja slučajnosti neobrađenih podataka putem autokorelacije i procjene minimalne entropije, koja je mjera slučajnosti neobrađenih podataka koja se može izdvojiti. Procijenjena minimalna entropija djeluje kao ulaz u algoritme za izdvajanje slučajnosti i hardver koji daje gotovo stvarne slučajne brojeve. Izdvojeni stvarni slučajni brojevi podvrgavaju se testovima slučajnosti, poput onih koje je definirao Nacionalni institut za standarde i tehnologiju (NIST); takozvani DIEHARD testovi, koji se odnose na naširoko korišten skup metoda sastavljanja i kombiniranja uniformnih nasumičnih brojeva, a zatim na izvođenje statističkih testova. [30,31]

QRNG-ovi izvlače svoje slučajne brojeve iz inherentno indeterminističkih kvantnih procesa. Nemogućnost predviđanja brojeva ne temelji se samo na složenosti, već je u načelu nemoguće predvidjeti nasumične brojeve koje proizvode QRNG-ovi – moglo bi se reći da čak ni priroda ne poznaje te nasumične brojeve prije nego što se proizvedu. Slika 8. prikazuje prototip QRNG. Foton nailazi na simetrični razdjelnik snopa i nakon razdjelnika snopa nalazi se u kvantnomehaničkoj superpoziciji "transmisije" i "reflektiranja". Na kraju, jedan od detektora D0 i D1 (također se odabiru slučajno) detektira ga i proizvodi slučajni bit.

QRNG-ovi imaju mnoge prednosti: iskorištavanje objektivne slučajnosti prirode i relativno jednostavno načelo funkcioniranja. Stoga je moguće izraditi realan fizički model QRNG-a koji može biti temelj za certificiranje proizvedenih slučajnih brojeva. QRNG ima visoku otpornost na napade i obično je naknadna obrada (izdvajanje slučajnosti) konceptualno jednostavna. Međutim, izazovno je napraviti mali i jeftini ili stvarno brzi QRNG. [32]



Slika 8. Prototip QRNG-a

Izvor: [32]

3.3. Kvantni repetitori

Distribucija kvantnih resursa kao što su isprepletenost i kubiti preko mreža optičkih vlakana na velike udaljenosti predstavlja ogroman izazov. Ako se pošalju pojedinačni fotoni preko 1000 km, čak i pri brzinama od 10 GHz, moralo bi se čekati stotine godina da se otkrije samo jedan, zbog gubitka u vlaknu što nikako nije praktično. Moderne telekomunikacije nadilaze ovaj problem s pojačalima koja usput pojačavaju signal. Međutim, to bi u ovom slučaju uništilo kvantne karakteristike fotona kao što je isprepletenost. Čak ni u načelu, te se kvantne informacije ne mogu kopirati - to nazivamo teorem zabrane kloniranja Stoga je potreban kvantni pristup za prevladavanje gubitaka u prijenosu - kvantni repetitor. [33]

Kvantni repetitori su uređaji zamišljeni da prošire isprepletenost preko prostora, unatoč temeljnim ograničenjima teorema o zabrani kloniranja. Njihova je svrha izazvati isprepletanje na osnovnoj razini preko fizičke veze i spajanje zapetljanih veza duž putanje od kraja do kraja. Postoje dvije alternativne metode za stvaranje kvantnih

repetitora: pristup čvrstog stanja, temeljen na statičkoj memoriji međuspremnika; i potpuno optički pristup, bez statičke memorije međuspremnika. [30]

Mnogo je izazova s kojima se suočava razvoj kvantnih repetitora budući da su to složeni sustavi koji zahtijevaju mnogo složenih kvantnih (i klasičnih) uređaja i podsustava kako bi funkcionirali na najvišim razinama performansi. Usprkos tome, posljednjih je godina značajan napredak iz inženjerske perspektive, ali i s novim pristupima. Kako se izvedba ovih sustava nastavlja poboljšavati, oni će također moći iskoristiti prednosti razvoja u QKD-u i osigurati kvantnu komunikaciju općenito, u smislu njihove integracije u standardne mreže optičkih vlakana. Čak i pored prednosti za osiguranje europske digitalne infrastrukture, pojavljuje se sve veći broj aplikacija koje pružaju viziju budućeg kvantnog Interneta. [33]

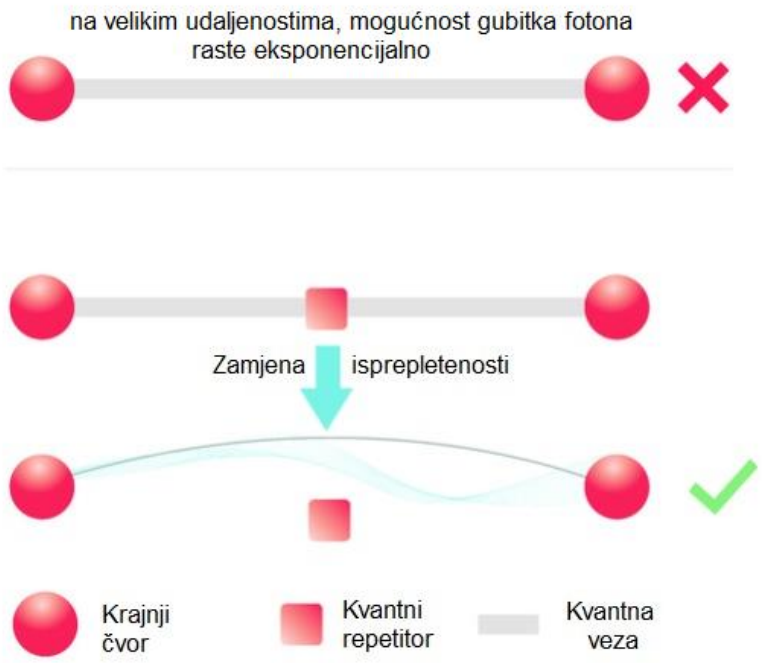
Unatoč svom nazivu, kvantni repetitori zapravo koriste vrlo različitu strategiju od klasičnih repetitora za rješavanje problema gubitka. Opća ideja temelji se na tehnici zamjene isprepletenosti. Primarni cilj kvantnih mreža je raspodijeliti isprepletenost između korisnika u mreži. Distribucija isprepletenosti otključava sve vrste aplikacija, uključujući čak i prijenos kubita. Zamjena isprepletenosti je pametna ideja koja zaobilazi problem gubitka bez kršenja teorema o zabrani kloniranja.

Zamjena isprepletenosti funkcionira generiranjem jedne isprepletenosti na velikoj udaljenosti od mnogih isprepletenosti koje su na kratkim udaljenostima. Jedna od najvećih prepreka distribuciji isprepletenosti na velikim udaljenostima je eksponencijalni gubitak koji nastaje zbog atenuacije vlakana[5]. Recimo da su Alice i Bob povezani vlaknom koje je predugo za prijenos fotona razumnom brzinom. Mogu dodati repetitor u sredini koji umjesto toga prihvaća isprepletene fotone od Alice i Boba i zatim ih pretvara u isprepletene fotone između Alice i Boba. Tako fotoni trebaju prijeći samo pola udaljenosti i imaju veće šanse stići do svog odredišta.

Iako čin "lijepljenja" dvije odvojene isprepletene karike može zvučati čarobno, repetitor to može učiniti pomoću jednostavne operacije koja se zove teleportacija. Sve dok repetitor ima kubite koji su isprepleteni s parovima na svakom od Alice i Boba, može izvršiti mjerenje i zatim izvijestiti Alice i Boba o informacijama koje su im potrebne za korištenje njihove nove isprepletene veze kako je prikazano na slici 9. Izgradnjom

[5] količina svjetlosti izgubljena između ulaza i izlaza

lanca repetitora, možemo rastaviti velike udaljenosti u segmente kojima je lakše upravljati preko kojih šaljemo naše fotone. [34]



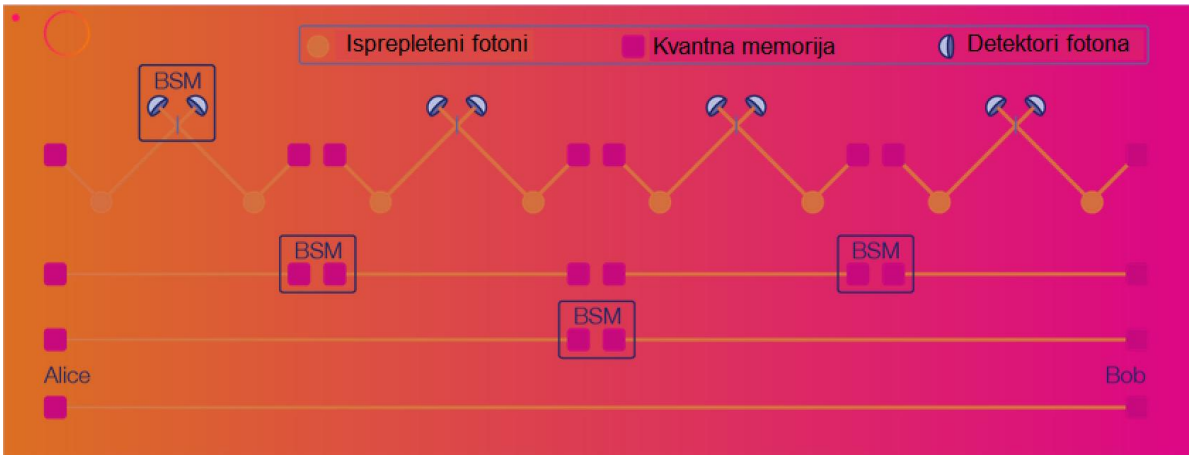
Slika 9. Opći prikaz zamjene isprepletenosti u kvantnoj komunikaciji

Izvor: [34]

Ako se detaljnije promatra način rada kvantnog repetitora kao na primjeru koji je prikazan na slici 10. vidljivo je kako je udaljenost prijenosa razbijena je u segmente gdje gubici nisu tako veliki. Isprepleteni fotoni mogu se odvojiti i poslati dalje; jedan na kvantnu memoriju, a drugi na mjerač Bellovog stanja (engl. Bell State Measurement (BSM)). Umjesto da se teleportira sam kubit, ovdje se teleportira isprepletenost ravno u kvantnu memoriju.

Foton poslan u kvantnu memoriju ne mjeri se i ne uništava, već se pohranjuje dok se čeka da sljedeća isprepletena veza bude spremna. Tako se završava s dužim optičkim vezama s isprepletenošću koja je sada pohranjena u tim kvantnim memorijama. Kvantne memorije dopuštaju da se čeka dok optičke veze ne budu spremne. Zatim se može ponoviti postupak, na primjer, ponovno emitirati fotone kako bi se izvršilo mjerenje Bellovih stanja između ovih susjednih kvantnih memorija, čime dodatno produžujemo udaljenost dok ne završimo s isprepletenošću koju dijele dvije

udaljene strane Alice i Bob.Memorije su očito ključni element u ovoj shemi i razvijaju se u širokom rasponu tehnoloških platformi koristeći ili skupine atoma, iona ili u nekim rijetkim slučajevima pojedinačne atome i ione.



Slika 10. Primjer teleportacije isprepletenosti fotona u kvantne memorije

Izvor: [34]

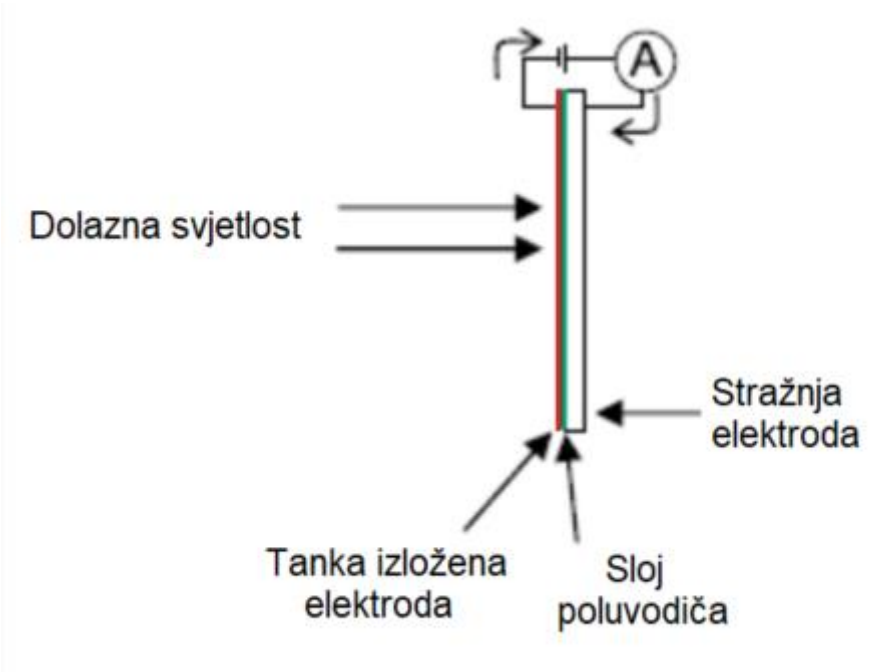
Kvantne memorije trenutačno su glavni fokus mnogih laboratorija s ciljem poboljšanja niza performansi kao što je vrijeme njihove pohrane i učinkovitost kojom se fotoni mogu vratiti. Napravljene su ključne demonstracije za ove elementarne veze, kao što su dvije isprepletene kvantne memorije, isprepletena pohrana i teleportacija. Nekoliko grupa objedinjuje sve kompetencije potrebne da se sve to spoji, a to sve više zahtijeva mnogo veći zajednički napor. U sljedećih nekoliko godina mogu se očekivati demonstracije u optičkim mrežama, ali jedna je od vizija da se razviju ove tehnologije kako bi se omogućila kvantna komunikacijska mreža koja se temelji na isprepletenosti. U tom smislu jedan od sljedećih velikih izazova također će biti početak povezivanja ovih elementarnih karika.

3.4. Jednofotonski detektori

Fotonski detektori broje fotone svjetlosti. Detektor fotona ima neku površinu koja apsorbira fotone i proizvodi određeni učinak (struja, napon) proporcionalan broju apsorbiranih fotona.

Kako je prikazano na slici 11. fotonaponska ćelija sastoji se od sloja nekog poluvodiča u „sendviču“ između dvije metalne elektrode, s izloženom elektrodom dovoljno tankom da bude prozirna. Poluvodič apsorbira fotone svjetlosti, stvarajući elektrone i rupe koje stvaraju struju proporcionalnu broju apsorbiranih fotona.

