

Kvantum alapú kommunikáció műholdas csatornában

Galambos Máté¹, Kiss András², Bacsárdi László^{2,1}

¹ Budapesti Műszaki és Gazdaságtudományi Egyetem, Híradástechnikai Tanszék

² Nyugat-magyarországi Egyetem, Informatikai és Gazdasági Intézet

Az űrkorszak hajnalán rádiójeleket használtak a műholdas kommunikációban, és napjainkban is ez az elterjedtebb technológia. Ugyanakkor egyre több helyen találkozhatunk a lézer alapú kommunikációval is, a lézerimpulzusok segítségével pedig a megszokott információ mellett kvantum biteket is átvihetünk. A következő fejezetben ismertetjük a műholdas kvantumcsatorna legfontosabb tulajdonságait, és bemutatjuk az általunk készített szimulációs programot.

A lézerkommunikáció tulajdonságai és előnyei

Napjainkban űrtávközlési célok megvalósításához többnyire rádiókommunikációt alkalmaznak. A lézer alapú kommunikáció kevesebb mint 20 éve jelent meg, de több szempontból is előnyösebb technológiát jelenthet a hagyományos rádióhullámokkal történő megvalósításokkal szemben. Az első sikeres mélyűri lézerkommunikációs kapcsolat létesítése 1992-re tehető, amelynek keretében a Földtől 6 millió kilométerre lévő Galileo-űrszonda képes volt érzékelni a küldött lézernyalábot. Itt egy egyirányú csatornáról volt szó, az űrszonda csak fogadó szerepet töltött be [1]. A kommunikációs csatorna hosszával felállított rekordot 2006-ban sikerült megjavítani [2]. A 24 millió kilométerre lévő MESSENGER űrszondával létesített Föld-űr illetve űr-Föld kapcsolat során az űrszonda érzékelte a küldött lézernyalábot, amelyre válaszolt a földi állomásnak.

A lézeres kommunikáció legnagyobb előnye a mikrohullámúval szemben, hogy az időegységenkénti adatátvitel legalább tízszerese a hagyományos rádiós kapcsolatnak, de ez az arány akár az ezerszeres értéket is elérheti. Jelenleg a Föld-Mars kapcsolat adatátviteli sebessége kb. 128 kbps [3], a 2010-re tervezett Föld-Mars lézerkommunikációs kapcsolat 1–30 Mbps adatátviteli sebességgel működött volna, a két bolygó közötti távolságtól függően. A projekt végül gazdasági problémák miatt nem valósult meg [4].

A lézerkommunikáció legnagyobb nehézsége, hogy a küldött nagyon precízen kell pozicionálni a fogadó felé, főleg ha több millió kilométeres csatornahosszról van szó. Ugyanakkor ez a tulajdonság lehetővé teszi, hogy a lézereket igen pontos távolságmérésre használjuk.

Azt, hogy mennyire befolyásolják a Föld-űr vagy űr-Föld csatornában a Föld légkörének különböző hatásai a fogadó által észlelhető jeleket, egy 2008-as kísérlet vizsgálta. Itt a német TerraSAR-X műhold és az amerikai NFIRE műhold között valósult meg a hibátlan adatátvitel, több mint 5000 kilométeres csatornahosszon. A csatorna sáv szélessége közel százszorosa (!) volt a hagyományos rádiós összeköttetés sáv szélességének, ami nagyjából 4 Gbps sebességet jelent [5].

A fentiek kísérleti eredmények voltak, amelyek azt támasztják alá, hogy a lézeres kommunikációt érdemes a nagy távolságok áthidalásában felhasználni. Azonban ha a jeleket annyira legyengítjük, hogy csak egy-két fotont tartalmazzon minden egyes lézerimpulzus, akkor a kommunikációnak egészen újfajta tulajdonságai lesznek, adott esetben olyanok is, amiket a hagyományos, klasszikus módszerekkel nem lehet megvalósítani. Az ilyen kommunikációt *kvantumkommunikációnak* nevezzük [6], és a következőkben elsősorban erre koncentrálnunk alacsony Föld körüli (LEO) pályán keringő műholdakkal kialakított Föld-űr és űr-Föld csatornák esetén.

