# Kvantumcsatorna a műhold–Föld és műhold–műhold kommunikációban

BACSÁRDI LÁSZLÓ, GALAMBOS MÁTÉ, IMRE SÁNDOR

*Budapesti Műszaki és Gazdaságtudományi Egyetem, Híradástechnikai Tanszék*
*{bacsardi, imre}@hit.bme.hu, galambos@mcl.hu*

*Kulcsszavak: kvantuminformatika, űrtávközlés, légköri modellezés*

**Napjaink egyik leggyakrabban használt titkosítási algoritmusa az RSA algoritmus, a számítógépek és a számítási kapacitás fejlődésével azonban felmerül a kérdés, mi lesz az RSA után. Az egyik lehetséges megoldást a kvantummechanikai elveken alapuló informatika, a kvantuminformatika kínálja. Már most léteznek olyan megoldások, amelyek segítségével kvantum módon oszthatunk szét kulcsokat, azonban az optikai kábeleket használó megoldások csak korlátozott távolságban működnek. A kisebb veszteségek miatt érdemes a kvantum-alapú kulcsszétosztást műholdak segítségével megvalósítani. Mivel ezekben az alkalmazásokban a kvantumbiteket fotonok segítségével továbbítjuk, ezért pontosan ismernünk kell a légkör optikai tulajdonságait. Cikkünkben bemutatjuk az űr-Föld és űr-űr csatornák néhány érdekes fizikai tulajdonságát, és megmutatjuk, hogyan tudunk ezeken a csatornákon kvantum módon kommunikálni.**

## 1. Bevezetés

Gordon Moore, az Intel egyik alapítója publikálta 1965-ben egy megfigyelését, miszerint egy integrált áramkörben költséghatékonyan elhelyezhető tranzisztorok száma nagyjából kétévente megduplázódik [1]. Az azóta Moore-törvényként ismertté vált összefüggés a mai napig pontosnak bizonyult, és ezzel egyidejűleg folyamatos méretcsökkenést is megfigyelhetünk az integrált áramkörök világában. Mindez azt jelenti, hogy ha a trend folytatódik, akkor előbb vagy utóbb eljutunk arra a pontra, amikor a jelenlegi technológiával nem tudunk több tranzisztort elhelyezni egyetlenegy lapkára. Ekkor már nem lesznek érvényesek a klasszikus fizikában létező Ebers-Moll-egyenletek, hanem helyettük kvantummechanikai modelleket kell használnunk. (A kvantuminformatikán kívül más megoldások is lehetségesek, például az elosztott rendszerek vagy a DNS-alapú számítások, de cikkünkben a kvantuminformatikai alkalmazásokkal foglalkozunk.) Ez jelentős működésbeli különbségeket fog jelenteni a mostani számítógépekhez képest. Ennek a hangsúlyozására az így tárolt biteket kvantumbiteknek (vagy röviden qbitnek) szokás nevezni, az ezekkel operáló számítógépeket kvantumszámítógépeknek, általánosságban pedig a kvantummechanikán alapuló információtárolást, feldolgozást és továbbítást összefoglaló néven kvantuminformatikának hívjuk.

Ahhoz, hogy kvantumszinten tároljunk digitális információt, olyan kvantummechanikai objektumokra van szükségünk, melyek legalább két, mérésekkel jól megkülönböztethető állapottal rendelkeznek. Ilyen lehet például az elektronok vagy atommagok spinje (perdülete), fotonok függőleges vagy vízszintes polarizációja, esetleg többletelektronok jelenléte vagy hiánya nanopötytyökön (vagyis igen kisméretű, legfeljebb néhány ezer atomból álló kristályokon).

Mivel nyújtanak többet a kvantum-alapú eszközök, mint a klasszikus informatika által kínált lehetőségek? A kvantumpárhuzamosság elvének kihasználásával nagy számításigényű műveleteket is könnyen el tudunk végezni (Deutsch-Jozsa-algoritmus), kvantum-alapú prímfaktorizációt is megvalósíthatunk (pl. a Shor-algoritmus segítségével) [2]. A klasszikus módszereknél hatékonyabban tudunk adatbázisban keresni (Grover-algoritmus), különböző kvantumkapukat és kvantumáramköröket építhetünk, szupersűrű kódolást alkalmazhatunk, sőt még kvantum-alapú Fourier-transzformációt is tudunk végezni [3]. A kvantum-kulcsszétosztás protokolljai (BB84, B92) révén biztonságos módon tudunk kulcsot szétosztani [4], az összefonódás jelensége miatt pedig képesek vagyunk információt teleportálni (kvantum teleportáció) [5].

## 2. Kvantumbit és kvantumalgoritmusok

Ebben a szakaszban a kvantuminformatika alapvető posztulátumai mellett a kriptográfiával való kapcsolatát és gyakorlati megvalósításának problémáit mutatjuk be.

### 2.1. A kvantuminformatika alapjai

A kvantuminformatika alapjait négy posztulátum definiálja [3]. Jelen cikkünkben nem szeretnénk mély matematikai részletekbe bocsátkozni, ezért szövegesen bemutatjuk ezt a négy posztulátumot, az érdeklődők pedig a [2,3] irodalomban megtalálhatják a konkrét matematikai leírásokat.

Az *első posztulátum* az állapotleírásról szól és abban nyújt segítséget, hogyan tudunk leírni egy kvantumvilágbeli állapotot. A *második posztulátum* a rendszer időbeli fejlődésére vonatkozik és abban segít, hogy zárt transz-

formációkkal le tudjuk írni a teljes rendszer viselkedését. A *harmadik posztulátum* teszi lehetővé a kapcsolatot a kvantum- és a klasszikus világ között a mérés segítségével. Maga a posztulátum két érdekességet is állít: egyrészt a mérés csak valószínűségi alapon jósolható véletlenszerű esemény, másrészt a mérés elvégzése hatással van magára a rendszerre. Ha van egy bizonytalan állapotban lévő bitünk (mondjuk 75% eséllyel mérünk 1-t, 25% eséllyel 0-t), azt megmérjük, és 1-es állapotot mérünk, akkor a kvantumbit onnantól kezdve 100%-osan az 1-s állapotban lesz. A *negyedik posztulátum* az összetett rendszerekről szól.