Fotocijev koristi fotoelektrični efekt za stvaranje struje iz apsorbirane svjetlosti. Svjetlost apsorbira metalna površina s niskom radnom funkcijom. Elektroni se emitiraju i privlače na pozitivno prednaprednu anodu. Elektronika mjeri struju, koja je proporcionalna broju apsorbiranih fotona. [35]



Slika 11. Fotonaponska ćelija

Izvor: [35]

U proteklom desetljeću zabilježen je dramatičan porast interesa za nove tehnologije jednofotonskih detektora. Glavni uzrok ovog trenda nedvojbeno je bio pomak prema optičkim kvantnim informacijskim aplikacijama kao što je kvantna distribucija ključeva (QKD). [36]

Detekcija jednog fotona ključna je za kvantne mreže. Znanstvenici NIST-a aktivno su uključeni u poboljšanje postojećih tehnologija detekcije, kao i u razvoju

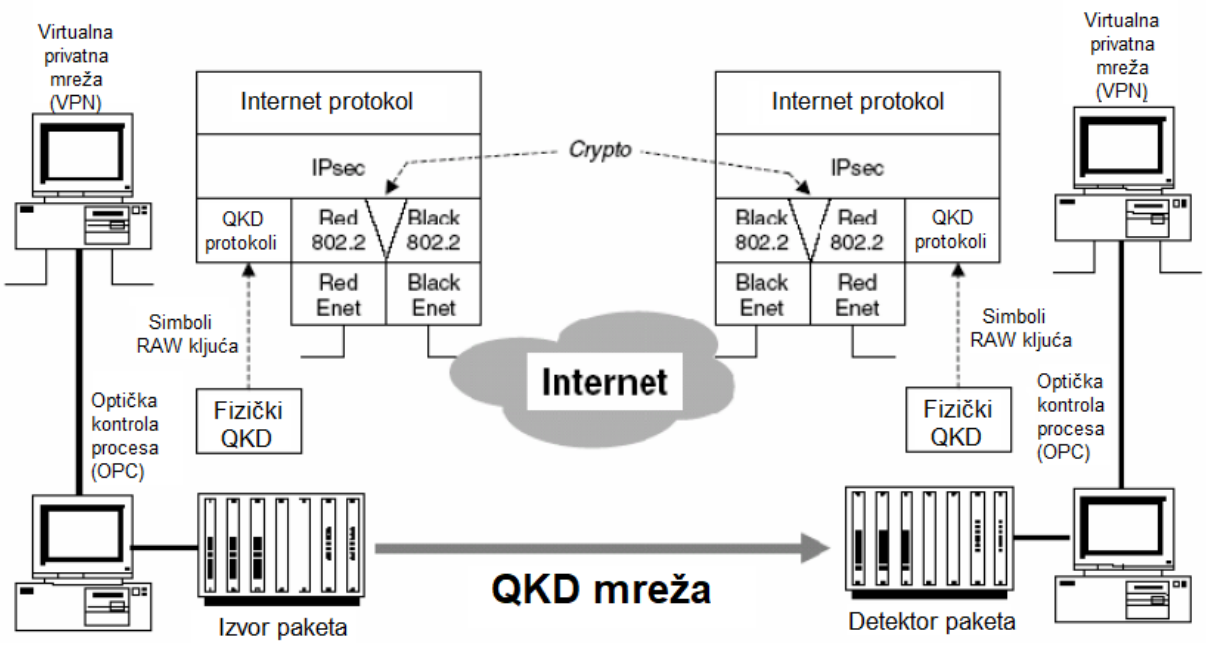
novih. Najvažniji cilj je približiti se 100% učinkovitosti detekcije. Druge karakteristike performansi detektora, kao što su latencija, jitter, maksimalna brzina brojanja i prisutnost naknadnog pulsiranja mogu biti jednako važne za praktične kvantne mreže, ali mogu biti specifične za aplikaciju. U nekim slučajevima, sposobnost određivanja broja fotona u pulsu može biti ključna. Stoga se cjelovita karakterizacija detektora provodi kao dio mjeriteljskih napora. [37]

Jednofotonski detektori moraju kombinirati visoku izvedbu s niskom cijenom i mogućnošću integracije, na primjer u istu platformu za fotoniku silicija koja se koristi za proizvodnju drugih komponenti. Niti jedno od trenutno dostupnih rješenja ne ispunjava ove zahtjeve, a razvoj radikalno novih komponenti će trajati mnogo godina. Stoga je pragmatična strategija koristiti trenutno dostupne detektore za demonstraciju ispravnog rada QKD sustava i protokola dok se čeka na razvoj novih tehnologija.

3.5. Arhitektura kvantne mreže s postojećom infrastrukturom

Trenutno se sigurnost kvantne mrežne ne pojavljuje kao neovisna aplikacija koja pruža kompletne protokole za sigurnu komunikaciju. Međutim, tehnike kvantne distribucije ključeva idu uz dobro uspostavljenu internetsku tehnologiju. Oni se koriste zajedno s javnim Internetom ili, vjerojatnije, s privatnim mrežama koje koriste skup internetskih protokola, kako bi se izgradili sigurni komunikacijski sustavi. Primjećujemo da su takve privatne mreže trenutno u širokoj upotrebi diljem svijeta s korisnicima koji žele sigurnu i privatnu komunikaciju, npr. financijske institucije, vladine organizacije, vojske i tako dalje, te da se spajanje QKD tehnologija s ovim vrstama privatnih mreža može pokazati izvedivim i odmah privlačnim u određenim kontekstima.

Danas je sigurna komunikacija između kriptografskih pristupnika ili još više između pojedinačnih računala na Internetu omogućena dobro definiranom arhitekturom IPsec-a. Određuje protokole, algoritme, baze podataka i politike potrebne za sigurnu komunikaciju. Stoga bi bilo optimalno spojiti QKD tehnologiju s trenutno dobro uspostavljenom internetskom sigurnosnom arhitekturom. Ovaj zajednički napor jamčio bi siguran internetski promet putem kvantne kriptografije. Slika 12. razlaže ovu osnovnu postavku u znatno više detalja.



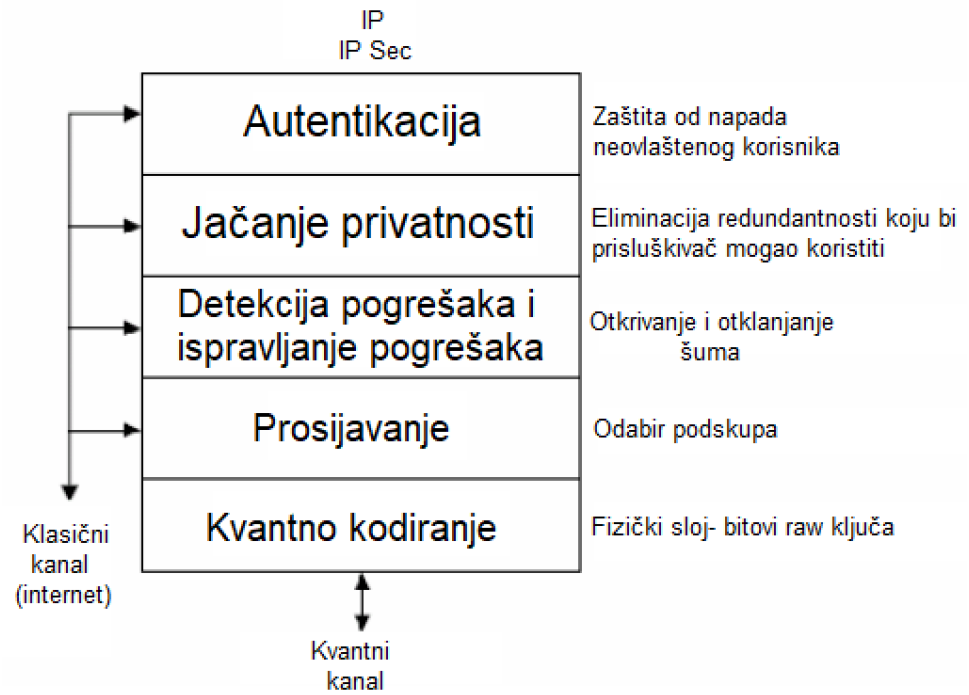
Slika 12. Arhitektura sustava za QKD vezu od kraja do kraja

Izvor: [38]

Osnovni pojmovi, međutim, nisu teški:

a) Dvije QKD krajnje točke uspostavljaju komunikaciju putem namjenskog vlakna ili valne duljine za kvantni put i putem Interneta za slanje poruka;
b) Odašiljačka strana priprema i prenosi neobrađene ključeve, iz kojih obje strane postižu dogovor o zajedničkom, tajnom ključu;
c) Ovaj tajni ključ se zatim koristi u kriptografskom pristupniku za zaštita prometa poruka koji će prolaziti Internetom unutar zaštićenih IPsec tunela

Slika 13. prikazuje višeslojni pristup za QKD protokol. Ti slojevi ocrtavaju stupanj slobode koji svaki sloj pokazuje kada traži alternative dizajnu. [38]



Slika 13. Unutarnja struktura i funkcionalnost paketa QKD protokola

Izvor: [38]

4. KVANTNA RAZMJENA KLJUČEVA

Distribucija ključeva je način distribucije šifriranih ključeva između dvije strane. Jednostavan način distribucije ključeva je „sastanak“ u sigurnom okruženju i razmjena ključeva. Ali danas se možemo razmjenjivati na bilo kojoj udaljenosti korištenjem javnih ključeva kao što su šifre, RSA, Diffie-hellman itd. za razmjenu ključeva. Problemi s konvencionalnom distribucijom ključeva su u tome što koriste jednostavne matematičke izračune za prijenos podataka koje je lako izračunati i trećoj strani im je lako pristupiti. [25]

Koncept kvantne distribucije ključa (QKD) prvi je put predložen 1970-ih, ali je tek 1980-ih stvarno izašao na vidjelo. Ideja je bila nevjerojatno jednostavna, ali sve do 1990-ih, kada je uspostavljena veza s isprepletenošću, fizičari su se počeli stvarno zanimati. Od tada je napredak bio izvanredan i sada je to možda najzrelija kvantna tehnologija, koja je komercijalno dostupna već više od 15 godina. [39]

Kvantna distribucija ključeva (QKD) sigurna je komunikacijska metoda za razmjenu ključeva šifriranja koja je poznata samo između ovlaštenih strana. Metoda komunikacije koristi svojstva kvantne fizike za razmjenu kriptografskih ključeva na način koji je dokaziv i jamči sigurnost. QKD omogućuje dvjema stranama da proizvedu i dijele ključ koji se zatim koristi za šifriranje i dešifriranje poruka. Konkretno, QKD je metoda distribucije ključa.

Distribucija ključeva na konvencionalnoj razini oslanja se na šifre javnih ključeva koje koriste komplicirane matematičke izračune i, stoga, zahtijevaju previsoku količinu procesorske snage za razbijanje. Održivost šifri javnih ključeva, međutim, suočava se s nekoliko problema, kao što je stalna implementacija novih strategija koje se koriste za napad na ove sustave, slabi generatori slučajnih brojeva i opći napredak u računalnim snagama. Osim toga, kvantno računalstvo učinit će većinu današnjih strategija enkripcije s javnim ključem nesigurnima i zastarjelima. [40]

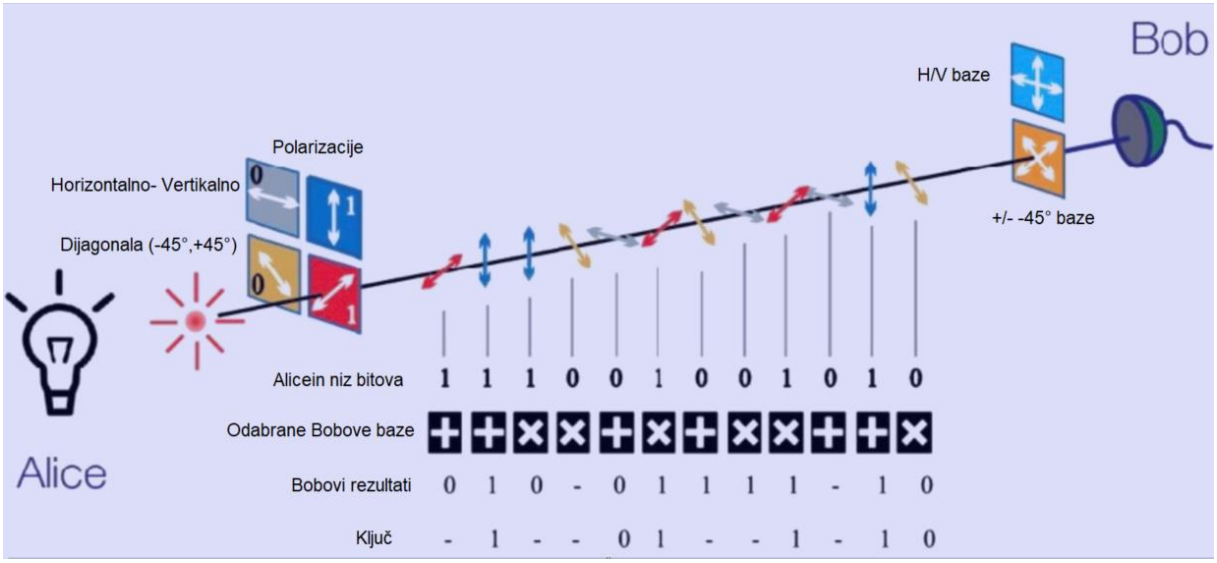
QKD sustav u osnovi uključuje dvije vrste kanala, a to su klasični kanal i kvantni kanal. Klasični kanal može se tretirati kao tradicionalni IP kanal (koji može, ali i ne mora biti optički). To u potpunosti ovisi o dizajnu sustava i može biti blisko povezan i posvećen kvantnom kanalu koji će ga koristiti u vremenskim zahtjevima. Kvantni kanal

je kanal s gubicima i probabilistički kanal koji se uglavnom koristi za prijenos kubita (pojedinačnih fotona) i sastoji se od optičkog puta koji mora biti transparentan. [27]

QKD radi na razini koja se mnogo razlikuje od konvencionalne distribucije ključeva utoliko što QKD koristi kvantni sustav koji se oslanja na osnovne i temeljne zakone fizike za zaštitu podataka, umjesto da se oslanja na matematiku. Kao primjer, teorem zabrane kloniranja navodi da je nemoguće stvoriti identične kopije nepoznatog kvantnog stanja, što sprječava napadače da jednostavno kopiraju podatke na isti način na koji danas mogu kopirati mrežni promet. Osim toga, ako napadač ometa ili pogleda sustav, sustav će se promijeniti na takav način da će zainteresirane strane znati. Ovo je proces koji nije osjetljiv na povećanu procesorsku snagu. [40]

QKD pruža način distribucije i dijeljenja tajnih ključeva koji su potrebni za kriptografske protokole. Ovdje je važno osigurati da oni ostanu privatni, tj. između strana koje komuniciraju. Da bismo to učinili, oslanjamo se na ono što se nekada smatralo problemom kvantnih sustava; ako ih “gledate” ili ih na bilo koji način uznemirite, “razbijate” kvantne karakteristike.

Tipično, informacije su kodirane na pojedinačnim fotonima, kao što je prikazano na slici 15. Alice može odabrati da ih kodira u "niz bitova" koristeći jedno od dva stanja, poput vertikalne (V) ili horizontalne (H) polarizacije, a također može odabrati da kodira u dva različita stanja; ovdje dvije kombinacije ovih stanja označenih s +45° i -45°. Bob zatim odabire mjerenje u jednoj od dvije, ono što nazivamo bazama – ili mjeri H,V ili mjeri +45°, -45°. Ako mjeri u bazi koja se razlikuje od one koju je Alice koristila za pripremu, tada će njegov odgovor biti nasumičan i odbačen, ali ako su odabrali isti, tada će imati savršeno korelirane rezultate; Alice šalje H, a Bob otkriva H i oni se čuvaju. Ovaj posljednji korak zahtijeva da Alice i Bob komuniciraju o tome koja je baza korištena, ali ne otkrivaju informacije o rezultatu, koji sada postaje tajni ključ. Ovo je samo jedan način, ali sada postoje mnoge varijacije.



Slika 14. Primjer generiranja tajnog ključa u QKD

Izvor: [39]

Kao što je prikazano na slici 14., ovo samo generira tajni ključ, koji se zatim mora ugraditi u kriptografske protokole kako bi se osigurala sigurnost u raznim aplikacijama u kojima se koriste. Ljepota koju kvantna fizika donosi ovom rješenju je u tome što će, ako špijun ili haker pokuša presresti generiranje ključa, unijeti pogreške i otkriti se. Važno je da se to događa prije nego što se bilo koja informacija kodira ili priopći.

Laboratorijske demonstracije i neki terenski testovi QKD-a u 1990-ima otvorili su put prvim komercijalnim sustavima u ranim 2000-ima. Od tada smo vidjeli razvoj svih temeljnih tehnologija i novih protokola za QKD i sigurnosne aplikacije koje ih mogu iskoristiti. Pokazane su visoke brzine (>Mbps) i velike udaljenosti (>400 km), a akademski i komercijalni sustavi i dalje postaju sve manji i jeftiniji. Očekuje se da će se to ubrzati u nadolazećim godinama i da će se integriranija rješenja prilagoditi za QKD. [39]

Glavna prednost koju QKD nudi u odnosu na konvencionalne kriptografske tehnike je ta što omogućuje kontinuirano generiranje apsolutno sigurnog ključnog materijala "u hodu" između dvije strane, pri čemu je sigurnost generiranog ključa zajamčena zakonima kvantne fizike. Uspostavlja sigurnu komunikaciju pružajući

sigurnost temeljenu na temeljnim zakonima fizike umjesto matematičkih algoritama ili računalnih tehnologija koje se danas koriste.

Još neke od prednosti QKD-a su:

a) gotovo ga je nemoguće hakirati
b) jednostavan je za korištenje.
c) za njegovo održavanje potrebno je manje resursa
d) koristi se za otkrivanje prisluškivanja. To je zbog činjenice da nije moguće kopirati podatke kodirane u kvantnom stanju
e) performanse takvih kriptografskih sustava kontinuirano se poboljšavaju

Neka ograničenja QKD-a mogu se naći očitati u slučaju isprepletenih fotona, koji se čine sigurnima ali postoji praktičan problem ne samo s cijenom, već i s držanjem fotona isprepletenim dovoljno dugo da zadovolje potrebe stvarnog svijeta. Još jedan problem je da kada udaljenosti premašuju 50 kilometara ili sl., razine buke postaju toliko visoke da stope pogrešaka vrtoglavo rastu. To kanal čini iznimno ranjivim na prisluškivače i slanje informacija čini gotovo nemogućim.