Kvantumkommunikáció

A kvantummechanikai posztulátumokon és összefüggéseken alapuló információ-tárolást és feldolgozást összefoglaló néven *kvantuminfomatikának* nevezzük [7]. Amerikában, Angliában, Ausztriában, Ausztráliában, Franciaországban, Németországban, Olaszországban és még sok más országban foglalkoznak kvantuminformatikai kutatással. Magyarországon többek között a Szegedi Tudományegyetemen, az MTA Szilárdtestfizikai és Optikai Kutatóintézetben és a Budapesti Műszaki és Gazdaságtudományi Egyetem több karán és tanszékén folyik ilyen irányú kutatás. A kvantuminformatika és az űrtávközlés kapcsolatának vizsgálatával, valamint redundanciamentes kvantumcsatorna elméleti leírásával a BME Híradástechnikai Tanszékén foglalkoznak [8] [9].

Habár David Deutsch már 1985-ben bemutatta a kvantumszámítógép elméleti tervét, és azóta jelentős előrelépéseket tettünk a megvalósítás felé, a mai napig nem sikerült még teljes egészében megépíteni. Azonban egy másik terület, a kvantumkommunikáció, vagyis a kvantumbiteken alapuló adatátvitel, ahol jóval egyszerűbb műveletekre van szükség, ugrásszerű fejlődést mutat. Az informatika új ágának alapkövéül szolgáló kvantumbitek (röviden qubit vagy qbit) megvalósításához itt elsősorban fotonokat használnak.

Optikai kábelekből a foton fázisát, szabadtéri kommunikációban inkább a foton polarizációját szokás a 0 és 1 bitértékek megjelenítésére felhasználni. Az úgynevezett „No Cloning” tétel értelmében ismeretlen tartalmú kvantuminformációt nem lehet lemásolni anélkül, hogy meg ne zavarjunkt [10], ami a kvantummechanikán alapuló titkosításban segíthet: mivel ezeket a zavarokat ki lehet mutatni, felismerhető, ha valaki megpróbálja lehallgatni a kvantumcsatornán küldött üzenetet.

A jelenlegi technológia mellett a kvantumcsatornán általában nem közvetlenül a titkosított üzenetet továbbítják, hanem egy véletlenszerű kulcsot, melyet „one-time pad”-nek szokás nevezni. A one-time pad [11], vagyis egyszer használatos titkosító kulcs segítségével a későbbiekben bármilyen üzenet titkosítható és dekódolható. Azokat a kvantumkriptográfiai eljárásokat, melyek célja ilyen kulcsok biztonságos továbbítása, kvantumkulcs-szétosztásnak szokás nevezni.

Az első szabadtéri kvantumkulcs-szétosztással 1991-ben találkozhattunk, ekkor sikerült ezt először egy 30 cm-es szakaszon megvalósítani [12]. 2006-ban egy nemzetközi kutatócsoport 144 km-es távolságon valósította meg mindezt [13]. 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 [14].

Kvantumcsatorna-modell a műholdas kommunikáció modellezésére

Mivel a kvantumkriptográfiai eljárásokat jelenleg fotonok segítségével valósítják meg, szükség van a légkör optikai tulajdonságainak pontos ismeretére. Megvizsgáltuk az irodalomban fellelhető, klasszikus fénysugarak gyengülésével kapcsolatos modelleket és ezeket átdolgoztuk úgy, hogy egyetlen, vagy néhány foton viselkedésének leírására alkalmassak legyenek, és így modellezhetővé váljon a kommunikáció folyamata.

A modellben figyelembe vettük a ma létező egyfoton források tulajdonságait és teljesítőképességét, a légkör gázai által okozott veszteségeket, illetve a por és pára járulékait. Megvizsgáltuk a légkör turbulenciáinak hatását a kvantumkommunikációra, számoltunk a detektorok véges méretével, és a diffrakcióból eredő fókuszálási hibákkal. Továbbá számoltunk a veszteségeken túl a légkör egyéb módosító hatásaival is, megvizsgáltuk a műholdas kommunikáció során a kapcsolat fenntartásakor jelentkező úgynevezett célzási hibákat. A

jelenleg létező detektorok jellemzőinek ismeretében a zajra vonatkozó számolásaink, és az irodalmi adatokon alapuló becsléseink alapján megvizsgáltuk a detektálás hatásfokát, végül pedig mindezek alapján számolásokat végeztünk arra vonatkozóan, hogy milyen paraméterek mellett valósítható meg egy ilyen kvantumcsatorna.

