ELEKTROTEHNIŠKI VESTNIK 92(N): 52–60, 2025
PREGLEDNI ZNANSTVENI ČLANEK

Priložnosti in izzivi kvantnih satelitskih komunikacij

Katarina Radaković[1], Vesna Eržen[1], Lara Ulčakar[2,3], Anton Ramšak[2], Boštjan Batagelj[1], Rainer Kaltenbaek[2], Andrej Lavrič[1]

[1]*Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška cesta 25, 1000 Ljubljana, Slovenija*
[2]*Univerza v Ljubljani, Fakulteta za matematiko in fiziko, Jadranska ulica 19, 1000 Ljubljana, Slovenija*
[3]*Institut Jožef Stefan, Jamova cesta 39, 1000 Ljubljana, Slovenija*
E-pošta: andrej.lavric@fe.uni-lj.si

Povzetek. Kvantna komunikacija prek optičnih satelitskih povezav je ključen korak h globalnim varnim komunikacijskim omrežjem. Ta članek ponuja celovit pregled priložnosti in izzivov povezanih z implementacijo kvantnih komunikacijskih tehnologij prek optičnih satelitskih povezav. Raziskujemo potencial sistemov za kvantno razdeljevanje ključev (angl. Quantum Key Distribution – QKD) na dolge razdalje, kvantno prepleteno razdeljevanje in izgradnjo globalnih kvantnih omrežij, ki presegajo omejitve zemeljskih sistemov temelječih na vlaknih. Edinstvene lastnosti optičnih satelitskih povezav, vključno z njihovo zmožnostjo pokrivanja velikih razdalj z minimalno izgubo signala, ponujajo obetavne priložnosti za robustne kvantne komunikacije. Vendar pa obstajajo pomembni tehnični in okoljski izzivi za uresničitev teh sistemov, ki se nanašajo na zračno turbulenco, sledenje in usmerjanje žarka ter izgubo fotonov. Poleg tega obravnavamo potrebo po mednarodnem sodelovanju, standardizaciji in regulativnih okvirih, da bi zagotovili brezhibno integracijo v obstoječo komunikacijsko infrastrukturo. Z analizo nedavnih poskusnih predstavitev in teoretičnega razvoja ta članek poudarja ključne mejnike, ki so bili doseženi, in opredeljuje področja za nadaljnji razvoj. Članek osvetljuje potencial satelitskih kvantnih komunikacij in njihovo vlogo pri oblikovanju naslednje generacije varnih komunikacijskih sistemov.

Ključne besede: kvantna tehnologija, telekomunikacije, kvantna komunikacija, satelitska komunikacija, kvantno razdeljevanje ključev, kibernetska varnost,

Opportunities and challenges of quantum satellite communications

Quantum communication via optical satellite links is a crucial step towards global secure communication networks. This paper provides a comprehensive overview of the opportunities and challenges associated with the implementation of quantum communication technologies over optical satellite links. We explore the potential of such systems for long-distance quantum key distribution (QKD), quantum entanglement distribution, and the construction of global quantum networks that overcome the limitations of terrestrial fiber-based systems. The unique properties of optical satellite links, including their ability to span long distances with minimal signal loss, offer promising opportunities for robust quantum communications. However, there are significant technical and environmental challenges to realizing these systems, including atmospheric turbulence, beam tracking and pointing, and photon loss. In addition, we address the need for international cooperation, standardization and regulatory frameworks to ensure seamless integration into the existing communications infrastructure. By analyzing recent experimental demonstrations and theoretical developments, this paper highlights the crucial milestones that have been achieved and identifies key areas for future research. Our findings highlight the transformative potential of satellite-based quantum communications and its role in shaping the next generation of secure communication systems.

Keywords: quantum technology, telecommunications, quantum communication, satellite communication; quantum key distribution, cybersecurity

Prejet 3. marec, 2025
Odobren 21. marec, 2025

1 UVOD

V sodobni informacijski družbi je zahtevana varna in zasebna komunikacija, pri čemer je računska kompleksnost določenih matematičnih operacij temelj tradicionalnega šifriranja [1]. Po drugi strani pa v zadnjih desetletjih prihaja v ospredje kvantno razdeljevanje ključev (angl. *Quantum Key Distribution* – QKD), ki je najbolj znan primer uporabe kvantnega šifriranja ter ponuja varno rešitev problema izmenjave šifrirnih ključev s pomočjo zakonov kvantne fizike [2]. Skupni, naključni niz skrivnih šifrirnih bitov, znan kot skrivni ključ, lahko ustvarita dva oddaljena uporabnika, zahvaljujoč zakonom kvantne mehanike, pa je varen pred kakršnimkoli prisluškovanjem [3]. Ta ključ ponuja varen način šifriranja (in dešifriranja) sporočila, zato ga je mogoče poslati po javnem komunikacijskem kanalu.

Zmožnost obeh uporabnikov, da identificirata katero koli tretjo osebo, ki poskuša zlonamerno prevzeti ključ, je pomembna lastnost QKD. To izhaja iz osnovnega načela kvantne mehanike, da postopek merjenja kvan-

tnega sistema v splošnem moti sam sistem. Ključ, ki ga želi izmeriti tretja oseba z namenom prisluškovanja, povzroči opazne nepravilnosti v originalnem ključu. To pomeni, da je z uporabo kvantne superpozicije ali kvantne prepletenosti in prenosa informacij v kvantnih stanjih mogoče implementirati komunikacijski sistem, ki zaznava prisluškovanje. Mogoče je ustvariti ključ, ki bo zagotovo varen, če ne bo zaznano prisluškovanje. V nasprotnem primeru se komunikacija prekine in ni mogoče uporabiti nobenega varnega ključa. Vsa ta načela so že dolgo znana in tudi implementirana v zemeljskih komunikacijah prek optičnih vlakenskih povezav, vendar zaradi slabljenja optičnega vlakna ne dosegajo globalnih razsežnosti.

Naraščajoče povpraševanje po višjih podatkovnih zmogljivostih se je v zadnjih letih odražalo v razvoju t.i. prostozračnih optičnih komunikacij (angl. *Free Space Optics Communication* – FSOC). FSOC je alternativna rešitev za dostop do končnega uporabnika [4]. Konvencionalne radiofrekvenčne (angl. *Radio Frequency* – RF) in mikrovalovne tehnologije imajo v primerjavi s FSOC omejeno frekvenčno pasovno širino. Dodatno pa FSOC v kombinaciji z optično vlakensko infrastrukturo poveča zanesljivost omrežja [5].

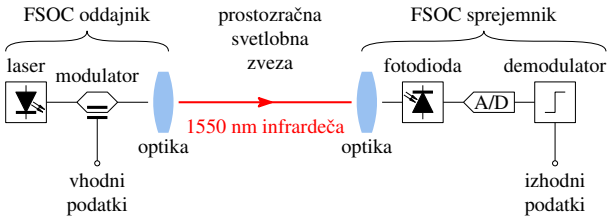
V zadnjem desetletju je komercializacija vesolja povzročila ogromno povečanje majhnih umetnih satelitov v nizki zemeljski tirnici (angl. *Low Earth Orbit* – LEO), kjer po številu nedvomno izstopajo sateliti Starlink [6], ki so za medsebojno neposredno komunikacijo prvi začeli uporabljati tehnologijo FSOC. S tem so se pokazale možnosti, da satelitske konstelacije v LEO na osnovi FSOC postanejo globalna rešitev za varno izmenjavo kvantnih šifrirnih ključev na dolge razdalje. To lahko preseže alternative osnovane na optičnih vlaknih. Prenos tehnoloških rešitev QKD, ki so zasnovane na optičnih vlaknih, na tehnologijo FSOC ni preprost in je povezan z nekaterimi tehnološkimi izzivi. Omejitve se nanašajo na raznovrstne motnje v ozračju, na potrebo po neposredni vidljivosti in nenazadnje po zanesljivih relejnih postajah (angl. *trusted nodes*), ki pa so seveda zahtevane tudi na daljših povezavah po optičnih vlaknih.