Kvantni ključevi, s druge strane, u budućnosti se mogu razmjenjivati putem zraka. Za detekciju signala moli bi se koristiti mali usmjereni teleskopi. Prema nekim procjenama, fotone bi mogao promatrati i satelit, omogućujući kontakt između bilo koje dvije točke na planetu. QKD je prva praktična primjena temelja kvantne mehanike, koja pokazuje važnost fundamentalnih znanstvenih studija. Da bi se kvantna distribucija ključa koristila u praksi, njena zaštita mora biti certificirana, što zahtijeva detaljan pregled aspekata kvantne mehanike na kojima se temelji. [41]

4.1. Vrste QKD-a

Postoje dva glavna pristupa QKD-u koji iskorištavaju čestične ili valne karakteristike kvantnog nositelja informacija:

a) Diskretna varijabla QKD (DV-QKD) (čestica): informacije se mogu kodirati o fizičkim svojstvima pojedinačnih fotona.

b) Kontinuirana varijabla QKD (CV-QKD) (val): informacija se može kodirati na kvadraturi amplitude i faze svijetlog lasera. [42]

	DV-QKD	CV-QKD
Izvor	Pojedinačni fotoni/prigušeni laser	Slabo modulirani laser
Detektor	Jednofotonski detektor	Homodini detektori
Protokol	Bennett and Brassard (BB84)	Silberhorn, Grangier
Da li je informacija teoretski sigurna?	Da	Ne

Tablica 3. Generalna usporedba sustava diskretne i kontinuirane varijable

Izvor: [42]

4.1.1. Sustavi diskretnih varijabli (DV-QKD)

U diskretnoj varijabli QKD (DV-QKD), čestična priroda svjetlosti iskorištava se za postizanje sigurne distribucije ključa. Odašiljač kodira informacije u stanju jednog fotona. Detektori jednog fotona koriste se za mjerenje primljenih kvantnih stanja. [43]

Pristup diskretne varijable (DV) QKD-u opsežno je proučavan i većina testnih površina i dostupnih komercijalnih uređaja je takve vrste. Temeljna ideja je da, budući da je dobro poznato da u kvantnomehaničkim sustavima svako mjerenje remeti sustav, ova se značajka može iskoristiti da se shvati pokušava li netko ukrasti podatke s kanala. BB84 protokol je primjer diskretne varijabilne kvantne distribucije ključa (DV-QKD), gdje se konačan broj polarizacijskih baza koristi za kodiranje bitova. Pošiljatelj (Alice) generira nasumični bit (tj. ili "0" ili "1") i kodira ga u jednoj od dvije različite baze, preko danog fizičkog parametra fotona (obično polarizacija). Prva baza se koristi za

kodiranje bita "0", a druga baza za bit "1". Budući da primatelj (Bob) ne zna pošiljateljev odabir baze, on mjeri (nakon širenja u vezi optičkog vlakna) polarizaciju dolaznih fotona nasumično koristeći jednu od dvije moguće baze. Ako koristi istu bazu kao pošiljatelj, izmjerit će točnu bitnu vrijednost; obrnuto, ako odabere pogrešnu bazu, rezultat mjerenja dat će točan rezultat tek s 50% vjerojatnosti. Nakon razmjene dugog niza fotona, Alice i Bob uspoređuju baze koje su upotrijebili za kodiranje i mjerenje svakog fotona, komunicirajući putem klasičnog kanala. Oni čuvaju samo bitove generirane i otkrivene s podudaranom bazom, za koje se kaže da sačinjavaju raw ključeve[6].

U idealnom sustavu bez buke, nesavršenosti i smetnji, raw ključevi su identični i mogu se koristiti kao privatni ključ. Tipično, dvije polarizacijske baze koje koristi pošiljatelj odabire polarizator i zakreću se jedna oko druge za 45°. One se zovu pravocrtne (0°, 90°) i dijagonalne (45°, 135°) baze. Na prijemniku, polarizacijski razdjelnik zrake (PBS) transformira polarizacijsko kodiranje u prostorno kodiranje, tako da se fotoni mogu detektirati pomoću dva odvojena fotodetektora lavine fotona (SPAD). [30]

4.1.2. Sustavi kontinuiranih varijabli (CV-QKD)

DV-QKD sustavi zahtijevaju ad-hoc uređaje za rad, kao što su jednofotonski detektori i jednofotonski izvori. Ovo je glavna prepreka industrijalizaciji zbog malih obujma proizvodnje (barem tijekom početnih faza uvođenja na tržište i potrebe za postavljanjem namjenskog opskrbnog lanca. Štoviše, učinkovito generiranje, detekcija i manipulacija pojedinačnim fotonima zahtijevaju uređaje s kriogenim hlađenjem[7]. Desetljeće kasnije od uvođenja sustava s diskretnim varijablama predložen je alternativni pristup QKD. Naziva se pristup kontinuirane varijable (CV), budući da se koriste fotonski parametri koji pretpostavljaju kontinuirane vrijednosti. Kvantna razmjena ključeva s kontinuiranim varijablama (CV-QKD) su sustavi koji koriste uređaje koji su već razvijeni za klasične optičke komunikacijske sustave i koji su

[6] zajednička binarna tajna niza nasumično polariziranih fotona oko koje se slažu izvorište i odredište
[7] kriogeno hlađenje je način hlađenja gdje se izravno koriste rashladna sredstva, poput tekućeg dušika ili krutog ugljičnog dioksida.

komercijalno dostupni desetljećima, kao što su PIN fotodiode[8], smanjujući složenost i cijenu sustava.

U kontinuiranoj varijabli QKD (CV-QKD), valna priroda svjetlosti iskorištava se za postizanje sigurne distribucije ključa. U ovom drugom pristupu, informacije se kodiraju na amplitudu i fazu ili na odgovarajuće kvadraturne komponente (nosače) koherentnog laserskog svjetla od strane odašiljača, a prijamnik mjeri sinfazne i kvadraturne komponente svjetla pomoću uravnoteženih homodinskih detektora [45].

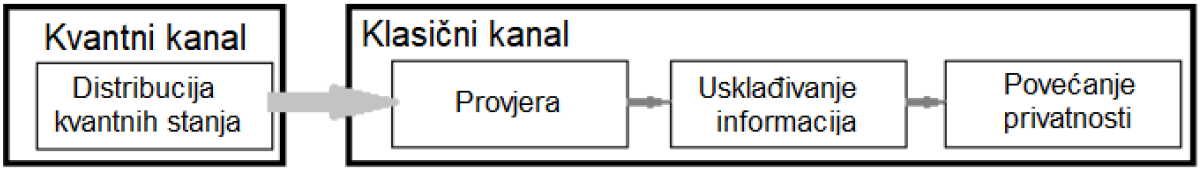
CV-QKD se odnosi na skupinu protokola koji su podijeljeni u dvije makro potklase, nazvane diskretna i Gaussova modulacija. CV-QKD možemo smatrati prilagodbom protokola BB84 za korištenje s nediskretnim karakteristikama svjetlosti. Koristi dobro proučenu homodinsku detekciju[9] koja odašilja pulseve energije umjesto pojedinačnih fotona. U prvom prijedlogu koriste se istisnuti optički impulsi. Svaki impuls može se prenijeti preko jedne od dvije kvadraturne komponente kompleksne ravnine, dodajući konstantan pomak za kodiranje bitova "0" ili "1". Prijemnik tada nasumično odabire kvadraturnu komponentu u kojoj će izvršiti mjerenja, usvajajući algoritam koji je analogan BB84, i zadržavajući samo mjere za koje je napravljen točan kvadraturni izbor. Ako se mjerenje izvodi na ispravnoj ravnini, rezultat je Gaussova raspodjela sa srednjom vrijednošću koja je jednaka primijenjenom pomaku koji se koristi za dekodiranje bitova.[30]

4.2. QKD protokoli

Kriptografija je „natjecateljska igra“ između legitimnih korisnika i prisluškivača. Postoje konvencionalno tri strane: Alice, Bob i Eve. Alice želi podijeliti tajnu poruku s Bobom, a Eve u isto vrijeme pokušava uhvatiti tajne dijelove bez otkrivanja svoje prisutnosti. Većina protokola kvantne distribucije ključa (QKD) ima sličnu temeljnu strukturu kako je prikazano na slici 15. Sljedeći koraci odvijaju se preko klasičnog

[8] vrsta foto detektora, može pretvoriti optičke signale u električne signale.
[9] detekcija homodina metoda je vađenja informacija kodiranih kao modulacija faze i / ili frekvencije oscilirajućeg signala, uspoređujući taj signal sa standardnom oscilacijom koja bi bila identična signalu ako nosi nultu informaciju

kanala – običnog javnog komunikacijskog kanala, za koji se pretpostavlja da je podložan prisluškivanju, ali ne i ubacivanju ili mijenjanju poruka. [43]



Slika 15. Opća temeljna struktura QKD-a

Izvor: [43]

Cilj bilo kojeg protokola distribucije kvantnog ključa (QKD) je generiranje zajedničkog tajnog ključa između dvije udaljene strane preko javnog komunikacijskog kanala. Ovdje je ključna točka da je protokol za generiranje ključa dokazano siguran protiv bilo kojeg mogućeg napada koji može izvesti prisluškivač. Zakon fizike (ili, zapravo, kvantna mehanika) je taj koji jamči sigurnost protokola, a ne samo tehnička ograničenja koja postoje u praktičnim implementacijama.

Dakle, možemo biti sigurni da će protokol biti siguran do vječnosti, a ne samo dok netko ne izumi ludo moćan stroj za dešifriranje (točnije, protokol će biti siguran sve dok se kvantna mehanika ne opovrgne). Općenito, protokol distribucije kvantnog ključa može se podijeliti u dva dijela: Prvi dio je faza kvantnog prijenosa, u kojoj Alice i Bob šalju i/ili mjere kvantna stanja. Drugi dio je klasična faza naknadne obrade, gdje se nizovi bitova generirani u kvantnoj fazi pretvaraju u par sigurnih ključeva. [44]

Tablicom 4. prikazana je usporedba QKD protokola između najvažnijih karakteristika .

Godina	Ime protokola	Princip na kojem su bazirani	Karakteristike	Autor
1984.	BB84	Heisbergovom načelu neodređenosti	Koristi stanje polarizacije fotona za prijenos informacija. Ima četiri stanja polarizacije (0°,45°,90°,135°).	C:H.Bennet i G. Brassard
1991.	E91	Kvantna isprepletenost	Koristi isprepleteni par fotona	Ekert A.K
1992.	BB92	Heisbergovom načelu neodređenosti	Jedina razlika između BB84 je u tome što su potrebna samo dva stanja umjesto četiri stanja polarizacije, tj. (0°, 45°).	C.H. Bennett
1999.	SSP	Heisbergovom načelu neodređenosti	To je BB84 protokol s dodatnom osnovom, tj. ima 6 stanja su ±x, ±y, ±z na Poincareovoj sferi	Bechmann-Pasquinucci.H i Gisin.N
2003.	DPS	Kvantna isprepletenost	Ima određene prednosti, uključujući jednostavnu konfiguraciju, učinkovito korištenje vremenske domene i otpornost na PNS napade	K.Inoue, E.Waks i Y.Yamanoto
2004.	SARG04	Heisbergovom načelu neodređenosti	Ekvivalent je BB84, ali je robusniji kada se koriste prigušeni laserski impulsi umjesto izvora pojedinačnih fotona. QBER SARG04 dvostruko je veći od BB84, tj. osjetljiviji na gubitke. Ali pruža više sigurnosti od BB84 u prisutnosti PNS napada.	Scarani.V, A.Acin, Ribordy G i Gisin.N
2004.	COW	Kvantna isprepletenost	Za rad sa slabim koherentnim impulsima pri visokim bitnim brzinama. Postavljanje je eksperimentalno jednostavno i tolerantno na smanjeni napad PNS-a, stoga neće biti izgubljene informacije	Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N i Scarani V

Tablica 4. Usporedba QKD protokola

Izvor: [46]

4.3. Protokoli temeljeni na Heisbergovom načelu neodređenosti

Prema Heisenbergovom principu nesigurnosti, nije moguće izmjeriti kvantno stanje bilo kojeg sustava bez ometanja tog sustava. Stoga se polarizacija fotona ili svjetlosne čestice može znati samo u trenutku kada se mjeri. Ovo načelo igra ključnu ulogu u sprječavanju pokušaja prisluškivanja u kriptosustavu temeljenom na kvantnoj kriptografiji. [46]

Najvažniji protokol koji se temelji na Heisbergovom načelo neodređenosti je BB84 koji je najzastupljeniji i prvi takav protokol i zbog toga je detaljnije definiran u sljedećem potpoglavlju. Još neki do protokola su BB92, SARG04, Six-State protokol (SSP).

4.3.1. BB92 protokol

Ubrzo nakon objave BB84 protokola, Charles Bennett je shvatio da nije potrebno koristiti dvije ortogonalne baze za kodiranje i dekodiranje. Ispada da se umjesto toga može koristiti jedna neortogonalna baza, bez utjecaja na sigurnost protokola od prisluškivanja. Ova ideja se koristi u protokolu BB92 [48], koji je inače identičan protokolu BB84. Ključna razlika u BB92 je da su potrebna samo dva stanja umjesto moguća 4 stanja polarizacije u BB84 protokolu. [49]

Kod ovog protokola „0“ se može kodirati kao 0° u pravocrtnoj osnovi, a „1“ se može kodirati kao 45° u dijagonalnoj bazi. Poput protokola BB84, Alice šalje Bobu niz fotona kodiranih nasumično odabranim bitovima, ali ovoga puta bitovi koje Alice odabere određuju koje baze Bob mora koristiti. Bob i dalje nasumično odabire osnovu po kojoj će mjeriti, ali ako odabere pogrešnu osnovu, neće ništa mjeriti; stanje u kvantnoj mehanici koje je poznato kao brisanje. Bob može jednostavno reći Alice nakon svakog bita koji Bob pošalje da li je to točno izmjerio [49].

4.3.2. SARG04 protokol

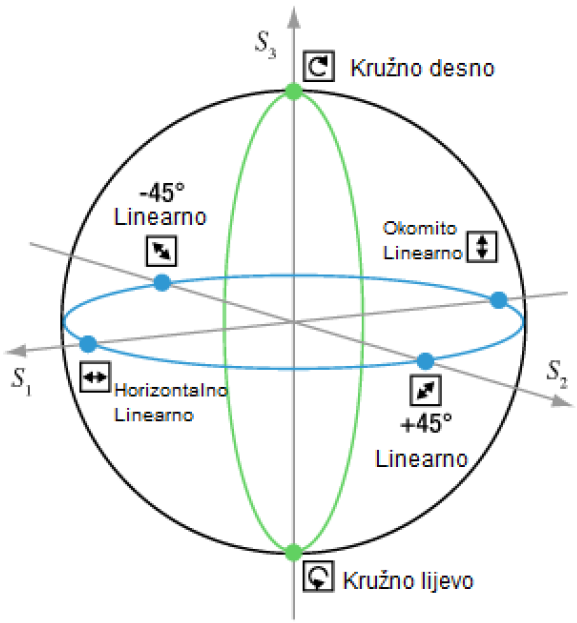
Protokol SARG04 izgrađen je kada su istraživači primijetili da korištenjem četiri stanja BB84 s različitim kodiranjem informacija mogu razviti novi protokol koji bi bio robusniji kada bi se umjesto izvora s jednim fotonom koristili prigušeni laserski impulsi. Protokol SARG04 predložio je 2004. godine V.Scarani. [50]

Protokol SARG04 dijeli potpuno istu prvu fazu kao i BB84. U drugoj fazi kada Alice i Bob određuju za koje bitove se podudaraju njihove baze, Alice ne objavljuje izravno svoje baze nego objavljuje par neortogonalnih stanja od kojih je jedno koristila za kodiranje svog bita. Ako je Bob koristio ispravnu osnovu, izmjerit će ispravno stanje. Ako je krivo odabrao, neće mjeriti niti jedno Aliceino stanje i neće moći odrediti bit. Ako nema grešaka, tada je duljina ključa preostalog nakon faze prosijavanja jedna četvrtina neobrađenog ključa. [46]

U PNS (engl. Photon Number Splitting) napadu na SARG04, Eve ne dobiva informacije koje baze koristiti pri mjerenju svog fotona čak ni nakon što su se Alice i Bob dogovorili o korištenim bazama. Međutim, nakon ovog postupka prosijavanja Bobu ostaje 1/4 neobrađenog popisa bitova, u usporedbi s 1/2 originalnog BB84 protokola. [43]

