

KVANTNI INTERNET

MATIC HOČEVAR

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Kvantna komunikacija je področje, ki se ukvarja s pošiljanjem kvantnih informacij. Za to potrebujemo kvantno internetno omrežje. V članku so predstavljeni kvantnomehanski pojavi, na katerih temelji kvantni internet, in sestavni deli omrežja kvantnega interneta.

QUANTUM INTERNET

Quantum communication is a field of study that focuses on the transmission of quantum information. For this, a quantum internet network is required. This article presents the quantum mechanical phenomena on which the quantum internet is based and the components of the quantum internet network.

1. Uvod

Kvantna informatika je mlado in aktualno področje, ki preučuje kvantno komunikacijo in kvantno računalništvo. Kvantni računalnik izvaja algoritme s pomočjo kubitov, ki so osnovni elementi kvantne informatike. Ko bodo kvantni računalniki prešli iz razvojne faze v komercialno rabo, bo za prenašanje informacij med računalniki potrebno kvantno internetno omrežje. Kvantni internet temelji na pojavu kvantne prepletenosti in kvantne teleportacije. Zaradi kvantnih lastnosti, kot sta kvantna superpozicija in kolaps valovne funkcije ob meritvi, se kvantno internetno omrežje obnaša precej drugače od klasičnega internetnega omrežja. Zato ima tudi drugačno izvedbo. Posamezni gradniki kvantnega internetnega omrežja imajo podobno funkcijo kot gradniki klasičnega internetnega omrežja, vendar se razlikujejo v načinu, kako nalogo izvedejo. Vsako kvantno internetno omrežje je sestavljeno iz končnih vozlišč in fizičnih povezav. Končna vozlišča so kvantni procesorji, katerih naloga je, da kvantna stanja pripravijo, izmerijo in z njimi računajo. Fizične povezave med končnimi vozlišči so ponavadi optična vlakna. Pri prenosu informacij na dolge razdalje moramo zaradi velike absorpcije optičnih vlaken uporabiti repetitorje. V vsakem kvantnem internetnem omrežju morajo vozlišča med seboj komunicirati tudi preko klasične komunikacije, ki je lahko kar klasično internetno omrežje [1, 2].

Kvantni internet lahko uporabimo za varno komunikacijo, sinhronizacijo ur, z njim lahko vzpostavimo omrežje kvantnih senzorjev in oddaljen dostop do kvantnih računalnikov. Najbolj razvita uporaba kvantnega interneta je distribucija kvantnih ključev, ki je vrsta varne komunikacije. Razvoj kvantnega interneta je trenutno v zgodnji fazi, zato je izključno predmet eksperimentalnih študij. Največje obstoječe omrežje lahko izvaja distribucijo kvantnih ključev med osmimi uporabniki naenkrat. Predvideva se, da bo kvantni internet postal dejansko uporaben v naslednjih desetletjih [1].

2. Kvantnomehanski koncepti

2.1 Kubit

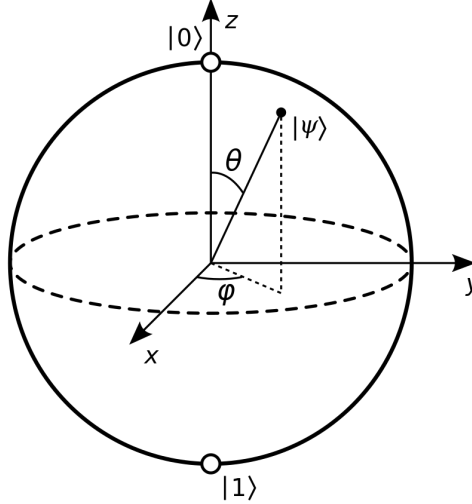
Osnovni gradnik kvantne informatike je kvantni bit ali krajše kubit. Kubit je kvantno stanje dvonivojskega sistema. Če bazna vektorja sistema zapišemo kot $|0\rangle$ in $|1\rangle$, lahko poljubno stanje zapišemo kot

$$|\Psi\rangle = c_0 |0\rangle + c_1 |1\rangle \quad \text{ali} \quad \psi = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}.$$

Kompleksni konstanti c_0 in c_1 sta normalizirani, torej velja $|c_0|^2 + |c_1|^2 = 1$. Ob upoštevanju normalizacije lahko konstante zapišemo drugače

$$|\Psi\rangle = c_0 |0\rangle + c_1 |1\rangle = e^{i\delta} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \right),$$

pri čemer velja $\theta \in [0, \pi]$ in $\phi \in [0, 2\pi)$. S pomočjo globalne umeritvene transformacije lahko člen $e^{i\delta}$ izenačimo z 1. Dana intervala kotov opišeta Blochovo sfero, kubit pa si lahko predstavljamo kot točko na sferi, ki je določena s kotoma θ in ϕ . Blochovo sfero vidimo na sliki 1 [3].



Slika 1. Blochova sfera. Vir: [4]

Primeri kubita so delec s spinom $1/2$, foton in ujeti ion. V primeru delca s spinom $1/2$ sta bazna vektorja z komponenti spina, $|\uparrow\rangle$ in $|\downarrow\rangle$. V primeru fotona, ki je primeren za prenašanje kubita na daljavo, sta bazni stanji horizontalna in vertikalna polarizacija, $|H\rangle$ in $|V\rangle$. V primeru ujetega iona, kot so iterbijev, stroncijev in kalijev ion, pa sta bazni stanji osnovno in vzbujeno stanje, $|g\rangle$ in $|e\rangle$, ali pa recimo hiperfini osnovni stanji, $|g_0\rangle$ in $|g_1\rangle$. Ujete ione se da dobro izolirati od okolja, zato jih lahko uporabimo za stacionarne dolgožive kubite [3].

2.2 Kvantna prepletenost

Kvantna prepletenost je pojav, pri katerem sta stanji dveh delcev med seboj odvisni. Valovne funkcije posameznega delca ne moremo zapisati neodvisno od valovne funkcije drugega delca [5].