A kvantuminformatikában több dimenziós kvantumbiteket is tudunk definiálni. Egy kétdimenziós kvantumbitet az alábbi módon írhatunk le:

$$|Q\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (1)$$

Ez azt jelenti, hogy a $|Q\rangle$ kvantumbitünk értéke nem más, mint az $\alpha|0\rangle$ (annak a valószínűsége, hogy 0 az érték) és a $\beta|1\rangle$ (annak a valószínűsége, hogy 1 az érték) az összege. (Az $\alpha$ és $\beta$ értékeket valószínűségi amplitúdóknak nevezzük.)

### 2.2. A kvantummechanika és a kriptográfia

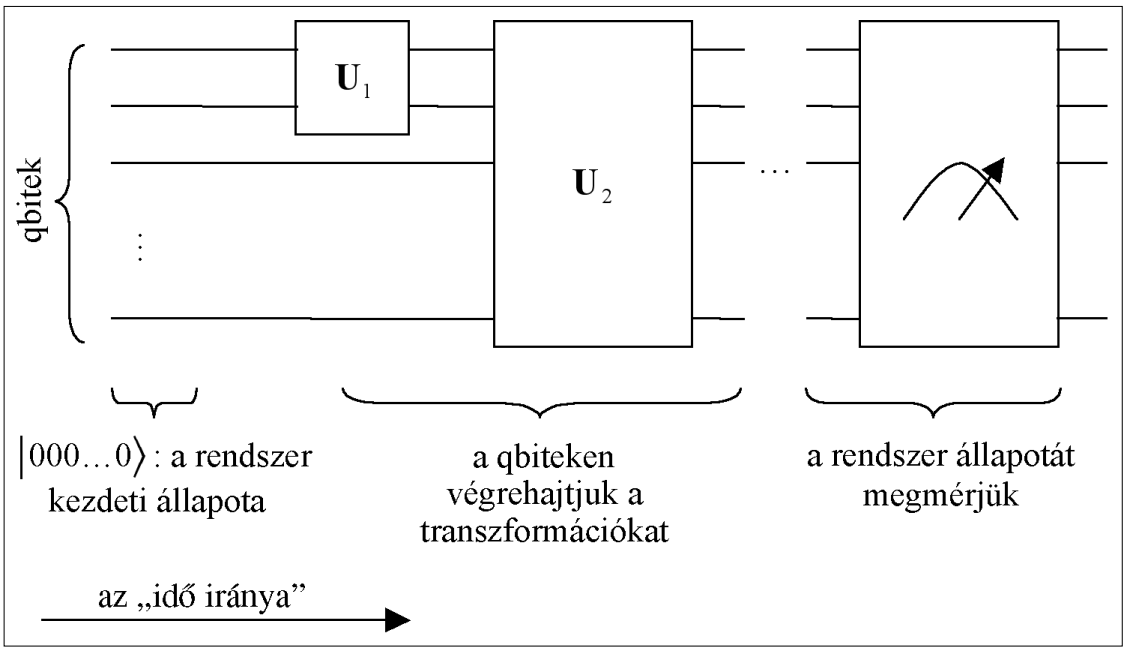
A kvantummechanika alapvető axiómái tulajdonképpen a kriptográfiához illeszkednek a legtermészetesebben. A biztonságos one-time pad tökéletes véletlenszámokat kíván, viszont a legelterjedtebb klasszikus módszerek csak ál-véletlenszámokat állítanak elő. Ezzel szemben a kvantummechanikai folyamatok valódi véletlenszámokat eredményeznek, olyannyira, hogy a jelenlegi ismereteink szerint nincsenek olyan rejtett paraméterek, amik előre meghatároznák egy kísérlet kimenetelét. Például egy kockadobás klasszikus véletlenszám-generálási algoritmusként fogható fel, azonban ebben az esetben vannak olyan rejtett paraméterek, mint a kocka sebessége, a dobás iránya, a kocka kezdeti helyzete, a súrlódás a kocka és az asztallap között stb., melyek a newtoni mechanika értelmében egyértelműen meghatározzák a végeredményt. A kockadobás eredményét mégis véletlenszerűnek tekinthetjük, mivel a rejtett paraméterek száma nagy, értékük nem ismert és a végeredmény ezeknek a paramétereknek a kis megváltozására is érzékeny lehet. A kvantummechanikában azonban ilyen rejtett paraméterek a Bell-tétel értelmében [3] nincsenek.

A másik, kriptográfia számára nagyon hasznos elve a kvantuminformatikának a No-Cloning tétel [3], mely azt mondja ki, hogy egy tetszőleges kvantumállapotról (speciális esetektől eltekintve) nem készíthető másolat. Ez rendkívül hasznos tulajdonság, hiszen ha ezt ügyesen kihasználjuk, biztosíthatjuk, hogy egy kvantumcsatornán folyó kommunikációba egy harmadik, illetéktelen fél – nevezzük Eve-nek – nem tud belehallgatni anélkül, hogy fel ne fedné a jelenlétét.