A szabadtéri kvantumcsatornák általában jól megőrzik a polarizációt, ugyanakkor az optikai veszteségek miatt a jel gyengülésére számíthatunk. Kvantumkommunikáció esetén, amikor a jel egyetlen fotonból áll, a gyengülést úgy kell érteni, hogy a küldött fotonoknak csak egy bizonyos százaléka érkezik meg a detektorba. Űr–űr kommunikáció esetén a veszteségeket a célzás hibája, és a diffrakcióból eredő hibák eredményezik. Föld–űr és űr–Föld csatornák során ehhez járulnak a légkör optikai turbulenciáiból, illetve a molekuláris és aeroszol szórásból és abszorpcióból adódó veszteségek.

Fontos megjegyezni, hogy mivel a légkör nem homogén közeg, a Föld–űr és űr–Föld csatornák tulajdonságai eltérnek egymástól. Ez azért van, mert földi adóállomás esetén a turbulenciák okozta kis szögeltérésekre az optikai út első szakaszán számíthatunk, ami nagyobb célzási hibát okoz, mint ha a műhold játssza az adóállomás szerepét. Ekkor ugyanez a szögeltérés az optikai út végső szakaszán következik be, és egyszerű trigonometriával belátható, hogy ez egy rövidebb úton alig okoz térbeli eltérést.

A jelenlegi egyfoton források gyengített lézerimpulzusokat használnak, melyekben elméletileg csak egyetlen foton van jelen. A gyakorlatban a gyengítést általában olyan nagyra választják, hogy a lézer bizonyos elsütéseikor egyáltalán nem jut ki fény a berendezésből. Ez lassítja ugyan a kommunikációt, de biztosítja azt, hogy egynél több foton semmiképpen ne hagyhassa el a berendezést, ami lehetőséget adna rá, hogy egy harmadik fél észrevétlenül lehallgassa az üzenetet, a fölösleges fotonokat felhasználva.

A klasszikus egyenletek fényintenzitását a kvantumos képben a fotonok száma váltja fel, és mivel nem tudjuk, a nyaláb melyik fotonjáról lesz szó, a teljes nyalábterjedésre vonatkozó egyenletet meg kell vizsgálnunk, a végeredmény intenzitás-eloszlása pedig a fotonokra vonatkozó statisztikai eloszlásként értelmezhető. A lézernyalábokat általában Gauss-eloszlású fénynyalábokként szokás közelíteni, így mi is ezt a módszert alkalmazzuk.

Űr–űr kommunikáció esetén a nyaláb ρ félértékszélessége az adó D_A apertúra-átmérő-jének, az L csatornahossznak és a lézer k hullámszámának függvényében:

$$\rho = \sqrt{\frac{4L^2}{k^2 D_A^2} + \frac{D_A^2}{4}}$$

Ez légkörben a következőképpen módosul [15]:

$$\rho = \sqrt{\frac{4L^2}{k^2 D_A^2} + \frac{D_A^2}{4} + \frac{4L^2}{(k \cdot \rho_0)^2} \left(1 - 0.62 \left(\frac{\rho_0}{D_A} \right)^{1/3} \right)^{6/5}}$$

ahol [15]:

$$\rho_0 = \left[1.46k^2 \int_{L_1}^{L_2} C_n^2(z) \left(1 - \frac{z}{L} \right)^{5/3} dz \right]^{-3/5}$$

Végül pedig a C_n^2 turbulencia-erősség a Hufnagel–Valley 5/7 modellből számolható:

$$C_n^2 = 0.00594 \cdot \left(\frac{W}{27}\right)^2 (h \cdot 10^{-5})^{10} \exp\left(-\frac{h}{1000}\right) + 2.7 \cdot 10^{-16} \cdot \exp\left(-\frac{h}{1500}\right) + A \cdot \exp\left(-\frac{h}{100}\right)$$

ahol h a tengerszint feletti magasság, W 21 m/s, A pedig $1,7 \cdot 10^{-14} \text{ m}^{-2/3}$ [16].