Primer prepletenega stanja je singletno stanje dvoatomne molekule $|\Psi^-\rangle$. Skupna vrtilna količina takega stanja je 0, spin posameznega atoma pa je $\frac{\hbar}{2}$. Valovna funkcija singleta je

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle_{z1} |\downarrow\rangle_{z2} - |\downarrow\rangle_{z1} |\uparrow\rangle_{z2}),$$

pri čemer indeksa 1 in 2 označujeta prvi in drugi atom molekule. Recimo, da želimo izmeriti projekciji spina v z smeri. Ko izvedemo meritev projekcije spina prvega delca, se valovna funkcija singleta kolapsira v stanje $|\uparrow\rangle_{z1} |\downarrow\rangle_{z2}$ ali $|\downarrow\rangle_{z1} |\uparrow\rangle_{z2}$. Recimo, da smo izmerili stanje prvega delca $|\uparrow\rangle_{z1}$. Sedaj sledi, da bo pri kasnejši meritvi projekcije spina drugega delca meritev gotovo pokazala $|\downarrow\rangle_{z2}$. Kolaps valovne funkcije se zgodi naenkrat, kar prizadane oba delca, tudi če sta zelo daleč narazen. Singletno stanje $|\Psi^-\rangle$ je eno izmed štirih Bellovih stanj

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle_{z1} |\downarrow\rangle_{z2} \pm |\downarrow\rangle_{z1} |\uparrow\rangle_{z2}),$$

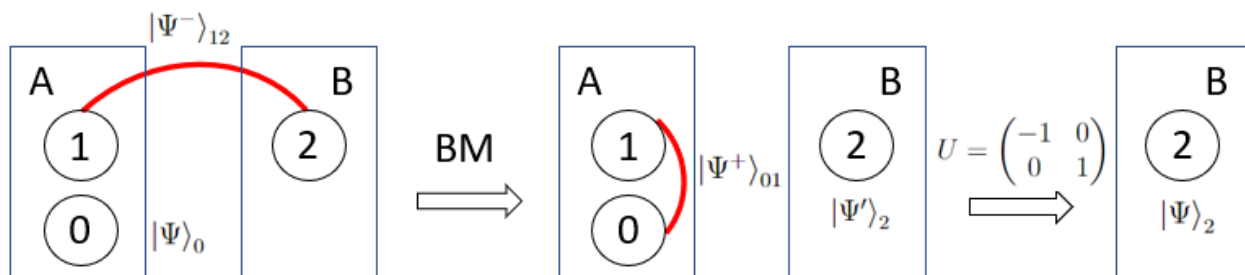
$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle_{z1} |\uparrow\rangle_{z2} \pm |\downarrow\rangle_{z1} |\downarrow\rangle_{z2}),$$

ki so maksimalno prepletena in predstavljajo ortonormalno bazo za par delcev [3].

2.3 Kvantna teleportacija

Kvantna teleportacija je pojav, ki temelji na kvantni prepletenosti. S postopkom kvantne teleportacije prenašamo kvantno informacijo, ne pa fizične snovi [3].

Prikazal bom korake protokola kvantne teleportacije, kjer prenesemo neznano kvantno stanje delca na mestu A na drug delec na mestu B. Na mestu A najprej izvedemo meritev Bellovih stanj, nato pa na mestu B na delec delujemo z ustrežno unitarno transformacijo. Shemo protokola, ki ga bom predstavil, vidimo na sliki 2.



Slika 2. Shema protokola kvantne teleportacije v primeru, ko je rezultat Bellove meritve stanje $|\Psi^+\rangle_{01}$. Slika prikazuje mesti A in B ob treh različnih časih. Na levi strani slike je prikazano začetno stanje sistema, delec 0 in delec 1 sta na mestu A, delec 2 pa je na mestu B. Stanje delca 0 želimo teleportirati na mesto B, delec 1 in 2 pa sta v prepletenem stanju. Na mestu A smo na delcu 0 in 1 izvedli Bellovo meritev in izmerili stanje $|\Psi^+\rangle_{01}$. Na delec 2 nato delujemo z unitarnim operatorjem U , ki stanje delca 2 transformira v stanje, ki je enako začetnemu stanju delca 0. Rdeči črti na sliki predstavljata prepletena para delcev.

Poglejmo si postopek teleportacije v primeru, ko pošljamo kvantno stanje elektrona, ki ga označimo z 0 in je v neznanem normiranem stanju

$$|\Psi\rangle_0 = a |\uparrow\rangle_0 + b |\downarrow\rangle_0.$$

Kvantno stanje elektrona bomo poslali z mesta A na mesto B. Poleg kubita, ki ga želimo poslati, potrebujemo za teleportacijo še par prepletenih delcev, ki sta v našem primeru elektrona v singletnem stanju z valovno funkcijo

$$|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}} (|\uparrow\rangle_1 |\downarrow\rangle_2 - |\downarrow\rangle_1 |\uparrow\rangle_2).$$

Indeksa 1 in 2 poimenujeta posamezna delca v singletu. Delec 1 fizično pošljemo na mesto A, delec 2 pa na mesto B. Iz elektrona in prepletenega para sestavimo produktno stanje

$$\begin{aligned} |\Psi\rangle_{012} &= |\Psi\rangle_0 |\Psi^-\rangle_{12} = \\ &= \frac{a}{\sqrt{2}} (|\uparrow\rangle_0 |\uparrow\rangle_1 |\downarrow\rangle_2 - |\uparrow\rangle_0 |\downarrow\rangle_1 |\uparrow\rangle_2) + \frac{b}{\sqrt{2}} (|\downarrow\rangle_0 |\uparrow\rangle_1 |\downarrow\rangle_2 - |\downarrow\rangle_0 |\downarrow\rangle_1 |\uparrow\rangle_2). \end{aligned}$$

Sedaj vpeljemo Bellova stanja delca 0 in 1 na mestu A:

$$\begin{aligned} |\Psi^\pm\rangle_{01} &= \frac{1}{\sqrt{2}} (|\uparrow\rangle_0 |\downarrow\rangle_1 \pm |\downarrow\rangle_0 |\uparrow\rangle_1), \\ |\Phi^\pm\rangle_{01} &= \frac{1}{\sqrt{2}} (|\uparrow\rangle_0 |\uparrow\rangle_1 \pm |\downarrow\rangle_0 |\downarrow\rangle_1). \end{aligned}$$