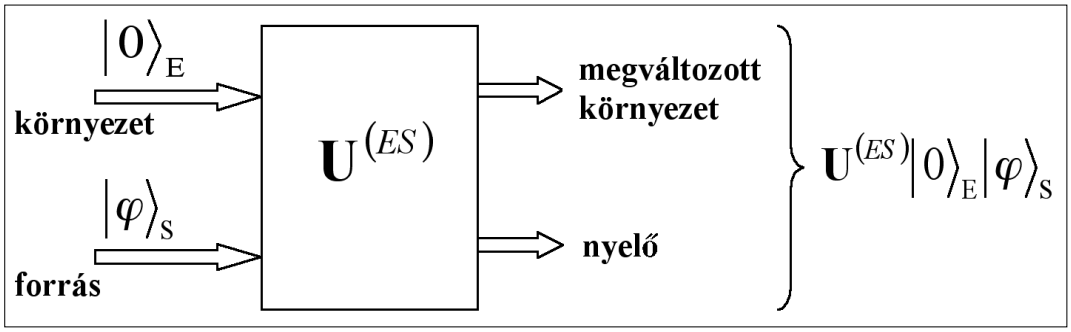
A harmadik fontos dolog, ami a kriptográfia szemszögéből előnyös, hogy a mérés befolyásolja az állapotot, ennek következtében pedig vannak olyan információk, amikhez egyidejűleg nem lehet hozzáférni. Ez azt jelenti, hogy ha azt használjuk a dekódoláshoz szükséges kulcsnak, hogy egy *n* db qbitből álló sorozat *i*-edik elemén egymással nem felcserélhető mérések közül melyiket kell végrehajtani, akkor biztosíthatjuk, hogy csak egyetlenegyszer legyen lehetőség a dekódolásra. Hibás dekódolási kísérlet után minden további kísérlet eleve kudarcra ítéltetett, hiszen az eredeti információt a mérés „felülírta”, így nem lehet az összes lehetséges kulcsot végigpróbálgatva feltörni a kódszót.

### 2.3. Problémák

Annak ellenére, hogy a kvantumszámítógépek teljesítőképessége bizonyos területeken messze meghaladja klasszikus társaikét, a gyakorlati alkalmazás még mindig gyerekcipőben jár. Ennek egyik oka, hogy meg kell találni a kényes egyensúlyt a manipulálhatóság és a környezeti hatásokkal szemben tanúsított ellenálló-




*1. ábra*
*Egy általános kvantumáramkör felépítése*




*2. ábra*
*A kvantumcsatorna vázlatos felépítése. A csatornában megjelenő zaj részben a környezettel történő összefonódás eredménye.*

képesség között. Egyrészt az algoritmusok működéséhez elengedhetetlen, hogy a qbiteket könnyű legyen egymással összefonni (vagyis könnyű legyen Bell-állapotokat vagy kettőnél több bitből álló, erősen korrelált qbit csoportokat létrehozni), másrészt a környezettel szemben a qbitek „robusztusak" kell, hogy legyenek, hogy a külső hatások ne zavarják a kvantumáramkörök működőképességét. Egy általános kvantumáramkör felépítése az *1. ábrán* látható.

Általánosságban elmondható tehát, hogy már létező qbitek összefonása és ezzel együtt a *CNOT* egy nehezen végrehajtható művelet. A legtöbb jelenleg létező kvantumszámítógép kevesebb, mint 20 qbitet tud kezelni és úgy tűnik, hogy további qubitek hozzáadása a bitek számának növelésével egyre nagyobb nehézségekkel jár. A rekordot jelenleg a D-wave cég tartja, akik szupravezető gyűrűkben tárolt fluxuskvantumokat használnak bitekként, és állításuk szerint 2008 decemberében egy 128 bites kvantumchipet hoztak létre.

A gyakorlati problémák mellett vannak elméleti nehézségek is, például a tény, hogy egy általános kvantumbitet nem lehet másolni, hasznos lehet a kriptogáfiában, viszont megnehezíti a kvantumszámítógépek hétköznapi alkalmazását.

## 3. Szabadtéri kvantumcsatorna

Ha kommunikációról beszélünk, akkor szükségünk van a kommunikáció lefolyását biztosító közvetítő közegre, azaz egy kommunikációs csatornára. Ez létezik a kvantumvilágban is.

A *2. ábrán* a kvantumcsatorna általános felépítését mutatjuk be. A $|\varphi\rangle_S$ forrásból érkező információk a nyelőn keresztül fognak távozni a csatornából. A $|0\rangle_E$ környezet is a csatorna bemeneti változója. A csatornát egy $\mathbf{U}^{(ES)}$ unitér transzformáció szimbolizálja. A csatorna hatása képpen a környezet is megváltozik, ezért mondható el, hogy a kimenet $\mathbf{U}^{(ES)}|\varphi\rangle_S|0\rangle_E$. A gyakorlatban azonban nem ismerjük sem a környezet kvantumállapotát, sem az $\mathbf{U}^{(ES)}$ transzformációt, így e helyett a megközelítés helyett kénytelenek vagyunk a légköri és műholdas kommunikáció félempirikus modelljeire támaszkodni és a klasszikus egyenletek felől közelíteni, melyek megoldása végső soron nem más, mint a kvantumos viselkedés mérés utáni statisztikája.

Az optikai kábelek kiváló lehetőséget nyújtanak a rövid távú kommunikációra, például egy városon belül a különböző bankfiókok vagy szomszédos városok esetén a nagy biztonságot igénylő polgári vállalkozások, esetleg katonai létesítmények között. Erre már több cég szakosodott, például az id Quanticque Genfben, a MagiQ Technologies New Yorkban, a Smart Quantum Franciaországban és a Quintessence Labs Ausztráliában, azóta pedig, hogy a svájci választások eredményét 2007-ben ilyen csatornán továbbították [6], széles körben elfogadott, hogy a módszer hatékony és biztonságos.

A műholdas kommunikáció során hatalmas információigény lép fel, ezért érdemes megvizsgálni, hogyan tudnánk használni a kvantumalgoritmusokat ezekben a kommunikációs folyamatokban. Az optikai kábelen megvalósított alkalmazásoktól eltérően ezekben az esetekben egy szabadtéri csatornára van szükség, amelyen keresztül áramlanak az adatok. Ezt a szabadtéri kvantumcsatornát számos fizikai tényező befolyásolja.