V zadnjem desetletju je bilo izvedenih več uspešnih demonstracij QKD prek satelita na osnovi prepletenih fotonov[7] in protokola BB84 [8], [9], [10], [11]. Evropska unija (EU) je leta 2025 razpisala projekt Connecting Europe Facility (CEF), katerega cilj je ustvariti prvo evropsko QKD satelitsko omrežje, pri katerem se bodo sodelujoče članice EU priklopile na evropski satelit Eagle-1, ki bo nosil napravo za QKD. QKD bo deloval na osnovi protokola BB84 z metodo vabe (angl. *decoy state*).

V tem preglednem članku so najprej izpostavljene edinstvene lastnosti optičnih satelitskih povezav, vključno z njihovim potencialom premagovanja velikih razdalj z minimalno izgubo signala, kar ponuja obetavne priložnosti za robustne kvantne komunikacije. Nadalje članek opisuje tehnologiji prostozračne optične zveze in kvantnega razdeljevanja ključev. V četrtem poglavju sledi opis strukture kvantnih komunikacijskih omrežij. Peto poglavje osvetli možnosti in podaja izzive, ki jih prinašajo satelitske omrežne arhitekture za kvantno razdeljevanje ključev. Pomembni tehnični in okoljski izzivi za uresničitev kvantnih komunikacijskih sistemov, vključno s turbulenco v ozračju, sledenjem in usmerjanjem žarka ter izgubo fotonov so izpostavljeni v šestem poglavju. V zaključku članka se opredeljujemo o napredku in razvoju na tem področju.

2 PROSTOZRAČNA OPTIČNA KOMUNIKACIJA

Delovanje FSOC, ki je prikazano na sliki 1, je precej preprosto. Modulirana laserska svetloba se prenaša med oddajnikom in sprejemnikom. Svetloba se fokusira proti sprejemniku z uporabo leč ali paraboličnih zrcal, kjer se ujame in usmeri na optični detektor. Z detekcijo na navadni polprevodniški fotodiodi se optični signal pretvori v električnega.



Slika 1: Gradniki optične komunikacije v prostem prostoru (angl. *Free Space Optics Communication* – FSOC)

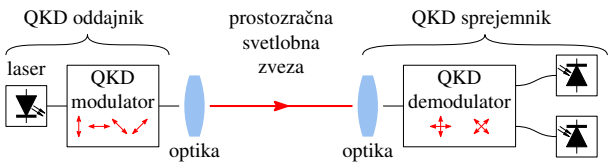
V nasprotju z drugimi brezžičnimi sistemi, ki uporabljajo RF-spekter, tehnologija FSOC uporablja vidni in infrardeči (IR) svetlobni spekter [12]. Prednost svetlobnega spektra je, da je ne-licenciran, saj naprave FSOC navadno delujejo na skoraj infrardečih (angl. *near-infrared* – NIR) valovnih dolžinah med 700 in 1600 nm [13]. Ta spekter ni podvržen licenciranju tudi zato, ker je signal oddan v manjšem prostorskem kotu in je posledično sistem manj dovzeten za motenje. Ker FSOC porabi manj energije kot brezžični RF-sistemi, je cenejši in ima manjši vpliv na okolje. Njegovi ozki žarki potujejo skozi manjši prostor, s čimer dosežejo večje gostote moči. Tako se odpravi potreba po oddajnikih visoke moči. V FSOC so mogoče tudi majhne izvedbe oddajnikov v nasprtju z RF-zvezami, kar je slabost, ki izvira iz velikosti RF-anten. Ker je optične povezave težje prestreči, FSOC zagotavlja tudi večjo varnost [14]. Tehnologija FSOC postaja vse pomembnejši del satelitskih komunikacij, ne glede na to, ali gre za komunikacijo med satelitom in Zemljo ali med dvema satelitoma. To je še zlasti uporabno v slednjem primeru, ko ni vplivov ozračja, s čimer so teoretično mogoče podatkovne hitrosti terabitov na sekundo [6].

Pri analizi delovanja FSOC je treba upoštevati številne zunanje in notranje veličine. Na zasnovo sistema FSOC

vplivajo notranje veličine, ki vključujejo občutljivost sprejemnika, stopnjo bitnih napak (angl. *bit error rate* – BER), premer sprejemne leče in vidno polje sprejemnika (angl. *Field of View* – FOV) na sprejemni strani ter optično moč, valovno dolžino, pasovno širino prenosa, divergenčni kot in optično izgubo na oddajni strani. Vidljivost in slabljenje v zraku, migotanje (scintilacija), medsebojna razdalja, izguba okna in izguba zaradi nepravilne poravnave so primeri zunanjih veličin, ki so povezani z okoljem, v katerem mora sistem delovati [12].

3 KVANTNO RAZDELJEVANJE KLJUČEV

Kvantno razdeljevanje ključev (angl. *Quantum Key Distribution* – QKD) temelji na razdeljevanju kvantnih bitov (kubitov) med dvema uporabnikoma. Ob meritvi kubitov generirata enaki naključni zaporedji števil tako, da je varno pred nepooblaščenim dostopom. Najbolj znan protokol QKD je BB84, ki sta ga razvila Charles Bennett in Gilles Brassard leta 1984 [15]. V nasprotju s tradicionalnimi metodami izmenjave ključev, ki temeljijo na matematičnih orodjih, se QKD zanaša na načela kvantne fizike. V ospredju sta predvsem dve načeli: načelo superpozicije in načelo kvantne prepletenosti fotonov; pomembno pa je tudi Heisenbergovo načelo nedoločenosti. QKD za kodiranje kubitov uporablja lastnosti fotona, kot sta polarizacija in faza, lahko pa za kodiranje uporabi tudi amplitudo signala. Ta kvantna stanja so občutljiva in jih ni mogoče izmeriti ali prestreči, ne da bi motnjo odkrili, zaradi česar je prisluškovanje mogoče zaznati. Tehnologija QKD omogoča varno izmenjavo šifrirnih ključev po optičnih povezavah, ki so lahko žične (z uporabo optičnih vlaken) ali brezžične (FSOC), kot prikazuje slika 2. Vendar pa se omrežja QKD, ki temeljijo na optičnih vlaknih, soočajo s številnimi izzivi pri razdeljevanju tajnih ključev na širših geografskih območjih. To je predvsem posledica eksponentnega povečanja izgube moči v odvisnosti od razdalje v optičnih vlaknih, kar močno omejuje izmenjavo šifrirnih ključev na velikih razdaljah [4].



Slika 2: Gradniki prostozračne optične komunikacije (angl. *Free Space Optics Communication* – FSOC) za kvantno razdeljevanje ključev (angl. *Quantum Key Distribution* – QKD)

Komunikacija za kvantno izmenjavo ključev se izvaja na dveh kanalih: kvantnem kanalu, ki se uporablja za prenos kvantnih stanj in klasičnem kanalu, ki se uporablja za usklajevanje ključev in odpravljanje napak.