A légköri veszteségeket a következő képlettel vehetjük figyelembe. A célzás hibáját a következő valószínűségi eloszlással vehetjük figyelembe [17]:

$$f(r, \theta) = \frac{1}{2\pi\sigma_{C\acute{E}L}^2} \cdot \exp\left(-\frac{r^2}{2\sigma_{C\acute{E}L}^2}\right)$$

ahol r és θ a detektor síkjában a nyaláb középpontjától vett távolság polárkoordinátákban, $\sigma_{C\acute{E}L}$ pedig a célzási hiba. A fotonok beérkezésének teljes félértéksszélessége:

$$\sigma_{SPREAD}^2 = \rho^2 + \sigma_{POINT}^2$$

amiből a τ_{DET} transzmittancia, mely megadja, hogy hány százaléka érkezik meg a fotonoknak egy R_B sugarú, kör alakú detektorba:

$$\tau_{DET} = 1 - \exp\left(-\frac{R_B^2}{2\sigma^2}\right)$$

Ehhez további veszteségek járulnak a légkör, illetve levegőben lebegő por és pára fényszóró és elnyelő tulajdonságai miatt, melyeket az s és a szórási és abszorpciós koefficienseken keresztül értelmezhetünk [18]:

$$\tau_{AIR} = \exp\left(-\sum_i (s_i + a_i) \cdot \Delta L_i\right)$$

A teljes transzmittancia a kettő szorzataként adódik:

$$\tau = \tau_{AIR} \cdot \tau_{DET}$$

A transzmittancia rendkívül fontos paramétere a csatornának, melyen keresztül számíthatjuk az úgynevezett kvantum hibaráta (*Quantum Bit Error Rate*, QBER) [19]:

$$QBER = p_{pol} + \frac{p_{dark} \cdot n}{\tau \cdot \eta \cdot 2 \cdot \mu}$$

ahol p_{pol} a polarizációmérés hibája, p_{dark} a hibásan regisztrált beütések gyakorisága, n a detektorok száma, η a lézerpulzusokban az átlagos fotonszám, μ pedig a detektorok hatásfoka. Amennyiben a QBER 0,11 fölé emelkedik, a kommunikáció többé nem biztonságos, mivel

nem lehet eldönteni, hogy a keletkező hibákat egy harmadik fél okozza-e, vagy a csatorna természetes zajjáról van szó.

A másik igen fontos fogalom a bitráta [19], mely megadja, hogy másodpercenként hány bitnyi kulcs továbbítható a kvantumcsatornán:

$$R = \frac{1}{2} \cdot f_{\text{LÉZER}} \cdot \mu \cdot \tau \cdot \eta$$

ahol $f_{\text{LÉZER}}$ a lézer elsütésének frekvenciája. A fentiek alapján készítettük el a csatornamodel-lünket.

Műholdas kvantumkommunikáció szimulációja

A kvantumcsatorna fizikai jellemzőinek számítását a *Quantum Satellite Communication Simulator* nevű, C# nyelven készült, .Net 4.0 keretrendszeren működő alkalmazás végzi. A fejlesztés alatt fontos szempontnak tartottuk az animációk grafikai megjelenítését, amihez az OpenTK könyvtárat használtuk fel [20]. A program öt különböző üzemmódban működik. Minden scenárió működésének célja a kvantumkommunikáció lényeges jellemzőjének, a QBER értékének meghatározása különböző használati eseteken keresztül. A fejlesztett program felépítése KISS (*Keep It Simple and Straightforward*) elv alkalmazásával történt [21]. Jelenleg a BB84, B92, S09 kvantumprotokollok QBER értékeit tudja meghatározni a program.

A *számítás állandó paraméterekkel* üzemmódban a bemeneti paraméterek a következők: Alice apertúra átmérője, zenitszög, hullámhossz, célzási szöghiba, Bob tükrőátmérője, csatornahossz, szélesség, éghajlat (mérsékelt, trópusi), időjárás (tisza, ködös), évszak (nyár, tél), polarizációmérés hibájának valószínűsége, Bob detektorának határfoka, fotonok átlagos száma lézerimpulzusonként, detektorok száma, detektor zaja, külső háttérzaj, teljes zaj. A számítás eredményeként a QBER érték a következő részeredmények által kerül meghatározásra: statikus veszteségek, koherenciahossz, légköri nyalábszélesedés, célzás hibája, dinamikus veszteségek.

