BACSÁRDI LÁSZLÓ* – OLÁH KITTI**

KVANTUMKOMMUNIKÁCIÓN ALAPULÓ MŰHOLDAS MEGOLDÁSOK

ÖSSZEFOGLALÁS: *A kvantumfizikai elveken működő kvantumkommunikáció számos érdekes megoldást kínál. Az Einsteint is meglepő összefonódás jelenségét felhasználva kvantuminternetet tudunk létrehozni, a fotonforrások működési elvét kihasználva igazi véletlenszámokat tudunk előállítani, míg a kvantumfizika törvényeire alapozva olyan kvantumos kulcscserélő berendezéseket tudunk építeni, amelyek jelentősen megnövelik a különböző titkosító rendszereink biztonsági szintjét. Nem meglepő, hogy 2022-ben a fizikai Nobel-díjat többek között kvantumkommunikációval foglalkozó fizikus kapta, ahogy az sem, hogy Európában 2019-ben megkezdődött egy európai szintű kvantumkommunikációs infrastruktúra kiépítése. Tanulmányunkban bemutatjuk a kvantumkommunikáció legfontosabb jellemzőit, ismertetünk néhány fontos hazai fejlesztési eredményt, és kitérünk a műholdas világ nyújtotta lehetőségekre is.*

KULCSSZAVAK: *kvantuminformatika, kvantumkommunikáció, kvantummemória, kvantumalapú kulcscsere, kvantuminternet*

ABSTRACT: *Quantum communication, based on quantum physics principles, offers several amazing solutions. We can use the phenomenon of entanglement, which surprised even Einstein, to create the quantum internet. We can exploit the principle of photon sources to generate true random numbers, while quantum physics laws can be used to build quantum key distribution devices that significantly increase the security level of our existing encryption systems. It is no coincidence that one of the recipients of the 2022 Nobel Prize in Physics was a physicist working on quantum communications, nor that the European Commission announced the development of an European quantum communication infrastructure in 2019. In this article, we present the key features of quantum communications, highlight the Hungarian development in this field and introduces the opportunities offered by quantum communication satellites.*

KEYWORDS: *quantum computing, quantum communication, quantum memory, quantum key distribution, quantum internet*

KVANTUMFORRADALOM A KLASSZIKUS VILÁGBAN

Manapság egyre több helyen hallhatunk a kvantummechanika alapjaira épülő kvantumérzékelés, kvantuminformatika, kvantumkommunikáció és kvantumszimuláció világáról. A második kvantumforradalomban élünk, amelynek fókuszában az említett tudományterületek klasszikus világunkba való kiépítése áll. [1] A kvantumszámítógépek világában a kvantummechanikai szempontból fontosabb atomok világa kerül előtérbe (például az alkálifémek, alkáliföldfémek), ugyanakkor a kvantumkommunikációs fejlesztésekben a fotonalapú technológiák kapnak nagyobb hangsúlyt. [2] A jövőbeni globális kvantumhálózat egyik technológiai kihívása, hogy ezeket a területeket együttesen felhasználjuk (például kvantummemóriák fejlesztéséhez). [3]

A kvantuminformatika alapegysége a kvantumbit. Egy hagyományos bit (amit a mi nézőpontunkból klasszikusnak nevezünk) 0 vagy 1 értéket vehet fel, ezzel ellentétben a kvantumbit egyszerre tud 0 és 1 értékkel rendelkezni, kihasználva a szuperpozíció jelenségét. Fizikai rendszerekben ilyen kétállapotú rendszer lehet a foton polarizációja, illetve bizonyos atomok magspinjei vagy elektronspinjei is. A szuperpozíciós tulajdonság teszi lehetővé, hogy olyan kvantumalgoritmusokat alkossunk, amelyek sokkal gyorsabbak, mint a hagyományos algoritmusok. [4]

Egy másik fontos kvantummechanikai jelenség az összefonódás, amikor két kvantumbit mérési eredménye korrelál egymáshoz – erről részletesen a következő fejezetben lesz szó.

Mind a szuperpozíciót, az összefonódást, valamint további kvantumfizikai törvényszerűségeket is fel tudjuk használni ahhoz, hogy különböző kvantumhálózatokat hozzunk létre.

NOBEL-DÍJAS ÖSSZEFONÓDÁS

A kvantuminformatika alapegységét jelentő kvantumbit állapotát többféle módszerrel írhatjuk le. Jelen cikkben erre két megoldást mutatunk: a Dirac-féle jelölést és a Bloch-gömbön történő megadást.

Az 1. ábrán a Bloch-gömb[1] segítségével szemléltetjük a kvantuminformatika I. posztulátumát, amely megadja a kvantumbit definícióját: egy rendszer aktuális állapota leírható a Hilbert-térben[2] értelmezett egységnyi hosszúságú bázisvektorok lineáris kombinációjaként. [5]

Ha a Bloch-gömbről leolvasva szeretnénk megadni a kvantumbit állapotvektorát, akkor azt az alábbi módon tudjuk definiálni [5]:

$$|\psi\rangle = e^{i\gamma}[cos(\pi/2)|0\rangle + e^{i\beta}\sin(\pi/2)|1\rangle]$$
ahol $\alpha, \beta, \gamma \in \mathbb{R}$

Ha a Dirac-féle[3] jelölési módszert választjuk, akkor pedig így lehet megadni [5]:

$$|\psi\rangle = a|0\rangle + b|1\rangle \text{ ahol } a,b \in \mathbb{C} \text{ és } |a|^2+|b|^2 = 1$$

* PhD, egyetemi docens, a BME Mobil Kommunikáció és Kvantumtechnológiák Laboratórium vezetője, Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar Hálózati Rendszerek és Szolgáltatások Tanszék. ORCID: 0000-0002-7337-317X

** Űrmérnök, doktorandusz hallgató, Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar. ORCID: 0009-0003-1171-1553

[1] A kvantummechanikában és a számítástechnikában a Bloch-gömb egy kétszintű kvantummechanikai rendszer (qubit) tiszta állapotterének geometriai ábrázolása. Névadója Felix Bloch svájci fizikus (Zürich, 1905. 10. 23. – Zürich, 1983. 09. 10.).