4.3.3. Six-state protokol (SSP)

Šest stanja ili tri baze kriptografske BB84 sheme s dodatnom osnovom. SSP su predložili H. Bechmann-Pasquinucci i N. Gisin 1999. godine. Kriptografska shema sa šest stanja ili tri baze nije ništa drugo nego dobro poznata BB84 shema s četiri stanja s dodatnom osnovom. Međutim, ova shema ima prednost u usporedbi s BB84 protokolom – veću simetriju. Simetričnost ovog protokola znatno pojednostavljuje sigurnosnu analizu (u usporedbi s protokolom s četiri stanja), smanjuje broj parametara potrebnih za opisivanje općih strategija. [51]



Slika 16. Poincarova sfera

Izvor: [52]

U protokolima šest stanja dva dodatna stanja odgovaraju ±z, tj. šest stanja su ±x, ±y i ±z na Poincareovoj sferi kako je prikazano slikom 16.. U ovom slučaju Alice šalje slobodno izabrano stanje (jedno od šest mogućih) i Bob mjeri da li je u x, y ili z-bazi. Ovdje je prethodna vjerojatnost da Alice i Bob koriste istu osnovu smanjena na 1/3, što znači da moraju odbaciti 2/3 prenesenih kubita prije nego što mogu izdvojiti kriptografski ključ. [46]

4.4. Protokoli temeljeni na kvantnoj isprepletenosti

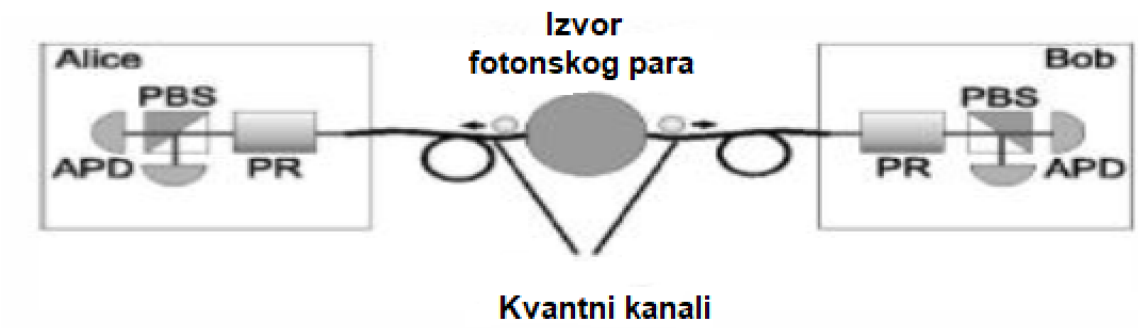
Protokoli koji se temelje na kvantnoj isprepletenosti koriste novi pristup kvantnoj distribuciji ključeva gdje se ključ distribuira pomoću kvantne teleportacije. [45]

Neki od protokola koji se temelje na kvantnoj isprepletenosti su E91 protokol, COW protokol, DPS protokol.

4.4.1. E91 protokol

Asthur Ekert je 1991. godine iznio shemu koja koristi isprepletene parove fotona [45]. Njih može stvoriti pošiljatelj Alice, primatelj Bob ili neki izvor odvojen od oboje, uključujući prisluškivača Eve. Fotoni su raspoređeni tako da Alice i Bob imaju po jedan foton iz svakog para.

Shema se oslanja na dva svojstva isprepletenosti. Prvo, zapetljana stanja savršeno su korelirana u smislu da ako Alice i Bob mjere imaju li njihove čestice vertikalnu ili horizontalnu polarizaciju, uvijek će dobiti isti odgovor sa 100% vjerojatnošću. Isto vrijedi ako oba mjere bilo koji drugi par komplementarne (ortogonalne) polarizacije. Međutim, određeni rezultati potpuno su slučajni, nemoguće je da Alice predvidi hoće li i Bob dobiti vertikalnu polarizaciju ili horizontalnu polarizaciju. Drugo, svaki Evin pokušaj prisluškivanja uništit će te korelacije na način koji Alice i Bob mogu otkriti. Tipična fizička postavka prikazana je na slici 17, koristeći aktivne polarizacijske rotatore (PR), polarizirajuće razdjelnike zrake (PBS) i lavinske fotodiode (APD). [46]



Slika 17. Tipičan sustav koji koristi isprepletene fotonske parove

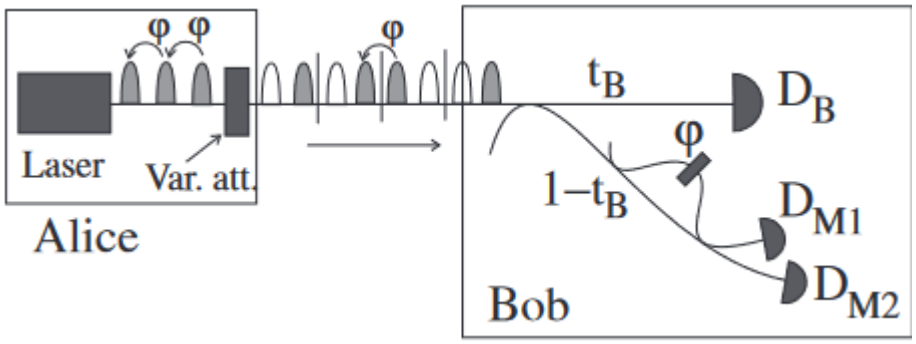
Izvor: [46]

Ekert je smatrao da ako su Alice i Bob uspjeli testirati isprepletenost između svojih kubita, tada su uspoređujući isprepletenosti mogli potvrditi da njihovi sustavi nisu u korelaciji s Evinim [54]. Statističkim testom koji potvrđuje očekivana kršenja Bellove nejednakosti, mogu potvrditi da EPR parovi nisu bili podvrgnuti Evinom prisluškivanju. Nakon prijenosa mogu javno objaviti baze koje su odabrali za pojedino mjerenje i

mjerenja podijeliti u dvije skupine: za koje su koristili različite baze i za koje su koristili iste baze. Tada mogu odbaciti sva mjerenja u kojima uopće nisu uspjeli registrirati česticu. [46]

4.4.2. COW (Coherent One-Way) protokol

Koherentni jednosmjerni protokol (COW protokol) novi je protokol za kvantnu kriptografiju koji su razradili Nicolas Gisin i suradnici 2004. godine. Novi protokol za QKD prilagođen za rad sa slabim usklađenim impulsima pri visokim bitnim brzinama. Prednost ovog sustava je u tome što je postavljanje eksperimentalno jednostavno i tolerantan je na smanjenu vidljivost smetnji i napade dijeljenja broja fotona (PNS), što rezultira visokom učinkovitošću u smislu destiliranih tajnih bitova po kubitu. [43]



Slika 18. Shema COW protokola, [55]

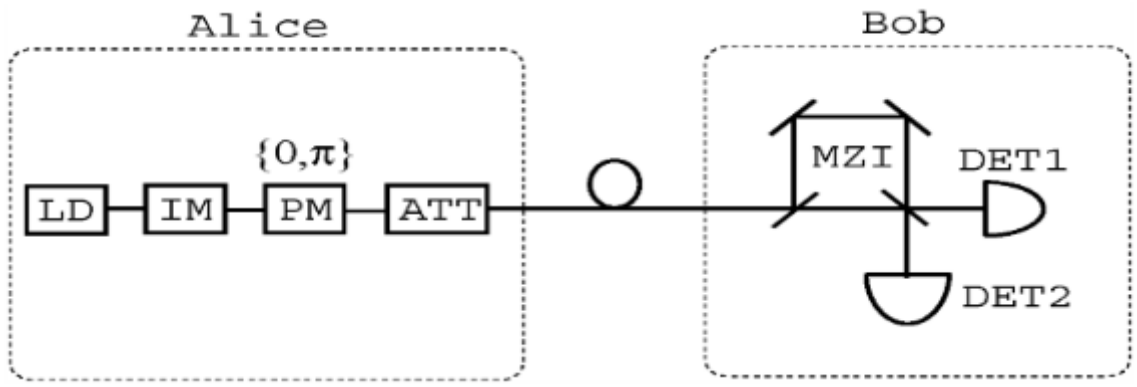
Slika 18. prikazuje COW protokol. Informacije su kodirane u vremenu. Alisa šalje koherentne impulse koji su ili prazni ili imaju srednji broj fotona μ<1, obično μ=0,5 (μ-puls). Svaki bit je kodiran sekvencama od dva impulsa, „μ-0“ za "bit 0" ili „0-μ“ za "bit 1". Alice također može slati sekvence mamaca „μ-μ“. Bob mjeri vrijeme dolaska fotona na njegovu podatkovnu liniju (detektor „DB“). Kako bi postigao kontinuiranu sigurnost, Bob nasumično mjeri usklađenost između uzastopnih nepraznih impulsa, sekvenci bitova "1-0" ili sekvenci mamaca, s detektorima „DM1“ i „DM2“. [46]

S idejom jednostavne podatkovne linije za kreiranje ključa i „komplementarne“ linije za praćenje, može se implementirati verzija BB84 protokola: Alice i Bob se slažu

proizvesti ključ koristeći samo pravocrtnu osnovu; ponekad Alice priprema jedno od svojstvenih stanja dijagonalne baze koje djeluje kao stanje mamac. [55]

4.4.3. DPS (Differential–phase-shift) protokol

Diferencijalni fazni pomak (DPS) nova je kvantna shema razmjene ključa koju su predložili K.Inoue i suradnici. Slika 19. prikazuje postavku DPS-QKD sheme. [56]



Slika 19. Shematski prikaz DPS protokola, [46]

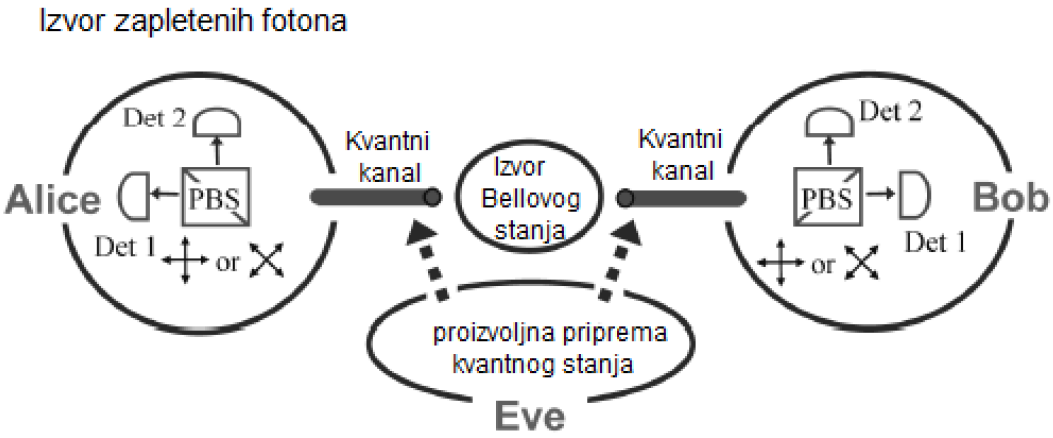
Alice fazno modulira niz impulsa slabih usklađenih stanja {0, π} za svaki impuls i šalje ga Bobu. Bob dijeli svaki dolazni impuls u dvije staze i razdvaja ih 50:50 i šalje razdjelnicima snopa fotona (engl. Photon Beam Spiltter (PBS)). Fotonski detektori postavljeni su na dva izlaza rekombinirajućeg razdjelnika snopa. Na detektorima, razdvojene valne funkcije dvaju sekvencijalnih impulsa interferiraju jedna s drugom. S odgovarajućom fazom u interferometru, Bobov prvi detektor klikne za 0 fazne razlike između dva uzastopna impulsa, a drugi detektor klikne za π faznu razliku. Nakon prijenosa, Bob govori Alice vremenske instance u kojima se foton broji. Prema dogovoru da klik detektora 1 označava '0', a klik detektora 2 označava '1', Alice i Bob dobivaju identičan niz bitova. Iz ove stope pogrešaka mogu otkriti postojanje

prisluškivanja. DPS sustav koristi sve fotone za kreiranje ključa; stoga je učinkovitost stvaranja ključa n [56].

4.4.4. BBM92 protokol

BBM92 je QKD protokol koji uključuje parove isprepletenih fotona i može se smatrati verzijom protokola BB84 koja se temelji na isprepletenosti. BB84 je QKD protokol koji se temelji na pripremi i mjerenju gdje Alice nasumično generira polarizacijska stanja koristeći RNG, dok je u BBM92 slučajnost svojstvena mjerenju zapletenih parova fotona. [58]

Način proizvodnje tajnog ključa koji koristi BBM92 protokol korištenjem EPR-Bell fotonskog para ilustriran je na slici 20. Izvor para fotona ponovno se postavlja na sredinu prijenosne linije i svaki foton iz para šalje se Alice i Bobu kroz kvantni kanal. Razmotrimo najprije mjerenje koje je izvršila Alice. Ona može nasumično odabrati bazu demodulacije između H-V baze i R-L baze za svaki foton.



Slika 20. Dijagram načina izrade tajnog ključa (BBM92)

Izvor: [58]

Zbog isprepletenosti, Bobov foton je uvijek kolapsiran na suprotnu i ortogonalnu polarizaciju u odnosu na izmjerenu polarizaciju Aliceina fotona. U određenom smislu

Alice može pripremiti Bobov foton u jedno od četiri polarizacijska stanja koja nisu ortogonalna jedno s drugim. Ovo je situacija BB84 protokola koji se proučava u nastavku rada. Bob nasumično bira bazu demodulacije između H-V baze i R-V baze. Alice i Bob javno objavljuju svoje baze i ako se poklapaju, znaju da su njihovi rezultati potpuno suprotni i da rezultate čuvaju kao pomaknute ključeve. Stvarno vrijeme kada su Alice i Bob otkrili foton ne mijenja rezultat.

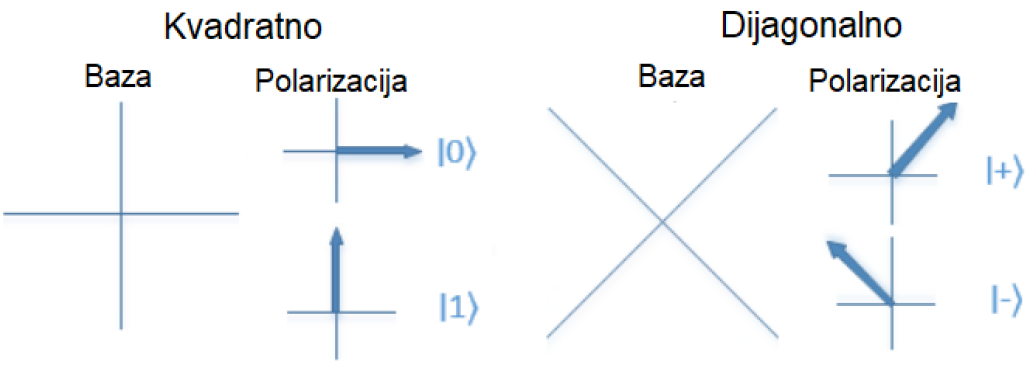
Jedina razlika i poboljšanje ovog novog protokola u odnosu na BB84 je u tome što ne postoji definitivna polarizacija, odnosno ključ ne postoji u prijenosnoj liniji. Umjesto toga, stvorena je mjerenjima. Stoga je Evin napad cijepanjem fotona nebitan. Čisto singletno stanje ne može se povezati s trećom česticom bez gubitka čistoće, pa ako Eva pokuša izvući djelomičnu informaciju o paru fotona, to nužno dovodi do bitne pogreške između Alice i Boba.[58]

4.5. Bennett and Brassard protokol (BB84)

Kvantna kriptografija temelji se na konvencionalnim kriptografskim metodama i proširuje ih korištenjem kvantnih učinaka. Distribucija kvantnog ključa (QKD) koristi se u kvantnoj kriptografiji za generiranje tajnog ključa koji se dijeli između dvije strane pomoću kvantnog kanala i klasičnog kanala s autentifikacijom. Dobiveni privatni ključ zatim se koristi za šifriranje poruka koje se šalju preko nesigurnog kanala (kao što je konvencionalna internetska veza). [46]

Ideja o kvantnoj kriptografiji pojavila se 1980-ih. C. H. Bennett i G. Brassard primijenili su teoriju kanala "kvantnog multipleksiranja" za rješavanje problema distribucije ključa u klasičnoj kriptografiji. Godine 1984. objavljen je dobro poznati BB84 QKD protokol. Protokol BB84 opisuje korištenje stanja polarizacije fotona za prijenos informacija. Izvorno su ga razvili Charles Bennett i Gilles Brassard 1984. [47]

BB84 u komunikaciji kvantnim kanalom funkcionira tako da Alice odabire nasumični niz bitova i nasumični niz polarizacijskih baza (kvadratnih ili dijagonalnih, vidi sliku 21.) i priprema kubite. Ona Bobu šalje niz fotona, od kojih svaki predstavlja jedan bit niza u bazi odabranoj za tu poziciju bita.