Az első szabadtéri kvantumkulcs-szétosztással 1991-ben találkozhattunk, ekkor sikerült ezt először egy 30 cm-es szakaszon megvalósítani [7]. A következő években folyamatos fejlődést figyelhettünk meg, elérték a 250 méteres távolságot laboratóriumon belül [8], valamint a 90 méteres távot laboratóriumon kívül [9]. 1998-ban a Los Alamos National Laboratory 950 méteres távolsággal végzett sikeres kísérletet [10]. A hibaarány (BER) 1,5%-os volt, ez a felhasznált optikai elemek (szűrők, cellák) tökéletlenségére vezethető vissza. Az elvégzett kísérletben Alice (a küldő fél) egy lézerdióda segítségével fényimpulzust küld Bobnak (fogadó fél). Mindegyik impulzus szabadtéri és egy interferenciaszűrőn megy keresztül. 2004 januárjában ugyanezen kutatócsoport már 9,81 km-es távolságban végzett sikeres kísérletről számolt be [11]. A kísérlethez 772 nm-es hullámhosszú fényt használtak és az eddigiektől eltérően nemcsak éjszaka, hanem nappali és szürkületi időpontokban is végrehajtották a teszteket. Ez azért érdekes, mert a külső fényből származó háttérzaj intenzitása a napszaknak megfelelően változik.

2006-ban egy nemzetközi kutatócsoport 144 km-es távolságon valósította meg mindezt [12]. Ez azért jelentős eredmény, mert a légkör lézeres kommunikáció szempontjából számottevő rétege csupán 20-25 km vastag, a világűrben pedig a veszteségek jóval kisebbek, így lehetőség nyílt Föld-űr, illetve űr-űr kvantumkommunikációra is. 2008-ban az Európai Űrügynökség (ESA) a következő öt év egyik legfontosabb áttörésének jelölte meg a kvantum-alapú űrkommunikáció sikeres gyakorlati megvalósítását. Az ESA terveiben szerepel többek

között a kulcsnövesztés megvalósítása műhold-Föld és műhold-műhold csatornán, illetve szupersűrű kódolás használata műholdas kommunikációban és mélyűr-missziók során [13].

## 4. A kvantuminformatika használata az űrtávközlésben

### 4.1. Műholdas kommunikáció

A műholdas kommunikáció azért érdekes számunkra, mert az űrben a veszteségek sokkal kisebbek, mint akár a legjobb minőségű optikai kábelben, így remélhetőleg nagyobb távolságban lehet megvalósítani ugyanazokat a protokollokat, amiket a földön már sikerrel kipróbáltak. A jelenleg létező technológiákra építő számításaink segítségével megvizsgáltuk ezeknek az elképzeléseknek a megvalósíthatóságát és teljesítőképességét.

Az általunk felállított egyik modell szerint a szabad légköri kvantumkommunikációt négy különböző (de egymásra épülő) lépésben érdemes alkalmazni [14]:

*1. Nyílt légköri*

Ez egyszerű szabadtéri kapcsolattartás, 100 km-nél kisebb távolságok jellemzik. A kvantumkommunikáció segítségével titkosítást valósíthatunk meg, valamint a BER csökkentésére szolgáló algoritmusokat használhatunk.

*2. Alacsony pályás műholdas kommunikáció*

300 és 800 km közötti távolság jellemzi ezt a csoportot, a jelek kódolására és dekódolására tudjuk felhasználni a kvantuminformatikán alapuló algoritmusokat. A kvantum hibajavítás algoritmusaival tudjuk csökkenteni a BER-t.

*3. Műholdas műsorszórás*

A jelenlegi műholdas műsorszóró rendszerek a geostacionárius pályán keringenek, 36 000 km magasan [15]. A műholdas műsorszórásra is elmondható, hogy nagy mennyiségű adatot kell eljuttatnunk viszonylag kis sávszélességgel. A kvantuminformatikai algoritmusok segítségével hatékonyabb effektív sávszélességet érhetünk el, mint jelenleg.

*4. Műhold-műhold kommunikáció*

A műholdak közötti kvantumkommunikáció azért lehet a közeljövőben jelentős, mert a légkör zavaró hatásai ebben a kommunikációban nem érvényesülnek.

Mostani cikkünkben azt vizsgáljuk, hogyan tudjuk modellezni az űr-Föld és űr-űr kommunikációs kapcsolatok kvantumcsatornáit.

### 4.2. Bitráták és hibaráták kvantumkommunikáció esetén

Nagy távolságokon zajló kvantumkommunikáció esetén a fotonok bizonyultak legpraktikusabbnak az információ hordozására. Optikai kábelekben a fotonok fázisában szokták a kvantumbitek *0-1* értékét kódolni, szabadtéri kommunikációban viszont inkább a polarizációt használják [16]. Az utóbbi esetben fontos kérdés, hogy mekkora depolarizációval kell számolnunk a kommunikáció során, hiszen részben ez lesz felelős a kialakuló hibákért. Szintén kulcsfontosságú ismerni a csatorna veszteségeit, vagyis azt, hogy az adó oldalán – a továbbiakban Aliz oldalán – útjára indított fotonok hány százaléka érkezik meg a vevő – a továbbiakban Bob – detektorához.