[2] A Hilbert-tér olyan skalárszorzatos vektortér, amely teljes a skalárszorzat által definiált normára nézve. A Hilbert-tereket a funkcionálanalízis tanulmányozza. Névadója David Hilbert német matematikus (Königsberg, 1862. 01. 23. – Göttingen, 1943. 02. 14.).

[3] A jelölést Paul Adrien Maurice Dirac brit Nobel-díjas fizikus (Bristol, 1902. 08. 08. – Tallahassee, 1984. 10. 20.) vezette be.

DOI: 10.23713/HT.58.5.09

Utóbbi felírásban az *a* és *b* értékeket komplex valószínűségi amplitúdóknak nevezzük, ezek abszolútérték négyzete határozza meg, hogy az adott kvantumbit melyik állapotba ugrik be, amikor mérést hajtunk végre rajta. Ahogy a leírásból is látható, az, hogy a kvantumbit kiolvasásakor a mérőberendezésünk nullás vagy egyes értékét mutat, valószínűségi alapon dől el – emiatt a kvantumvilág alapjaiban különbözik a klasszikus világtól.

A több kvantumbitből álló rendszert kvantumregiszternek nevezzük, amelynek állapotát a tenzorszorzás műveletével kapjuk meg az alapállapotokból. S ezzel el is jutottunk az összefonódás definíciójáig. Vannak olyan összetett állapotok, amelyeket fel tudunk írni két (vagy több) kvantumbit tenzorszorzataként: ezek az ún. szorzatállapotok. S vannak olyan állapotok, amelyeket nem tudunk ilyen módon felírni: ezek az összefonódott állapotok. [6]

Mit is jelent ez a gyakorlatban? Ha veszünk egy összefonódott kvantumbitet, és a pár egyik tagját elküldjük az Antarktiszra, a másikat pedig az Északi-sarkra, majd megmérjük az egyiket, akkor abban a pillanatban a másik kvantumbit állapota is bebillen.

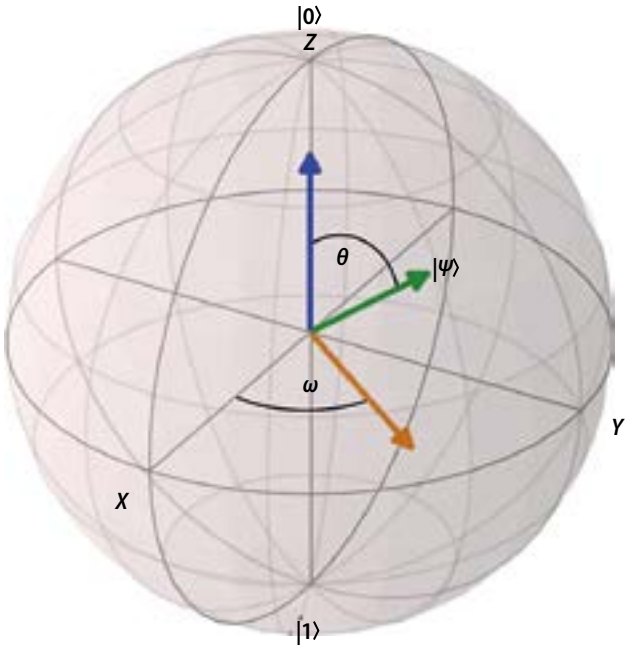
Ennél a pontnál az érdeklődő olvasóban felmerülhet a kérdés: képesek vagyunk a fénysebességnél gyorsabban kommunikálni? A válasz: nem. Ugyanis a mérés eredménye teljesen véletlenszerű, azaz semmilyen módon nem tudjuk befolyásolni, hogy az Északi-sarkon 0 vagy 1 értéket mértünk, így információt nem tudunk vele továbbítani. De abban biztosak lehetünk, ha az Északi-sarkon nullát mértünk, akkor tudjuk, mi az érték az Antarktiszon.

Ugyanezt a kérdést tette fel magának Albert Einstein is, aki szerint a valószínűség-alapú állapotleírás nem illik a kvantumfizikába. Úgy gondolta, hogy a mérés előtt már meghatározott minden egyes összefonódott kvantumbit állapota, egyfajta rejtett változókba tárolva. 1935-ben megszületett az EPR-paradoxon (Einstein–Podolsky–Rosen), amely azt is magában foglalja, hogy a Heisenberg-féle bizonytalansági elvet nem sértve képesek vagyunk a távolhatás jelenségére, miszerint egyik összefonódott részecske helyzetéből (vagy impulzusából) meghatározható a pár másik tagjának helyzete (vagy impulzusa).[4] Érdemes megjegyezni, hogy az EPR-paradoxonban az összefonódást részecskékre nézték, de David Bohm[5] kifejtette spinekre nézve, amely a későbbiekben hozzájárult a terület teljesebb vizsgálatához. Ez a jelenség azonban megcáfolja a klasszikus értelemben vett lokalitás fogalmát, amely kimondja, hogy két egymástól távoli részecske egymás állapotaira nem hat. [7]

John Bell[6] is vizsgálta az EPR-paradoxon lokalitását. 1964-ben bevezette a később róla elnevezett Bell-egyenlőtlenség fogalmát, amelyen a rejtett változók lokalitásának matematikai korlátját értjük. A Bell-egyenlőtlenségek igazolására számos módszert dolgoztak ki, erre egyik példa a Clauser–Horne–Shimony–Hold egyenlőtlenség[7] [8], a legelső sikeres mérést pedig az 1980-as évek elején hajtották végre. Az összefonódás egy igazán fontos összetevővé vált, annyira, hogy 2022-ben fizikai Nobel-díjjal ismerték el Alain Aspect, John Clauser és Anton Zeilinger kvantumfizikai tevékenységeit[8] – mindannyiuk munkássága kapcsolódik a Bell-egyenlőtlenséghez és az összefonódáshoz. [9]

KVANTUMALAPÚ KULCSSZÉTOSZTÁS

A kvantuminformatikai elveken működő kvantumszámítógép segítségével gyorsan tudunk majd szimulálni különböző összetett rendszereket és hatékonyan tudunk megoldani különböző optimalizációs problémákat.