Bellova stanja predstavljajo ortonormalno bazo za delca 0 in 1. Celotno valovno funkcijo zapišemo

v bazi Bellovih stanj

$$\begin{aligned} |\Psi\rangle_{012} &= \frac{1}{2} |\Psi^+\rangle_{01} (-a |\uparrow\rangle_2 + b |\downarrow\rangle_2) \\ &\quad + \frac{1}{2} |\Psi^-\rangle_{01} (-a |\uparrow\rangle_2 - b |\downarrow\rangle_2) \\ &\quad + \frac{1}{2} |\Phi^+\rangle_{01} (-b |\uparrow\rangle_2 + a |\downarrow\rangle_2) \\ &\quad + \frac{1}{2} |\Phi^-\rangle_{01} (b |\uparrow\rangle_2 + a |\downarrow\rangle_2). \end{aligned}$$

Na mestu A sedaj na delcu 0 in 1 hkrati izvedemo Bellovo meritve, to je meritve, pri kateri je rezultat eno izmed štirih Bellovih stanj. Vidimo, da je izid meritve neodvisen od začetnega stanja $|\Psi\rangle_0$ in verjetnost, da izmerimo posamezno Bellovo stanje, je $\frac{1}{4}$. Recimo, da na mestu A izmerimo stanje $|\Psi^+\rangle_{01}$. Ob meritvi celotna valovna funkcija kolapsira in je v stanju

$$|\Psi\rangle_{012} = |\Psi^+\rangle_{01} (-a |\uparrow\rangle_2 + b |\downarrow\rangle_2).$$

Valovna funkcija delca 2 po meritvi je torej

$$|\Psi'\rangle_2 = -a |\uparrow\rangle_2 + b |\downarrow\rangle_2 = \begin{pmatrix} -a \\ b \end{pmatrix}_2.$$

Z mesta A nato preko klasične komunikacije pošljemo rezultat Bellove meritve, torej da smo izmerili stanje $|\Psi^+\rangle_{01}$, mestu B. Sedaj lahko na delec 2 delujemo z unitarno transformacijo $U = -\sigma_z = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, ki predstavlja rotacijo za 180° okoli osi z in spremembo faze. Stanje delca 2 je po rotaciji enako stanju kubita, ki smo ga želeli teleportirati:

$$|\Psi\rangle_2 = U |\Psi'\rangle_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -a \\ b \end{pmatrix}_2 = \begin{pmatrix} a \\ b \end{pmatrix}_2 = a |\uparrow\rangle_2 + b |\downarrow\rangle_2.$$

V primeru, da na mestu A izmerimo katero drugo Bellovo stanje, delujemo na delec z drugo unitarno transformacijo. V tabeli 1 vidimo unitarne transformacije, s katerimi moramo delovati na delec 2 pri različnih izidih meritve na mestu A, da je končno stanje delca 2 enako začetnemu stanju delca 0.

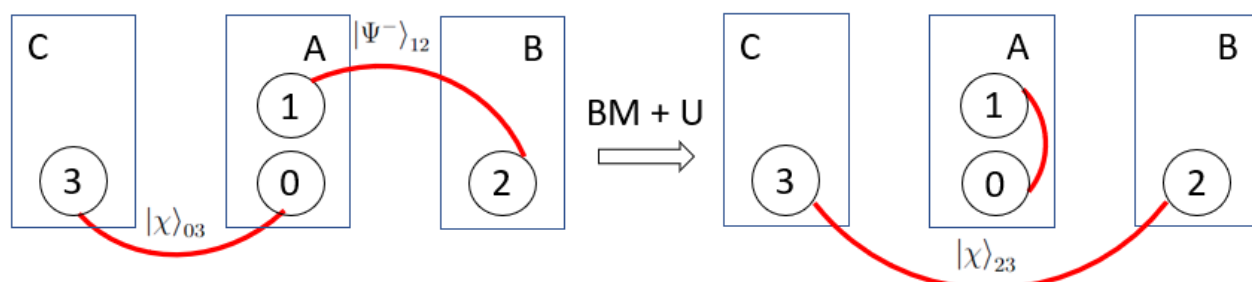
Rezultat Bellove meritve	Unitarna transformacija	Stanje delca 2 pred unitarno trans.	Stanje delca 2 po unitarni trans.
$ \Psi^+\rangle_{01}$	$-\sigma_z = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -a \\ b \end{pmatrix}$	$\begin{pmatrix} a \\ b \end{pmatrix}$
$ \Psi^-\rangle_{01}$	$-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -a \\ -b \end{pmatrix}$	$\begin{pmatrix} a \\ b \end{pmatrix}$
$ \Phi^+\rangle_{01}$	$i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -b \\ a \end{pmatrix}$	$\begin{pmatrix} a \\ b \end{pmatrix}$
$ \Phi^-\rangle_{01}$	$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} b \\ a \end{pmatrix}$	$\begin{pmatrix} a \\ b \end{pmatrix}$

Tabela 1. Unitarne transformacije s katerimi delujemo na delec 2 pri različnih rezultatih Bellove meritve in stanje delca 2 pred in po unitarni transformaciji.

Zavedati se moramo, da kvantna teleportacija ne krši postulata posebne teorije relativnosti, ki omeji hitrost prenosa informacije na svetlobno, saj informacije pošljamo preko klasične komunikacije. Za teleportacijo pa velja izrek o nekloniranju kvantnega stanja, ki pravi, da nepoznanega

stanja ni mogoče kopirati, brez da bi to stanje spremenili. V našem primeru izrek velja, saj smo kvantno stanje delca 0 prenesli na delec 2, delec 0 pa je postal prepleten z delcem 1, njuna valovna funkcija pa je eno izmed štirih Bellovih stanj [3, 6].

Teleportacijo lahko podobno izvedemo tudi s fotoni in celo s prepletenimi delci. Teleportacijo delca, ki je del prepletenega para, imenujemo zamenjava prepletenosti. Protokol zamenjave prepletenosti je podoben postopku teleportacije in ga zato ne bom še enkrat prikazal. Recimo, da je delec 0 v prepletenem stanju z nekim drugim delcem, ki ga poimenujemo delec 3, njuna začetna valovna funkcija pa je $|\chi\rangle_{03}$. Delec 3 se lahko nahaja na poljubnem mestu C, ki je lahko daleč stran od mesta A in B. Ponovno teleportiramo stanje delca 0 z mesta A na mesto B. Po teleportaciji sta delca 2 in 3 v prepletenem stanju, $|\chi\rangle_{23}$, ki je enako začetnemu stanju delcev 0 in 3, $|\chi\rangle_{03}$. Delca 2 in 3 sta po teleportaciji prepleteni par delcev, čeprav sta bila na začetku del različnih parov prepletenih delcev. Shema zamenjave prepletenosti vidimo na sliki 3 [6, 7].