Az egyik legegyszerűbben megvalósítható és manapság leginkább elterjedt kvantumkriptográfiai algoritmus az úgynevezett BB84 protokoll. Ennek egyik különlegessége, hogy hagyományos értelemben lehallgathatatlan, ugyanis ha egy harmadik nemkívánatos személy – a továbbiakban Eve – méréseket végez a csatornában, ezzel akaratlanul is olyan hibákat okoz a kvantumkommunikáció folyamatában, amelyek Aliz és Bob számára felismerhetőek, így azonnal észlelhető Eve jelenléte. Éppen ezért fontos ismerni a csatorna veszteségeit és torzító hatását, hiszen ha ez meghalad egy bizonyos értéket, már nem tudjuk eldönteni, hogy a lehallgatás által okozott hibákat, vagy a csatorna természetes zaját látjuk és így azt sem tudjuk eldönteni, hogy a csatorna biztonságos-e.

A csatornában keletkező hibák mennyiségének méréséhez fontos segédfogalom a kvantumbithiba-ráta (QBER – *Quantum Bit Error Rate*), ami a hibás bitek arányát adja meg a csatornán átküldött összes bithez viszonyítva [16]. Ennek kiszámításához számos paramétert ismerni kell, ezek közé tartozik a csatorna $t$ transzmittanciája (vagyis annak fényáteresztő képessége), a detektálás $\mu$ hatásfoka, az egyfoton forrás elsütésének $f$ frekvenciája és $\eta$ átlagos fotonszáma, a detektorok $n$ száma, a zajból származó beütések $p_{dark}$ gyakorisága, illetve annak $p_{depol}$ valószínűsége, hogy egy foton rossz detektorba érkezik.

Mindezek alapján a QBER BB84-es protokoll esetén a következőképpen számolható ki [16]:

$$QBER = \frac{N_{Hibás}}{N_{Összes}} = p_{pol} + \frac{p_{dark} \cdot n}{t_{link} \cdot \eta \cdot 2 \cdot \mu} \qquad (2)$$

Elméleti úton megmutatták, hogy amennyiben a QBER meghaladja a 11%-ot, a kommunikáció nem biztonságos [16]. Ez egyúttal korlátot jelent arra is, hogy milyen távolságban lehet a BB84-es protokollt használni, ugyanis az optikai út növekedésével nő a veszteség, ami adott zaj- illetve fotonforrás és detektorhatásfok mellett korlátot jelent az áthidalható távolságra.

BB84 segítségével egy titkos kulcs kialakításának bitrátája szintén függvénye a transzmittanciának és ezzel a kábel hosszának, pontos értéke a következőképpen számolható ki [16]:

$$\mathrm{R} = \frac{1}{2} \cdot f_{pulz} \cdot t_{link} \cdot \eta \cdot \mu \qquad (3)$$

ahol $f_{pulz}$ Aliz oldalán a lézer elsütés frekvenciája.

## 5. Űr-Föld és űr-űr kapcsolat modellezése

### 5.1. Veszteségek

Az űr-űr kommunikációs csatorna esetén Aliz és Bob szerepét is egy-egy műhold játssza. Ebben az esetben eltekinthetünk a légkör hatásától, azonban így is számolnunk kell veszteségekkel. Az egyik tényező, amit fi-

gyelembe kell vennünk, a célzás hibája. Ez a két műhold közötti távolság és a detektor átmérőjének függvényében okozhat veszteségeket, hiszen előfordulhat, hogy a foton elhalad a detektor mellett. A célzás hibája általános esetben egy kétdimenziós Gauss-eloszlással modellezhető, néhány mikroradián nagyságrendjébe eső szórással [17].

A másik lehetséges veszteségforrás a fotonok detektálási valószínűségének térbeli különbségeiből származik. Ennek nagyságára Gauss-eloszlású nyalábok vizsgálatából következtethetünk (ugyanis a fény intenzitása és a fotonok detektálásának valószínűsége egymásnak megfeleltethető fogalmak), melyek terjedése az irodalomból ismert [18].

A két hiba hatását együttesen kell kezelni, így kaphatjuk meg azoknak a fotonoknak az arányát, melyek nem jutnak el a detektorhoz.

A modell teljességének érdekében olyan veszteségeket is figyelembe kell venni, melyek nem képezik ugyan a szigorú értelemben vett csatorna részét, de mégis befolyásolják a fotonok detektálásának hatásfokát.

Aliz oldalán veszteségeket jelent a fotonforrások tökéletlensége. Bob oldalán a legnagyobb veszteséget maga a detektor adja. A legpraktikusabb egy-foton detektorok a szilícium alapú lavina fotodiódák, melyek detektálási hatásfoka elérheti a 70%-ot [16].

Légkörben folytatott kommunikáció esetén egyéb veszteségekkel is számolhatunk. Elsőként figyelembe kell vennünk, hogy a légkör elnyelheti és szórhatja fényt. Ebben az esetben kétféle veszteségforrást különböztethetünk meg: az egyik a molekuláris veszteség, mely a fény és a légkör gázainak kölcsönhatásából adódik, a másik az aeroszolok, vagyis a levegőben lebegő szilárd szemcsék és folyadékcseppek hatása (a felhőket és ködöt az aeroszolokhoz sorolhatjuk). Általánosságban elmondható, hogy az aeroszolok hatása nagyobb szokott lenni, mint a molekuláris nyalábgyengítés (előbbi az időjárástól függően a fotonoknak akár 15-45%-át is elnyelheti, utóbbi jól megválasztott hullámhossz esetén a fotonoknak kevesebb, mint 5%-át nyeli el).

Második közelítésben az optikai turbulenciákat is figyelembe kell vennünk. A levegő fénytörése hőmérséklettől függő jelenség, így a különböző hőmérsékletű légrétegek keveredése a törésmutató térbeli és időbeli ingadozása miatt megváltoztathatja a fotonok útját. Mivel a légkörben turbulens szélesedéssel kell számolnunk, ami nagyobb, mit a világűrben tapasztalható diffrakciós szélesedés, ezért a Föld-műhold és műhold-Föld csatorna vesztesége alapvetően különbözik egymástól, hiszen földi adóállomás esetén rögtön az optikai út elején a lehető legnagyobb szélesedést szenvedi el a nyaláb (ami felfogható az egyes fotonoknak a nyaláb középpontjától való szögeltéréseként is), így hosszú út megtétele után a kezdeti hiba egyre nagyobbá válik. Ellenkező esetben, amikor a műhold játssza az adó, és a földi adóállomás a vevő szerepét, több száz vagy akár több ezer kilométeren keresztül csak a diffrakciós nyalábszélesedés hat a lézersugárra, és csak az utolsó 20-30 km-es szakaszon kezdődik meg a turbulens nyalábszélesedés.