1. ÁBRA.
Kvantumbit szemléltetése Bloch-gömbbel
(A szerzők saját szerkesztése)

Sajnos azonban a kvantumszámítógép olyan feladatokat is gyorsan végre tud hajtani, amelyek veszélyt jelentenek a biztonságra. Napjainkban a kommunikációnk titkosítását legnagyobb részben az úgynevezett aszimmetrikus kulcsú kriptográfia biztosítja. Ennek során nyilvános (bárki által megismerhető) kulcsokat és titkos (csak általunk ismert) kulcsokat használunk. A rendszer biztonsága abban rejlik, a nyilvános kulcsból a titkos kulcs kiszámítása egy nagyon időigényes feladat. A kvantumszámítógép megjelenésével azonban a kommunikációnál használt biztonságtechnikai protokolljaink már nem lesznek elegendőek. Ráadásul nem csak a titkosított adatokat tudjuk feltörni, hanem a digitális aláírásokat és az azokon alapuló tanúsítványokat is.

Szerencsére vannak olyan matematikai algoritmusok, amelyek a kvantumszámítógép támadásainak is ellenállnak. Ilyen például a szimmetrikus kulcsú algoritmusok körébe tartozó One-time pad. [10] (A szimmetrikus kulcsú titkosítás során ugyanazt a kulcsot használjuk az adatok kódolásához és dekódolásához.) A One-time pad

[4] A paradoxont Albert Einstein, Boris Podolsky és Nathan Rosen publikálta 1935-ben.

[5] Bohm, David Joseph (Wilkes-Barre, 1917. 12. 20. – London, 1992. 10. 27.) apai ágról magyar származású kvantumfizikus, jelentős eredményeket ért el az elméleti fizikában, a filozófiában, a neuropszichológiában és részt vett az ún. Manhattan-tervben is.

[6] Bell, John Stewart (Belfast, 1928. 06. 28. – Genf, 1990. 10. 01.) északír fizikus 1964-ben kidolgozta a kvantumfizika egyik fontos tételét a rejtett változós elméletekkel kapcsolatban.

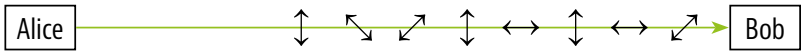
[7] A CHSH egyenlőtlenség lehetőséget biztosít a kvantumrendszerek közötti összefonódások tesztelésére és meghatározására.

[8] Aspect francia, Clauser amerikai és Zeilinger osztrák kutató külön-külön olyan úttörő kísérleteket folytattak összefonódott kvantumállapotok felvonultatásával, amelyekben két különálló részecske úgy viselkedett, mintha egy egység lenne, még akkor is, ha el voltak választva egymástól.

2. ÁBRA. **BB84 protokoll** (A szerzők saját szerkesztése)

Bázis	0	1
É–D, K–Ny	↔	↕
ÉK–DNy, ÉNy–DK	⤢	⤡

Bázis		+
		×



Átküldendő bitek (Alice)	1	1	0	1	0	1	0	0
Bázis (Bob)	+	+	×	×	+	×	+	×
Találatok (Bob)	1	0	0	0	0	0	0	0
Kulcsbitek (Bob)	0	–	0	–	0	–	0	0

biztonságosnak tekinthető, ha a szimmetrikus kulcs hossza és a küldendő üzenet hossza azonos nagyságú, továbbá egy kulcsot csak egyszer használunk fel. A kérdés csupán az, hogyan osztoznak meg a kommunikáló felek a titkosításhoz használt kulcson. Erre kínál megoldást a kvantumalapú kulcsszétosztás (Quantum Key Distribution – QKD).

A QKD-alapú protokollokat többféle módon is tudjuk csoportosítani, generációk szerint kettőt különböztetünk meg. [11] Az első generációba tartoznak a fotonrészecske tulajdonságát kihasználó, úgynevezett diszkrét változójú protokollok (Discrete Variable QKD – DV-QKD). A második generáció a fény hullámtulajdonságát használja ki, ezt folytonos változójú QKD-nak (Continous Variable QKD – CV-QKD) nevezzük.

A legelső QKD-protokollt, a BB84-et Charles Bennett és Gilles Brassard publikálta 1984-ben. [12] A 2. ábrán látható a protokoll működésének vázlata, ahol Alice a küldő fél, Bob pedig a vevő.

Elsőként a küldő véletlenszerűen sorsol 0-ból és 1-esből álló bitsorozatot: ez fogja meghatározni a kódolás bázisát. Előállít egy második véletlen bitsorozatot is, amely tartalmazza a fogadó fél számára küldendő kulcsbiteket. A 2. ábrán a zöld nyíl jelenti a kvantumcsatornát, amelyen átküldi a vevőnek a kulcsbiteket, valamilyen bázisba kódolva.