Glede na tip spremenljivke lahko protokole QKD razdelimo v dve skupini, odvisno od vrste kvantnih stanj, uporabljenih za kodiranje informacij. Razlikujemo kvantno razdeljevanje ključa z uporabo zveznih spremenljivk (angl. *Continuous Variable QKD* – CV-QKD) in kvantno razdeljevanje ključa z uporabo diskretnih spremenljivk (angl. *Discrete Variable QKD* – DV-QKD). Gre za dva različna pristopa kvantnega razdeljevanja ključev, ki temeljita na različnih načelih in metodah prenosa kvantnih informacij, zahtevata pa tudi drugačno strojno opremo na fizičnem nivoju [16].

3.1 DV-QKD

Ključni koncept protokolov DV-QKD je uporaba diskretnih kvantnih stanj (navadno posameznih fotonov) za kodiranje informacij. Vsak kubit lahko predstavlja stanje 0, 1 ali superpozicijo obeh, kar omogoča inovativno in učinkovito kodiranje informacij. Kvantni lastnosti, ki se v tem primeru uporabljata, sta polarizacija in faza fotona. Najpogosteje uporabljena protokola pa sta BB84 in E91, ki ga je predlagal Artur Ekert leta 1991 [17]. Izmenjava ključev po protokolu BB84 z uporabo polarizacije poteka po naslednjem zaporedju: oddajnik generira šibki impulz na nivoju posameznih fotonov, recimo z močno oslabljenim laserjem. Oddajnik nato naključno izbira med dvema polarizacijskima bazama: premočrtno (horizontalna in vertikalna) ali diagonalno (+45° in -45°). Vsak kubit je kodiran v polarizaciji šibkega impulza glede na izbrano bazo. Kubiti se nato pošljejo prek kvantnega kanala do sprejemnika, ki jih pomeri. Navadno se za merjenje polarizacije prejetih kubitov uporabljajo polarizacijski žarkovni razcepnik (angl. *Polarization Beam Splitter* – PBS) in detektorji posameznih fotonov. Sprejemnik prav tako naključno izbere eno od dveh polarizacijskih baz in izmeri polarizacijo kubita. Rezultatom meritev se pripiše bitne vrednosti, recimo 0 se pripiše meritvi horizontalne ali diagonalne polarizacije, 1 pa meritvi vertikalne ali antidiagonalne. Meritve kubitov, ki so bili zakodirani in pomerjeni v isti bazi, se ohranijo, preostale se zavrže. Po opravljeni meritvi se napake odpravljajo z usklajevanjem izbranih baz med oddajnikom in sprejemnikom prek klasičnega komunikacijskega kanala. Ta postopek vključuje primerjavo izmerjenih vrednosti, da se ugotovi morebitna neskladnost, ki lahko nastane zaradi šuma ali poskusov prisluškovanja, kar je ključno za zagotavljanje varnosti in zanesljivosti komunikacije v klasičnih sistemih. Po meritvah je treba izvesti algoritem odpravljanja napak. Najprej se oceni pogostnost kubitne napake (angl. *Quantum Bit Error Rate* – QBER), in če ta preseže teoretično določeno vrednost, to pomeni, da nekdo prisluškuje. Če je nižji, pa se izvede algoritem odpravljanja napak. S tem QKD ponuja dodatne mehanizme za zaščito pred napakami in prisluškovanjem s pomočjo kvantnih lastnosti, kar povečuje celotno varnost ključa. Odkritje prisluškovanja, ki je mogoče s prekomerno povečanim QBER, dodatno krepi integriteto prenesenega ključa. Varnost QKD je bila potrjena v številnih raziskavah in eksperimentalnih testiranjih, prav tako študije, povezane s protokolom

BB84, potrjujejo njegovo učinkovitost, kar ga še naprej uvršča med temeljne pristope v kvantni komunikaciji.

Eden od mogočih napadov na protokole QKD je napad prestrezanja in ponovnega pošiljanja. To se zgodi, ko prisluškovalec prestreže fotone, jih izmeri in ponovno pošlje prejemniku. Ker prisluškovalec ne pozna baze polarizacije oddajnika, lahko pomeri polarizacijo v napačni bazi in s tem podre valovno funkcijo, kar privede do končne QBER. Z rednim preverjanjem stopnje napak oddajnik in sprejemnik zaznata prisluškovanje in če zaznata preveč napak, se protokol prenosa šifrirnega ključa prekine.

BB84 je bil pozneje nagrajen v različico, poimenovano QKD z metodo vabe. Ta uporablja posebne šibke koherentne impulze, ki delujejo kot "vabe"in prisluškovalcem preprečujejo, da bi ugotovili, kateri šibki koherentni impulzi so pravi in kateri ne.

Poleg protokola BB84 in QKD z metodo vabe se v kvantni kriptografiji uporabljajo tudi drugi protokoli, kot sta že omenjeni protokol E91 in BBM92 (Bennter, Brassard, Mermin, 1992). Medtem ko uporabne implementacije protokola E91 še ni, na BBM92 temeljijo vsi protokoli na osnovi kvantne prepletenosti. Njegov princip je deljenje prepletenih parov fotonov in njihova uporaba za ustvarjanje ključev. Pri tem varnost temelji na Bellovem izreku [18].

3.2 CV-QKD

Kvantno razdeljevanje ključa z uporabo zveznih spremenljivk (CV-QKD) je pozneje razviti pristop h QKD, ki kodira informacije z uporabo zveznih lastnosti svetlobe, kot so amplitudne in fazne kvadrature koherentnih stanj [19]. Njegova bistvena prednost je, da je združljiv z obstoječimi klasičnimi optičnimi sistemi, kar ima pomemben ekonomski učinek; v določenih pogojih ponuja tudi hitrejši prenos. Za generiranje koherentnih stanj svetlobe se uporabljajo obstoječi laserski viri, za merjenje kvadratur vhodne svetlobe pa homodinska ali heterodinska detekcija, ki je lažje izvedljiva kot detekcija posameznega fotona. Amplitudna (X) in fazna (P) kvadratura protokolov CV-QKD sta zvezni in modulirani glede na Gaussovo porazdelitev.

Protokoli CV-QKD na splošno delujejo tako, da oddajnik ustvari naključni Gaussov porazdeljeni niz vrednosti, ki kodirajo informacije v amplitudnih in faznih kvadraturah svetlobe. Kvadrature so modulirane z uporabo standardnega laserskega vira, koherentna stanja pa so poslana sprejemniku po obstoječem optičnem kanalu. Sprejemnik nato izmeri kvadraturo z uporabo homodinske ali heterodinske detekcije. Pri homodinski detekciji gre za merjenje kvadrature X ali P, medtem ko heterodinska vključuje sočasno merjenje obeh kvadratur. Pri sprejemu lahko pričakujemo nepopolnosti prejetih podatkov, ki so posledica izgub in šuma na prenosni poti. Oddajnik in sprejemnik primerjata svoje merilne baze in se tako kot pri DV-QKD odločita, katere meritve bosta obdržala in katere ne. Obdržita le tiste, pri katerih se baze ujemajo.

