BACSÁRDI LÁSZLÓ

Biztonságos kommunikáció kvantumalapú hálózatokban

Egy lassú folyamat

Pár évtizeddel ezelőtt a technika területén izgalmas folyamat indult el: az analóg rendszerekről fokozatosan átálltunk a digitális világra. Ennek következményeként az információt immáron egyre több helyen digitális jelekbe kódoljuk, és ez egyre inkább kihat a mindennapi életünkre. 2013-ban például hazánkban is a digitális műsorterjesztés lépett az analóg földfelszíni sugárzás helyére, és ennek megfelelő készülékeket vagy dekódereket kellett beszereznünk. Ez egy hosszú technikai folyamat egyik jelentős állomása volt. A háttérben azonban jelenleg is zajlik egy másik, szintén lassú folyamat, amely egy napon ugyanúgy a mindennapunk része lehet, ahogyan az analógról a digitálisra történt átállás megjelent. Ez pedig nem más, mint a kvantummechanikai elveken alapú informatika, a kvantuminformatika.

A kvantummechanika úttörői a XX. század első felében megalkották azt a keretrendszert, amellyel le tudjuk írni a nagyon kisméretű részecskék világát. *Niels Bohr* (1885–1962) dán fizikus alkalmazta elsőként a kvantumelméletet a hidrogénatom spektrumának magyarázatára, amiért 1922-ben Nobel-díjat kapott. 1927-ben fedezte fel *Werner Heisenberg* (1901–1976) a később róla elnevezett Heisenberg-féle határozatlansági relációt. A határozatlansági reláció azt mondja ki, hogy egymással kanonikusan konjugált mennyiségek, pl. egy részecske helye és impulzusa, nem mérhetők meg egyidejűleg teljes pontossággal. Felfedezését 1932-ben Nobel-díjjal jutalmazták, egy évvel később pedig *Erwin Schrödinger* (1887–1961) osztrák elméleti fizikus munkáját ismerték el Nobel-díjjal, akinek a nevéhez a kvantummechanika alapegyenletének – az ún. Schrödinger-egyenlet – megalkotása fűződik.

Felhasználva a kvantummechanikai keretrendszert, 1981-ben *Richard Fenyman* amerikai fizikus már kvantum számítástechnikáról beszélt, 1985-ben pedig egy brit-izraeli fizikus, *David Deutsch* megalkotta az univerzális kvantumszámítógép fogalmát. A magyar szakkifejezéssel kvantuminformatikának nevezett területen azóta számos kutató dolgozik, s bár általános célú kvantumszámítógépet még nem sikerült építeni (a kanadai D-Wave cég által gyártott D-Wave Two nevű kvantumszámítógép is csak bizonyos célzott problémák megoldására alkalmas), az eddigi eredmények igen biztatóak [1]. A közeljövőben a kapcsolódó eszközök egyre inkább megjelenhetnek majd a tudományos és üzleti életben.

De mi is az a kvantumbit?

A kvantuminformatika alapvető információs egysége a kvantumbit (angolul quantum bit vagy qubit). A hagyományos (nézőpontunkból klasszikusnak nevezett) informatikában bitekről beszélünk, amelyek két lehetséges értéket vehetnek fel (0 és 1). A kvantumbit azonban a két alapállapot tetszőleges kombinációjában (szakszóval szuperpozíciójában) lehet, azaz végtelen sok állapotban létezhet [2].

Sokféle módon tudjuk illusztrálni a kvantumbitnek ezt a szuperpozícióját; a szerző egyik kedvenc példája az ételek világához kapcsolódik. Napjaink rohanós ebédszünetében egyre többször fordul elő, hogy egy hagyományos többfogásos ebéd helyett valami egyszerűbb ételhez fordulunk, mint például a gyros vagy a pizza. Jobb pizzériák azonban kínálnak egy különleges kombinációt, amelyet gyrosos pizzának neveznek. Bár a szakácsok ezzel biztosan nem értenek egyet, és a receptje is némileg mást tükröz, de egy absztrakt módú megközelítésben mi más lenne ez, mint egy olyan étel, ami egyszerre gyros, illetve pizza is. Ha sok húst szórtak rá, akkor inkább gyros, mintsem pizza, ha pedig spóroltak a feltéttel, akkor inkább pizza, mintsem gyros. Valami hasonló a kvantumbit is, amely egyszerre található meg a két bázisállapot valamilyen szuperpozíciójában. A kvantumbitnek azonban van még egy érdekessége: amikor ránézünk, és egy méréssel kiolvassuk az értéket, a kvantumbit megszűnik szuperpozícióban lenni, és a két alapállapot valamelyikét veszi fel. Mintha egy lezárt pizzásdoboz lenne előttünk, aminek az illatáról érezzük, hogy gyrosos pizza van benne, de amikor éhesen felnyitjuk a dobozt, vagy egy teljesen hagyományos gyrost, vagy egy teljesen normális – feltét nélküli – pizzát találunk benne.