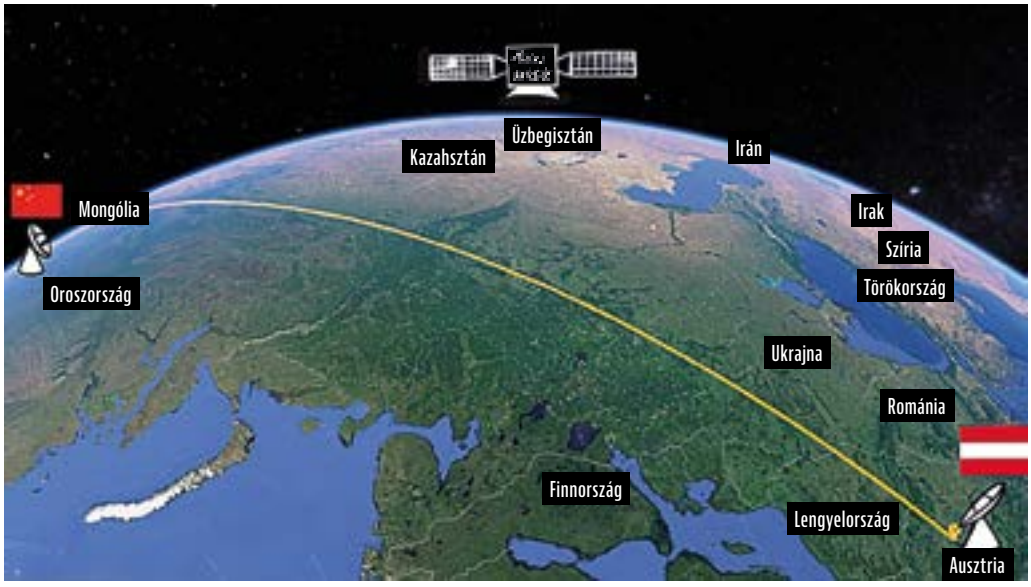
A protokoll kétféle kódolási és mérési bázist használ. A könnyebb megértés érdekében – a példa kedvéért – bevezetjük az égtájakat mint bázisirányítottságokat. Tehát az egyik északdél és kelet-nyugat irányú ortogonált (azaz egymásra merőleges) bázisok. Míg a másik ettől 45°-kal elforgatott (ÉK–DNy, ÉNy–DK), szintén ortogonált bázis.

A zöld nyílon láthatóak a küldő bázishelyes bitjei, amelyek megfelelnek a táblázat első sorában látható a 0 és 1-gyel leírt átküldendő bitsorozatnak. A vevő azonban nem tudja, milyen bázisban küldte az adó a jeleket. Ezért véletlenszerűen sorsolja a saját mérőbázisát, amelyben elvégzi a beérkezett kvantumbitek mérését. Ezt követően a vevő oldal klasszikus csatornán keresztül megbeszéli a küldő oldallal, mely mérési bázisok voltak azonosak. Ahol ugyanis a kódolási és a mérési bázis megegyezett, ott a vevő helyesen tudta megmérni az átvitt bitsorozatot, ezért ezeket fogják felhasználni ahhoz, hogy szimmetrikus kriptográfiában alkalmazható kulcsot készítsenek.

KVANTUMKOMMUNIKÁCIÓS MŰHOLDAK A LÁTHATÁRON

A kvantumcsatorna mint közvetítő közeg lehet optikai szál vagy szabadtéri csatorna – utóbbi esetben akár műholdas konstelláció is. Bár már számos gyártó kínál kereskedelmi forgalomban vezetékes környezetben használható QKD-berendezést, sajnos a kvantumfizika „nincs másolás tétele" miatt a nagy távolságok leküzdése jelentős kihívás. Hagyományos értelemben vett erősítőt nem tudunk építeni a kvantumos rendszerek számára, így az üvegszál csillapítása nagy távolság esetén egyáltalán nem elhanyagolható. A vezetékes világban emiatt jelenleg csak pont-pont rendszereket tudunk kiépíteni, amely azt jelenti, hogy bizonyos távolságonként megbízható csomópontnak tekintett eszközöket kell elhelyezni. Ha szeretnénk mondjuk a Budapest–Miskolc közötti nagyságrendileg 200 kilométeres távolságot lefedni, akkor elképzelhető, hogy ahhoz 50 kilométerenként kellene elhelyezni vezetékes QKD-eszközpárokat, azaz a távolságot csak 4 darab eszközpár felhasználásával tudnánk áthidalni. Nem véletlen, hogy nagy távolságú összeköttetések megvalósításához sokan foglalkoznak szabadtéri, illetve műholdas rendszerek vizsgálatával.

3. ÁBRA. **A Micius műhold és vevőállomásai az osztrák-kínai kísérletben** (A szerzők saját szerkesztése)



1991-ben már 30 centiméteres távolságon hajtottak végre szabadtéri kulcscserét, 1998-ban a Los Alamos Nemzeti Laboratórium munkatársai sikeresen tesztelték 1 kilométeres szabadtéri kvantumkulcselosztó rendszerüket, majd ezt a távolságot 2002-re 10 kilométerre növelték. [13] Európai kutatók 2006-ban már 144 kilométeres távolságban demonstrálták a szabadtéri kulcsszétosztás működőképességét a Kanári-szigeteken. [14] 10 évvel később, 2016-ban Kína felbocsátotta a Micius műholdat, a világ első kvantumkommunikációs műholdját, amely 635 kilogramm tömegű és 500 kilométeres magasságban, napszinkron pályán kering. [15] Különböző kvantumtechnológiai tudományos kísérletek elvégzésén túl, számos módon demonstrálták a műholdas kvantumkommunikáció működőképességét, többek között a 3. ábrán látható Bécs–Peking közötti szakaszon is, ahol kvantumkulcsokkal titkosított videókonferenciahívás is történt. [16]

2019-ben felbocsátották a 2,6 kg tömegű, 3U Cubesat kategóriájú, szingapúri SpooQy–1 kisműholdat. (A 3U egy 30×10×10 cm-es hasábot jelent). A műhold fedélzetén hoztak létre polarizációval összefonódott kvantumbitpárokat, amelyeket detektormodullal meg is mértek, mindezt 408 km magas Föld körüli pályán keringve. Ezzel a misszióval egy újabb lépéssel közelebb kerültünk a kisműhold-alapú kvantuminternet kiépítéséhez. [17]

Az Európai Unió felkérésére az Európai Űrügynökség (European Space Agency – ESA) fejleszti az Eagle–1 műholdat, amely majd alacsony Föld körüli pályán keringve tud szerepet vállalni a kvantumkommunikáció globalizációjában.