Slika 21. Kvadratne i dijagonalne mjerne baze i stanja polarizacije fotona

Izvor: [43]

Dok Bob prima fotone, on odlučuje nasumično za svaki foton i neovisno o Alice, koju će osnovu koristiti za mjerenje fotona i tumači rezultat mjerenja kao binarnu 0 ili Proizvodi se slučajni odgovor i sve informacije se gube kada se pokušava izmjeriti pravocrtna polarizacija dijagonalnog fotona, ili obrnuto. Stoga Bob dobiva značajne podatke samo od polovice fotona koje detektira – onih za koje je pogodio točnu osnovu polarizacije. Bob i Alice javnom razmjenom poruka prvo utvrđuju koji su fotoni uspješno primljeni i koji je mjeren na ispravnoj osnovi.

Ako je kvantni prijenos bio nesmetan, Alice i Bob bi se trebali složiti oko bitova kodiranih ovim fotonima, iako se o tim podacima nikad nije razgovaralo putem javnog kanala. Alice i Bob mogu testirati prisluškivanje javno uspoređujući neke od bitova, iako to žrtvuje tajnost tih bitova. Pozicije bitova korištene u ovoj usporedbi trebale bi biti nasumični podskup ispravno primljenih bitova, tako da je malo vjerojatno da će prisluškivanje više od nekoliko fotona izbjeći detekciju. [43]

U komunikaciji javnim kanalom BB84 protokolom postoje dvije faze. Prva faza je ekstrakcija raw ključa gdje postoje dva koraka, a to su:

a) Preko javnog kanala klijent Bob priopćava Alice koju je kvantnu abecedu koristio za svako svoje mjerenje
b) Kao odgovor Alice priopći Bobu preko javnog kanala koja su njegova mjerenja bila točna abeceda. Alice i Bob zatim brišu sve bitove za koje su upotrijebili nekompatibilnu kvantnu abecedu da proizvedu svoje

rezultirajuće neobrađene ključeve. Ako treća osoba nije prisluškivala, tada će njihovi ključevi biti isti. Ako je treća osoba prisluškivala, njezin ključ se neće u potpunosti slagati.

Druga faza je procjena pogreške gdje preko javnog kanala, Alice i Bob uspoređuju mali dio svojih neobrađenih ključeva kako bi procijenili stopu pogreške R, a zatim brišu otkrivene bitove iz svojih neobrađenih ključeva kako bi proizveli svoje probne konačne ključeve. Ako kroz svoje javne objave Alice i Bob ne pronađu greške (tj. R=0), onda znaju da treća osoba nije prisluškivala i da njihovi probni ključevi moraju biti isti konačni ključ. Ako otkriju barem jednu pogrešku tijekom svojih javnih objava (tj. R>0), onda znaju da je treća osoba prisluškivala. U tom slučaju odbacuju svoje probne konačne ključeve i počinju ispočetka.

5. PRIKAZ RAZVIJENOSTI/ RASPROSTRANJENOSTI KVANTNE KOMUNIKACIJE U EUROPI

Europi su potrebna hrabra strateška ulaganja kako bi vodila novu kvantnu revoluciju. Nadovezujući se na svoju znanstvenu izvrsnost, Europa ima priliku poticati konkurentnu industriju kvantne tehnologije koja je neophodna za pružanje dugoročnog prosperiteta i sigurnosti. Europa razvija mnoge inicijative i stvara nove programe koji potiču razvoj kvantne tehnologije.[54] Mnoge države podržavaju taj razvoj i aktivno su uključene i isti sa svojim znanstvenim, tehnološkim i financijskim doprinosom.

Jedna od najvažniji programa razvoja kvantne tehnologije u Europi je „Quantum Flagship“. Pokrenut je 2018. kao jedna od najvećih i najambicioznijih istraživačkih inicijativa Europske unije. S proračunom od najmanje jedne milijarde eura i trajanjem od 10 godina, vodeći projekt okuplja istraživačke institucije, akademsku zajednicu, industriju, poduzeća i kreatore politika u zajedničkoj i suradničkoj inicijativi neviđenih razmjera. Cilj je konsolidirati i proširiti europsko znanstveno vodstvo i izvrsnost u ovom području istraživanja, pokrenuti konkurentnu europsku industriju kvantnih tehnologija i učiniti Europu dinamičnom i privlačnom regijom za inovativna istraživanja, poslovanje i ulaganja u ovom području. Dugoročni plan je "kvantna mreža": kvantna računala, simulatori i senzori međusobno povezani preko kvantnih mreža koje distribuiraju informacije i kvantne resurse kao što su koherencija i isprepletenost.

U lipnju 2019. nekoliko zemalja EU-a potpisalo je deklaraciju kojom se slažu da će zajedno istražiti kako razviti i implementirati kvantnu komunikacijsku infrastrukturu (QCI) diljem EU-a u sljedećih deset godina. Od tada su još tri države članice također potpisale deklaraciju. U razdoblju 2021. – 2027. kvantne tehnologije podržavat će program Digital Europe, koji će razviti i ojačati europske strateške digitalne kapacitete, kao i program Komisije Horizon Europe, koji će pridonijeti istraživačkim aplikacijama.[60]

Brz napredak u teoriji i eksperimentu QKD tehnika odražava se u nizu uspješnih demonstracija u posljednjih nekoliko godina. Mnoge grupe diljem svijeta iznijele su QKD postavke koje rade u standardnom načinu od točke do točke, ostvarujući tako ono što se označava kao QKD-veze. [61]

Rješenja za sigurnu komunikaciju koja se traže obično se temelje na namjenskim vrhunskim uređajima za simetrično šifriranje s čestom promjenom ključa, pri čemu QKD uređaji stalno generiraju novi ključ. Širenje razvoja QKD tehnologije ometaju, međutim, brojne prepreke koje se obično vrte oko: paradigme od točke do točke i odgovarajućeg kvadratnog skaliranja početnih tajni s brojem korisnika, pitanja integrabilnosti postojećih mreža, visoke cijene QKD uređaja, ali i oko pitanja kao što su nedostajući standardi.

5.1. Europski plan za kvantne tehnologije (QT Roadmap)

Napredak u kvantnom računalstvu ilustrira tri čimbenika koja su neophodna da bi se QT izbacio iz laboratorija: relevantni slučajevi upotrebe sa značajnim tržišnim potencijalom, profesionalni inženjering u velikim razmjerima i značajno istraživanje za prevladavanje trenutnih znanstvenih i tehnoloških ograničenja. Mnoge države članice EU-a prepoznale su ovu situaciju i u prošlosti su snažno ulagale u nacionalne QT programe ili centre. Europska komisija (EC) financirala je QT istraživanje u posljednja dva desetljeća s visokim iznosom novčanih sredstava, uglavnom kroz program za buduće i nove tehnologije (FET) za zajedničke napore, Europsko istraživačko vijeće (ERC) za pojedinačne istraživače , i aktivnosti Marie Skłodowska-Curie za mobilnost i obuku istraživača. **Europski plan za kvantne tehnologije** (engl. European QT Roadmap) rezultat je ovih aktivnosti, što je u konačnici dovelo do Quantum Flagship-a. [62]

Unutar posljednja dva desetljeća, Quantum Technologies (QT) su postigle ogroman napredak, prelazeći iz eksperimenata o kvantnoj fizici nagrađenih Nobelovom nagradom u međudisciplinarno polje primijenjenih istraživanja. Sada se razvijaju tehnologije koje se eksplicitno bave pojedinačnim kvantnim stanjima i koriste "čudna" kvantna svojstva, kao što su superpozicija i isprepletenost.

Polje se sastoji od četiri domene:

- Kvantna komunikacija, gdje se pojedinačni ili zapleteni fotoni koriste za prijenos podataka na dokazano siguran način,

- Kvantna simulacija, gdje se dobro kontrolirani kvantni sustavi koriste za reprodukciju ponašanja drugih, manje dostupnih kvantnih sustava,
- Kvantno računanje, koje koristi kvantne efekte za dramatično ubrzanje određenih izračuna, kao što je faktoring brojeva i
- Kvantna osjetljivost i mjerenje, gdje se iskorištava visoka osjetljivost koherentnih kvantnih sustava na vanjske poremećaje kako bi se poboljšala učinkovitost mjerenja fizičkih veličina

Jedan čimbenik uspjeha za brzi napredak QT-a je dobro usklađena globalna istraživačka zajednica sa zajedničkim razumijevanjem izazova i ciljeva. U Europi je ova zajednica profitirala od nekoliko koordinacijskih projekata koje je financirala EK, a koji su, između ostalog, koordinirali stvaranje QT Roadmapa. Važno je napomenuti da, iako se QT Roadmap puta temelji na europskim koordinacijskim naporima i svi su autori iz Europe, znanstveni i tehnološki status kao i izazovi i potreban napredak opisani u njemu autori ne doživljavaju kao specifične za Europu, nego i za razvoj globalno za polje QT. Na ove procjene razvijeni su prioriteti europskog kvantnog vodećeg projekta.[63]

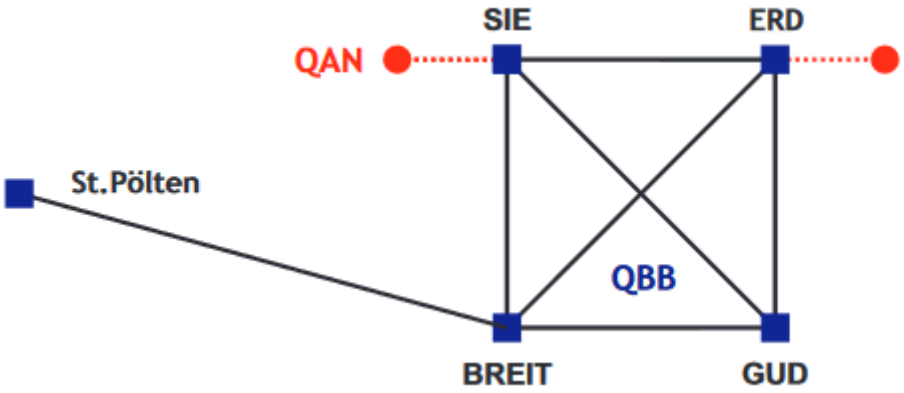
5.2. SECOQC

SECOQC mrežu kvantne distribucije ključeva (QKD) osmislio je i implementirao europski SEcure COmmunication temeljen na kvantnoj kriptografiji (SECOQC) (2004. – 2008.), ujedinjujući napore 41 istraživačke i industrijske organizacije Iz Europske unije, Švicarske i Rusije. Glavni cilj bio je odlučno potaknuti i otvoriti put za praktičnu primjenu tehnologije kvantne distribucije ključeva (QKD), koja se najčešće naziva "kvantna kriptografija". QKD je postupno sazrio od početnog teorijskog konstrukta, preko prvih eksperimentalnih realizacija do širokog raspona različitih QKD tehnologija i početnih komercijalnih proizvoda čiji se primjer može naći u postrojenju ID Quantique čije proizvode danas koriste vlade, poduzeća i industrijski kupci te akademski istraživački laboratorji u više od 60 zemalja i na svim kontinentima. [64, 65]

Temeljna ideja je ovog projekta bila je izgraditi mrežu za distribuciju tajni iz pojedinačnih QKD veza od točke do točke. Odgovarajuće QKD-Link krajnje točke

(tj. QKD uređaji) nalaze se u mrežnim čvorovima. Ovi su čvorovi sigurna mjesta u kojima se nalazi jedan ili više QKD uređaja zajedno s modulom središnjeg čvora, posvećenom obradi, pohrani i komunikaciji. Ovi čvorni moduli su mrežni agenti koji preuzimaju (u SECOQC pristupu) potpunu kontrolu nad klasičnim komunikacijskim kanalima, upravljanjem generiranim tajnim ključevima, njihovim informacijsko-teorijski sigurnim prijenosom od čvora do čvora na način hop-by-hop, i pitanja poput pronalaženja puteva do udaljenih čvorova i osiguravanja sinkronizacije pružanja tajnih ključeva aplikacijama koje troše ključeve diljem mreže.

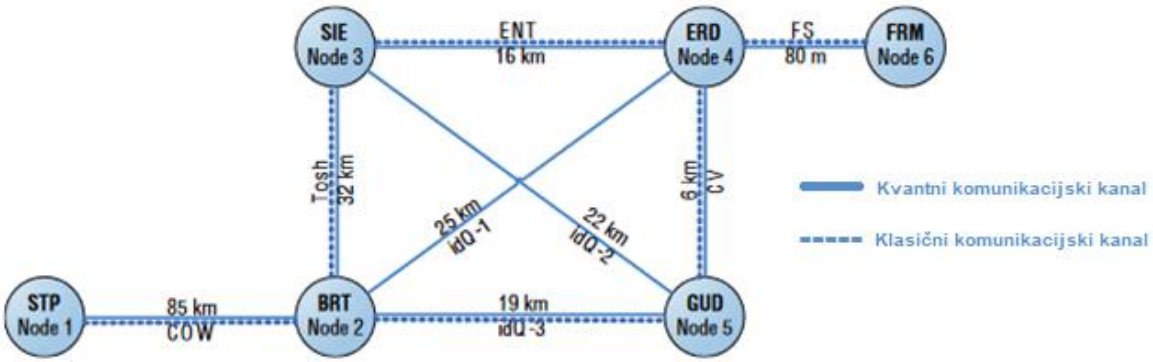
Kako bi se predstavile i demonstrirale nove mrežne funkcionalnosti i pokazale razne prednosti u odnosu na pojedinačne veze, implement je univerzalni pravokutni građevni blok (slika 22.) od četiri stanice u Beču (SIE, ERD, GUD, BREIT) koji se proširuje za jedan čvor u obližnjem gradu St. Polten. Sve QBB-veze su implementirane uključujući dvije dijagonale i dvije kratke QKD-veze prema krajnjim korisnicima. [61]



Slika 22. Koncept postavljenog univerzalnog gradivnog bloka za umrežavanje distribucije kvantnih ključeva, [61]

Prednost korištenog pristupa ovog projekta je njegova modularnost, koju uglavnom osiguravaju moduli čvorova, koji maskiraju mrežu za QKD uređaje. Oni rade na standardnoj osnovi od točke do točke bez da 'primjećuju' mrežu. Istovremeno čvorovi enkapsuliraju temeljnu QKD tehnologiju u mrežu. Iz perspektive potonjeg nije bitno koja se posebna QKD tehnologija koristi u vezi sve dok odgovarajući QKD uređaji komuniciraju s odgovarajućim modulima čvora i guraju QKD ključ.