Slika 3. Shema zamenjave prepletenosti. Na mestu A izvedemo Bellovo meritev, na mestu B pa z unitarno transformacijo delujemo na delec 2. Rdeče črte na sliki predstavljajo prepletene pare delcev.

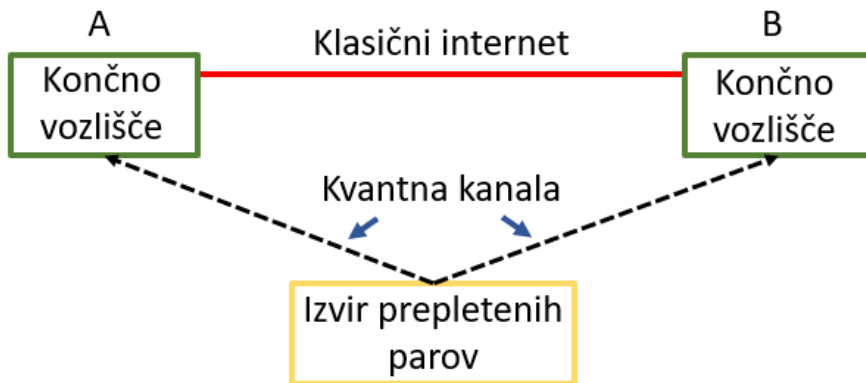
3. Sestavni deli kvantnega interneta

Kvantno omrežje sestavljajo trije glavni elementi: končna vozlišča, fizične povezave in kvantni repetitorji. Končna vozlišča so kvantni procesorji, ki jih povežemo na kvantni internet. Naloga končnih vozlišč je sprejemanje, obdelava in pošiljanje kvantne informacije. Preprosta končna vozlišča lahko pripravijo in izmerijo kubitno stanje. Bolj zapletena končna vozlišča upravljajo z večimi kubitami, imajo kvantni spomin in lahko izvajajo kvantne logične operacije. Končni vozlišči sta fizično povezani preko kvantnega kanala in klasičnega komunikacijskega omrežja. Kvantna teleportacija, s katero pošiljamo kubite med vozlišči, temelji na pojavu prepletenosti, zato potrebujemo tudi izvir prepletenih parov. Prepletene pare iz izvira pošljemo do vozlišč preko kvantnega kanala bodisi po optičnem vlaknu bodisi po ozračju in vakuumu. Prepustnost optičnega vlakna pada z razdaljo eksponentno, zato je na večjih razdaljah potrebno uporabiti repetitorje, ki vzpostavljajo prepletene pare med končnimi vozlišči. Nekatero informacije, kot so rezultati posameznih Bellovih meritev, pa pošiljamo kar preko klasičnega komunikacijskega omrežja (npr. klasični internet) [1, 2, 8].

3.1 Preprosto omrežje

Najpreprostejše kvantno omrežje je sestavljeno iz dveh končnih vozlišč, izvira prepletenih parov in fizičnih povezav. Končni vozlišči sta med seboj povezani preko klasične komunikacije, izvir prepletenih parov pa je s končnima vozliščema povezan preko kvantnega kanala, na primer preko optičnega vlakna. Shema takega omrežja vidimo na sliki 4. Poglejmo si, kako poteka pošiljanje kubita z mesta A na mesto B. Najprej v izviru prepletenih parov nastane par prepletenih fotonov. En foton pošljemo na mesto A, drugi foton pa na mesto B. Na mestu A nato na kubit in fotonu izvedemo Bellovo meritev. Rezultat meritve pošljemo preko klasične komunikacije končnemu vozlišču na mesto B, kjer na fotonu izvedemo unitarno transformacijo. Foton na mestu B je tedaj v enakem stanju,

kot je bil kubit, ki smo ga želeli teleportirati. Za lažje sledenje delcem si lahko še enkrat pogledamo sliko 2, kjer mesti A in B ustrežata vozliščema A in B na sliki 4.



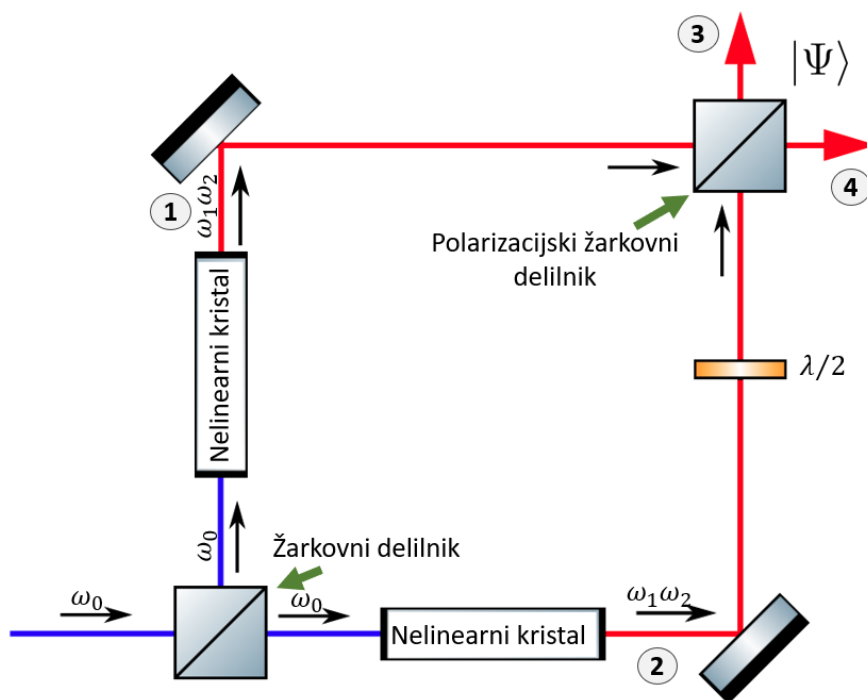
Slika 4. Shema preprostega kvantnega omrežja.