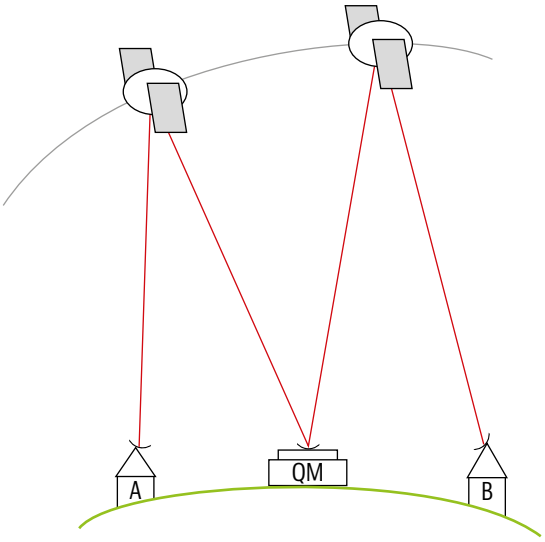
ÉPÜLŐ EURÓPAI KVANTUMKOMMUNIKÁCIÓS HÁLÓZAT

Bár a kvantummechanika Európában született, a második kvantumtechnológiai forradalomban sajnos kontinensünk lemaradt. Ezt felismerve 2016-ben hirdették meg a Quantum Manifestót, azt a kiáltványt, amelyben négy területen – kvantumszámítógép, kvantumkommunikáció, kvantumszimuláció és kvantumszenzorok – jelölték ki az európai fejlesztési irányokat. [18] A négy irányhoz kapcsolódóan 2018-ban indult el az európai kvantumtechnológiai flagship projekt (Quantum Technologies Flagship), majd 2019 júniusában meghirdették az Európai Kvantumkommunikációs Infrastruktúra kezdeményezést (European Quantum Communications Infrastructure – EuroQCI), amelyhez Magyarország már 2019 júliusában csatlakozott. Hosszú előkészítő tevékenységet követően 2023 januárjában indultak el az Európai Unió tagállamaiban különböző nemzeti projektek, ezzel párhuzamosan pedig egy európai szintű kvantumkommunikációs rendszer tervezése is zajlik, amelynek földi (optikai szálas) szegmense mellett, műholdra alapozott űrszegmense is lesz.

MŰHOLDAS KVANTUMINTERNET

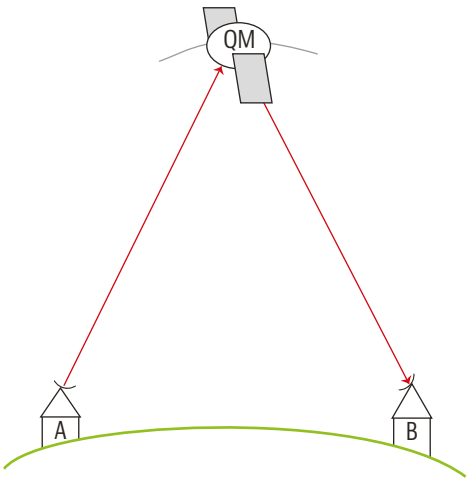
A gyorsan fejlődő kvantumkommunikáció egyik fő hajtóereje a klasszikus rendszerek biztonsági szintjének növelése. Ugyanakkor ez csak az első lépés. Világszerte sokakat foglalkoztat a kvantuminternet kiépítése. [19] Azonban számos kihívással kell szembenéznünk, ha klasszikus bitjeinket felváltja a kvantumbit, amely igen érzékeny a környezeti hatásokra. A környezettel való összefonódás, azaz a dekoherencia miatt a kvantumbit állapota könnyen megsérül, ami a kvantuminformáció vesztéséhez vezet. A globális kommunikációnál nehezítő tényező, hogy a kvantumbit állapotát nagy távolságokon keresztül meg kell őrizni, és továbbítani a kommunikáló felek között.

Ahhoz, hogy a jövő kvantuminternetén nagy távolságokon keresztül képesek legyünk kvantuminformációt küldeni, szükségünk van kvantummemóriára. Ennek fő feladata, hogy a beérkezett kvantumbitet nagy hatékonysággal beírja a memóriába, majd adott idő múlva szintén nagy hatékonysággal kiolvassa ugyanazt a kvantumbit állapotot, és továbbküldje a vevő felé. Ennek egyik legnagyobb kihívása, hogy a beérkező kvantumbit állapotát nem mérheti meg, mert akkor a kvantumbit bebillen egyik állapotba, és egy klasszikus információt hordozó rendszerré alakul. Sokféle kvantummemória-implementációs kísérlet zajlik világszerte, ahol fő szempont a minél hosszabb koherenciaidő (az-az időmennyiség, ameddig képesek vagyunk a kvantumbit állapotát változatlanul megőrizni) elérése, illetve minél nagyobb hűséggel tudjuk tartani a beérkező kvantumállapotot. [20] A további kihívások között a miniatürizálás szerepel, hiszen a cél, hogy könnyű, kisebb műholdakra is szerelhetővé váljon a technológia [21], illetve a felbocsátás során a mechanikai rezgésekkel szemben is nagy hibatűrőképességgel rendelkezzen. [22]