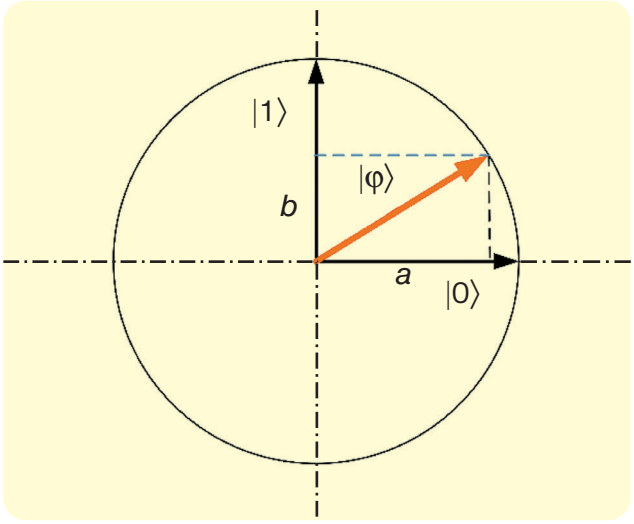
De mielőtt bárki azt hinné, hogy a kvantuminformatikusok elhízott szakemberek, akik pizzásdobozokba csomagolt gyrost fogyasztanak, definiáljuk a kvantumbitet szakszerű módon is. Egy kvantumbitet a bázisállapotaival és komplex valószínűségi amplitúdóival adunk meg, az alábbi módon:

$$|\varphi\rangle = a|0\rangle + b|1\rangle,$$

ahol az a és b olyan komplex számok, amelyek abszolútértéknégyzete egyet ad. Az a és b valószínűségi amplitúdó abszolútértékének négyzete azt mutatja meg, mekkora valószínűséggel kapunk 0-t illetve 1-et, ha kiolvassuk a $|\varphi\rangle = 0{,}8|0\rangle + 0{,}6|1\rangle$ kvantumbit értékét (szakszóval mérést hajtunk végre). Például a kvantumbitet megmérve 0,64 valószínűséggel 0-át kapunk a mérés végén, 0,36 valószínűséggel pedig 1-et. Mivel egységnyi hosszú vektorokról beszélünk, a legegyszerűbb egy Descartes-féle koordinátarendszerben körként elképzelni a kvantumbitet, a körvonal tetszőleges pontja lehet a bitünk értéke, a két tengely pedig a két bázisállapot, ahogy az **1. ábrán** is látható. (Ez a kétdimenziós kvantumbit, de tudjuk definiálni magasabb dimenziókra is.) Még nagyon sok más módon ábrázolhatjuk a kvantumbitet, egy fiatal műegyetemi fizikushallgató, *Galambos Máté* egy fraktál alapú kvantumbit-reprezentációval ért el első helyezést a 2013-as Országos Tudományos Diákköri Konferencián.

A gyakorlati megvalósítást tekintve, a kvantumbit lehet bármilyen két jól megkülönböztethető állapottal rendelkező kvantumrendszer (pl. elektron töltése, elektron spinállapotai, atomi hiperfinom állapotok stb.). A kommunikációban lézert használunk, így a foton különböző polarizációs állapotait (tipikusan vízszintes, illetve függőleges) feleltetjük meg a bázisállapotoknak.

Kvantumbiten kívül azonban még szükségünk van egyéb eszközökre is, hogy kvantum alapú kommunikációról beszéljünk. Ebben nyújt segítséget a kvantummechanika négy posztulátuma. Az első a rendszer állapotát írja le, a második az időbeli fejlődésre



1. ábra. Egy kétdimenziós kvantumbit reprezentációja. A narancssárga vektor jelöli a kvantumbitet, míg a vízszintes és függőleges vektorok az alapállapotokat reprezentálják

vonatkozik, és abban segít, hogy a teljes rendszer viselkedését zárt transzformációkkal tudjuk leírni. A harmadik a mérésre vonatkozik, és definiálja a kapcsolatot a kvantumvilág és a klasszikus világ között, a negyedik pedig az összetett rendszerekre vonatkozik [3]. A posztulátumokról és különböző egyéb érdekes jelenségekről részletesen a Természet Világa 2013. januári számában Bacsárdi–Imre szerzőpárostól megjelent *Kommunikáció mélyben és magasban* című cikkben lehet olvasni [4].