A turbulenciának ezenkívül egyéb torzító hatása is van, például a szcintilláció, vagyis pontszerű detektor esetén a befogott fényintenzitás ingadozása, amit a hétköznapi életből a csillagok pislákolásaként ismerhetünk, azonban műhold-Föld csatornánál 0,5 m-nél nagyobb detektorátmérő esetén ez a hatás elhanyagolható az úgynevezett apertúra-átlagolás miatt [18,19].

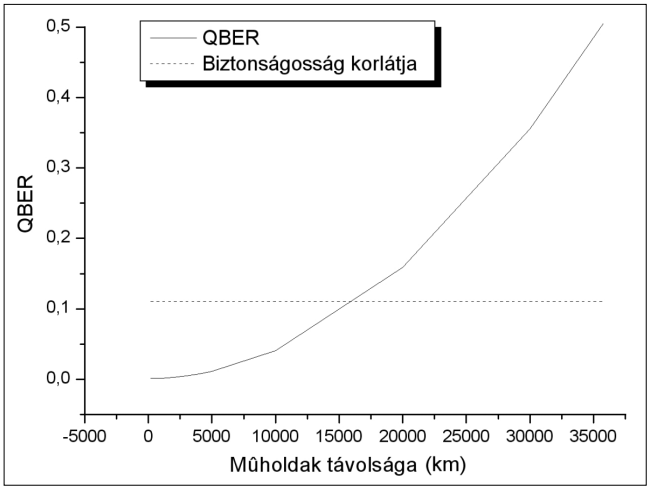
#### 5.2. Zaj és egyéb hibák

Léteznek egyéb hibák is, melyeket nem lehet a veszteségekhez sorolni, azonban a QBER kiszámításánál fontos szerephez jutnak. Az egyik ilyen hibaforrás lehet a zaj, ami két tényezőből tevődik össze. Az egyik a detektor úgynevezett sötétzaja, ami a teljes sötétségben regisztrált hibás beütések számát jelenti. Szilícium alapú lavina-fotodiódák esetén ez a hűtés függvényében változhat [16] (mivel a sötétzaj a termikus gerjesztésekből származik, ez a detektor hűtésével kompenzálható). A másik a háttérzaj, ami a nem Aliztól származó fotonok detektálását jelenti. Ez erősen függhet az időjárástól és napszaktól, műhold-Föld csatorna esetén elsősorban a légkörben és aeroszolokon szóródó napsugárzás, illetve éjszaka a csillagok és a hold fénye okozzák. Ez első ránézésre lehetetlenné teszi a kommunikációt, valójában azonban kellő mértékben le lehet szorítani a zajt erős sávszűrőkkel (melyek néhány nanométeres hullámhossz tartományban eresztenek át fotonokat), illetve rövid detektálási időablak használatával (ami *10 ns* vagy rövidebb).

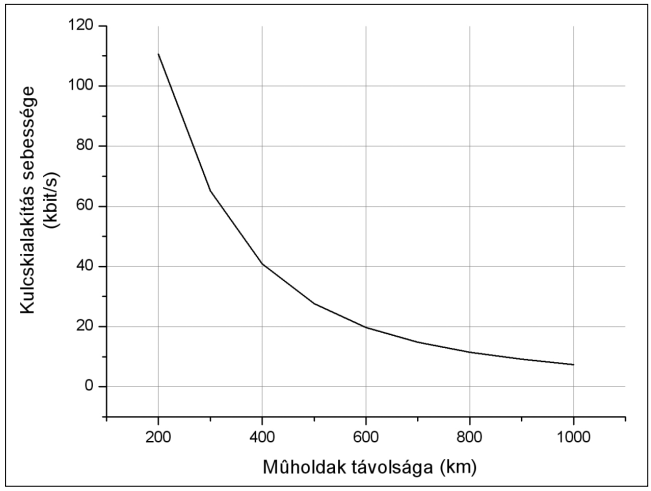
A másik lehetséges hibaforrás a polarizációmérés hibája, vagyis egy olyan helyzet, amikor Aliz fotonja megérkezik Bob detektorához, azonban a polarizációmérés hibás eredményt ad. Ennek több oka lehet: egyrészt a foton polarizációja a csatornában megváltozhat a Faraday-effektus, optikai turbulencia vagy kisszögű szórás miatt [20], másrészt a nyaláb pozícionálásához használt tükör (illetve a detektortükör) mozgása okozhat depolarizációt a fény beesési szögének változása miatt. Ennek hatása a kommunikációra csökkenthető eltérő hullámhosszú referencialézerek használatával, így a depolarizációból adódó hibák arányát kisebbé lehet tenni 1%-nál.

#### 5.3. Eredmények különféle csatornák esetén

Az első kérdés, amire kereshetjük a választ, hogy két műhold mennyire távolodhat el egymástól ahhoz, hogy a BB84 protokoll segítségével még biztonságos kommunikációt tudjanak folytatni. Ennek a kérdésnek a megválaszolásához ismerni kell a kvantumhiba rátát a távolság függvényeként. Tegyük fel, hogy Aliz műholdjának apertúra-átmérője 20 cm, és a célzás hibája 1 μrad. Bob műholdján a detektortükör átmérője legyen 1 méter, a kommunikációt folytassuk 800 nm-es hullámhosszon (ugyanazon a hullámhosszon, ahol az eddigi legsikeresebb Föld-Föld kísérletet végrehajtották [12]). A detektor hatásfoka legyen 0,7, vagyis 70%, Aliz oldalán pedig a nyalábgyengítési tényező legyen 0,1. A zajból adódó beütések száma legyen átlagosan $5 \times 10^{-7}$ egy 10 ns-os detektálási időablakban.