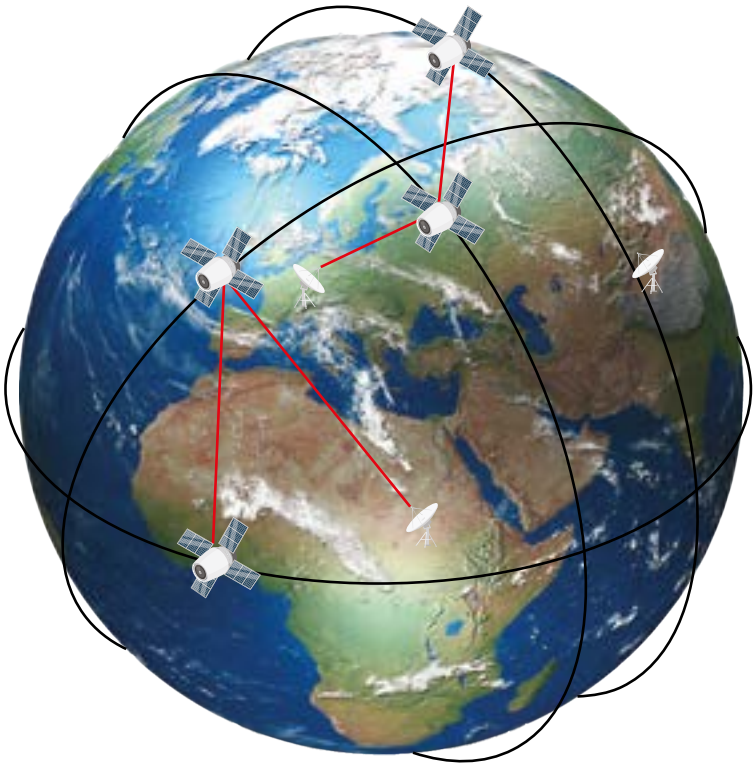


4. ÁBRA. **Földre telepített kvantummemória-alapú kvantumhálózat** (A szerzők saját szerkesztése)

Jelen pillanatban többféle architekturális elképzelés is létezik a műholdas kvantuminternettel kapcsolatban. Az egyik elv a 4. ábrán látható, ahol a kvantummemória (QM) a Földön helyezkedik el, rögzített helyzettel. Alice (A) kvantuminformációt küld Bobnak (B), de a nagy távolság leküzdése érdekében elsőként egy, a műholdon található kvantumjelismétlőnek (Quantum Repeater) sugározza fel a jelet,



5. ÁBRA. **Műholdas kvantummemória-alapú kvantumhálózat** (A szerzők saját szerkesztése)



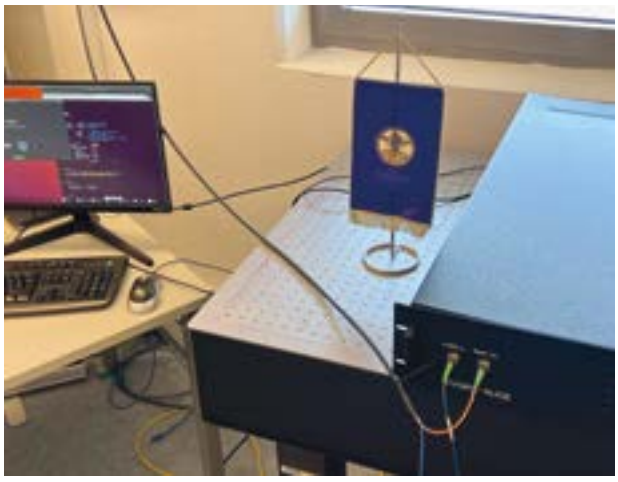
6. ÁBRA. **Kvantummemória-alapú műholdas konstelláció** (A szerzők saját szerkesztése)

amely – átjátszó állomásként – rögtön tovább is adja a kvantumbitet a földi kvantummemóriának. Adott idő után a tárolt állapotot visszaküldi ugyanannak a műholdnak, ami azonnal tovább küldi Bobnak. Ennek egyik nagy előnye, hogy nagy távolságokat le tudunk fedni. Az eljárásnak azonban komoly ára van: ahogy a 4. ábra is mutatja, a kvantumbitnek négyszer is szembe kell néznie az atmoszférikus hatásokkal, amelyek miatt a jel-zaj viszony romlik.

Erre a problémára az 5. ábrán látható elrendezés adhat megoldást. Ha a kvantummemóriát műholdas rendszerre építjük ki, akkor a kvantumbit atmoszférikus hatásoknak csupán csak kétszer van kitéve, azaz felére csökkentettük az ebből eredő dekoherencia mértékét.

Azonban még ez sem mondható teljesen tökéletes megoldásnak, hiszen egy műholddal egyszerre két, egymástól távol lévő vevőállomást belátni nehéz technológiai feladat. Ezért érdemes elgondolkozni a kvantummemória-alapú műholdas konstellációban, ahol a memóriák egymás között kis veszteséggel kommunikálnak (hiszen az űrben már nincs atmoszférikus hatás), ezzel megnövelhetik a rendszer együttes koherenciaidejét, így nagyobb távolságokat is képesek lefedni. Ez a rendszerstruktúra látható a 6. ábrán.