Kvantum alapú átvitel, dióhéjban

Bármennyire is varázslatosnak hangzik a kvantum alapú kommunikáció világa, a célunk itt is ugyanaz, mint a hagyományos informatikában: információt átvinni a küldőtől a fogadóig. Azért, hogy ne *A* és *B* betűként kelljen a két kommunikáló félre hivatkozni, keresztnévvel ruháztuk fel őket, így lettek Aliz és Bob. Amíg hagyományos informatikában egy klasszikus információelmélettel leírható közvetítő közeget használunk, addig kvantum alapú kommunikáció esetében kvantumcsatornát. Egy lehetséges megoldást szemléltet a **2. ábra**. Az A_i jelölésű klasszikus információt $|\varphi_A\rangle$ kvantum állapotba kódolunk egy klasszikus-kvantum konverziót megvalósító *A'* transzformáció által, amely transzformálja a klasszikus 0 vagy 1 bitet a $|0\rangle$ vagy $|1\rangle$ alapállapot valamelyikébe. Ezután ezt a kezdeti kvantumbitet egy következő művelet – az ábrán *C-vel* jelölt transzformáció – tovább alakítja egy $|\varphi_A\rangle$ állapotba. Ezeket a kvantumállapotokat küldjük át Bobnak egy a kvantumcsatornán. Ideális világban az átvitel tökéletes (hibamentes) lenne, de a valóságban a csatorna különböző hibákat eredményez a kvantumbitekben. A lehetséges csatornahiba miatt Bob a $|\varphi_A\rangle$ állapotot kapja meg. A dekódolási fázisban Bobnak végre kell hajtania valamilyen hibajavítást (*D* transzformáció), majd elvégezve egy kvantum-klasszikus átalakítást (szakszóval mérést) visszatérünk a klasszikus világba. A mérés eredménye a B_i klasszikus információ, amely – ha mindent jól csináltunk – meg fog egyezni a kezdeti A_i értékkel.

Teleportáció, tömörítés

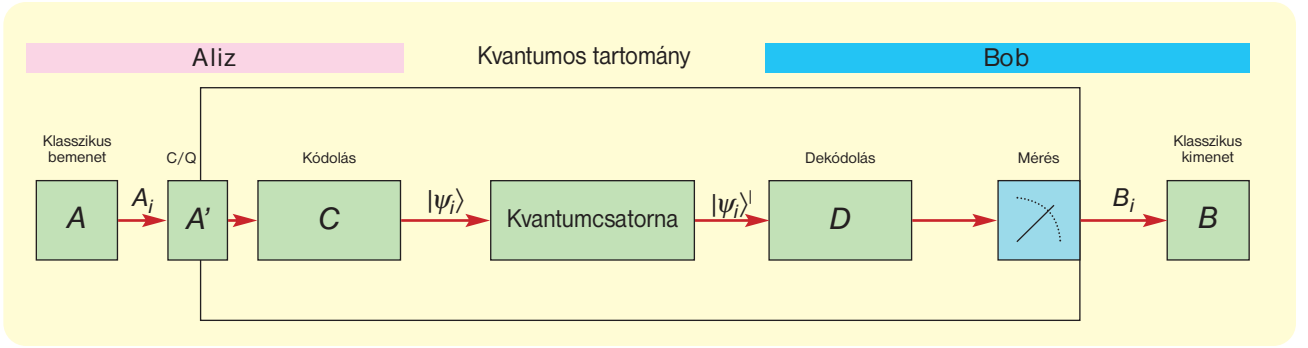
Kvantum alapú hálózatok működési módjait – a kommunikáció szempontjából – alapvetően három csoportba oszthatjuk:

1. *Kvantuminformáció átvitele*: Van egy kvantuminformációnk, amelyet szeretnénk eljuttatni egyik pontból a másikba, és ott további műveleteket végrehajtani rajta. Az átvitelhez kvantumcsatornát és/vagy klasszikus csatornát használunk. Erre jó példa a teleportálás.
2. *Klasszikus információ átvitele, kvantumcsatornán*: Van egy klasszikus információnk, amelyet szeretnénk átvinni két pont között, és ehhez kvantumbiteket használunk fel. Ilyen a szupersűrű tömörítés.
3. *Klasszikus kommunikáció, kvantum biztonság*: Alapvetően klasszikusan kommunikálunk, de szeretnénk, ha ez biztonságos lenne, ezért titkosítjuk a kommunikációnkat. A titkosításhoz szükséges kulcsokat kvantuminformatikai eljárások segítségével, kvantumcsatornán osztjuk meg a kommunikáló felek között. A kvantum alapú kulcsszétosztó eljárások alapvetően ebbe a csoportba tartoznak.

A kvantumteleportáció elméletét 1993-ban publikálták, és a publikáció címe nagyon jól összefoglalja, miről is szól ez a kommunikációs protokoll: *„Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels”* (Ismeretlen kvantumállapot teleportálása két klasszikus és egy összefonódott csatornán keresztül).

Aliz előállít egy olyan kvantumbitet, amelyet nagyon szívesen megosztana Bobbal. Anélkül, hogy megismerné a nála lévő kvantumbit értékét, képes arra, hogy két klasszikus információ elküldésével átjuttassa Bobhoz. Ahhoz, hogy ezt megtehesse, még a kvantumbit előállítása előtt találkozik Bobbal, és megosztoznak egy speciális kvantumbit-páron, amelyet összefonódott párnak nevezünk.