Izzivi CV-QKD izhajajo iz kompleksne narave tovrstnih protokolov, zlasti pri oblikovanju in izvajanju varnostnih analiz. Teoretična podlaga CV-QKD vključuje zahtevne matematične modele kvantnih mehanizmov, kar otežuje preverjanje varnosti protokolov pred morebitnimi napadi. Poleg tega je raznolikost detektorjev, uporabljenih v sistemih CV-QKD, povezana z dodatnim šumom, ki lahko vpliva na natančnost meritev. Visokozmogljivi detektorji, kot so tisti, ki delujejo na osnovi kvantnega šuma, lahko vnašajo napake v meritev, kar otežuje odkrivanje prisluškovanja in zmanjšuje skupno zanesljivost prenosa informacij [20], [21], [22], [23]. V tabeli 1 je podana primerjava med DV-QKD in CV-QKD.

4 STRUKTURA IN TEHNOLOGIJE KVANTNIH KOMUNIKACIJSKIH OMREŽIJ

Kvantna omrežja imajo podobno osnovno strukturo kot klasična omrežja [24]. Vsebujejo vozlišča, kjer se uporabljajo kvantni procesorji z vsaj enim kubitom. V zapletenejših primerih je treba imeti več kubitov in kvantni pomnilnik, kar poveča kompleksnost. Glavna prednost kompleksnejših vozlišč je, da lahko shranjujejo in ponovno prenašajo kvantne podatke, ne da bi motili kvantna stanja [25].

Nekateri ključni elementi strojne opreme, ki bistveno ločijo kvantne komunikacijske sisteme od klasičnih, so enofotonski viri in detektorji. Oslabljeni laserji so najpogostejša vrsta enofotonskih virov. So stroškovno učinkoviti, preprosti za izvedbo in imajo zelo visoko stopnjo ponavljanja. Ustvarjajo šibke koherentne svetlobne impulze, kjer je povprečno število fotonov na impulz nadzorovano tako, da je zelo majhno. S tem lahko posnemajo enofotonske vire, zato so uporabni tudi v protokolih DV-QKD. Porazdelitev števila fotonov sledi Poissonovi porazdelitvi: večina impulzov vsebuje nič ali en foton; verjetnost, da vsebuje več fotonov, je majhna.

Drugi pogosti viri fotonov so viri prepletenih fotonov. Proizvajajo prepletene pare fotonov, pri čemer je stanje enega fotona močno korelirano z drugim, ne glede na razdaljo med njima. Ti viri se generirajo s pomočjo nekaterih metod, kot so: spontana parametrska pretvorba navzdol (angl. *Spontaneous parametric down-conversion* – SPDC) [26], spontano štirivalovno mešanje (angl. *Spontaneous Four-wave Mixing* – SFWM) [27], kvantne pike [28] ali hladni atomi [29] in ujeti ioni [30]. Vendar pa so ti viri zelo kompleksni, saj zahtevajo natančno usklajevanje in visokozmogljivo nelinearno optiko, kar lahko znatno poveča stroške njihove izvedbe[4], [31].

Najpogosteje uporabljeni detektorji posameznih fotonov so t.i. plazovni detektorji (angl. *Single-photon avalanche diode* – SPAD) in superprevodni nano-žični enofotonski detektorji (angl. *Superconducting nanowire single-photon detector* – SNSPD). SPAD je zgrajen iz

Vidik	CV-QKD	DV-QKD
kodiranje	zvezne vrednosti (amplituda, faza)	diskretne vrednosti (binarna stanja, 0/1)
vir	koherentni vir svetlobe (laser)	enofotonski in koherentni viri
detekcija	homodinska ali heterodinska	enofotonska detekcija
baza	kvadrature X (amplituda) in P (faza)	diskretne polarizacije (horizontalna/vertikalna, diagonalna)
združljivost	soobstoj s klasičnimi optičnimi sistemi	namenski kvantni kanal
dokazovanje	zapleteni postopki dokazovanja varnosti	enostavni in uveljavljeni varnostni dokazi
občutljivost	velika občutljivost na šum in turbulence	manjša občutljivost na šum
kompleksnost	enostavnejša detekcija	kompleksno detektiranje posameznih fotonov
integracija	enostavna integracija v obstoječa optična omrežja	zahteva namensko kvantno opremo in kanal
protokoli	Gaussovo modulirana koherentna stanja (GMCS), protokoli zveznih spremenljivk	BB84, E91, stanje vabe QKD
izzivi	šum, dokazovanje varnosti, načelo nedoločenosti pri detekciji	izgube kanala, neučinkovita detekcija, izguba polarizacije

Tabela 1: Primerjava lastnosti metode za kvantno razdeljevanje ključa z uporabo zveznih spremenljivk (angl. *Continuous Variable QKD* – CV-QKD) in metode za kvantno razdeljevanje ključa z uporabo diskretnih spremenljivk (angl. *Discrete Variable QKD* – DV-QKD).

polprevodnikov, ki delujejo v tako imenovanem Geigerjevem načinu, kjer lahko en sam foton sproži velik plaz nabitih nosilcev naboja. Obrnjena polariteta diode omogoča, da električno polje pospeši nosilce naboja ob vstopu fotona v napravo, kar sproži plaz drugih nosilcev in vodi do električnega impulza. Povedano drugače: ko foton vstopi v diodo, to povzroči ionizacijo, kar sproži proces množične reprodukcije nosilcev naboja. Ta proces je ključen za delovanje plazovnega detektorja. Detektorji SPAD so idealni za uporabo v stroškovno občutljivih in kompaktnih rešitvah, zlasti pri zaznavanju fotonov v vidnem spektru pri nižjih temperaturah.

SNSPD temeljijo na tankih superprevodnih nanožicah, ohlajenih na kriogene temperature. Ko foton zadene nanožice SNSPD, je superprevodno stanje moteno, kar posledično ustvari napetostni impulz. Ti detektorji se ponašajo z visoko učinkovitostjo zaznavanja do 90 odstotkov in nižjim termičnim šumom, vendar zahtevajo kriogeno hlajenje in so posledično dražji.

Za prenos kubitov v okviru kvantnih komunikacij lahko uporabimo standardna optična vlakna ali FSOC. Kvantno optično zemeljsko omrežje je mogoče zgraditi z opremo, podobno tisti v klasičnih optičnih komunikacijskih omrežjih, z obstoječimi enorodovnimi in mnogorodovnimi vlakni. Komunikacije FSOC pa se v nasprotju z optičnim vlaknom zanašajo na neposredno vidljivost (angl. *line of sight* – LOS). FSOC omogoča hitrejši prenos šifrirnega ključa, vendar naleti na težave pri komunikaciji na večjih razdaljah zaradi motenj v ozračju.