7. ÁBRA. **A 2022. májusi kísérleten készült fénykép a műegyetemi fejlesztésű QKD-berendezésről** (A szerzők felvétele)



HAZAI FEJLESZTÉSEK

A Budapesti Műszaki és Gazdaságtudományi Egyetemen több mint 20 éve foglalkozunk kvantuminformatikával és kvantumkommunikációval kapcsolatos kutatással, és 2012 óta saját rendszereket fejlesztünk. Munkánkat többek között a 2017–2021 között a HunQuTech hazai kvantumtechnológiai kiválósági projekt, 2020–2025 között a Kvantuminformatikai Nemzeti Laboratórium, míg 2023–2025 között a QCIHungary nevű projekt is támogatja. A Műegyetem és az Ericsson Magyarország együttműködésében készült egy, BB84 protokollt használó QKD-rendszer. [23] Fejlesztettünk egy második generációs kvantumkulcscsere prototípust is. Ezt a Műegyetemen fejlesztett rendszert éles hálózatban 2022. április 29-én teszteltük sikeresen, ekkor a Magyar Telekom által biztosított optikai szálon küldtünk át néhány fotonból álló jelet a Magyar Telekom kelenföldi központja és a BME I épülete között, több mint 2 kilométeres távolságon, felhelyezve ezáltal Magyarországot a kvantumkommunikáció nemzetközi térképére. Ezt követően új hazai távolsági rekordot állítottunk fel a kvantumkommunikáció területén 2022. május 25-én, a BME és a HUN-REN Wigner Fizikai Kutatóközpont közötti több mint 20 kilométeres távolságban megvalósított kvantumkommunikációval (7. ábra). A demonstráció során kvantuminformációkat kiolvasva állítottunk elő olyan kulcssorozatot, amelyet fel lehetett használni üzenetek és képek titkosítására. [24]

2023-ban továbbfejlesztettük a laboratóriumi körülmények között működő kvantum véletlenszám-generátorunkat is. [25] Ennek révén kvantumfizikai folyamatokra alapozva tudunk előállítani jó minőségű véletlenszámokat, amelyek fontos alapját jelentik a különböző titkosítási eljárásoknak. A saját fejlesztésű véletlenszám-generátorunk által előállított számok egy belső weboldalon keresztül elérhetők a Műegyetem polgárai számára.

A vezetékes kvantumkommunikációs terület mellett szabadtéri kvantumkulcsszétosztó rendszer fejlesztésével is foglalkozunk, együttműködve a Vodafone Magyarországgal. Az összeköttetés során a BME Természettudományi Karon fejlesztett összefonódott fotonforrást használjuk, valamint olyan, saját szinkronizációs berendezéseket, amelyek építését az Európai Űrügynökség is támogatja. A kísérleti demonstrációkon túl vizsgáljuk a műholdas kvantumkommunikáció különböző kérdéseit, többek között a több kvantumkommunikációs műholdból álló QKD-rendszerek, valamint a kvantuminternet technológiai megvalósíthatóságával kapcsolatban.

Nagy hangsúlyt fektetünk a jövő generációjának az oktatására is. 2022 őszén hazánkban elsőként a Műegyetemen indult el az űrmérnök mesterszak, amelyről részletesen a Haditechnika 2024/1. számában számoltunk be.[9] Fél évvel később, 2023 tavaszán az országban elsőként a BME Villa-

[9] https://doi.org/10.23713/HT.58.1.07

mosmérnöki és Informatikai Karon indult el kvantuminformatikai mellékspecializáció. Ennek során a mérnökinformatikus mesterképzés hallgatói előadások, gyakorlatok és laboratóriumi mérések segítségével mélyedhetnek el a kvantumszámítógépek és a kvantumkommunikáció különböző technológiai kérdéseiben.

Az Európai Unió támogatásával 2023. január elején kezdődött az EuroQCI-hoz kapcsolódó magyar kvantumkommunikációs projekt. A QCIHungary projektben a Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) koordinálásával a Budapesti Műszaki és Gazdaságtudományi Egyetem, az Eötvös Loránd Tudományegyetem és a HUN-REN Wigner Fizikai Kutatóközpont szakemberei közösen dolgoznak egy hazai kvantumkommunikációs infrastruktúra kialakításán. A projekt során a Műegyetem koordinálja az oktatással kapcsolatos feladatokat, valamint a kutatás-fejlesztési tevékenységeket is. Utóbbi keretében különböző vezetékes és szabadtéri rendszereket fejlesztünk és felkészülünk a műholdas kvantumkommunikációs rendszerekhez történő kapcsolódásra.

ÖSSZEFOGLALÁS

Cikkünkben a műholdas kvantumkommunikáció gyakorlati megvalósításának kérdéseivel foglalkoztunk. Miután bevezettük az olvasót a kvantumfizikai elveken alapuló távközlés legfontosabb jellemzőibe, részletesen is bemutattunk néhány területet és kitértünk a jövőbeli fejlesztés irányaira. Napjainkban a legnépszerűbb alkalmazási terület a kvantumalapú kulcsszétosztás, ami már nemcsak a laboratóriumban létezik, hanem a világon több cég kínál kapcsolódó terméket, számos helyen üzemeltetnek vezetékes hálózatot és terveznek műholdas rendszereket. Cikkünkben nagy hangsúlyt fektettünk az összefonódáson alapuló műholdas kvantuminternetre, bemutatva többféle architektúrális elképzelést is. Ezek közül a műszakilag legizgalmasabb a kvantummemória-alapú műholdas konstelláció, ahol a memóriák egymás között kis veszteséggel kommunikálnak. ■

HIVATKOZÁSOK

[1] Hanzo, L., Haas, H., Imre, S., O'Brien, D., Rupp, M., Gyongyosi, L. „Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless", IEEE, Proceedings of the IEEE, 2012. Volume 100, Special Centennial Issue, pp. 1853–1888., ISSN 0018-9219. https://doi.org/10.1109/JPROC.2012.2189788;

[2] Bacsárdi László. Az igazi kvantum csendje: Kvantumeszközök a hatékony kommunikáció szolgálatában. Tudományos Ismeretterjesztő Társaság, Természet Világa, 2016, 147. évf. 1. szám, pp. 11–14., ISSN 0040-3717. https://matarka.hu/cikk_list.php?fusz=135569 (Letöltve: 2024.6.3.);