2. ábra. Klasszikus információ átvitele egy kvantumcsatornán. A küldő (Aliz) kvantumbitbe kódolt klasszikus információt küld kvantumcsatornán a fogadónak (Bob)



Az összefonódás jelensége még *Einstein*t is megdöbbentette, mert az összefonódott pár tagjai meghatározott módon viselkednek, még akkor is, ha azokat nagyon nagy távolságra visszük egymástól. Ha fogjuk a legegyszerűbb összefonódott párt, amelyet Bell-párnak is nevezünk, és megmérjük a pár egyik tagját, akkor, ha 0 értéket kaptunk, biztosak lehetünk abban, hogy a pár másik tagja is 0 értéket vett fel. Ha azonban 1 lesz a mérés eredménye, akkor a pár másik tagja is 1 értéket vesz fel. Ha a pár két tagját nagyon messze visszük egymástól, az egyiket mondjuk a Földön hagyjuk, a másikat pedig elvisszük a 67P/Csurjumov–Geraszimenko üstököshöz, ahova nem olyan régen leszállt a Philae leszállóegység, akkor is ugyanígy viselkednek – maga a jelenség a fénysebességnél gyorsabban megtörténik. Fénysebességnél gyorsabb kommunikációról azonban nem beszélhetünk, mert a mérés teljesen véletlenszerű: 50% eséllyel kapunk 0 értéket, 50% eséllyel pedig egyet, így információt nem tudunk vele továbbítani.

Aliz és Bob tehát a teleportálás megkezdése előtt megosztoztak egy összefonódott páron. Aliz előállítja azt a kvantumbitet, amit Bobnak szeretne eljuttatni, végrehajt pár műveletet az előállított kvantumbiten és az összefonódott pár nála lévő felén. Majd végrehajt két mérést, megsemmisítve a méréssel mind az általa előállított kvantumbitet, mind az összefonódott pár nála lévő tagját. A mérés eredményeként kap két klasszikus információt (két darab 0 vagy 1 érték), amelyet átküld Bobnak. Bob ezután végrehajt néhány transzformációt az összefonódott pár nála lévő felén, amely ezek hatására átváltozik azzá a kvantumbitté, amit Aliz át szeretett volna küldeni Bobnak. Így a teleportálandó kvantumbit Aliz oldalán ugyan megsemmisült, de néhány másodperccel később megjelenik Bobnál. A teleportálás jelenségét 1997-ben kísérletileg is igazolták, a jelenlegi távolsági rekordot pedig osztrák kutatók tartják a 2012-ben felállított 143 kilométeres távolsággal **(3. ábra)**.

A szupersűrű tömörítés (angolul *superdense coding*) a második csoportra egy jó példa. A protokoll során klasszikus információt szeretnénk átvinni kvantumcsatorna használatával. Aliz és Bob jó előre megosztozik sok-sok összefonódott páron, majd egy kvantumcsatornán kvantumbiteket küldenek egymásnak. Egy kvantumbit átküldésével azonban képesek lesznek egyszerre két klasszikus bitet eljuttatni – innen a szupersűrűségű elnevezés.

Másolási problémák

Korábban már említettem, hogy a mérést elvégezve a kvantumbit megsemmisül. Ez azt jelenti, hogy ha van egy ismeretlen állapotú kvantumbitünk, akkor mi annak a kvantumos értékét nem tudjuk megismerni, hiszen a mérés után csak 0 vagy 1 értéket kapunk vissza. A mérést pedig ismételten nem tudjuk elvégezni, hiszen nincs már meg a kvantumbitünk. Ha van olyan berendezésünk, ami legyártotta a kvantumbitet, akkor elő tudunk állítani egymillió ugyanolyan darabot, meg tudjuk mérni mind az egymilliót, és az így kapott statisztikából már tudunk valamilyen szinten következtetni arra, hogy mi lehetett az eredeti kvantumbit. A fogalmazás azért ilyen óvatos, mert a mérés során a komplex valószínűségű amplitúdó abszolútérték négyzetét kapjuk vissza, amiből mind az előjelek, mind a komplex értékek már eltűntek, így a mérési statisztikánk eredményeként még mindig végtelen hosszú listából kell találgatnunk.

Kvantumbit újragyártása helyett jobb megoldásnak tűnne, ha lemásolnánk a kvantumbitet a mérés előtt sok-sok példányban, és a másolatokon végeznénk el a méréseket. Sajnos azonban ezt a kvantummechanika nem teszi számunkra lehetővé. A *Nincs másolás tétel* értelmében ismeretlen állapotú kvantumbitről nem készíthető másolat. A tételbizonyításban jártas olvasók számára érdekes lehet, hogy a kapcsolódó bizonyítás indirekt úton történik, azaz abból a feltételezésből indulunk ki, hogy létezik egy univerzális másológép, de a bizonyítás során sajnos pár lépés után igen jelentős ellentmondásba kerülünk a kiindulási feltételekkel. Fontos hangsúlyozni, hogy a kijelentés ismeretlen állapotú kvantumbitekre vonatkozik. Ha ismerjük a kvantumbitet – például tudjuk, hogy a 0 bázisállapotról van szó –, akkor gond nélkül le tudjuk másolni. Ha azonban nem ismerjük a kvantumbitünket, sem mi, se senki más nem tud róla másolatot készíteni – s ez több szempontból is egy nagyon fontos tulajdonság [5].