Ebben a scenárióban a felhasználó döntheti el, hogy melyik csatornatípust használja Föld–űr, űr–űr és űr–Föld közül; beállíthatja az input paraméterek értékeit és a szoftver előállítja az eredményt. Ez ajánlott az egyszerű és gyors számításokhoz.

A *számítás változó paraméterekkel* scenárió egy részletes elemzést hajt végre a különböző protokollok QBER képletein. Futás ideje alatt minden képletben minden változó felvehet különböző értékeket. A számítás megkezdéséhez minden paraméterhez meg kell adni az értékváltozás intervallumát és léptetésének mértékét.

Nagy intervallummal és kis lépésközökkel történő számítás esetén a végrehajtás hosszú ideig tarthat. Ez a scenárió akkor hasznos, ha sok paraméter vizsgálata szükséges, amelyek viszonylag alacsony QBER értékeket eredményeznek.

Az *érzékenységvizsgálat* scenárió elgondolásában hasonlít az előzőhöz, viszont az alábbi területeken végezhetünk vele számos vizsgálatot: nyalábszélesedés vákuumban, dinamikus veszteségek, teljes szórás, turbulencia-erősség, QBER.

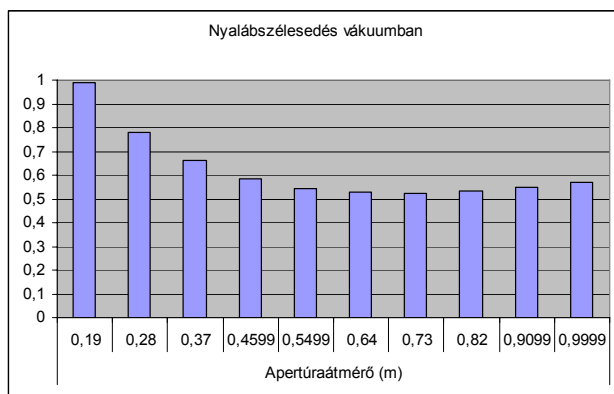
Az *idővezérelt kommunikáció* scenárió az előzőektől különböző jellegű. Ez a mód megmutatja a felhasználónak, hogyan működne a lézerkommunikáció valós földi pozíciók között. A szimuláció során, amelyben a Föld különböző pontjain lévő városokban elhelyezkedő állomások kommunikálnak műholdakkal, egymással különböző hálózati tulajdonságokat mérhetünk.

Az *optimalizálás* scenárió a lehető legjobb (legkisebb) QBER eredményt határozza meg, illetve az ennek eléréséhez szükséges műholdak számát és a pozíciójukból származta-

tott csatornánkénti QBER értékeket. További vizsgálatokhoz érdekes lehet elemezni a különbségeket ezen szcenárió eredményei és az idővezérelt kommunikáció szcenárió által adott QBER értékek között.

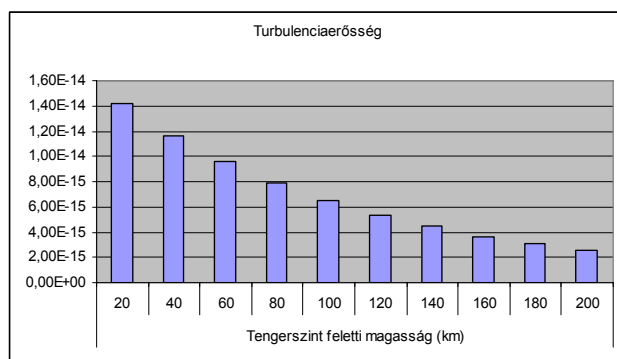
Eredmények

Érzékenységvizsgálat szimulációs eredményére mutatunk két példát.



1. ábra Nyalábszélesedés a vákuumban

Az 1. ábrán a szimulátor érzékenységvizsgálatának egy eredménye látszik, egy példa szerint a vákuumbeli nyalábszélesedés alakulására Alice apertúra-átmérőjétől függően. A legszélesebb nyalábot az értelmezett intervallumon 0,1 m apertúra-átmérőnél éri el. Növelve ennek a paraméternek az értékét, a nyalábszélesedés legalacsonyabb pontja viszonylag hamar elérhető, és ez után a pont után a kapott érték majdnem lineárisan növekszik. A 2. ábrán a turbulencia-erősséget vizsgáltuk a tengerszint feletti magasság függvényében. A feltételezett szélsősebesség: 21 m/s.