[3] Bacsárdi László, Galambos Máté, Imre Sándor. Kvantumcsatorna a műhold–Föld és műhold–műhold kommunikációban. Hírközlési és Informatikai Tudományos Egyesület. Híradástechnika, LXV. évf. 2010/3–4., pp. 23–29., ISSN 0018-2028. https://regi.hiradastechnika.hu/data/upload/file/2010/2010_03_04/Pages_from_HT2010_3_4_3.pdf (Letöltve: 2024.6.3.);

[4] Bacsárdi László, Kiss András. „Kvantumkommunikáción alapuló műholdas hálózat vizsgálata", Magyar Asztronautikai Társaság, Űrtan Évkönyv 2014. Budapest, 2015, ISSN 1788-7771. https://www.mant.hu/kiadvanyok/urtan_evkonyv_2014.pdf (Letöltve: 2024.6.3.);

[5] Imre, S., Balázs, F. Quantum Computing and Communications: An Engineering Approach, John Wiley & Sons Ltd., 2004. https://doi.org/10.1002/9780470869048;

[6] Hughes, C., Isaacson, J., Perry, A., Sun, R.F., Turner, J. 2021, Entanglement. In: Quantum Computing for the Quantum Curious. Springer, Cham. https://doi.org/10.1007/978-3-030-61601-4_7;

[7] Griffiths, R. „Quantum Locality", Springer, Foundations of Physics, 2010, Vol. 41, pp. 705–733. https://doi.org/10.1007/s10701-010-9512-5;

[8] Khrennikov, A. „CHSH Inequality: Quantum Probabilities as Classical Conditional Probabilities", Springer, Foundations of Physics, 2015, Vol. 45, pp. 711–725. https://doi.org/10.1007/s10701-014-9851-8;

[9] Asbóth János. „A 2022. évi Nobel-díj: A Kvantumos Összefonódás, a »Kísérteties Távolhatás« Kísérleti Igazolása", Eötvös Loránd Fizikai Társulat, Fizikai Szemle, 2022, pp. 341–346.;

[10] Lugrin, T. „One-Time Pad." In: Mulder, V., Mermoud, A., Lenders, V., Tellenbach, B. (eds.) Trends in Data Protection and Encryption Technologies. Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-33386-6_1;

[11] Najeeb, M., Masood, A., Fazil, A. „Quantum Key Distribution for Secure Communications". Semantic Scholar. International Journal of Innovations in Science and Technology, 2022, pp. 173–183. https://doi.org/10.33411/IJIST/2022040406;

[12] Bennett, C. H., Brassard, G. „Quantum cryptography: Public key distribution and coin tossing". IEEE, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984. Volume 175, p. 8. New York. https://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf (Letöltve: 2024.6.3.);

[13] Hughes, Richard J., et al. „Practical free-space quantum key distribution over 10 km in daylight and at night", IOPScience, New J. Phys., 2002, 4–43. https://doi.org/10.1088/1367-2630/4/1/343;

[14] Fürst, M., et al. „Free-space quantum key distribution over 144 km", SPIE, Proc. SPIE, 2006, 6399, https://doi.org/10.1117/12.690174;

[15] Liao, S. K., Cai, W. Q., Liu, W. Y. et al. „Satellite-to-ground quantum key distribution." Nature. Nature 549, 2017, pp. 43–47. https://doi.org/10.1038/nature23655;

[16] Chao-Yang, Liu, et al. „Micius quantum experiments in space", American Physical Society, APS Physics, Rev. Mod. Phys., 2022, pp. 035001. https://doi.org/10.1103/RevModPhys.94.035001;

[17] Villar, A., et al. „Entanglement demonstration on board a nano-satellite", Optica Publishing Group, Optica, 2020, pp. 734–737. https://doi.org/10.1364/OPTICA.387306;

[18] Quantum Manifesto. Európai Unió, 2016. https://qt.eu/media/pdf/93056_Quantum-Manifesto_WEB.pdf (Letöltve: 2024.6.3.);

[19] Kaltenbaek, R. et. al. „Quantum technologies in space". Springer, Experimental Astronomy 51, 2021, ISSN 1572-9508. https://doi.org/10.1007/s10686-021-09731-x (Letöltve: 2024.6.3.);

[20] Ramakrishnan, R. K., et al. „The Quantum Internet: A Hardware Review", Springer, J Indian Inst Sci 103, 2022, pp. 547–567. https://doi.org/10.1007/s41745-022-00336-7;

[21] Ma, Lijun, Slattery, Oliver, Tang, Xiao. Optical quantum memory based on electromagnetically induced transparency, IOP Publishing, Journal of Optics, 2017, Volume 19. https://doi.org/10.1088/2040-8986/19/4/043001;

[22] Mol, Jan-Michael, et al. Quantum Memories for Fundamental Physics in Space, IOP Publishing, Quantum Science and Technology, 2023, Vol. 8. https://doi.org/10.1088/2058-9565/acb2f1;

[23] Czermann, M., Trócsányi, P., Kis, Z., Kovács, B., Bacsárdi, L. „Demonstrating BB84 Quantum Key Distribution in the Physical Layer of an Optical Fiber Based System", Hírközlési és Informatikai Tudományos Egyesület, Infocommunications Journal, 2021, VIII. pp. 45–55. https://doi.org/10.36244/ICJ.2021.3.5;

[24] Márton, B. L., Kis, Z., Bacsárdi, L. „Testing the First Hungarian CV-QKD System on a Real Optical Line", IEEE, SoftCOM 2023: 1–6, 2023. https://doi.org/10.23919/SoftCOM58365.2023.10271613;

[25] Schranz, A., Solymos, B., Telek, M. „Stochastic performance analysis of a time-of-arrival quantum random number generator". Wiley, IET Quantum Communication, 2021, 1–17. https://doi.org/10.1049/qtc2.12080.