3. ábra. Lézerjel az Európai Űrügynökség (ESA) optikai földi állomásán Tenerife szigetén. La Palma és Tenerife között 143 kilométeres távolságban sikerült teleportációt megvalósítaniuk osztrák kutatóknak
(Forrás: ESA)

Kvantum jelismétlők

A távközlésben használt optikai szálakon fényjelekkel kommunikálunk, nagy átviteli sebességet elérve akár országon belül, akár kontinensek között. Az optikai szálban haladó jel azonban csillapítást szenved, és nagyságrendileg 100 km megtétele után a jel annyira gyengül, hogy már alig tudjuk észlelni. Azért, hogy a jel elvesztését megakadályozzuk, erősítőket használunk: az erősítő egyik oldalán beérkezik a gyengült jel, a másik oldalán pedig újra egy erős jel indul tovább, hogy később egy újabb erősítőbe érkezzen. A kvantum alapú kommunikáció fotonokon alapul, így itt is lézerimpulzusokkal dolgozunk, azonban van egy jelentős különbség: nem tudunk erősítést végrehajtani. Az erősítés ugyanis nem más, mint egy másolás – ismeretlen állapotot pedig nem tudunk másolni. Az erősítőre megérkező kvantumjelet nem érdemes megmérni sem, hiszen az így visszakapott 0 vagy 1 értékből nem tudunk következtetni arra, mi volt az eredeti kvantumbit. A kvantum jelerősítő (angol szakszóval *quantum repeater*) jelenleg a kvantuminformatikai kutatások egyik Szent Grálja. Tudjuk, hogy tökéletes erősítőt nem lehet építeni, de már az segítség lenne, ha ismert állapotok halmazát tartalmazó jeleket tudnánk erősíteni, lehetővé téve ezáltal a nagytávolságú, többpontos kvantumátvitelt.

Kvantum alapú kulcsszétosztás

Vannak olyan területek, ahol előny, hogy nem tudunk másolni. A kvantum alapú kulcsszétosztó eljárások (angol szakkifejezéssel *quantum key distribution*, QKD) során ezt tulajdonságot ugyanis a biztonságos kommunikáció érdekében nagyon jól ki tudjuk használni. Ahhoz, hogy biztonságosan tudjunk adatot küldeni két fél között, titkosításra van szükség. A napjainkban használt titkosítási megoldások két nagy csoportba oszthatóak: az egyik során ugyanazt a kulcsot használjuk a kódoláshoz mint a dekódoláshoz. A másik során pedig a kódoláshoz során használt kulcsnak van egy pár-

ja, amivel dekódolni tudjuk az üzenetet. Előbbit szimmetrikus, utóbbit pedig aszimmetrikus kulcsú titkosításnak nevezzük. Ennek egy nagyon jó példája a nyilvános kulcsú titkosítás, amelyben egy nyilvánosan, bárki számára elérhető kulccsal lehet kódolni az üzenetet, de visszafejteni csak az üzenet címzettje tudja, aki rendelkezik a nyilvános kulcshoz tartozó úgynevezett titkos kulccsal. Jelenleg ezt használjuk nagyon sok helyen az internet világában, ezen alapul például a https protokoll – amikor a biztonságos böngészés jegyében egy lakat jelenik meg a böngészőnkben. A háttérben egy olyan matematikai elmélet áll, amely prímszámokról és prímtényezős felbontástól szól. Erről azonban sajnos tudjuk, hogy törhető, azaz egy támadó rájöhet a dekódoláshoz szükséges kulcsra. De ha elegendően nagy kulcsot választunk (amely sok-sok bitből áll), akkor ez a támadási folyamat viszonylag időigényes, napokig, hónapokig is eltarthat. Ha megépül az első univerzális kvantumszámítógép, akkor azonban ez a titkosítás nagyon gyorsan törhetővé válik: az 1994-ben *Peter Shor* által publikált Shor-algoritmus használatával a törési idő hónapokról másodpercekre csökken. Az elméleti algoritmusok gyakorlati megvalósítása (a kapcsolódó berendezések építésének nehézsége miatt) azonban lassan halad, a Shor-algoritmussal 2001-ben a 15-ös számot sikerült prímtényezőkre bontani, és csak 2012-ben tudtak kicsivel előrébb lépni, a 21-es szám felbontásával. Még ugyanebben az évben azonban egy másik algoritmus használatával kínai kutatóknak sikerült a 143-at prímtényezőkre bontaniuk. Sőt, 2014 végén egy angol–japán szerzőpáros azt bizonyította be, hogy a kínai kísérletben igazából az 56 153-as szám prímtényezős felbontása is előállt.