3.2 Izvir prepletenih parov

Za izvajanje protokola kvantne teleportacije potrebujemo par prepletenih fotonov, ki lahko nastane na več različnih načinov. Najpogostejši način ustvarjanja prepletenega para je spontano parametrično sipanje tipa II v nelinearnem kristalu. V nelinearnem kristalu se foton iz laserja s frekvenco ω_0 pretvori v dva fotona s frekvencama ω_1 in ω_2 , kjer zaradi ohranitve energije velja $\omega_0 = \omega_1 + \omega_2$. Za spontano parametrično sipanje tipa II je značilno, da imata nastala fotona pravokotno polarizacijo, kar pomeni, da sta v stanju $|H\rangle$ in $|V\rangle$. Kristal postavimo v primerno sestavljen interferometer in dobimo par prepletenih fotonov. Primer interferometra, ki lahko tvori par prepletenih fotonov, je prikazan na sliki 5. Foton s frekvenco ω_0 je po vhodnem žarkovnem delilniku v superpoziciji fotona veje 1 in 2. Foton v veji 1 ustvari 2 fotona v stanju $|H\rangle_1 |V\rangle_1$ s frekvencama ω_1 in ω_2 , foton v veji 2 pa v kombinaciji s ploščico $\lambda/2$ ustvari 2 fotona v stanju $|V\rangle_2 |H\rangle_2$, s frekvencama ω_1 in ω_2 . Obe veji se ponovno združita na polarizacijskem žarkovnem delilniku, prepletena fotona pa izstopita na ločenih izhodih. Na izhodu takega interferometra ima par prepletenih fotonov valovno funkcijo

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle_3 |V\rangle_4 + e^{i\theta} |V\rangle_3 |H\rangle_4 \right).$$

Indeksi v valovni funkciji nam povedo, skozi kateri izhod gre posamezni foton prepletenega para. Tak interferometer lahko uporabimo v preprostem omrežju, kot je omrežje na sliki 4. V tem primeru lahko foton, ki gre skozi izhod z oznako 3, pošljemo na mesto A, foton, ki gre skozi izhod z oznako 4, pa na mesto B [9, 10].



Slika 5. Primer interferometra, ki ustvari par prepletenih fotonov. Foton s frekvenco ω_0 gre skozi žarkovni delilnik in obstaja polovična verjetnost, da potuje po vsaki izmed vej. Stanje fotona je sedaj v superpoziciji stanja v veji 1 in veji 2. V nelinearnem kristalu iz fotona nastaneta dva fotona s frekvencama ω_1 in ω_2 z valovno funkcijo $|H\rangle|V\rangle$. V veji 2 je tudi ploščica $\lambda/2$, ki fotonsko stanje nato še zavrti v stanje $|V\rangle_2|H\rangle_2$. Obe veji se ponovno združita v polarizacijskem žarkovnem delilniku, kjer gre en foton skozi izhod z oznako 3, drugi foton pa skozi izhod z oznako 4. Valovna funkcija prepletene para fotonov je na izhodu enaka $|\Psi\rangle = \frac{1}{\sqrt{2}} (|H\rangle_3|V\rangle_4 + e^{i\theta}|V\rangle_3|H\rangle_4)$. Vir: [9]

3.3 Distribucija prepletenih parov

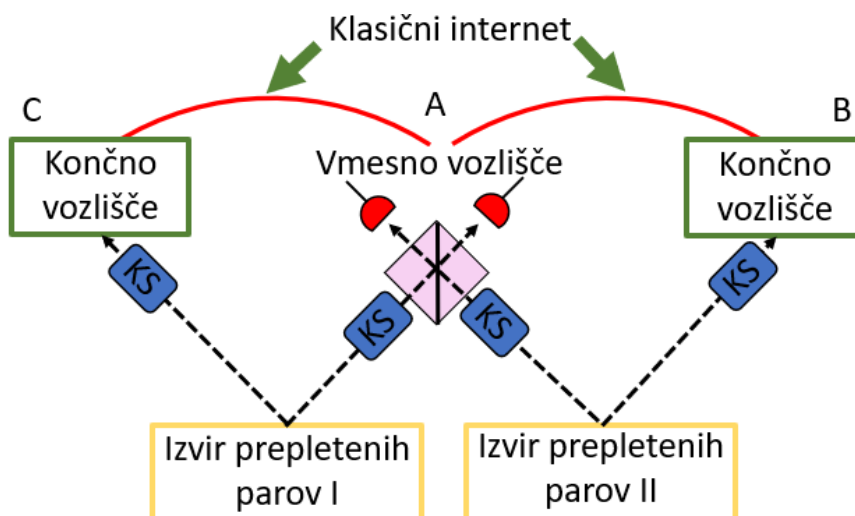
Prepleteni fotoni med vozlišči potujejo preko kvantnih kanalov po praznem prostoru ali optičnih vlaknih. Običajno za kvantno komunikacijo uporabljamo optična vlakna, za katera je značilno, da z razdaljo prepustnost fotonov pada eksponentno. Komunikacija po praznem prostoru poteka po ozračju in vakuumu. Ozračje ima sicer zelo nizko absorpcijo, vendar je podvrženo vplivom okolja, kot je na primer slabo vreme. V primeru, da komuniciramo na daljši razdalji, je smiselno pošiljati fotone tudi preko satelitov, saj je absorpcija tako najmanjša [1].

3.4 Kvantni repetitor

Po tvorbi para prepletenih fotonov pošljemo vsakega izmed fotonov po optičnem vlaknu na sosednji vozlišči. Prepustnost fotonov v mediju se z razdaljo manjša eksponentno. Karakteristična dolžina optičnih vlaken je nekaj 10 km. V primeru kvantnega interneta želimo pošiljati kvantne informacije tudi na razdalje, ki so veliko večje od karakteristične dolžine optičnih vlaken. Z večanjem razdalje med vozliščema postane verjetnost, da foton prispe na cilj, manjša. Fotone moramo zato večkrat poslati, to pa pomeni, da bo naše kvantno omrežje delovalo počasi. Želimo torej povečati verjetnost, da delca iz prepletenega para prispeta na cilj. V primeru klasičnega interneta lahko oslavljeni signal okrepimo z ojačevalcem; ta pristop pa za kvantno uporabo ni primeren, saj kubitov zaradi izreka o nekloniranju kvantnega stanja ne moremo kopirati. Namesto tega verjetnost za uspešno distribucijo prepletenih fotonov povečamo z uporabo kvantnega repetitorja. Kvantni repetitor se torej uporablja za pošiljanje kvantnih informacij na velike razdalje [2, 8].