*3. ábra*
*A kvantumbithiba-ráta űr-űr csatorna esetén a két műhold távolságának függvényében.*
*A biztonságos kulcskialakítás 0,11-nél nagyobb QBER esetében nem lehetséges, így az adott paraméterek mellett legfeljebb 15 000 km hidalható át.*




*4. ábra*
*A kulcskialakítás sebessége űr-űr csatorna esetén, a műholdak távolságának függvényében. Látható, hogy, a távolság függvényében a kulcskialakítás bitrátája rendkívül gyorsan csökken.*

Ezzel a (2) képlet szerint számolt eredményeink az *3. ábrán* láthatóak.

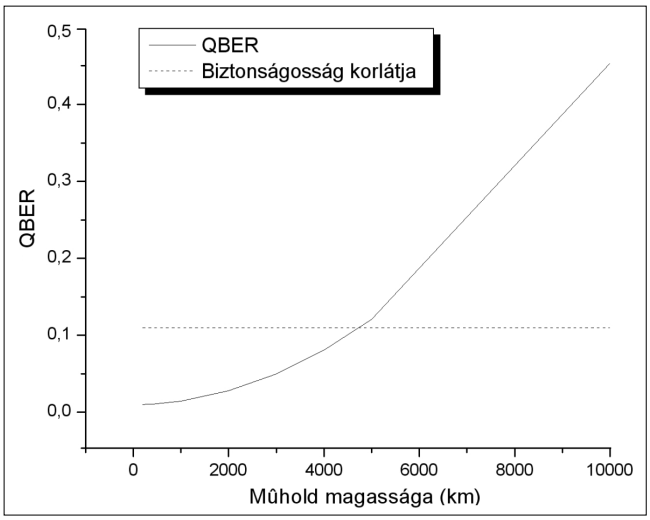
A biztonságos kommunikáció korlátja tehát nagyjából 15 000 km, a két műhold maximum ennyire távolodhat el egymástól. Műholdas kvantumkommunikációval akár interkontinentális távolságokat is át lehet hidalni, azonban az alacsony (LEO műholdas) pályák és a geostacionárius GEO pályák közötti körülbelül 35 000 km-es távolság összehasonlításából látszik, hogy még egy alacsonyan keringő műhold sem képes elérni egy geostacionárius pályán mozgót. A második kérdés, amire választ várhatunk, hogy a műholdak milyen sebességgel képesek kulcsot kialakítani a BB843 protokoll segítségével a távolság függvényében. Tegyük fel, hogy Aliz oldalán a lézer elsütésének frekvenciája 1000 Hz és minden egyéb paraméter a fent leírtakkal egyezik meg.

A kulcskialakítás bitrátája a (3) képlet alapján számolható ki, eredményeink a *4. ábrán* láthatóak, melyen az is megfigyelhető, hogy a távolság függvényében a kulcskialakítás bitrátája rendkívül gyorsan csökken.

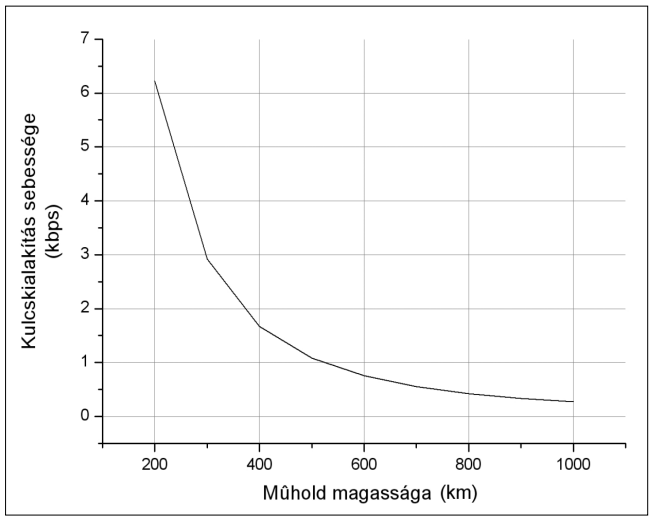
Ugyanezeket a kérdéseket feltehetjük Föld-műhold kommunikáció (uplink) esetén is. Tegyük fel, hogy Aliz műholdja 20°-os zenitszög alatt látszik, a légkör a fotonok 82,5%-át engedi át, ami mérsékelt égövön tiszta nyári időnek felel meg [21] és minden egyéb paraméter a korábbiakkal egyezik meg. Az optikai turbulenciák hatását is figyelembe véve a QBER értékeit az *5. ábrán* láthatjuk.

Az eredmények alapján megállapíthatjuk, hogy a 200-300 km felett kezdődő LEO pályák biztonságosan elérhetőek, azonban a geostacionárius pályák nem, ami a korábbi eredmények fényében nem meglepő. Ugyanebben az elrendezésben a kulcskialakítás sebessége a *6. ábrán* látható, amelyből egyértelmű, hogy az alacsonyabb műholdpályák sokkal előnyösebbek.

*5. ábra*
*Kvantumbithiba-ráta Föld-űr csatorna esetén, a műhold magasságának függvényében.*
*Az alacsony LEO műholdpályákat biztonságosan el lehet érni BB84 protokoll segítségével, a magasabb pályákat azonban (például a geostacionárius pályát) már nem.*




*6. ábra*
*Kulcskialakítás sebessége Föld-űr csatorna esetén a műhold magasságának függvényében.*



## 6. Összefoglalás

A Moore-törvény hatására történő méretcsökkenés problémái miatt új megoldásokat kell keresnünk. Az egyik kínálkozó megoldás a kvantummechanikán alapuló kvantumszámítógép. A kvantummechanika azonban arra kényszerít minket, hogy újraalkossuk az információról, az információfeldolgozásról és a számítási komplexitásról alkotott képünket.