Ugyanakkor a szimmetrikus kulcsú titkosítók családjában vannak olyan algoritmusok, amelyek matematikailag bizonyított biztonságot és lehallgatatlanságot nyújtanak. A kritikus kérdés csupán az, hogyan osztoznak meg a kommunikáló felek a titkosításhoz használt kulcson – hiszen mind a kódoláshoz, mind a dekódoláshoz ugyanazt a kulcsot kell használniuk. Erre egy jó megoldás, ha egy megbízható futárt használnak, de igen lassú dolog mindenhova mindig embert küldeni. A kvantum alapú kulcsszétosztás pont erre a kulcscserére kínál hatékony és biztonságos megoldást. Mivel ismeretlen állapotú kvantumbiteket nem tudunk másolni, ezért a támadónak nincsen arra lehetősége, hogy lemásolja Aliz és Bob között áramló információt (nem lehetséges a passzív támadás), hanem aktívan közbe kell lépnie. A kulcsszétosztó protokollok azonban úgy működnek, hogy egy támadó aktív megjelenése elrontja a kommunikációt, zajt visz a kvantumcsatornába. Aliz és Bob pedig értesül arról, hogy a megszokottnál zajosabb lett a csatorna, így tudomást szereznek a támadó jelenlétéről.

Az első generációs QKD protokollok egyfoton forrásokon alapulnak, azaz egyszerre egy fotont küld Aliz Bobnak, és ebbe az egy fotonba kódolja be a kulcs előállításához szükséges információt. Azonban egyetlen egy foton előállítása mérnökileg nem könnyen megvalósítható feladat, a detektálása pedig még nehezebb, ezért az elmúlt években megjelentek a második generációs kulcsszétosztó eljárások. Ezek során gyengített lézerjelekkel olyan fotoncsomagokat küldenek, amelyek néhány tíz (maximum pár száz) fotont tartalmaznak, a vevőoldalon pedig egy speciális mérést végeznek el. Az eljárások mögött lévő matematikai elméletek azt mutatják, hogy ha egy lehallgató megpróbál megszerezni néhány fotont a fotoncsomagból, akkor abból semmilyen információra nem tud következtetni az előállított kulccsal kapcsolatban. Ha pedig néhány tíz fotont rabol egy támadó, az akkora zajt visz a rendszerbe, hogy észlelni fogják, és leállítják a kulcscserét.

Hazai vonalon

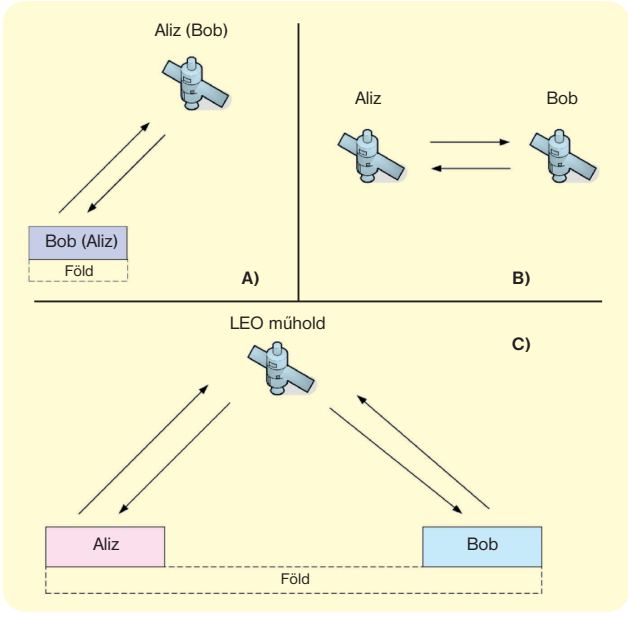
Magyarországon több helyen is foglalkoznak kvantuminformatikához kapcsolódó matematikai, fizikai és mérnöki kutatással, többek között az MTA Wigner Fizikai Kutatóközpontban, a Szegedi Tudományegyetemen, a Pécsi Tudományegyetemen, a Nyugat-magyarországi Egyetemen és a Műegyetemen. Utóbbin a Természettudományi Karon a kvantumszámítógép fizikai leírásával, valamint kvantumoptikai kutatásokkal, a Villamosmérnöki és Informatikai Karon pedig Számítástudományi és Információelméleti Tanszéken kvantumalgoritmusokkal foglalkoznak. A kommunikáció terén a BME Hálózati Rendszerek és Szolgáltatások Tanszékén működő Mobil Kommunikáció és Kvantumtechnológiák Laboratórium munkatársai folytatnak kutatást kvantumcsatorna szuperaktiválása, kvantum-ismétlők, pilot kvantumbit alapú csatornakódolás, kvantumhálózat tervezése, kvantum alapú kulcsszétosztás területén. A BME és a Nyugat-magyarországi Egyetem kutatói műholdas kommunikáció modellezésével és szimulációjával is foglalkoznak. Az ipari területet tekintve egy hazai támogatású pályázatban egy balatonfüredi cég vezetésével, hazai kutatók részvételével épül az első magyar kvantum alapú kulcsszétosztó berendezés, amely egy hagyományos, a mindennapi távközlésben is használt optikai szálon valósítja meg a titkosításhoz szükséges kulcsok biztonságos és lehallgathatatlan cseréjét.