Arhitektonski dizajn SECOQC QKD mreže jamči besprijekornu skalabilnost, tj. mogućnost proizvoljnog proširenja mreže i integracije dodatnih QKD uređaja u već postavljene čvorove. SECOQC prototip posebno ima šest čvorova povezanih s osam QKD veza. Mreža je postavljena u internom komunikacijskom prstenu od staklenih vlakana u Beču u Austriji. Pregledni dijagrami ove QKD mreže dani su na slikama 23. i 24. [64]



Slika 23. Mrežna topologija prototipa SECOQC QKD mreže

Izvor: [64]

Čvorovi SIE, BRT, GUD, ERD i FRM smješteni su u Beču, dok je čvor STP smješten u repetitorskoj stanici, blizu St Poltena u Donjoj Austriji. [64]

Slika 24. Satelitska karta s lokacijama čvorova prototipa, [64]

Distribucijska mreža kvantnog ključa koja pokriva punu gradsku mrežu unutar grada koristeći sedam QKD uređaja temeljenih na optičkim vlaknima, realizirana pomoću pet različitih principa rada i dva QKD postava slobodnog prostora demonstrirana je u Beču. Ova implementacija u okviru SECOQC koji financira EU jasno pokazuje izvedivost izgradnje visoko integriranih QKD mreža. Heterogeni moderni QKD uređaji kombiniraju se putem zajedničkih sučelja i modula univerzalnih čvorova u jedinstvenu tajnu distribucijsku infrastrukturu. [62]

5.3. Međueuropska kvantna mreža

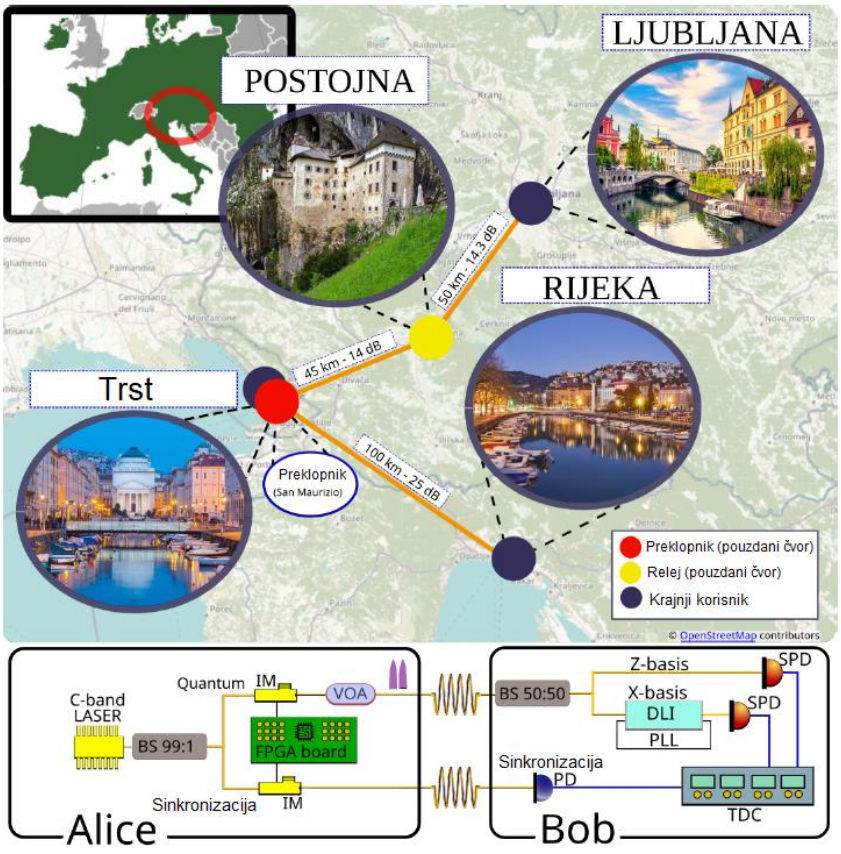
Otprilike četrdeset godina je prošlo od prvih pionirskih radova koji su uveli mogućnost korištenja kvantne fizike za snažno poboljšanje sigurnosti komunikacija. Danas je kvantna kriptografija, a posebice kvantna distribucija ključa (QKD) izašla iz laboratorija fizike i postala komercijalna tehnologija koja sve više privlači pažnju država, vojnih snaga, banaka i privatnih korporacija.

Kvantna distribucija ključa (QKD), koju su predložili Bennett i Brassard 1984., je protokol koji može pružiti bezuvjetno sigurnu komunikaciju podataka omogućenu zakonima kvantne fizike. QKD je najrazvijenija kvantno omogućena tehnologija, a mnoge su zemlje već implementirale praktične slučajeve korištenja diljem svijeta. Na primjer, veze s optičkim vlaknima, sateliti ili oboje korišteni su za stvaranje kvantne mreže koja poboljšava sigurnu komunikaciju između različitih gradova i dviju različitih država. Vrijedno je primijetiti da su optičke komunikacije preko tisuća kilometara moguće samo zahvaljujući scenariju pouzdanog čvora (kvantna stanja se mjere i potom ponovno kodiraju). Tako je moguće produžiti maksimalni domet veze od točke do točke i omogućiti povezivanje više korisnika. Međutim, dugoročni cilj jedinstvene kvantne mreže u cijelom svijetu ometaju praktične poteškoće (tj. različite optičke infrastrukture, različiti telekom operateri itd.) međusobnog povezivanja više zemalja kroz već postojeću optičku infrastrukturu. U tom kontekstu, jedan od ciljeva projekta European Quantum Communication Infrastructure (EuroQCI) je **uspostaviti europsku kvantnu mrežu**, sposobnu prevladati trenutna ograničenja.

Ovaj projekt pokrenuo je inicijativu EuroQCI povezujući Italiju, Sloveniju i Hrvatsku, tri različite europske zemlje, preko kvantne mreže unutar vlakana. Za

različite veze korišten je BB84 protokol koji koristi shemu kodiranja vremenskog polja i metodu one-decoy stanja. Izmjerene ključne brzine na poveznicama Trst-Postojna i Ljubljana-Postojna iznose preko 2,0 kbps odnosno 3,1 kbps, dok je ključna brzina na vezi Trst-Rijeka s velikim gubicima (25 dB) 610 bps. Distribuirani kvantni ključevi korišteni su za osiguranje virtualnog privatne mreže (VPN) među korisnicima, koja je korištena za kvantno osigurane video-pozive tijekom G20 događaja održanog u Trstu. [66,67]

Implementirana mreža, čija je infrastruktura ilustrirana na slici 25., a arhitektura prikazana na slici 26., sastoji se od dva odašiljača, također nazvana Alice, i tri prijamnika, poznata kao Bob, povezana s dva optička vlakna; jedan se koristi za kvantni signal, a drugi za servisni signal, tj. sinkronizaciju, procjenu parametara itd.

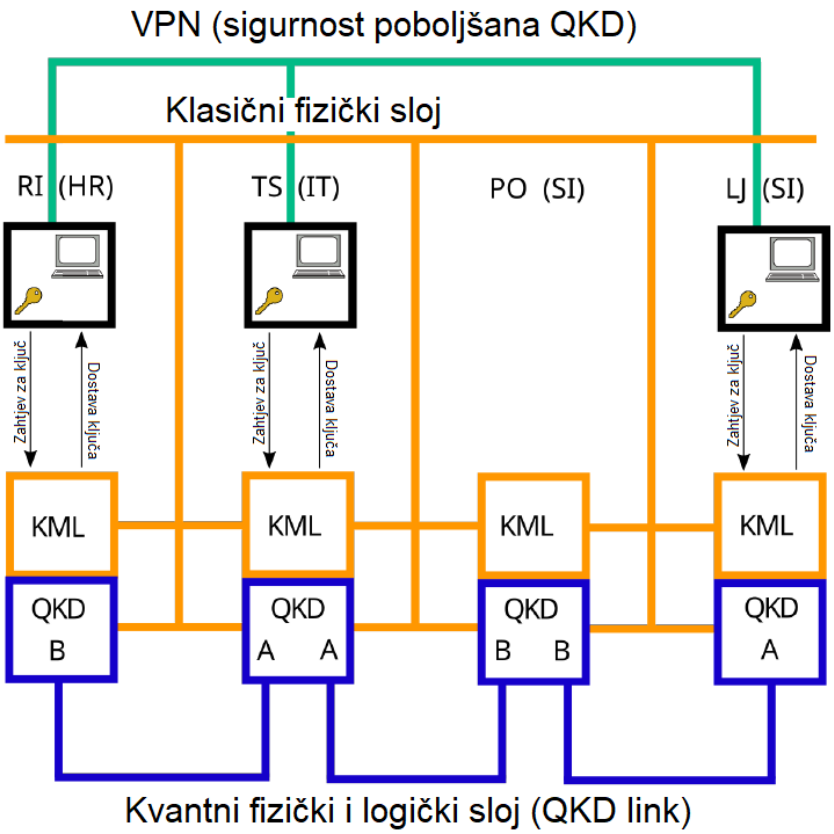


Slika 25. Sheme mreže i postavljanja

Izvor: [66]

Prvi odašiljač, smješten u kongresnom centru u Trstu (TCC), šalje sinkronizaciju i kvantne signale koji kodiraju ključ u San Maurizio telekom centar u Trstu, tri kilometra udaljen od TCC-a. Ovdje se dva signala dijele u omjeru 50:50 pomoću dva razdjelnika snopa koji se usmjeravaju na dva različita čvora; to čini San Maurizio mjestom gdje počinju kvantni kanali. Oba prihvatna čvora nalaze se izvan talijanskih granica, jedan u Telekomu Slovenije d.d. telekom centru u Postojni (Slovenija), a drugi u OIV telekom centru u Rijeci (Hrvatska). Čvor Postojna nije krajnji korisnik naše mreže, budući da djeluje kao još jedno pouzdano čvorište za dolazak do glavnog grada Ljubljane, veza nije moguća jednom izravnom vezom jer su ukupni gubici bili previsoki (oko 30 dB). Točnije, druga Alice bila je smještena na Fakultetu za matematiku i fiziku Sveučilišta u Ljubljani: radila je na način analogan Alice smještenoj u Trstu, ali je opsluživala samo jedan čvor.

C-pojasni laser dijeli se razdjelnikom snopa 99:1 (BS 99:1) i šalje modulatorima intenziteta (IM) kojima upravlja FPGA ploča; 1% izlaza razdjelnika snopa ide prema kvantnom dijelu, dok se dodaje varijabilna optička atenuacija (VOA) kako bi se postigao željeni srednji broj fotona po impulsu. 99% BS izlaza koristi se za generiranje signala sinkronizacije s niskim podrhtavanjem s frekvencijom od 145 kHz. Na Bobovoj strani, 50:50 BS koristi se za izbor osnove; za Z-bazu fotoni se izravno šalju na jednofotonski detektor (SPD), dok fotoni usmjereni na detektor na X-bazi prolaze prethodno kroz interferometar s linijom kašnjenja (DLI); u vezi Trst-Postojna interferometar je stabiliziran faznom petljom (PLL). Dva SPD-a, zajedno s brzom foto-diodom koja čita sinkronizacijski signal (sync PD), povezani su s vremenskim-digitalnim pretvaračem (TDC) koji registrira vremenske oznake događaja iz kojih se, nakon faze naknadne obrade, ključ je izvučen. [66]



Slika 26. Mrežna arhitektura

Izvor: [66]

Mreža radi na različitim razinama. Crni kvadrati, koji predstavljaju računala u sobama za sastanke, djeluju i kao aplikacijski sloj i kao klasični logički sloj; na zahtjev za pokretanjem VPN-a koji povezuje Trst (TS), Rijeku (RI) i Ljubljanu (LJ) čvorove. Klasični logički sloj šalje zahtjev sloju upravljanja ključevima (KML), koji provjerava je li već pohranjen ključ spreman za korištenje za osiguranje VPN-a. Nakon što prođe ovaj test, sloj upravljanja ključem šalje ključ klasičnom logičkom sloju, u suprotnom, zahtjev za generiranje novog ključa šalje se kvantnom sloju (plavi okvir). Kvantni sloj je izrađen pravilnom optičkom postavom (fizički podsloj) i svim metodama naknadne obrade potrebne za proizvodnju konačnog ključa (logički podsloj); slovo A (Alice) ili B (Bob) u okviru kvantnog sloja govori je li čvor odašiljač ili prijamnik. Kada je ključ spreman, kvantni sloj ga šalje sloju za upravljanje ključevima koji će ga isporučiti prvom sloju. Sloj upravljanja ključevima, zajedno s internetskom infrastrukturom, čini klasični fizički sloj.

Za svaku vezu korišteno je jedno tamno vlakno za kvantni kanal, a drugo tamno vlakno za sinkronizaciju. Komunikacija za protokole gornjeg sloja uspostavlja se standardnom TCP/IP Internet vezom. Izmjerena atenuacija kvantnih kanala iznosila je oko 14 dB za vezu Trst – Postojna i Ljubljana – Postojna, odnosno 25 dB za vezu Trst – Rijeka. Cijela mreža postavljena je u nekoliko dana, od nule, koristeći već postojeća vlakna različitih pružatelja usluga. Ova kvantna mreža korištena je za pružanje QKD dokazne demonstracije principa na sastanku digitalnih ministara G20 održanom u Trstu 5. kolovoza 2021. Dva koncerta orkestra konzervatorija u Ljubljani i Rijeci emitirana su u sjedištu G20 u Trstu putem videa konferencija (otvoreni sastanci) uspostavljena putem virtualne privatne mreže (VPN) pojačana kvantnim ključem; isto tako, orkestar Konzervatorija u Trstu podijelio je koncert s Ljubljanom i Rijekom. Kvantna mreža temeljila se na vlaknima koja se inače koriste za pričuvne veze i redoviti podatkovni promet, te je stoga bila dostupna samo za vrijeme potrebno za konfiguriranje QKD postavki i emitiranje triju koncerata. [66]

5.4. Europske države i kvantna mreža

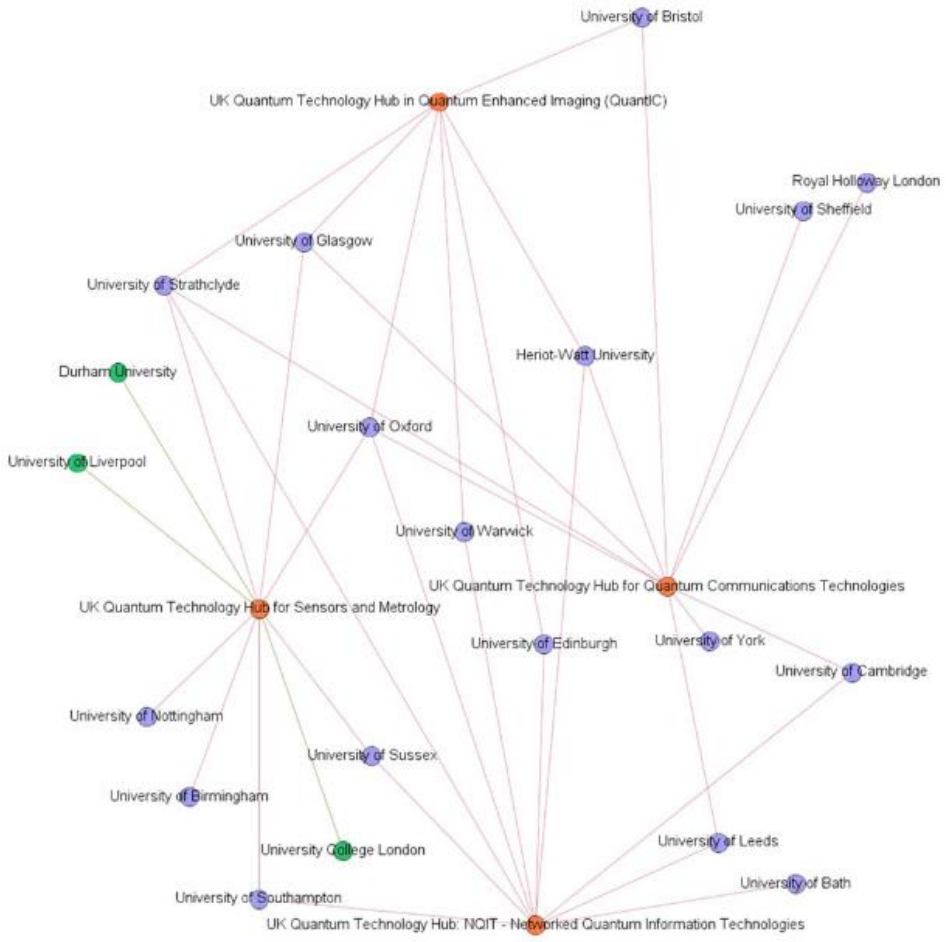
Osim prethodno navedenih projekata, inicijativa kvantna mreža u razvoju je i u ostalim Europski državama poput Ujedinjenog kraljevstva, Njemačke, Francuske, Portugala itd. Velika ulaganja posljednjih godina dovela su do želje za razvojem kvantne mreže diljem Europe U nastavku se spominju stanja kvantne mreže u nekim Europskim državama.

5.4.1. Britanski nacionalni program kvantne tehnologije (NQTP)

Ujedinjeno Kraljevstvo je, kroz kombinaciju financiranja vlade i industrije, posvetilo više od 1 milijarde funti tijekom deset godina za koordinirani program u kvantnoj tehnologiji. Pet godina nakon ovog programa, Nacionalni program kvantne tehnologije Ujedinjenog Kraljevstva izazvao je značajnu promjenu u sposobnostima nacije za uspostavu novog sektora u budućim kvantnim informacijskim tehnologijama.

Preduvjet za veliko poboljšanje potpore vlade Ujedinjenog Kraljevstva kvantnoj tehnologiji ovisio je o pokazanoj snazi kvantne znanosti. Potaknuta naporima brojnih pojedinaca, vlada Ujedinjenog Kraljevstva najavila je NQTP 2013. kako bi kvantnu informacijsku znanost u UK-u usmjerila prema kvantnoj tehnologiji koja bi pružila novu, vodeću svjetsku tehnologiju obrade informacija i zasadila tehnološki sektor koji bi otvoriti nove poslovne mogućnosti i stvoriti gospodarske prilike za UK.

Na slici 27.prikazano je kako se složeni ekosustav čvorišta i povezanih sveučilišta razvio u Ujedinjenom Kraljevstvu u ovom koordiniranom programu.