Kvantni repetitorji so ključna tehnologija za prenos kubitov na velike razdalje. Delujejo na načelu kvantne prepletenosti, kjer se stanje kubita razdeli na več repetitorjev. Klasično ojačenje signala ni mogoče zaradi kvantne zakonitosti, ki se nanaša na izrek o prepovedi kloniranja. Koncept kvantnega repetitorja je podoben klasičnemu, pri čemer je razdalja prenosa razdeljena na posamezne segmente. Vsak segment vsebuje enega ali več kvantnih repetitorjev. Kvantni repetitor prejme fotone iz drugih vozlišč in na njih izvede Bellovo meritev, ki vzpostavi kvantno prepletenost med kubiti na oddaljenih vozliščih. Zmanjšanje izgub omogoča uporaba tehnik, kot so zamenjava prepletenosti ter čiščenje (purifikacija) in shranjevanje (angl. *entanglement swapping, purification and storage*) [32]. Zamenjava prepletanja je proces, ki povezuje prepletena stanja med različnimi repetitorji, kar podaljšuje njihov doseg in omogoča prenos informacij na daljših razdaljah. Postopek purifikacije izboljšuje kakovost prepletenih stanj, odpravlja napake in zagotavlja zanesljivejši prenos informacij. Shranjevanje kvantnih stanj omogoča, da se ti uporabijo pozneje za sinhronizacijo med repetitorji. Učinkovit prenos kvantnih informacij zahteva sinergijski učinek opisanih tehnik za ohranjanje in izboljšanje kakovosti oznak in stikov med repetitorji, kar povečuje zanesljivost in razdaljo komunikacije. Kvantni repetitorji skupaj s preostalimi kvantnimi tehnologijami tvorijo hrbtenico kvantnega interneta s povezovanjem končnih vozlišč. Izzivi v povezavi s kvantnimi repetitorji so: odpravljanje napak pri prenosu in izboljšanje kakovosti prenosa;

implementacija učinkovitih tehnik za korekcijo napak; vsak dodatni repetitor poveča kompleksnost omrežja, kar vodi do večjih izzivov pri sinhronizaciji in obvladovanju prepletenih stanj kubitov; shranjevanje kubitov je izziv zaradi težnje kubitov k hitri dekoherenci stanja; proizvodnja zadostnih količin prepletenih kubitov; integracija v obstoječo infrastrukturo.

5 SATELITSKE OMREŽNE ARHITEKTURE ZA KVANTNO RAZDELJEVANJE KLJUČEV

V zadnjem desetletju je bilo izvedenih več pomembnih projektov in poskusov na področju satelitske QKD, ki so temeljili na prepletenih fotonih [7] in protokolu BB84 [8], [9]. Prvi ključni dosežek je bil leta 2016 dosežen na Kitajskem s satelitom Micius, ki velja za prvi satelit, prek katerega so uspešno demonstrirali QKD na velike razdalje. Leta 2017 je bil izveden prvi medcelinski kvantno šifrirani videoklic. Kitajska je ta eksperiment izvedla tudi v sklopu svojega zemeljskega kvantnega komunikacijskega omrežja [10].

Singapurska vesoljska agencija je s pomočjo univerze Nanyang Technological University (NTU) in evropskih partnerjev leta 2019 izstrelila SpooQy-1 [33], manjši satelit [34], namenjen testiranju kvantnih komunikacij v LEO, kar je bila prva uspešna demonstracija generiranja prepletenih fotonov v vesoljski tirnici.

Evropska vesoljska agencija (ESA) in zasebni operater SES sta v obdobju od 2020 do 2024 v okviru projekta QUARTZ (Quantum Cryptography Telecommunication System) razvila QKD rešitve za komercialne komunikacije z uporabo tehnologije BB84 na geostacionarnih satelitih SES O3b. To je bila prva uspešna demonstracija QKD v realnih satelitskih omrežjih.

V obdobju od 2023 do 2025 je kanadska vesoljska agencija razvija Quantum EncrYption and Science Satellite (QEYSSat), ki je namenjen testiranju satelitske infrastrukture QKD [35]. Cilj je vzpostaviti kvantno varne povezave med vladnimi in raziskovalnimi ustanovami v Kanadi.

Projekti, kot so Micius, SpooQy-1, QUARTZ in QEYSSat, so pokazali, da je satelitska QKD tako rekoč izvedljiva in obetavna tehnologija za globalno varno komunikacijo. EU s projektom Connecting Europe Facility in satelitom Eagle-1 zdaj vstopa v fazo razvoja lastnega kvantnega komunikacijskega omrežja.

Za namene vzpostavitve varnih komunikacijskih povezav na velikih razdaljah se bodo tudi v bodoče uporabljale satelitske komunikacije. Pričakujemo lahko, da bo večina satelitov za globalno razdeljevanje kvantnih ključev v LEO [36]. Pozicionirani na višinah od 500 do 2000 kilometrov prinašajo številne prednosti v primerjavi z zemeljskimi sistemi QKD, predvsem z vidika izgube fotonov in pokritosti. Konstelacija LEO bi lahko zagotavljala globalne storitve QKD tako, da bi delovala kot varna relejna vozlišča. Njihova glavna prednost je nizka tirnica, ki odstrani potrebo po zemeljskih varnih relejnih postajah in s tem globalizira komunikacijo. V nasprotju s sistemi QKD, ki temeljijo na optičnih vlaknih, lahko satelitski sistem deluje na razdalji več tisoč kilometrov, ne da bi potrebovali kvantne repetitorje, ker je izguba signala manjša [37].

Pri povezovanju iz satelita na Zemljo pa je velik izziv ozračje, ki ga prepotuje kubit na poti iz vesolja na Zemljo [38]. Spremembe temperature in tlaka povzročajo spremembe gostote in s tem spremembo faze. Prav tako turbulenca v ozračju povzroča rotacijo in depolarizacijo fotonov, zaradi česar je težko meriti stanja polarizacije na sprejemniku. Rešitev za to težavo je uporaba adaptivne optike (angl. *Adaptive optics*) za popravljanje popačenj valovne fronte in kvantnega sledenja stanju. DV-QKD ima tudi omejeno podatkovno hitrost ključev (angl. *key rate* – KR), ki se močno zmanjšuje z razdaljo, zlasti v FSOC, ki so tudi zelo občutljivi za izgube kanala.

Sateliti služijo kot zaupanja vredna porazdeljena vozlišča, ki omogočajo varno porazdelitev ključev med zemeljskimi in drugimi sateliti. Satelitski QKD se uporablja skupaj z zemeljskim QKD v optični infrastrukturi. Gre pravzaprav za hibridni sistem, ki zagotavlja varnost na celotni povezavi. Ideja je, da bi bila večsatelitska omrežja zasnovana tako, da bi zagotovila neprekinjeno vidljivost vsake zemeljske postaje z vsaj enim satelitom.

Da bi dosegli neprekinjeno storitev, morajo sateliti v omrežju vzpostaviti neposredne medsebojne povezave. Medsatelitski FSOC zagotavlja hitre izmenjave podatkov z nizko zakasnitvijo [39]. Minimalna degradacija signala je pomembna značilnost tega sistema, ki ni posledica motenj v ozračju. Te povezave omogočajo tudi razširitev konstelacije, kar omogoča dodajanje novih satelitov brez motenj v sistemu in zmanjšanja zmogljivosti. Glavne naloge medsatelitske FSOC so: kvantni ključni releji, porazdelitev prepletenosti in kontinuiteta storitev.

Nekateri izzivi v teh sistemih se nanašajo na dodeljevanje virov. Omejitve vidnosti se pojavijo, ker imajo sateliti omejena časovna okna za komunikacijo, zato je za čim večje ustvarjanje ključev zahtevano natančno načrtovanje. Prav tako mora biti strojna oprema optimizirana tako,, da se zagotovi ustrezna moč signala. Ena izmed rešitev bi lahko bilo dinamično razporejanje, kjer bi bile zemeljske postaje prednostno razvrščene glede na vreme in kakovost povezave [40]. Izravnavanje obremenitve bi bilo tudi rešitev za preprečevanje preobremenitve posameznih vozlišč.