Kvantni repetitorji so vmesna vozlišča. Njihova naloga je vzpostaviti par prepletenih delcev med dvema oddaljenima končnima vozliščema. Njihovo delovanje poteka v treh korakih. Prvi

korak je dostava prepletenih delcev sosednjima vozliščema. Iz izvira prepletenih delcev vodimo prepletena fotona po optičnih vlaknih do sosednjih vozlišč. Tudi v tem primeru velja, da verjetnost prepustnosti pada eksponentno. Zaradi krajše razdalje je sedaj verjetnost, da se foton absorbira, precej manjša. Drugi korak je očiščevanje prepletenosti. V tem postopku iz večjega števila šibko prepletenih parov ustvarimo en močnejše prepleten par. Postopek očiščevanja prepletenosti je izven obsega tega članka, v nadaljevanju predpostavimo, da so vsi prepleteni pari močno prepleteni. Tretji korak je zamenjava prepletenosti. Ta pojav je opisan v razdelku 2.3. Na vozlišču se srečata fotona iz dveh različnih izvirov in na teh dveh fotonih se izvede Bellovo meritev. Iz dveh prepletenih parov nastane en prepleten par, ki nam omogoči povezavo med bolj oddaljenimi vozlišči. Da lahko fotonoma izmerimo Bellovo stanje, morata biti sočasno na istem mestu. Fotona v vozlišče ne priletita naenkrat, zato ju shranimo v kvantnem spominu in s tem zagotovimo sočasnost fotonov v vozlišču. Primer kvantnega spomina je opisan v razdelku 3.5[2].



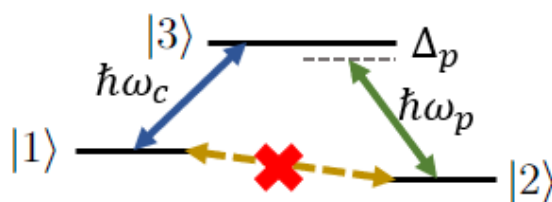
Slika 6. Shema kvantnega omrežja s tremi vozlišči A, B in C. Na vmesnem vozlišču A, ki je v tem primeru repetitor, izvajamo meritve Bellovih stanj. Vozlišča so med seboj povezana s klasičnim internetom. Iz dveh izvirov prepletenih parov vodimo prepletene fotone do posameznih vozlišč. Vozlišča imajo kvantni spomin, ki je na sliki označen s KS in zagotovi sočasnost fotonov, ki je potrebna za izvajanje Bellovih meritev.

Na sliki 6 si pogledjmo shemo preprostega omrežja, ki vključuje repetitor. To omrežje vsebuje končni vozlišči B in C ter vmesno vozlišče A, ki je v tem primeru repetitor. Iz izvira prepletenih parov I pošljemo en foton prepletenega para na vozlišče C, drugi foton prepletenega para pa na vmesno vozlišče A. Iz izvira prepletenih parov II pa pošljemo en foton prepletenega para na vmesno vozlišče A, drugi foton prepletenega para pa na vozlišče C. V vmesnem vozlišču A imamo sedaj dva fotona iz različnih prepletenih parov in izvedemo protokol zamenjave prepletenosti, torej na mestu A izvedemo Bellovo meritev, na mestu B pa na foton delujemo z ustrežno unitarno transformacijo. Rezultate Bellovih meritev ponovno pošljemo preko klasičnega interneta. Po zamenjavi prepletenosti si vozlišči B in C delita par prepletenih fotonov. Sedaj lahko izvedemo protokol teleportacije in pošljemo kubit iz vozlišča B na vozlišče C ali obratno. Za lažjo sledenje prepletenosti fotonov si lahko še enkrat pogledamo sliko 3, kjer mesta A, B, C ustrezajo vozliščem A, B, C na sliki 6.

Ko izvedemo vse tri korake, smo povezali vozlišči, ki imata skupno sosedno vozlišče. Če želimo povezati oddaljena vozlišča, moramo tretji korak večkrat ponoviti. Omrežje vozlišč najprej povežemo znotraj posameznih odsekov, nato pa odseke povežemo še med sabo. Ker se ta proces izvaja po posameznih odsekih, lahko korake izvršimo v vseh odsekih vzporedno. Vzporedno delovanje je ključno, saj poveča hitrost delovanja kvantnega interneta. V vseh treh naštetih korakih lahko pride do neuspeha. V tem primeru moramo ponoviti vse korake na tem odseku [2].

3.5 Kvantni spomin

V kvantnem spominu shranimo kvantno stanje. Pogost način izvedbe kvantnega spomina je elektromagnetno inducirana transparentnost. Gre za enostavno, poceni izvedbo, ki kvantno stanje shrani za relativno veliko časa, reda velikosti $100 \mu\text{s}$, kar je za svetlobo zelo veliko. Metoda shrani fotonsko kvantno stanje tako, da zelo upočasnimo hitrost svetlobnega pulza in s tem podaljša čas preleta. Shema atoma, ki je primeren za pojav elektromagnetne inducirane transparentnosti, vidimo na sliki 7. Ti atomi so običajno rubidijevi ali cezijevi. Vzorec atomskega plina z dvema osnovnima stanjema, $|1\rangle$ in $|2\rangle$, in enim vzbujenim stanjem, $|3\rangle$, osvetlujemo s svetlobnim pulzom s frekvenco ω_p in močnim kontrolnim laserjem s frekvenco ω_c . Frekvenca kontrolnega laserja ω_c je resonančna frekvenca za prehod med stanjema $|1\rangle$ in $|3\rangle$, zato velja $E_{31} \approx \hbar\omega_c$. Frekvenca svetlobnega pulza ω_p pa je resonančna frekvenca za prehod med stanjema $|2\rangle$ in $|3\rangle$ in velja $E_{32} = \hbar\omega_p + \Delta_p$, pri čemer je Δ_p majhen odmik od resonančne frekvence. Za naš trionovski atom prehod iz stanja $|1\rangle$ v stanje $|2\rangle$ in obratno ni mogoč [11].



Slika 7. Shema trionovskega atoma, ki je primeren za pojav elektromagnetne inducirane transparentnosti.