A műholdas világ kérdései

Az első kvantum alapú kulcsszétosztó protokollt, a BB84-et 1984-ben publikálták, és pár évvel később kísérletileg is igazolták a működését. Optikai szálon azonban nem tudunk erősítést végrehajtani, így a kutatók érdeklődése elég korán a szabadlégköri csatornák felé fordult. Az első szabadtéri kvantum alapú kulcsszétosztást 1991-ben hajtották végre 30 centiméteres távon, 2006-ben pedig egy nemzetközi kutatócsoport a Kanári-szigeteken 144 kilométeres távon demonstrálta a szabadtéri kulcscsere megvalósíthatóságát. Az újabb és újabb sikeres demonstrációk mind azt mutatják, képesek leszünk ezt a technikát akár műhold-műhold, akár Föld-űr kommunikációban alkalmazni. Nem véletlen, hogy mind a NASA, mind az Európai Űrügynökség (ESA) a következő évek egyik fontos feladatának jelölte meg a kvantum alapú űrkommunikáció megvalósítását.

Amikor műholdas kvantumkommunikációról beszélünk, akkor általában három különböző megoldásra gondolunk, ahogy a **4. ábra**

4. ábra. Három lehetőség a műholdas kvantum alapú kommunikációra. A: földi állomás és egy műhold között. B, két műhold között, C: két földi állomás között, egy (vagy több) műholdon keresztül



is szemlélteti. Történhet egy földi állomás és egy műhold között, vagy két műhold között, vagy két földi állomás között egy (vagy több) műholdon keresztül [6].

Az Országos Tudományos Kutatási Alapprogramok (OTKA) támogatásával a 2015–2017 közötti időszakban jelen cikk szerzője a Nyugat-magyarországi Egyetemen zajló kutatásában a kvantum alapú műholdas kommunikáció megoldatlan kérdéseire fókuszál. A hároméves kutatási projekt az alábbi területeket érinti: kvantum alapú műholdas kommunikáció számára fontos csatornák modellezése; egy komplex hálózati modell készítése, amely lehetővé teszi a globális kulcsszétosztást műholdakon keresztül; klasszikus és kvantum alapú hibajavítás a globális kulcscserélési eljárásban.

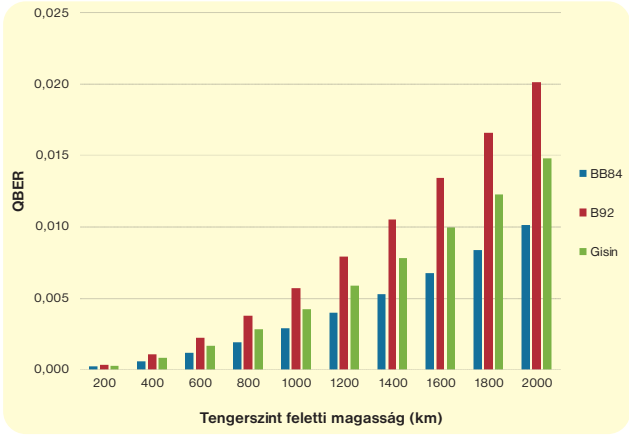
Megközelítésünkben a kommunikáló felek klasszikus információt szeretnének kicserélni egymással, ehhez szimmetrikus kulcsú kódolási eljárásokat használnak, a szükséges kulcscserét pedig kvantum alapon hajtják végre. Ilyen jellegű komplex hálózat vizsgálatával korábban nem foglalkoztak. Az elmúlt évek során matematikai modellünk segítségével elkezdtük megvizsgálni a kvantumalapú műholdas kommunikáció gyakorlati megvalósításának bizonyos paramétereit. Az előzetes kutatási eredményeket felhasználva szeretnénk megvizsgálni, milyen kvantuminformatikai kódolási eljárásokat tudunk alkalmazni a Föld-műhold, műhold–Föld, Föld–Föld kommunikációban.

A kutatásban olyan szimulációs vizsgálatokat végzünk, amelyek a gyakorlati kvantum alapú megoldások megvalósíthatóságának korlátjait vizsgálják (pontosan milyen kommunikációs költségekkel jár a kvantum-kulcscserén alapú kommunikáció, hogyan változik a teljes rendszer hibázása különböző fizikai paraméterek függvényében – különös tekintettel a műhold pályamagasságára valamint a műhold és a földi állomás látószögére). Komplex modellünk a Föld–műhold, műhold–műhold és műhold–föld irányokat is tartalmazni fogja, és ezáltal lehetővé válik a műholdas QKD klasszikus és kvantum-folyamatainak modellezése. A rendszer modelljét a QKD protokollok mellett kiterjesztjük további kvantum alapú protokollok vizsgálatára és elemzésére (pl. kvantum hibajavító kódolás).