5.1 Izzivi satelitskih kvantnih komunikacijskih omrežij

Učinki ozračja so velik izziv pri satelitski FSOC in QKD. Spremenljivost pogojev v ozračju lahko znatno poslabša prenos kvantnih stanj. Ključna izziva sta turbulenca in širjenje žarka, saj povzročata zmanjšanje števila fotonov, ki dosežejo sprejemnik. Ti učinki so občutno bolj očitni v kanalih navzgornje povezave, ker morajo signali potovati skozi gostejši del ozračja. Vremenske

razmere, kot so megla, dež, oblaki, turbulence v ozračju in sončna svetloba, povzročajo sipanje in absorpcijo, kar se odraža v nihanju prepustnosti komunikacijskega kanala. Ukrepi, ki bi jih lahko sprejeli, da bi se izognili tem težavam, bi bila uporaba prilagodljive optike (angl. *adaptive optics*) za popravljanje popačenj v realnem času, skupaj z naprednimi modulacijskimi shemami in odpravljanjem napak, ter načrtovanje komunikacijskih operacij med ugodnimi vremenskimi okni, da bi zmanjšali izgube [18], [41]. Za izvedbo se potrebuje dva žarka: enega za prenos QKD, drugega za prilagodljivo optiko. Pri uporabi FSOC za QKD nastaja razlika med uporabo ob dnevni svetlobi ali ponoči. Za ublažitev vplivov na kanal in odpravo šuma se uporablja pametno filtriranje (angl. *smart filtering*) [42]. Eden od načinov za premagovanje težav s satelitsko komunikacijo podnevi in izgub zaradi turbulenc v ozračju je uporaba široke palete tehnologij, kot so filtriranje dnevne svetlobe, uporaba robustnega optičnega vira velike hitrosti in ekstrakcija ključev v realnem času na osnovi laserske komunikacije. Z uporabo teh tehnologij je bil izveden QKD, ki je pokrival vseh 24 ur dneva v 20-kilometski zemeljskei FSOC s povprečno hitrostjo ključev približno 495 bit/s [11].

Dekoherenca kvantnega stanja je drugo kritično vprašanje, ki se pojavi med prenosom kvantnih stanj skozi prosti prostor ali optična vlakna, zlasti na velike razdalje. Turbulenca v ozračju lahko popači lastnosti polarizacije in prepletenosti kvantnih stanj, prenosi na dolge razdalje pa povečajo izgubo fotonov, kar zmanjša natančnost kvantnih stanj. Rešitev bi bila uporaba visokokakovostnih kvantnih virov z veliko svetlostjo in nizkim šumom za izboljšanje razmerja med signalom in šumom (angl. *Signal-to-noise ratio* – SNR).

Druga težava je shranjevanje kubitov v kvantnem pomnilniku, saj so izzivi ravnanje s kubiti, izdelanimi iz različnih materialov, sinhronizacija vzpostavitve prepletenosti med segmenti omrežja in razširitev zmogljivosti shranjevanja za sprejem več kubitov. Mogoče rešitve so oblikovanje pomnilniških sistemov, ki so sposobni shranjevati kubite iz različnih materialov, razvoj pomnilniških enot z veliko časovno natančnostjo in splošno povečanje učinkovitosti pomnilnika. Poseben poudarek v prihodnjem razvoju bo na izvedbi distribucije vesoljskih fotonov prek podaljška zemeljskih vlakenskih zvez brez uporabe zaupanja vrednega vozlišča na mestu zemeljskega teleskopa, s čimer se odprejo vrata za konvergenco vesoljske in zemeljske QKD [43], [44], [45].

Težave se pojavljajo tudi pri uporabi obstoječih protokolov, kot sta BB84 in B92, ki podpirata varno razdeljevanje ključev, vendar se soočata s tehničnimi težavami, kot so: pretvorba brez izgub med kvantnimi in optičnimi signali, visoke ravni šuma in neustrezno obravnavanje izgube paketov. Mogoče rešitve so napredna zasnova protokola, hibridni nosilci signala in napredne tehnike zmanjševanja šuma.

Težave se pojavljajo tudi pri prilagajanju omrežij za globalno komunikacijo. Izzivi vključujejo omejeno razširljivost in neučinkovito povezavo med relejnimi moduli. Mogoče rešitve so napredna relejna infrastruktura, ki temelji na kvantnih repetitorjih z visoko zmogljivimi zmožnostmi razdeljevanja prepletenosti, in večslojna omrežja, ki združujejo različne satelite, brezpilotna letala in zemeljske postaje za razširitev pokritosti [46].

6 Zaključek

Projekt CEF, ki ga je EU razpisala leta 2025, je namenjen razvoju prvega evropskega satelitskega omrežja QKD. Cilj tega projekta je okrepiti varnost komunikacijskih sistemov v EU in povečati suverenosti na področju varne komunikacije. Z uporabo lastne satelitske infrastrukture QKD bo EU zmanjšala odvisnost od tretjih držav in okrepila kibernetsko varnost kritične infrastrukture, finančnih institucij in vladnih komunikacij. Gre za namenski evropski satelit Eagle-1, ki bo nosil napravo za izvajanje QKD s pomočjo katere si bodo države članice EU, ki sodelujejo v projektu, izmenjevale kvantne ključe.

Vsekakor pa bo nadaljnji napredek na področju adaptivne optike in sistemov za sledenje ključen za izboljšanje stabilnosti kvantnih satelitskih povezav. Kvantni repetitorji nove generacije, ki omogočajo ohranjanje kvantnega stanja, bodo igrali pomembno vlogo pri razširitvi dosega povezav. Kvantni pomnilniki, ki bodo lahko shranjevali kubite iz različnih materialov in omogočali sinhronizacijo med segmenti, so še ena ključna tehnologija, ki bo izboljšala delovanje kvantnih omrežij.

V prihodnosti bo prav razvoj hibridnih omrežnih arhitektur, ki vključujejo satelite v nizki, srednji in geostacionarni orbiti, pomemben korak k vzpostavitvi globalnega kvantnega interneta. Ta internet bo zagotavljal varno komunikacijo na mednarodni ravni z uporabo satelitov, dronov in zemeljskih postaj ter omogočil izmenjavo podatkov brez tveganja kibernetskih napadov. Kvantne komunikacije med sateliti prek FSO so ključni korak k vzpostavitvi robustnega, globalnega kvantnega omrežja, ki bo temeljilo na varnosti, odpornosti in zanesljivosti. S stalnimi izboljšavami pri natančnosti detekcije, zmanjšanju šuma in razvoju naprednih protokolov se bližamo prihodnosti, kjer bo kvantna komunikacija omogočala popolnoma varen prenos informacij po vsem svetu.

Zahvala

Sredstva za izvedbo je zagotovila Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije na internem interdisciplinarnem projektu Univerze v Ljubljani: Kvantne tehnologije za transport in komunikacije v 21. stoletju (KTTK21) s pogodbo št. SN-ZRD/22-27/0510.

L. Ulčakar, R. Kaltenbaek in A. Ramšak so bili financirani s strani Republike Slovenije (MVZI) in Evropske

unije – NextGenerationEU (SiQUID-101091560).