2. ábra Turbulencia-erősség a tengerszint feletti magasság függvényében

Összefoglalás

A műholdas kommunikációban a lézeres információátvitel előnyös lehet a hagyományos technikához képest. A fotonokon alapuló kvantumkommunikáció segítségével biz-

tonságos kulcskialakítás valósítható meg, a légkör tulajdonságainak pontos ismeretében pedig optimalizálható a berendezések felépítése. A fentiekben ismertetett eredményeket 2011-ben a Nemzetközi Asztronautikai Kongresszuson is publikáltuk [22].

Irodalomjegyzék

- [1] Galileo Probe Was A NASA Space Probe Sent To Study Planet Jupiter, *Universe – Galaxies and Stars* (http://www.universe-galaxies-stars.com/Galileo_probe.html, utolsó látogatás: 2011. 10. 27.)
- [2] Record Set for Space Laser Communication, *Space.com* (<http://www.space.com/1900-record-set-space-laser-communication.html>, utolsó látogatás: 2011. 10. 27.)
- [3] 10Mbps Laser Broadband Link, *DSLreports.com* (<http://www.dslreports.com/shownews/10Mbps-Laser-Broadband-Link-89210>, utolsó látogatás: 2011. 11. 22.)
- [4] M. Toyoshima: Trends in satellite communications and the role of optical free-space communications (http://publik.tuwien.ac.at/files/pub-et_10214.pdf, utolsó látogatás: 2011. 11. 22.)
- [5] Astrium GEO-Information Services: Infoterra GmbH (http://www.infoterra.de/terrasar-x_laser_communication_terminal_successfully_tested, utolsó látogatás: 2011. 10. 27.)
- [6] M.A. Nielsen, I.L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press, 2000
- [7] S. Imre, B. Ferenc: *Quantum Computing and Communications: An Engineering Approach*, Wiley, 2005
- [8] Bacsárdi L.: Műholdas kommunikáció kvantumcsatorna segítségével. *Űrtan Évkönyv az űrkorszak ötvenedik évében*. MANT, pp. 93–95 (2007)
- [9] Bacsárdi L., Galambos M., Imre S.: Kvantumcsatorna a műhold–Föld és a műhold–műhold kommunikációban, *Híradástechnika* LXV:(3-4), pp. 23–29 (2010)
- [10] W.K. Wootters, W.H. Zurek: A single quantum cannot be cloned, *Nature* 299, pp. 802–803 (1982)
- [11] G.S. Vernam, Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications, *Journal of the IEEE* 55, pp. 109–115 (1926)
- [12] C.H. Bennett et al.: Experimental quantum cryptography, *Lecture Notes in Computer Science* 473, pp. 253–265 (1991)
- [13] T.S. Manderbach et al.: Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, *Physical Review Letters* 98, 010504 (2007)
- [14] J.M.P. Armengol et al.: Quantum Communications at ESA: Towards a space experiment on the ISS, *Acta Astronautica* 63, pp. 165–178 (2008)
- [15] R.L. Fante: Electromagnetic Beam Propagation in Turbulent Media, *Proc. IEEE* 63, pp. 1669–1692 (1975)
- [16] M. Brass: *Handbook of Optics*, Vol. I. (2nd. ed.), McGraw-Hill, 1995
- [17] S.G. Lambert, W.L. Casey: *Laser Communications in Space*, Artech House, 1995
- [18] W.G. Discoll: *Handbook of Optics*, McGraw-Hill, 1978
- [19] N. Gisin et al.: Quantum Cryptography, *Reviews of Modern Physics* 74, pp. 145–195 (2002)
- [20] Home of the Open Toolkit library (<http://www.opentk.com>, utolsó látogatás: 2011. 10. 27.)
- [21] AMIS Technology blog (<http://technology.amis.nl/blog/>, utolsó látogatás: 2011. 10. 27.)
- [22] M. Galambos, L. Bacsárdi, A. Kiss, S. Imre: Redundancy-free Quantum Coding Methods in Space Communications. *Proc. International Astronautical Congress 2011*, Cape Town, South Africa, Oct 3–7, 2011.