A 2015-ben kezdődött kutatás eredménye olyan vizsgálati modell lesz, amely lehetővé teszi műholdas kommunikációs folyamatok szimulálását klasszikus és kvantum alapú eljárások felhasználásával (pl. klasszikus hibajavítás, kvantum alapú kulcsszétosztás stb.). A kutatási időszak végére olyan elemzések és vizsgálatok állnak majd rendelkezésre a kvantum alapú műholdas kommunikáció gyakorlati megvalósíthatóságával kapcsolatban, amelyek felhasználhatóak a hazai és a nemzetközi űripar számára.

Műholdak közelében

A szabadtéri kvantumcsatorna működését rengeteg paraméter befolyásolja. Műhold–műhold közötti kapcsolat esetében az egyfoton források teljesítőképessége és a detektorok véges mérete mellett a diffrakció miatti fókuszálási hibák eredményeznek zajt. Műhold–Föld, illetve Föld-műhold csatorna esetén pedig a légkör gázai, valamint a pára és a por is veszteséget generálnak. A légkör alsó rétegeiben megjelennek az optikai turbulenciák is, amelyek szintén jelentős vesztességet okoznak. Ráadásul egy kommunikáció esetében figyelembe kell venni mind a kulcsszétosztásra, mind a később használt kommunikációs protokollokat, amelyek eltérő módon működnek. Mindenesetre, az eddigi előzetes eredményeink biztatóak, és azt mutatják, egyfoton forrásokat feltételezve megvalósítható a kvantum alapú kulcsszétosztás űrbeli környezetben. Az **5. ábrán** három kvantum alapú kulcsszétosztó protokoll alkalmazását vizsgáltuk, kékkel a BB84, pirossal a B92, zölddel a Gisin-protokollt jelöltük. A zaj mértékét a kvantumcsatornán a kvantum-bithibaaránnyal mérjük (angolul *quantum bit error rate*, innen származik a QBER rövidítés). Minél kisebb a QBER értéke, annál kevesebb hiba történik a kommunikáció során [7]. Vízszintes tengelyen a Föld körül keringő műholdak pályamagassága, függőleges tengelyen pedig a zaj látható.



5. ábra. Különböző QKD protokollok kvantum-bithibaarány értékei a műhold pályamagassága függvényében

A következő évek elé

2008-ban Ausztriában a gyakorlatban is demonstrálták egy kvantum alapú kulcsszétosztó hálózat működését, összekötve a Siemens cég négy bécsi és St. Pölten-i központját. 2012 végén pedig egy kínai és egy osztrák kutatócsoport meglebegtette annak a lehetőségét, hogy együtt fognak dolgozni egy Bécs és Peking közötti, műhold alapú kvantumkulcscsere megvalósításán. A kanadai D-Wave cég eddig két kvantumszámítógépet gyártott: 2011-ben a D-Wave One az amerikai Lockheed Martin céghez, míg 2013-ban a D-Wave Two gép a Google és a NASA által közösen felállított kutatóközpontba került. Amerikai, ausztrál és svájci cég mellett egy francia cég is belépett a vezetékes kvantum alapú kulcsszétosztó berendezéseket kínáló gyártók sorába, és hamarosan Magyarországon is megépül az első kvantummechanikai elveken működő, második generációs kulcsszétosztó berendezés. Ugyan a kvantum alapú hálózatok a közeljövőben nem lesznek még a mindennapjaink része, de a háttérben zajló folyamatok egyre látványosabbak.

A szerző köszönetet mond Imre Sándornak a cikk elkészítéséhez nyújtott segítségért.

A szerző kutatását az OTKA PD-112529 pályázat támogatta.

Irodalom

[1] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, L. Gyongyosi: „Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless", Proceedings of the IEEE, Volume: 100 , Issue: Special Centennial Issue, pp. 1853–1888.
[2] M. A. Nielsen, I. L. Chuang, „Quantum Computation and Quantum Information", Cambridge University Press, 2000.
[3] S. Imre, B. Ferenc. „Quantum Computing and Communications: An Engineering Approach", Wiley, 2005.
[4] Bacsárdi László, Imre Sándor, „Kommunikáció mélyben és magasban", Természet Világa, 2013. január.
[5] Bacsárdi László, Galambos Máté, Imre Sándor, „Kvantumalapú algoritmusok", Informatikai Algoritmusok 3., Vác: MondAt Kiadó, 2013, pp. 1785–1827.
[6] L. Bacsardi. „Efficient Quantum Based Space Communications", Lambert Academic Publishing, 2013.
[7] L. Bacsardi, A. Kiss, „Overview of a Space Based Quantum Key Distribution Network", In.Poc. 65th International Astronautical Congress, Toronto, Canada, 2014.