LITERATURA

[1] A. Umek, "Varne komunikacije: študijsko gradivo 2011/2012," 2011. [Online]. Available: http://www.lkn.fe.uni-lj.si/gradiva/VarKom/Varne_komunikacije.pdf

[2] J. Tratnik and B. Batagelj, "Predstavitev ideje kvantnega šifriranja in pregled osnovnih tehnik kvantnega razdeljevanja ključa," *Elektrotehniški vestnik*, vol. 75, no. 5, pp. 257–263, 2008.

[3] A. Ramšak, *Kvantna mehanika*. Založba Univerze, 2023.

[4] Z. Ghassemlooy et al., "Final White Paper, NEWFOCUS CA19111 COST Action: European network on future generation optical wireless communication technologies," COST (European Cooperation in Science and Technology) Action CA19111 NEWFOCUS, Tech. Rep., Jun. 2024. [Online]. Available: https://hal.science/hal-04671609

[5] A. K. Garg, V. Janyani, B. Batagelj, N. Zainol Abidin, and M. Abu Bakar, "Hybrid FSO/fiber optic link based reliable & energy efficient WDM optical network architecture," *Optical Fiber Technology*, vol. 61, p. 102422, 2021.

[6] Ž. Andrejc and B. Batagelj, "Vrednotenje tehničnih lastnosti komunikacijskega omrežja majhnih satelitov starlink," *Elektrotehniški Vestnik*, vol. 88, no. 1–2, pp. 1–7, 2021.

[7] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, "Entanglement-based secure quantum cryptography over 1, 120 kilometres," *Nature*, vol. 582, no. 7813, p. 501–505, Jun. 2020. [Online]. Available: http://dx.doi.org/10.1038/s41586-020-2401-y

[8] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, p. 43–47, Aug. 2017. [Online]. Available: http://dx.doi.org/10.1038/nature23655

[9] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, p. 030501, Jan 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.120.030501

[10] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, "An integrated space-to-ground quantum communication network over 4, 600 kilometres," *Nature*, vol. 589, no. 7841, p. 214–219, Jan. 2021. [Online]. Available: http://dx.doi.org/10.1038/s41586-020-03093-8

[11] W.-Q. Cai, Y. Li, B. Li, J.-G. Ren, S.-K. Liao, Y. Cao, L. Zhang, M. Yang, J.-C. Wu, Y.-H. Li, W.-Y. Liu, J. Yin, C.-Z. Wang, W.-B. Luo, B. Jin, C.-L. Lv, H. Li, L. You, R. Shu, G.-S. Pan, Q. Zhang, N.-L. Liu, X.-B. Wang, J.-Y. Wang, C.-Z. Peng, and J.-W. Pan, "Free-space quantum key distribution during daylight and at night," *Optica*, vol. 11, no. 5, p. 647, May 2024. [Online]. Available: http://dx.doi.org/10.1364/OPTICA.511000

[12] S. Bloom, E. Korevaar, J. Schuster, and H. Willebrand, "Understanding the performance of free-space optics [Invited]," *J. Opt. Netw.*, vol. 2, no. 6, pp. 178–200, Jun 2003.

[13] M. Abasifard, C. Cholsuk, R. G. Pousa, A. Kumar, A. Zand, T. Riel, D. K. L. Oi, and T. Vogl, "The ideal wavelength for daylight free-space quantum key distribution," *APL Quantum*, vol. 1, no. 1, p. 016113, 03 2024.

[14] Z. Ghassemlooy, W. O. Popoola, and S. Rajbhandari, *Optical wireless communications: system and channel modelling with Matlab®, Second Edition*. CRC Press, 2019.

[15] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014, theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[16] M. Lasota, O. Kovalenko, and V. C. Usenko, "Robustness of entanglement-based discrete- and continuous-variable quantum key distribution against channel noise," *New Journal of Physics*, vol. 25, no. 12, p. 123003, dec 2023.

[17] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[18] M. Aspelmeyer, H. R. Böhm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, and A. Zeilinger, "Long-Distance Free-Space Distribution of Quantum Entanglement," *Science*, vol. 301, no. 5633, pp. 621–623, 2003.

[19] I. Paparelle, F. Mousavi, F. Scazza, M. Paris, A. Bassi, and A. Zavatta, "A continuous-variable quantum secure direct communication protocol with squeezed states," in *2023 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC)*, 2023, pp. 1–1.

[20] Y. Zheng, H. Shi, W. Pan, Q. Wang, and J. Mao, "Security Analysis of Continuous-Variable Measurement-Device-Independent Quantum Key Distribution Systems in Complex Communication Environments," *Entropy*, vol. 24, no. 1, 2022.

[21] Y. Guo, H. Zhang, and Y. Guo, "Practical Security of Continuous Variable Measurement- Device-Independent Quantum Key Distribution with Local Local Oscillator," *Mathematics*, vol. 12, no. 23, 2024.

[22] R. K. Goncharov, A. D. Kiselev, E. O. Samsonov, and V. I. Egorov, "Continuous-variable quantum key distribution: security analysis with trusted hardware noise against general attacks," *Nanosistemi: fizika, kemija, matematika*, vol. 13, no. 4, pp. 372–391, 2022.

[23] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," *Applied Physics Reviews*, vol. 11, no. 1, p. 011318, 03 2024.

[24] A. Manzalini and L. Artusio, "The rise of quantum information and communication technologies," *Quantum Reports*, vol. 6, no. 1, pp. 29–40, 2024.

[25] R. Van Meter, *Quantum networking*. John Wiley & Sons, 2014.

[26] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, pp. 4337–4341, Dec 1995. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.75.4337

[27] X. Li, P. L. Voss, J. E. Sharping, and P. Kumar, "Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band," *Phys. Rev. Lett.*, vol. 94, p. 053601, Feb 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.94.053601

[28] R. M. Stevenson, R. J. Young, P. Atkinson, K. Cooper, D. A. Ritchie, and A. J. Shields, "A semiconductor source of triggered entangled photon pairs," *Nature*, vol. 439, no. 7073, p. 179–182, Jan. 2006. [Online]. Available: http://dx.doi.org/10.1038/nature04446

[29] D. N. Matsukevich and A. Kuzmich, "Quantum state transfer between matter and light," *Science*, vol. 306, no. 5696, p. 663–666, Oct. 2004. [Online]. Available: http://dx.doi.org/10.1126/science.1103346

[30] B. B. Blinov, D. L. Moehring, L.-M. Duan, and C. Monroe, "Observation of entanglement between a single trapped atom and a single photon," *Nature*, vol. 428, no. 6979, p. 153–157, Mar. 2004. [Online]. Available: http://dx.doi.org/10.1038/nature02377

[31] Y.-C. Liu, D.-J. Guo, R. Yang, C.-W. Sun, J.-C. Duan, Y.-X. Gong, Z. Xie, and S.-N. Zhu, "Narrowband photonic quantum entanglement with counterpropagating domain engineering," *Photon. Res.*, vol. 9, no. 10, pp. 1998–2005, Oct 2021.

[32] M. Victora, S. Tserkis, S. Krastanov, A. S. de la Cerda, S. Willis, and P. Narang, "Entanglement purification on quantum networks," *Phys. Rev. Res.*, vol. 5, p. 033171, Sep 2023.

[33] A. Reezwana, T. Islam, J. A. Grieve, C. F. Wildfeuer, and A. Ling, "Generating Quantum Random Numbers on a CubeSat (SpooQy-1)," in *2020 Conference on Lasers and Electro-Optics (CLEO)*, 2020, pp. 1–3.