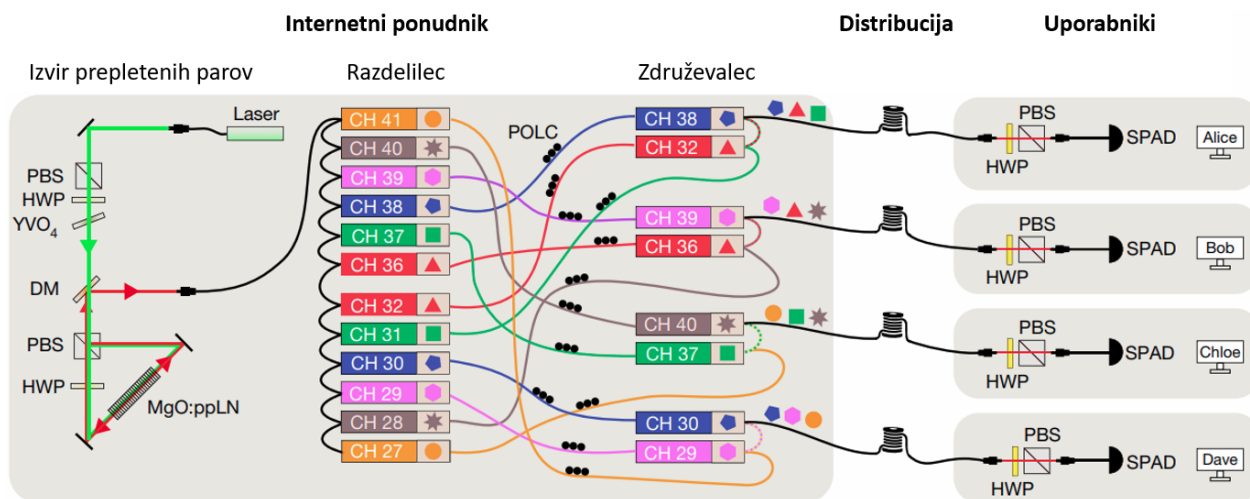
Ko z obema laserjema naenkrat posvetimo na atomski plin, ta preide v temno stanje, ki je superpozicija stanja $|1\rangle$ in $|2\rangle$. Temno stanje je tako stanje, ki se z vzbujenim stanjem $|3\rangle$ ne prekriva. Atomi plina, ki so v temnem stanju zaradi neprekrivanja ne morejo absorbirati fotonov in snov postane transparentna. Snov je popolno transparentna samo v primeru, ko velja $\Delta_p = 0$. V primeru, da ne velja $\Delta_p = 0$, se absorpcija zelo poveča. Absorpcija je sorazmerna z imaginarno komponento lomnega količnika. S pomočjo Kramers-Kronigovih relacij lahko izračunamo tudi realno komponento lomnega količnika. Grupna hitrost je definirana kot

$$v_g = \frac{c}{\text{Re } n + \omega_p \frac{\partial \text{Re } n}{\partial \omega_p}}.$$

Izkaže se, da je odvod $\frac{\partial \text{Re } n}{\partial \omega_p}$ zelo velik in zato za grupno hitrost valovnih paketov fotonov svetlobnega pulza velja $\frac{v_g}{c} \ll 1$. Grupno hitrost svetlobe je tako mogoče zmanjšati na nekaj 100 m/s , torej smo na ta način povečali čas preleta fotona za približno faktor 10^6 . Kvantno stanje lahko ob poljubnem času izpustimo iz spomina tako, da izklopimo kontrolni laser in s tem zagotovimo sočasen prihod do vozlišča z ostalimi fotoni. Fotoni morajo na vozlišče priti sočasno, da lahko na njih naredimo meritev Bellovih stanj [11].

4. Razvejana omrežja

Do sedaj smo obravnavali samo omrežje z dvema uporabnikoma, torej omrežje brez razvejanih vozlišč. Za praktično uporabo omrežja moramo omrežje razširiti na več uporabnikov. Lokalno omrežje, torej omrežje brez vmesnih vozlišč, lahko zasnujemo na več različnih načinov. Na primer, lahko pristopimo z aktivnim preklapljanjem. To pomeni, da s časom fizično spreminjamo, kateri dvojici uporabnikov pošljemo par prepletenih fotonov. Ta metoda je počasna, saj ne omogoča hkratne komunikacije večih dvojic. Naprednejša tehnika povezovanja uporabnikov je frekvenčni multipleks, ki celotno frekvenčno območje razdeli na frekvenčne kanale, to je na frekvenčne intervale,



Slika 8. Primer kvantnega omrežja s štirimi uporabniki, ki so med seboj hkrati povezani. Na levi strani slike vidimo izvir prepletenih parov. Iz izvira vodimo fotone v razdelilec, kjer se fotoni razvrstijo v frekvenčne kanale. Fotone, ki so namenjeni posameznemu uporabniku, nato v združevalcu preusmerimo v posamezno optično vlakno, ki vodi do uporabnika. Pozorni bodimo na barve frekvenčnih kanalov, saj frekvenčni kanali z enakimi barvami vsebujejo med seboj prepletene fotone. Vidimo, da do Alice vodi frekvenčni kanal, ki je obarvan modro. Drugi frekvenčni kanal, ki je tudi obarvan modro, pa vodi do Davea. Tako Alice prejme en foton iz prepletenega para, Dave pa drugega. Sedaj lahko Alice pošlje en kubit Daveu ali obratno. Analogno so povezani ostali uporabniki. Vir: [12]

ki so namenjeni posameznim signalom. Spomnimo se, da pri spontanem parametričnem sipanju tipa II iz fotona s frekvenco ω_0 nastaneta fotona s frekvencama ω_1 in ω_2 , pri čemer velja $\omega_0 = \omega_1 + \omega_2$ zaradi ohranitve energije. Zapišemo lahko

$$\omega_1 = \omega_0/2 + \Delta\omega,$$

$$\omega_2 = \omega_0/2 - \Delta\omega,$$

kjer je $\Delta\omega$ odmik od srednje frekvence $\omega_0/2$. Vidimo, da lahko taki dvojici namenimo simetričen par frekvenčnih intervalov. Fotone iz različnih frekvenčnih intervalov ločimo v razdelilcu oziroma multiplekserju s pomočjo disperzije svetlobe. Primer razdelilca je prizma, kjer se fotoni z različnimi frekvencami lomijo pod različnimi koti. Fotone iz frekvenčnih kanalov, ki so namenjeni posameznemu uporabniku, nato v združevalcu oziroma demultiplekserju preusmerimo v enojno optično vlakno, ki ga vodimo do uporabnika. Najpreprostejši način izvedbe je, da povežemo vse uporabnike med seboj. V primeru mreže z N uporabniki je vsak uporabnik povezan z ostalimi $N - 1$ uporabniki. V tem primeru je število frekvenčnih kanalov enako $N(N - 1)$, število fizičnih povezav pa je enako $N(N - 1)/2$. Primer take izvedbe s štirimi uporabniki vidimo na sliki 8. Prednost take izvedbe je, da lahko vsi pari uporabnikov komunicirajo hkrati, vendar ta metoda ni razširljiva zaradi kvadratne odvisnosti števila frekvenčnih kanalov in fizičnih povezav [12, 13].