Cikkünkben megvizsgáltuk a kvantumalapú műholdas kommunikáció gyakorlati megvalósításának bizonyos paramétereit. Úgy véljük, hogy ha a szabadtéri kvantumkulcscsere-kísérletek sikerrel járnak, ha megfelelően tudjuk szimulálni a szabadtéri kvantumcsatorna, a kvantuminformatikai algoritmusok és a műholdas kommunikáció kapcsolatát, valamint sikerül ezeket fizikailag is megvalósítani, akkor a műholdas kommunikáció történelmében ugyanolyan nagy váltást érhetünk el, mint amilyen az analóg technikáról digitális technikára történő átállás volt.

### A szerzőkről

**BACSÁRDI LÁSZLÓ** 1982-ben született Sopronban. 2006-ban okleveles mérnök-informatikus diplomát szerzett a Budapesti Műszaki és Gazdaságtudományi Egyetem Híradástechnikai Tanszékén. Jelenleg doktoranduszként vesz részt a tanszéken folyó oktatási és kutatási feladatokban. Kutatási területei közé a kvantumkommunikáción alapuló távközlés és az ad-hoc hálózatokban zajló információterjesztés tartoznak.

**GALAMBOS MÁTÉ** 1985-ben született Budapesten. Jelenleg a Budapesti Műszaki és Gazdaságtudományi Egyetem Természettudományi Karának mérnök-fizikus szakos hallgatója. Szakmai érdeklődési körébe tartozik a szén nanocsövek elektronikus szerkezetének ESR módszerrel történő vizsgálata és a műholdas kvantumkommunikáció modellezése.

**IMRE SÁNDOR** Budapesten született 1969-ben. A BME Villamosmérnöki és Informatikai Karán szerzett diplomát 1993-ban. 1996-ban Dr. Univ., 1999-ben PhD, 2007-ben MTA Doktora fokozatott szerzett. Jelenleg a BME Híradástechnikai Tanszékének vezetője, valamint a BME Mobil Innovációs Központjának tudományos kutatási igazgatója. Főbb kutatási területei a korszerű mobil infokommunikációs rendszerek rádiós és hálózati kérdései, valamint a kvantumalapú informatika.

### Irodalom

[1] Gordon E. Moore,
'Cramming More Components Into Electrical Circuits',
Electronics, Vol. 38, No. 8, 19 April 1956.

[2] S. Imre, B. Ferenc,
'Quantum Computing and Communications:
An Engineering Approach', Wiley, 2005.

[3] Michael A. Nielsen, Isaac L. Chuang,
'Quantum Computation and Quantum Information'
Cambridge University Press, 2000.

[4] Charles H. Benett, Gilles Bassard,
'Quantum Cryptography:
Public Key Distribution and Coin Tossing',
Int. Conf. on Computers, Systems & Signal Processing,
Bangalore, India, 10-12 December 1984.

[5] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa,
A. Peres, W.K. Wooters,
Teleporting an Unknown Quantum State via dual
Classical and Einstein-Podolsky-Rosen Channels,
Phys. Rev. Lett., Vol. 70, No. 13, pp.1895., March 1993.

[6] Paul Marks,
Quantum cryptography to protect Swiss election,
New Scientist,
www.newscientist.com (elérhető: 2010. március 3.).

[7] C.H. Bennett et al.,
Lecture Notes In Computer Science 473, 253 (1991).

[8] W.T. Buttler et al.,
Phys. Rev. A 57, pp.2379-2382., 1998.

[9] B.C. Jacobs, J.D. Franson,
Opt. Lett. 21, pp.1854-1856., 1996.

[10] W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux,
G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson,
and C.M. Simmons,
Practical free-space quantum key distribution over 1 km,
(arXiv:quant-ph/9805071).

[11] Richard J. Hughes, Jane E. Nordholt, Derek Derkacs
and Charles G. Peterson,
Practical free-space quantum key distribution over 10 km
in daylight and at night,
New Journal of Physics 4 (2002) 43., pp.1-43.

[12] Tobias S-Manderbach et al.,
'Experimetal Demostration of Free-Space Decoy-State
Quantum Key Distribution over 144 km',
Phys. Rev. Lett. 98, 010504, 2007.

[13] Josep Maria Predigues Armengol et al.,
'Quantum Communications at ESA:
Towards a space experiment on the ISS',
Acta Astronautica 63, pp.165-178., 2008.

[14] L. Bacsardi,
Satellite Communication Over Quantum Channel,
Acta Astronautica 61:(1-6) pp.151-159., 2007.

[15] Dr. Gschwindt András,
Műholdas műsorszórás,
Műszaki Könyvkiadó, Budapest, 1997.

[16] Nicolas Gisin et al.,
'Quantum Cryptography',
Reviews of Modern Physics, 1 February 2008.

[17] Stephen G. Lambert, William L. Casey,
'Laser Communications in Space', Artech House, 1995.

[18] Ronald F. Lante,
'Electromagnetic Beam Propagation inTurbulent Media',
Proc. IEEE, Vol. 63, No. 12, December 1975.

[19] Larry C. Andrews, Ronald L. Phillips,
'Laser Beam Propagation through Random Media',
SPIE Press Book, 2005.

[20] C. Bonato et al.,
'Polarization transformation induced on qubits
in a Space-to-Earth quantum communication link',
Quantum Electronics and Laser Science Conf., 2007.

[21] Walter G. Discoll,
'Handbook of Optics', McGraw-Hill, 1978.