[34] S. Sivasankaran, C. Liu, M. Mihm, and A. Ling, "A CubeSat platform for space based quantum key distribution," in *2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, 2022, pp. 51–56.

[35] H. Podmore, I. D'Souza, D. Hudson, T. Jennewin, J. Cain, B. Higgins, C. Midwinter, A. Scott, A. McColgan, D. Caldwell, and S. H. Zheng, "Optical Terminal for Canada's Quantum Encryption and Science Satellite (QEYSSat)," in *2019 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, 2019, pp. 1–5.

[36] M. Bakyt, L. L. Spada, K. Moldamurat, Z. Kadirbek, and F. Yermekov, "Review of Data Security Methods using Low-Earth Orbiters for High-Speed Encryption," in *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*, 2024, pp. 1366–1375.

[37] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan *et al.*, "Ground test of satellite constellation based quantum communication," *arXiv preprint arXiv:1611.09982*, 2016.

[38] A. Ntanos, N. K. Lyras, A. Stathis, G. Giannoulis, A. D. Panagopoulos, and H. Avramopoulos, "Satellite-to-ground qkd in urban environment: A comparative analysis of small-sized optical ground stations," *IEEE Aerospace and Electronic Systems Magazine*, vol. 39, no. 6, pp. 16–29, 2024.

[39] N. Jothi, S. Krishnan *et al.*, "Design and comparative analysis of Inter SatelliteOptical Wireless Communication (IS-OWC) for Return to Zero (RZ) & Non-Return to Zero (NRZ) modulation formats through channel diversity technique," *Informacije MIDEM: Journal of Microelectronics, Electronic Components & Materials*, vol. 53, no. 1, 2023.

[40] V. Vrh, L. Kavčič, J. V. M. Peer, M. Zeme, J. L. Verček, N. Flogie, L. Mlakar, A. Pavliha, G. Blatnik, M. Jankovec *et al.*, "Trajnostni pristopi k satelitskemu teleportu," *Elektrotehniški vestnik*, vol. 91, no. 3, pp. 138–142, 2024.

[41] G. G. Rozenman, N. K. Kundu, R. Liu, L. Zhang, A. Maslennikov, Y. Reches, and H. Y. Youm, "The quantum internet: A synergy of quantum information technologies and 6G networks," *IET Quantum Communication*, vol. 4, no. 4, pp. 147–166, 2023.

[42] H. Ko, K.-J. Kim, J.-S. Choe, B.-S. Choi, J.-H. Kim, Y. Baek, and C. J. Youn, "Experimental filtering effect on the daylight operation of a free-space quantum key distribution," *Scientific Reports*, vol. 8, no. 1, 2018.

[43] A. Stathis, A. Ntanos, N. K. Lyras, G. Giannoulis, A. D. Panagopoulos, and H. Avramopoulos, "Toward Converged Satellite/Fiber 1550 nm DS-BB84 QKD Networks: Feasibility Analysis and System Requirements," *Photonics*, vol. 11, no. 7, 2024.

[44] ——, "Converged Satellite to Fiber QKD Links: A Feasibility Analysis," in *2024 14th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, 2024, pp. 500–505.

[45] G. Giannoulis, A. Stathis, A. Ntanos, N. K. Lyras, I. Papastamatiou, P. Kourelias, O. Prnjat, K. Koumantaros, A. D. Panagopoulos, and H. Avramopoulos, "Satellite-to-ground QKD Feasibility Analysis for High Altitude Rural Areas: A Case Study in Greece," in *2024 International Workshop on Fiber Optics in Access Networks (FOAN)*, 2024, pp. 38–42.

[46] P. Zhang, N. Chen, S. Shen, S. Yu, S. Wu, and N. Kumar, "Future Quantum Communications and Networking: A Review and Vision," *IEEE Wireless Communications*, vol. 31, no. 1, pp. 141–148, 2024.

Katarina Radaković je študentka 2. letnika magistrskega študijskega programa 2. stopnje elektrotehnika na smeri Informacijsko komunikacijske tehnologije (IKT) na Fakulteti za elektrotehniko Univerze v Ljubljani. Zanima jo delo, povezano z novimi in inovativnimi izzivi informacijsko-komunikacijskih tehnologij.

Vesna Eržen je diplomirala leta 2012 na Fakulteti za elektrotehniko Univerze v Ljubljani. Zaposlena je kot učiteljica strokovnih predmetov na srednji šoli za strojništvo in kot predavateljica s področja avtomatizacije in robotike na višji strokovni šoli v okviru ŠC Škofja Loka. Njena raziskovalna zanimanja vključujejo kvantne fizikalne pojave v optiki, pasivne optične sisteme in spremljanje razvoja na področju optičnih komunikacij.

Lara Ulčakar je doktorirala leta 2020 na Fakulteti za matematiko in fiziko v Ljubljani na področju teoretične fizike kondenzirane snovi. Zaposlena je na inštitutu Jožefa Stefana in na Fakulteti za Matematiko in Fiziko Univerze v Ljubljani. Njena raziskovalna področja so kvantni materiali in kvantna optika. Na fakulteti uči Nanofiziko in Klasično mehaniko.

Prof. dr. Anton Ramšak je leta 1991 doktoriral na Fakulteti za matematiko in fiziko Univerze v Ljubljani, kjer je zaposlen kot redni profesor in je bil tudi tri mandate dekan. Deloval je na Institutu Max Planck, na King's College, na Imperial College in na University College v Londonu. Ukvarja se s teorijo kvantnih sistemov, in sicer s fizikalnimi lastnostmi kvantnih pik in kvantnih žic, z generiranjem kvantne prepletenosti, z manipulacijo kvantnih bitov in kvantnih faz ter z lastnostmi topoloških izolatorjev. Trenutno vodi projekt SiQUID za vzpostavitev kvantne izmenjave ključa.

Prof. dr. Boštjan Batagelj je doktoriral leta 2003 na Fakulteti za elektrotehniko Univerze v Ljubljani, kjer je trenutno prodekan za znanstveno-raziskovalno dejavnost in predava predmete s področja informacijsko-komunikacijskih tehnologij. Njegova bibliografija obsega preko 800 enot, od tega 12 patentov. Aktiven je na številnih raziskovalnih projektih s področja optičnih, radijskih, satelitskih in kvantnih komunikacij ter soustanovitelj dveh zagonskih podjetij.

Rainer Kaltenbaek je leta 2008 doktoriral na Fakulteti za fiziko Univerze na Dunaju. Trenutno je izredni profesor na Fakulteti za matematiko in fiziko (FMF) Univerze v Ljubljani. Na FMF vodi laboratorij za kvantno optiko in kvantne temelje ter predava predmete s področja kvantne optike in fotonike. Je strokovnjak za kvantne komunikacije, optično kvantno obdelavo informacij, kvantno optomehaniko, optične pasti in testiranje kvantne fizike v vesolju.

Andrej Lavrič je doktoriral leta 2025 na Fakulteti za elektrotehniko Univerze v Ljubljani na temo merjena faznega šuma z uporabo tehnik mikrovalovne fotonike. Kot gostujoči raziskovalec je eno leto preživel na Univerzi Duisburg-Essen v Nemčiji, kjer se je ukvarjal z optičnimi frekvenčnimi glavniki. Raziskovalno je aktiven na področju merjenja faznega šuma, mikorvalovne fotonike in kvantnih tehnologij.