Slika 27. Mreža povezanih partnera uključenih u UK NQTP, [68]

Tehnološki centri su u narančastoj boji, a akademski partneri u ljubičastoj. Znanstveni centri usmjereni su na obuku i radnu snagu i označeni su zelenom bojom. [68]

5.4.2. PTQCI (Portugal)

Prvi segment europske kvantne komunikacijske mreže u Portugalu, nazvan PTQCI, dodijeljen je od strane Europske komisije konzorciju u kojem surađuje nekoliko portugalskih tvrtki. Cilj je implementirati prvu ultrasigurnu kvantnu komunikacijsku infrastrukturu diljem zemlje. Cilj je implementirati prvu ultra-sigurnu kvantnu komunikacijsku infrastrukturu na nacionalnoj razini, putem zemaljskih veza, ali također namjerava imati prostornu vezu, koristeći tehnologije kao što je Quantum Cryptographic Key Distribution (QKD).

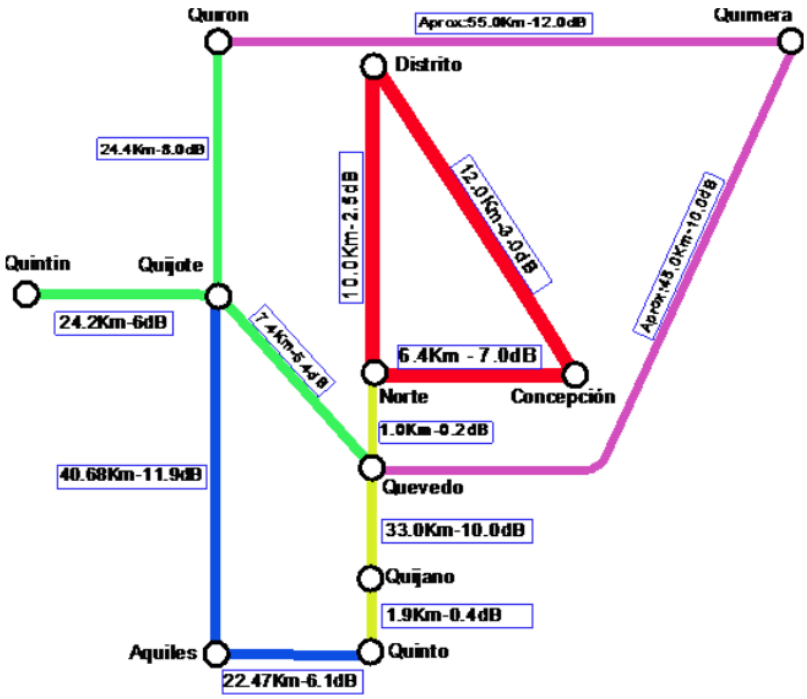
Projekt PTQCI temelji se na Discretionu, još jednom projektu započetom u prosincu 2021. koji također predviđa razvoj kvantnih komunikacija za portugalska obrambena tijela. Diskrecija je već u fazi implementacije na infrastrukturi optičkih vlakana u metropolitanskom području Lisabona, međusobno povezujući javna tijela i mrežu ispitnih stolova, uključujući akademsku zajednicu i zainteresirane tvrtke, otkriva. Jedan od QKD čvorova koji će se razviti u DISCRETION-u također će biti postavljen u PTQCI mreži. [69,70]

PTQCI će započeti 2023. godine s projektiranjem faza implementacije. Standardi i integracija koja je prva faza koja će se implementirati, a nakon toga slijedi implementacija funkcionalnih i sigurnosnih testova. Faza implementacije infrastrukture bez presedana dogodit će se 2026. godine. [69]

5.4.3. Španjolska (Madridska kvantna mreža)

Madrid Quantum Network započela je s radom 2006. godine i godinama raste i razvija se. U 2013. godini prototip mreže dizajniran za maksimiziranje dijeljenja infrastrukture za kvantnu mrežu izgrađen je u prostorijama Telefónice - najveće telekomunikacijske tvrtke u zemlji - za izradu prototipa. Kasnije je redizajniran kako bi

pokazao sposobnost distribucije isprepletenosti 2014. Veliki korak dogodio se 2018., kada je instaliran u proizvodnim pogonima Telefonice. Trenutno je to metropolitanska mreža temeljena na pouzdanim repetitorima s 12 čvorova raspoređenih među različitim točkama prisutnosti smještenim u istraživačkim centrima, tvrtkama i sveučilištima (vidi sliku 31.). Prijenosni medij (kvantni kanali) fotonskih kubita je kroz optičko vlakno. Specifičnost Madrid Quantum Network je to što je ona SDN- mreža temeljena na softveru (engl. Software Defined Network). Fleksibilnost i programabilnost SDN-a omogućuje integraciju kvantnih komunikacija u infrastrukturu. [71]



Slika 28. Linkovi Madridske kvantne mreže, [71]

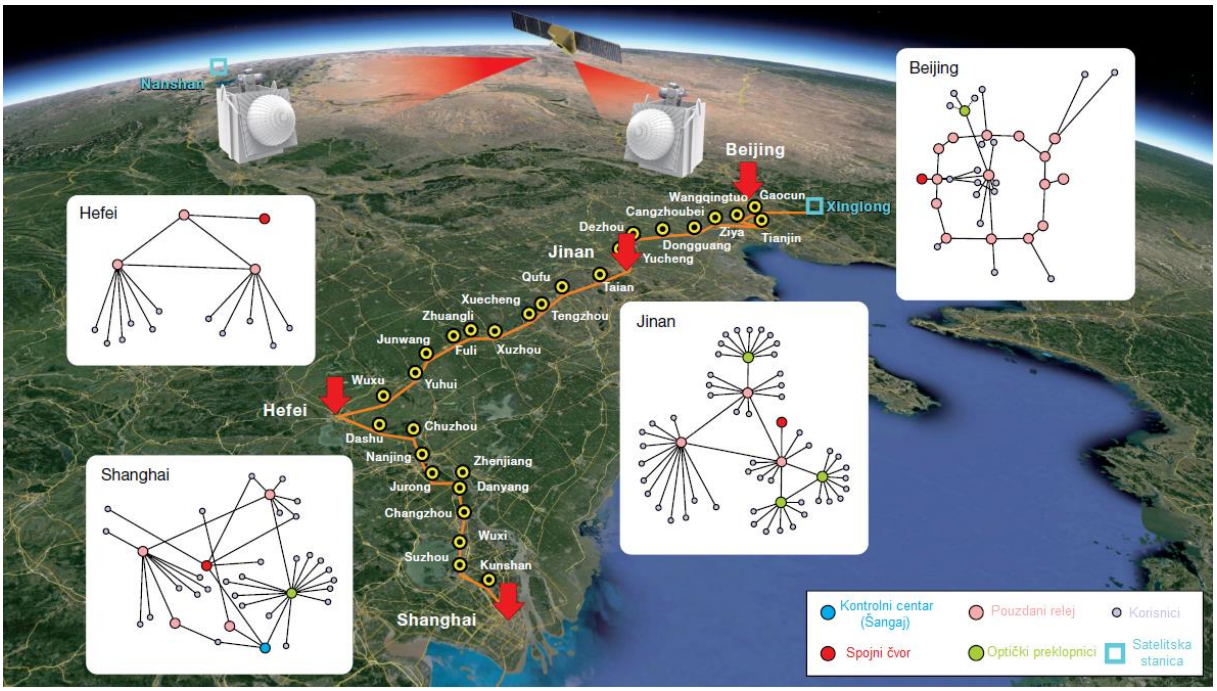
Glavni cilj u projektiranju i izgradnji Madridske kvantne mreže može se interpretirati kao smanjenje prepreka za široko usvajanje kvantnih komunikacijskih tehnologija. Kako bi se postigao ovaj cilj, postavlja se nekoliko strategija:

a) Izbjeći potrebu za odvojenom, samo kvantnom, fizičkom infrastrukturom., pokazati spremnost za proizvodnju

b) Koristiti mrežne tehnologije kompatibilne s tehnologijama nositelja za jedinstvenu logičku infrastrukturu.
c) Koristiti kvantne tehnologije koje su što je više moguće kompatibilne s komunikacijskim tehnologijama i imaju jasan put industrijalizacije. Kvantni komunikacijski uređaji moraju imati mogućnost umrežavanja.
d) Integrirati QKD u postojeći sigurnosni ekosustav, a ne kao alternativu; pokazati praktične slučajeve uporabe [72]

5.5. Europa i svijet

Osim europskim demonstracija i inicijativa kvantna komunikacijska mreža, njezin razvoj i istraživanja rasprostranjena su diljem svijeta. Kina i SAD prednjače u tom području. To potvrđuje činjenica da je Kina integrirala prvu kvantnu komunikacijsku mrežu kombinirajući više od 700 optičkih vlakana na zemlji s dvije veze zemlja-satelit kako bi se postigla kvantna distribucija ključeva na ukupnoj udaljenosti od 4600 kilometara za korisnike diljem zemlje. U 2016. Kina je lansirala prvi svjetski kvantni komunikacijski satelit (QUESS, ili Mozi/Micius) i postigla QKD s dvije zemaljske postaje koje su međusobno udaljene 2600 km. U 2017. dovršena je preko 2000 km duga mreža optičkih vlakana za QKD između Pekinga i Šangaja. Korištenjem pouzdanih releja, zemaljska optička mreža i veze satelit-zemlja integrirane su za opsluživanje više od 150 industrijskih korisnika diljem Kine, uključujući državne i lokalne banke, općinske električne mreže i web stranice e-uprave. [73]



Slika 29. Ilustracija integrirane kvantne mreže svemir-zemlja

Izvor [74]

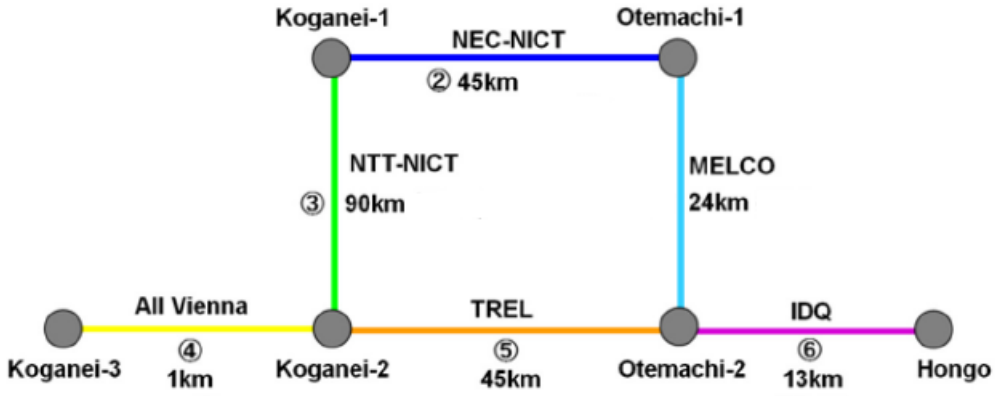
Na slici 29. prikazana je ilustratura kvantne mreže integrirana u Kini. Mreža se sastoji od četiri QMAN-a (u Pekingu, Jinanu, Šangaju i Heifeiju; crvene strelice), okosnice optičke veze preko 2000 km (narančasta linija) i dvije zemaljsko-satelitske veze koje povezuju Xinglong i Nanshan (plavi kvadratići), dužine 2600 km. Postoje tri vrste čvorova u mreži: korisnički čvorovi (ljubičasti krugovi), svepropusni optički preklopnici (zeleni krugovi) i pouzdani releji (ružičasti krugovi). Okosnicu povezuju pouzdani releji (prikazani kao žuti i crni krugovi). Kvantni satelit povezan je sa zemaljskim stanicama Xinglong i Nanshan; Xinglong je također povezan s pekinškim QMAN-om preko vlakana. U Pekingu, čvor Pekinškog kontrolnog centra nalazi se na istoj lokaciji kao i čvor okosnice veze (označen crvenim krugom). [74]

S druge strane, SAD, po mnogima i vodeća zemlja u kvantnoj komunikaciji je po mnogima u prednosti u osvajanju patenata, osnivanju startupa i ulaganjima. [75]

Kogres SAD-a 2019. godine usvojio je usvojio Zakon o nacionalnoj kvantnoj inicijativi, koji je iznio planove zemlje za brzo stvaranje sposobnosti kvantnog računalstva. Nedavno, kao svojevrsni dokaz potencijala i prvi korak prema funkcionalnim kvantnim mrežama, tim istraživača s Illinois-Express Quantum Network

(IEQNET) uspješno je postavio kvantnu mrežu na velike udaljenosti između dva laboratorija američkog Ministarstva energetike (DOE). koristeći optičko vlakno. [76]

Također , Japan je jedna od država koja je već implementirala kvantnu mrežu. Tokyo Quantum Network jedno je od načela velikih istraživanja u ovom području. kvantna mreža postavljena je u 4 okruga Tokija, sigurnost je uvijek bila u prvom planu, ali su napravljene i posebne studije za druge kvalitete kao što je brzina komunikacije. Različiti protokoli testirani su na različitom hardveru postavljanjem jedne ili više stanica u četvrtima Koganei, Otemachi, Hakusan i Hongo u Tokiju. Mreža ima ukupno 6 stanica, postoji klasična mreža između uređaja s istim hardverom koja povezuje svaku stanicu međusobno kvantnim kanalima i cijela stanica može pristupiti jedna drugoj. Neke od tih stanica koriste jednostavniji BB84 protokol, dok neke druge koriste složenije protokole. Tokijska kvantna mreža prikazana je na slici 30.



Slika 30. Konfiguracija logičke veze sa 6 čvorova

Izvor: [77]

6. ZAKLJUČAK

Današnji Internet povezuje nas globalno. Šalje pakete informacija koje prenose našu komunikaciju u klasičnim signalima - šalju se bljeskovima svjetlosti kroz optička vlakna, električnim putem kroz bakrenu žicu ili mikrovalovima radi uspostavljanja bežičnih veza. Kvantna fizika upravlja domenom vrlo malog. Omogućuje nam razumijevanje – i korištenje u našu korist – jedinstvenih kvantnih fenomena za koje ne postoji klasičan pandan. Možemo koristiti principe kvantne fizike za dizajn senzora koji vrše preciznija mjerenja, računala koja simuliraju složenije fizikalne procese i komunikacijske mreže koje sigurno međusobno povezuju te uređaje i stvaraju nove prilike za znanstvena otkrića.

Velika očekivanja i velika ulaganja idu u smjeru kvantne tehnologije. Pretpostavlja se da bi onda trebala zamijeniti kritične komunikacijske sustave u budućnosti. Možda ne one „malog“ čovjeka, ali u području vladinih organizacija, banaka, vojska i sl. gdje je i najmanji dio podatka kritičan i ne smije se dopustiti da dođe do neovlaštenih korisnika definitivno ima veliki potencijal da se to dogodi. Samim time što već postoje primjeri gdje je su kvantne tehnologije primijenjene i dokazano djeluju kako je od njih očekivano testiranjima, što u labosu, što na terenu.

Najveći problem naravno nalazi se u financijskom pitanju. Samostalna infrastruktura teško je realan izbor za bližu budućnost zbog svoje cijene, no kvantne tehnologije koje koriste uređaje postojeće infrastrukture apsolutno su isplative i održive. Važno je da je Europska unija prepoznala kvantni potencijal i spremna je ulagati velika financijska sredstava u ovo područje.

Do sada je nekoliko zemalja diljem svijeta već uspostavilo QKD mreže koje su pokrenute i implementirane za različite slučajeve uporabe. npr. banke, vlade, medicinski centri, itd. Na sličan način, Europa se usredotočuje na razvoj europske kvantne komunikacijske mreže koja se suočava s nekoliko izazova: više dobavljača, različiti standardi, različite implementacije QKD protokola i "klasične" infrastrukture .

Tijekom sljedećih godina kvantne tehnologije će početi igrati ulogu u mnogim područjima primjene, od zdravstvene zaštite, vladinih organizacija, banaka do mobilnosti i sigurnosti. Već danas se kvantna komunikacija koristi za posebne

aplikacije, ali razvojem tehnologije, njezina će se uporaba širiti i ima potencijal da postane standardna, integrirana komponenta naših komunikacijskih mreža koje se protežu diljem svijeta. Kako bi se postigao ovaj cilj, osim rješavanja raznih teoretskih izazova, značajna količina softverskog i hardverskog inženjeringa, kao i integracije sustava, još uvijek treba biti provedena u bliskoj suradnji između akademske zajednice i industrije. U period koji slijedi do 2027. godine svi se imaju pravo nadati i s očekivanjem čekati veliki razvoj kvantne komunikacije, tehnologija i mreže.