Obstaja še boljši pristop k frekvenčnemu multipleksu. Poglejmo si primer izvedbe omrežja kvantnega interneta z osmimi uporabniki v Bristolu [14], kjer so omrežje uporabljali za distribucijo kvantnega ključa med uporabniki. V eksperimentu so demonstrirali hkratno povezavo vseh 28 dvojic osmih uporabnikov. Omrežje ne uporablja vmesnih vozlišč in je trenutno omrežje z največjim številom uporabnikov. Novost eksperimenta v Bristolu je drugačna topologija omrežja, ki omogoča linearno odvisnost frekvenčnih kanalov od števila uporabnikov. Tudi ostali sestavni deli omrežja so linearni s številom uporabnikov, zato je tak pristop razširljiv na večje število uporabnikov [14].

V primeru, da želimo povezati več oddaljenih lokalnih omrežij, pa lahko pristopimo podobno kot v primeru klasičnega interneta. Vsakemu uporabniku dodelimo internetno številko. Pošiljatelj posreduje sporočilo lokalnemu centru, ki posreduje sporočilo regionalnemu centru, ta pa posreduje sporočilo prejemniku. Tako mora pošiljatelj poznati samo številko prejemnika, ne pa celotne poti

do prejemnika [2].

5. Zaključek

Kvantni internet temelji na osnovnih kvantnomehanskih principih, kot sta superpozicija in prepletenost. Kubit je enota kvantnomehanske informacije in za prenos le-te po omrežju se uporabljata kvantna teleportacija in izmenjava prepretenosti. Sestavni deli kvantnega omrežja so izvori prepletenih parov, fizične povezave, kvantni repetitorji, kvantni spomin in končna vozlišča.

Kvantni internet bo v prihodnosti vezan na uporabo kvantnega računalnika, ki se uporablja v znanosti in industriji, povezovanje kvantnih senzorjev in na distribucijo kvantnega ključa, ki zagotovi varno komunikacijo.

Razvoj kvantne informatike bo v prihodnje omogočil obdelavo informacij na način, ki presega trenutne zmožnosti klasičnih informacijskih tehnologij. Pomemben element v razvoju bo kvantna komunikacija, ki zagotavlja varen prenos kvantnih informacij. Kvantni internet je še v zgodnji fazi razvoja in postavlja pomembne izzive za zanesljivo in učinkovito uporabo. V prihodnje bo gotovo prišlo do izboljšave vseh gradnikov kvantnega omrežja. Pomembna pa je predvsem nadgradnja kvantnih repetitorjev, kar bo povečalo hitrost prenosa informacij na večje razdalje. Velik izziv predstavlja razvejanje omrežja, saj bo temu potrebno prilagoditi vse gradnike omrežja.

LITERATURA

- [1] Stephanie Wehner, David Elkouss, and Ronald Hanson, *Quantum internet: A vision for the road ahead*, *Science* **362** (2018), no. 6412, eaam9288.
- [2] William J Munro, Koji Azuma, Kiyoshi Tamaki, and Kae Nemoto, *Inside quantum repeaters*, *IEEE Journal of Selected Topics in Quantum Electronics* **21** (2015), no. 3, 78–90.
- [3] A. Ramšak, *Kvantna mehanika*, Fizika : zbirka fizikalnih učbenikov in monografij, Založba Univerze, 2021.
- [4] Wikipedia, *Bloch sphere*, 2024, [Spletna stran: https://en.wikipedia.org/wiki/Bloch_sphere#; pridobljeno 28.2.2024].
- [5] Wikipedia, *Quantum entanglement*, 2024, [Spletna stran: https://en.wikipedia.org/wiki/Quantum_entanglement; pridobljeno 28.2.2024].
- [6] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters, *Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels*, *Physical review letters* **70** (1993), no. 13, 1895.
- [7] Marek Zukowski, Anton Zeilinger, M Horne, and Artur Ekert, *"event-ready-detectors"bell experiment via entanglement swapping.*, *Physical Review Letters* **71** (1993), no. 26.
- [8] Wikipedia, *Quantum network*, 2024, [Spletna stran: https://en.wikipedia.org/wiki/Quantum_network; pridobljeno 5.3.2024].
- [9] Žiga Pušavec, *Interferometric stabilization for a narrowband source of entangled photons*, Master's thesis, 2020.
- [10] Wikipedia, *Spontaneous parametric down-conversion*, 2023, [Spletna stran: https://en.wikipedia.org/wiki/Spontaneous_parametric_down-conversion; pridobljeno 5.3.2024].
- [11] Kenneth DeRose, Kefeng Jiang, Jianqiao Li, Macbeth Julius, Linzhao Zhuo, Scott Wenner, and Samir Bali, *Producing slow light in warm alkali vapor using electromagnetically induced transparency*, *American Journal of Physics* **91** (2023), no. 3, 193–205.
- [12] Sören Wengerowsky, Siddarth Koduru Joshi, Fabian Steinlechner, Hannes Hübel, and Rupert Ursin, *An entanglement-based wavelength-multiplexed quantum communication network*, *Nature* **564** (2018), no. 7735, 225–228.
- [13] Wikipedia, *Frequency-division multiplexing*, 2024, [Spletna stran: https://en.wikipedia.org/wiki/Frequency-division_multiplexing; pridobljeno 12.3.2024].
- [14] Siddarth Koduru Joshi, Djeylan Aktas, Sören Wengerowsky, Martin Lončarić, Sebastian Philipp Neumann, Bo Liu, Thomas Scheidl, Guillermo Currás Lorenzo, Željko Samec, Laurent Kling, et al., *A trusted node-free eight-user metropolitan quantum communication network*, *Science advances* **6** (2020), no. 36, eaba0959.