LITERATURA

[1] PicoQuant, *Quantum mechanics guarantee secure communication*, Preuzeto s: https://www.picoquant.com/applications/category/quantum-optics/quantum-communication (Zadnje pristupano: 01.07.2022.g.)

[2] Giles M. Explainer: *What is quantum communication?* Preuzeto s: https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/ (Zadnje pristupano: 01.07.2022.g.)

[3] Djordjevic, I B. *Quantum Information Theory Fundamentals. In Quantum Information Processing, Quantum Computing, and Quantum Error Correction*; 2021. Preuzeto s:: https://doi.org/10.1016/b978-0-12-821982-9.00012-5 (Zadnje pristupano:02.07.2022.g.)

[4] Bennett, C H, Shor P, W. *Quantum Information Theory. In IEEE TRANSACTIONS ON INFORMATION THEORY*

[5] Band Y. B, Avishai Y. *Quantum Mechanics with Applications to Nanotechnology and Information Science*

[6] Francoise J. P, Naber G. L, Tsun T. S. *Encyclopedia of Mathematical Physics*

[7] Jaksch D. *Quantum Communication.* University of Oxford

[8] Castelvecchi D. *Quantum network is step towards ultrasecure internet* Preuzeto s: https://www.nature.com/articles/d41586-021-00420-5 (Zadnje pristupano 07.07.2022.g.)

[9] Winton D. *What are Bell States* Preuzeto s: https://www.aliroquantum.com/blog/what-are-bell-states (Zadnje pristupano 05.07.2022.g.)

[10] Ekert A. K. *Quantum cryptography based on Bell"s Theorem*

[11] Emspak, J.,*Quantum entanglement: A simple explanation* Preuzeto s: https://www.space.com/31933-quantum-entanglement-action-at-a-distance.html (Zadnje pristupano: 05.07.2022.g.)

[12] NIST, *Entangled Photon Pair Sources* Preuzeto s: https://www.nist.gov/itl/entangled-photon-pair-sources (Zadnje pristupano 05.07.2022.g.)

[13] Tate K. *How Quantum Entanglement Works (Infographic)* Preuzeto s: https://www.livescience.com/28550-how-quantum-entanglement-works-infographic.html (Zadnje pristupano 05.07.2022.g.)

[14] Winton D. *What are Bell States* Preuzeto s: https://www.aliroquantum.com/blog/what-are-bell-states (Zadnje pristupano 06.07.2022.g.)

[15] Sych D, Leuchs G. *A complete basis of generalized Bell states;* 2009. Preuzeto s: https://doi.org/10.1088/1367-2630/11/1/013006, (Zadnje pristupano 06.07.2022.g.)

[16] Djordjevic I. *Quantum Information Processing and Quantum Error Correction*

[17] C/CS/Phys, C191 *No Cloning, Teleportation* Preuzeto s: https://inst.eecs.berkeley.edu/~cs191/fa05/lectures/lecture6_fa05.pdf, Zadnje pristupano: 24.08.2022.g.]

[18] Chapter 13. *Quantum Communication Preuzeto s: https://www.nii.ac.jp/qis/first-quantum/e/forStudents/lecture/pdf/noise/chapter13.pdf* Zadnje pristupano: 07.09.2022.g.

[19] Brennen G. *Focus on Quantum Memory* Preuzeto s: https://iopscience.iop.org/article/10.1088/1367-2630/17/5/050201/pdf Zadnje pristupano: 07.09.2022.g.

[20] Quantum Information & Communication. *Quantum Memories* Preuzeto s: https://www.unige.ch/gap/qic/qram/quantum-memories Zadnje pristupano: 09.07.2022.g.

[21] Lvovsky, A I, Sanders B: C, Tittel W. *Optical quantum memory* Preuzeto s: https://www.nature.com/articles/nphoton.2009.231 Zadnje pristupano: 07.09.2022.g.)

[22] Will F. *What is quantum network?* Preuzeto s: https://www.aliroquantum.com/blog/what-is-a-quantum-network, Zadnje pristupano: 07.07.2022.g.)

[23] Office of Science. *DOE Explains...Quantum Networks* Preuzeto s: https://www.energy.gov/science/doe-explainsquantum-networks, (Zadnje pristupano 07.07.2022.g.)

[24] Gillis A. S. *quantum cryptography* Preuzeto s: https://www.techtarget.com/searchsecurity/definition/quantum-cryptography, (Zadnje pristupano: 09.07.2022.g.)

[25] Maneesh Y. *Quantum Cryptography* Preuzeto s: http://dx.doi.org/10.13140/RG.2.2.34447.61601, (Zadnje pristupano: 12.07.2022.g.)

[26] Pirandola S, Andersen U. L, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira J. L, Razavi M. Shamsul Shaari J, Tomamichel M, Usenko V. C, Vallone G, Villoresi P, Wallden P. *Advances in quantum cryptography* Preuzeto s: https://doi.org/10.1364/aop.361502, (Zadnje pristupano: 09.07.2022.g.)

[27] Bennett C. H, Brassard G, Ekert A. K. *Quantum Cryptography* Preuzeto s: https://doi.org/10.2307/24939253 (Zadnje pristupano: 09.07.2022.g.)

[28] Quantum Exchange. *Quantum Cryptography Explained* Preuzeto s: https://quantumxc.com/blog/quantum-cryptography-explained/ (Zadnje pristupano: 09.07.2022.g.)

[29] RF Wireless World. *Advantages of Quantum Cryptography* | *disadvantages of Quantum Cryptography* Preuzeto s: https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-Quantum-Cryptography.html (Zadnje pristupano: 15.07.2022.g.)

[30] Cavaliere F, Prati E, Poti L, Muhammad I, Catuogno T, *Secure Quantum Communication Technologies and Systems: From Labs to Markets*

[31] Abellan C. *Quantum Random Number Generator (QRNG)* Preuzeto s: https://quside.com/quantum-random-number-generators-why-how-where/ (Zadnje pristupano: 20.07.2022.g.)

[32] Quantum Flagship. *Quantum Random Numbers Generator* Preuzeto s: https://qt.eu/discover-quantum/underlying-principles/qrng/ (Zadnje pristupano: 25.07.2022.g.)

[33] Quantum Flagship. *Quantum Repeaters* Preuzeto s: https://qt.eu/discover-quantum/underlying-principles/quantum-repeaters/ (Zadnje pristupano: 25.07.2022.g.)

[34] Will F. *What are quantum repeaters?* Preuzeto s: https://www.aliroquantum.com/blog/what-are-quantum-repeaters (Zadnje pristupano: 25.07.2022.g.)

[35] Ball W. D. *Field Guide to Spectroscopy*

[36] Hadfield H. R. *Single-photon detectors for optical quantum information applications Preuzeto s:* https://www.nature.com/articles/nphoton.2009.230 (Zadnje pristupano: 30.07.2022.g.)

[37] NIST. *Single-Photon Detectors* Preuzeto s: https://www.nist.gov/pml/quantum-networks-nist/technologies-quantum-networks/single-photon-detectors (Zadnje pristupano: 30.07.2022.g.)

[38] Aoun B, Tarifi N. *Quantum Networks Preuzeto s: https://arxiv.org/ftp/quant-ph/papers/0401/0401076.pdf (*Zadnje pristupano: 02.08.2022.g.)

[39] Quantum Flagship. *Quantum Key Distribution (QKD)* Preuzeto s: https://qt.eu/discover-quantum/underlying-principles/quantum-key-distribution-qkd/ (Zadnje pristupano: 02.08.2022.g.)

[40] Gillis S, A. *quantum key distribution (QKD)* Preuzeto s: https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD (Zadnje pristupano: 02.08.2022.g.)

[41] Pokiya K, Kothari J, Mahur D. *Quantum Key Distribution* Preuzeto s: https://www.researchgate.net/publication/351835879_Quantum_Key_Distribution (Zadnje pristupano: 02.08.2022.g.)

[42] ID-3. *Quantum Key Distribution* Preuzeto s: https://id-3.co.uk/wp-content/uploads/2020/10/ID-3-QKD.pdf (Zadnje pristupano: 04.08.2022.g.)

[43] Trizna A, Ozols A*, An Overview of Quantum Key Distribution Protocols*

[44] Wolf R, *Quantum Key Distribution Protocols* Preuzeto s: https://link.springer.com/chapter/10.1007/978-3-030-73991-1_4 (Zadnje pristupano: 06.08.2022.g.)

[45] Quintessence labs. *Quantum Key Distribution Systems Compared*

[46] Singh H, Gupta D. L, Singh A. K. *Quantum Key Distribution Protocols: A Review*

[47] Bennett C. H, Brassard G. *Quantum cryptography: public key distribution and coin tossing*

[48] Bennett C. H. *Quantum cryptography using any two non orthogonal states*

[49] Haitjema M. *A Survey of the Prominent Quantum Key Distribution Protocols* Preuzeto s: https://www.cs.wustl.edu/~jain/cse571-07/ftp/quantum/index.html#b92 (Zadnje pristupano: 10.08.2022.g.)

[50] Scarani V, Ribordy G, Avin A, Ginis N. *Quantum Cryptography protocols robust against Photon number Splitting attacks* Preuzeto s: http://aqis-conf.org/archives/eqis03/program/papers/O26-Scarani.pdf (Zadnje pristupano: 15.08.2022.g.)

[51] Bechmann-Pasquinucci H, Gisin N. *Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography* Preuzeto s: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.59.4238 (Zadnje pristupano: 15.08.2022.g.)

[52] ThorLabs. *Using the Poincare Sphere to Represent the Polarization State* Preuzeto s: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=14200, (Zadnje pristupano: 15.08.2022.g.)

[53] Artuh E. *Quantum cryptography based on Bell"s theorem*

[54] Wang D, Wu J, Yi X. *Optical quantum computing* Preuzeto s: https://ieeexplore.ieee.org/document/7378022/authors#authors (Zadnje pristupano: 17.08.2022.g.)

[55] Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N, Scarani V. *Towards practical and fast quantum cryptography* Preuzeto s: https://arxiv.org/pdf/quant-ph/0411022.pdf (Zadnje pristupano: 17.08.2022.g.)

[56] Inoue K, Waks E, Yamamoto Y. *Differential-phase-shift quantum key distribution using coherent light* Preuzeto s: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.68.022317, (Zadnje pristupano: 20.08.2022.g.)

[57] Quantum Manifesto. *A New Era of Technology* Preuzeto s: https://qt.eu/app/uploads/2018/04/93056_Quantum-Manifesto_WEB.pdf (Zadnje pristupano: 22.08.2022.g.)

[58] Mishra S, Bisaws A, Patil S, Chandravanshi P, Mongia V, Sharma T, Rani A, Prabhakar S, Ramachandran S, Singh R.P. *BBM92 quantum key distribution over a free space dusty channel of 200 meters* Preuzeto s: https://arxiv.org/pdf/2112.11961.pdf (Zadnje pristupano: 20.08.2022.)

[59] Quantum Flagship. *Introduction to the Quantum Flagship* Preuzeto s: https://qt.eu/about-quantum-flagship/introduction-to-the-quantum-flagship/ (Zadnje pristupano: 22.08.2022.g.)

[60] European Commission, *New quantum project aims for ultra-secure communication in Europe* Preuzeto s: https://digital-strategy.ec.europa.eu/en/news/new-quantum-project-aims-ultra-secure-communication-europe (Zadnje pristupano: 22.08.2022.g.)

[61] Poppe A, Peev M, Maurhart O. *Outline of the SECOQC Quantum-Key-Distrivution Network in Vienna* Preuzeto s: https://arxiv.org/pdf/0804.0122.pdf, (Zadnje pristupano: 25.08.2022.g.)

[62] Riedel M. *Europe's Quantum Flagship initiative* Preuzeto s: https://iopscience.iop.org/article/10.1088/2058-9565/ab042d/pdf (Zadnje pristupano: 22.08.2022.g.)

[63] Acin A. *The quantum technologies roadmap: a European community view* Preuzeto s: https://iopscience.iop.org/article/10.1088/1367-2630/aad1ea/pdf (Zadnje pristupano: 01.09.2022.g.)

[64] Peev M. *The SECOQC quantum key distribution network in Vienna* Preuzeto s: https://iopscience.iop.org/article/10.1088/1367-2630/11/7/075001/pdf (Zadnje pristupano: 23.08.2022.g.)

[65] IDQ. *About IDQ* Preuzeto s: https://www.idquantique.com/about-idq/company-profile/ (Zadnje pristupano: 29.08.2022.g.)

[66] Ribezzo D, Zahidy M, Vagniluca I, Biagi N, Francesconi S, Occhipinti T, Oxenlowe L. K, Lončarić M, Cvitić I, Stipčević M, Pušavec Ž, Kaltenbaek R, Ramšak A, Cesa F, Giorgetti G, Scazza F, Bassi A, De Natale P, Cataliotti F. S, Inguscio M, Bacco D, Zavatta A. *Deploying an inter-European quantum network*

[67] Bacco D, Da Lio B, Cozzolino D, Da Ros F, Guo X, Ding Y, Sasaki Y, Aikawa K, Miki S, Terai H, Yashimita T, Neergaard-Nielsen J. S, Galili M, Rottwitt K, Andersen U. A, Morioka T, Oxenløwe L. K. *Boosting the secret key rate in a shared quantum and classical fibre communication system*

[68] Knight P, Walmsley I. *UK national quantum technology programme* Preuzeto s: https://iopscience.iop.org/article/10.1088/2058-9565/ab4346/pdf (Zadnje pristupano: 01.09.2022.g.)

[69] Mizzy S. *Quantum network starts in Portugal! 6.8 million euros* Preuzeto s: https://europe-cities.com/2022/08/14/quantum-network-starts-in-portugal-6-8-million-euros/ (Zadnje pristupano: 04.09.2022.g.)

[70] Altice labs. *Altice Labs participates in the creation of a quantum communication network in Portugal* Preuzeto s: https://www.alticelabs.com/blog/altice-labs-participates-in-the-creation-of-a-quantum-communication-network-in-portugal/ (Zadnje pristupano: 04.09.2022.g.)

[71] Garcia Cid M. I, Ortiz Martin L, Martin V. *Madrid Quantum Network: A First Step To Quantum Internet* Preuzeto s: https://dl.acm.org/doi/pdf/10.1145/3465481.3470056 (Zadnje pristupano: 04.09.2022.g.)

[72] Martin V, Aguando A, Salas P, Sanz A.L, Brito J.P, Lopez D.R, Lopez V, Pastor A, Folgueira J, Brunner H.H, Vettelli S, Fung F, Hillerkuss D, Comanda L.C, Wang D, Poppe A, Peev M. *The Madrid Quantum Network: A Quantum-Classical Integrated Infrastructure* Preuzeto s: http://www.gcc.fi.upm.es/publications/TheMadridQuantumNetworkAQuantum-ClassicalIntegratedInfrastructure-OSA.pdf (Zadnje pristupano: 04.09.2022.g.)

[73] University of Science and Technology of China. The world's first integrated quantum communication network Preuzeto s: https://phys.org/news/2021-01-world-quantum-network.html Zadnje pristupano (07.07.2022.g.)

[74] Chen Y, Zhang Q, Chen T., Cain W, Liao S, Zhang J, Zhou F, Yuan X, Zhao M, Want T, Jiang X, Zhang L, Liu W, Li Y, Shen Q, Cao Y, Lu C, Shu R, Wang J, Li L, Liu L, Xu F, Wang X, Peng C, Pan J. *An integrated space-to-ground quantum communication network over 4,600 kilometres* Preuzeto s: https://doi.org/10.1038/s41586-020-03093-8 (Zadnje pristupano: 07.09.2022.g.)

[75] Candelon F, Bobier J. F. *Can Europe Catch Up with the US (and China) in Quantum Computing?* Preuzeto s: https://www.bcg.com/publications/2022/can-europe-catch-up-in-quantum-computer-race (Zadnje pristupano: 07.09.2022.g.)

[76] Spizzirri J. *Quantum network between two national labs achieves record synch* Preuzeto s: https://www.anl.gov/article/quantum-network-between-two-national-labs-achieves-record-synch (Zadnje pristupano: 07.09.2022.g.)

[77] Ceylan O, Yilmaz I. *Simulation Tests of Tokyo Quantum Network Preuzeto s: https://iopscience.iop.org/article/10.1088/1757-899X/1187/1/012023* (Zadnje pristupano: 07.09.2022.g.)

POPIS SLIKA

POPIS TABLICA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom „Pregled stanja kvantne komunikacijske mreže u državama EU“ , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 12.09.2022.

Goran Mihovljanec

(ime i prezime, *potpis*)