KISMŰHOLDON ALAPULÓ KVANTUM KULCSSZÉTOSZTÁS VIZSGÁLATA

TDK - 2019

Szerző:
Jakab Dominik

Konzulens:
Dr. Bacsárdi László

Tartalomjegyzék

1. Bevezetés

1.1. Titkosítás napjainkban

Az információ az egyik legnagyobb érték a mai társadalomban. Magától értetődő, hogy ennek védelmezése fontos ágazata a technológiáknak. Alapvetően két típusú titkosítást különböztetünk meg: szimmetrikus és aszimmetrikus. Az előbbinél nagy probléma, hogy ugyanannak a kulcsnak kell mindkét félnél meglennie, melynek eljuttatására nincs teljesen biztonságos módszer. Az utóbbi működése, hogy előállítunk egy publikus és egy privát kulcsot, melyből a publikusat megosztjuk a világgal. A lényeg, hogy a publikus kulcs által kódolt adatot csak a privát kulccsal lehet dekódolni. Az egyik legelterjedtebb asszimmetrikus eljárás az RSA titkosítás, melynek alapja, hogy a kulcs előállításának számításigénye nagyságrendekkel kisebb, mint a publikus kulcsból annak prímtényezői, ezáltal privát kulccsának visszafejtése. Így az RSA arra a matematikai tényre alapul, hogy egy szám prímtényezőinek meghatározása nehezen számolható.

A kvantumtechnológia egy olyan megoldást biztosít erre a problémára, mely a számítástechnika fejlődésével is megállja a helyét. Már jó ideje létezik egy elméleti algoritmus, mellyel egy kvantumszámítógép képes feltörni a másodperc töredéke alatt az RSA-t. Az algoritmus neve Shor-algoritmus, és segítségével logaritmikus komplexitással lehet prímfaktorra bontani számokat. Emiatt az RSA kulcshosszának drasztikus növelése sem okoz majd a jövőben problémát. Az algoritmust már tesztelték, és működőképesnek bizonyult. Az algoritmussal az IBM kvantumszámítógépein már a 15-öt és a 21-et is sikeresen felbontották. Jelenleg a legnagyobb kvantumosan prímfaktorizált szám a 4088459, és bár ez nem Shor algoritmusával készült, de jól mutatja a kvantumszámítógépek fejlődését. [1]

De a kvantumos világ nem csak a régi titkosítások feltörésére kínál megoldást, hanem új, biztonságos eljárásokat is kínál. Már létezik olyan titkosítási protokoll is, mellyel nem bízzuk magunkat a számítási igény nagyságára. A kvantumos kulcsszétosztás (QKD, Quantum Key Distribution) elmélete már több protokollal (pl. BB84) rendelkezésre áll, és földi viszonyokban tesztelve is van. Ezt a titkosítást nem lehet lehallgatni anélkül, hogy a felek ne értesüljenek erről, így teljesen biztonságos, ha a csatorna megfelelő.

Kvantumos kulcsszétosztásnál a biteket fotonok szállítják, mely egyből számos korlátozással állít minket szembe. A fotonokat küldhetjük optikai szálakon, vagy szimplán a levegőben. Az előbbinél a kulcsszétosztás távolsága limitálva van a kábel csillapítása miatt. Pár száz km után a vezetéken akkora csillapítás lép fel, hogy jelismétlőre lenne szükség. Kvantumos jelismétlő nem létezik, ezt a kvantummechanika posztulátumai tiltják, így más megoldáshoz kell folyamodni.

Kézenfekvő megoldás, hogy optikai szálak helyett a légkört használjuk közvetítő közegnek, mely ígéretesnek hangzik. Sajnos itt nem olyan egyszerű a helyzet mint a rádiónál, a foton sugárban terjed, nem úgy, mint egy elektromágneses hullám. Emellett könnyen árnyékolható is. Ezáltal az út, melyen bármely két pont között árnyékolás mentes kapcsolat létesíthető a föld felszínén, csak egy műholdon át vezethet. A kínai kvantumműhold (Micius) [2] sikerén

felbuzdulva az egész világ elkezdett foglalkozni kvantumos műholdak tervezésén és feljuttatásán.

Sajnos a legtöbb kutatócsoport nem engedhet meg magának egy 600 kilós műholdat. Szerencsére létezik egy alternatíva: a CubeSat-ek.

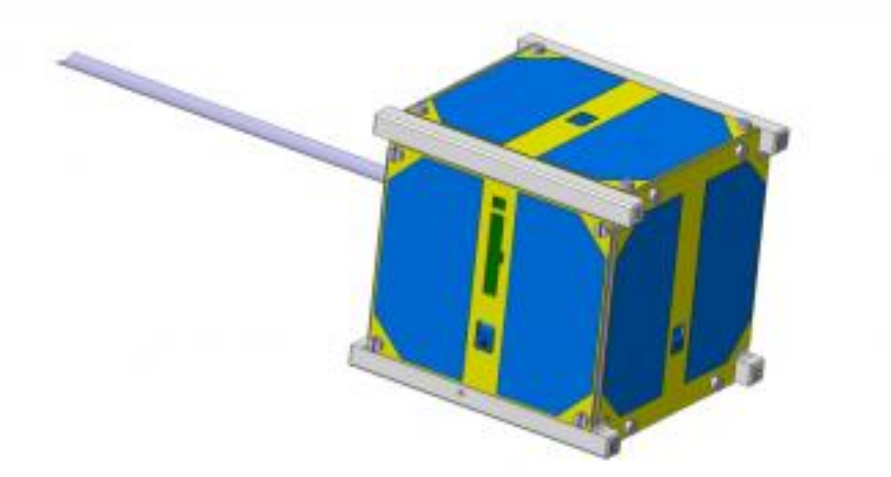

Figure 1 - A Masat-1 CubeSat vázlata: Ekkora egy 1 U-s pikoműhold (CubeSat), melyet a BME-n terveztek.

Ezek párszor 10 centis, átlagban kevesebb mint 1,5 kilós szerkezetek, melyeknek nem csak tervezése és megépítése, de feljuttatása sem "annyira" drága. Viszont ezek a súly és méretkorlátok számos problémát vetnek fel a tervezésben, melyekre ebben a dokumentumban igyekszek rávilágítani. Jelenleg is számos kvantumos CubeSat tervezése történik a világban, ebből érzékelhető a technológia fontossága.

A szimuláció során egy 6U-os, azaz 10x20x30 centis pikóműholdat feltételezek, melyben már elméletben elfér a 0.2m átmérőjű távcső, amit a számolásokhoz használok. Ezen dolgozat keretein belül eltekintek attól, hogy a payload, azaz a valós szimulációt megvalósító eszközök ténylegesen elférnek-e ekkora helyen.

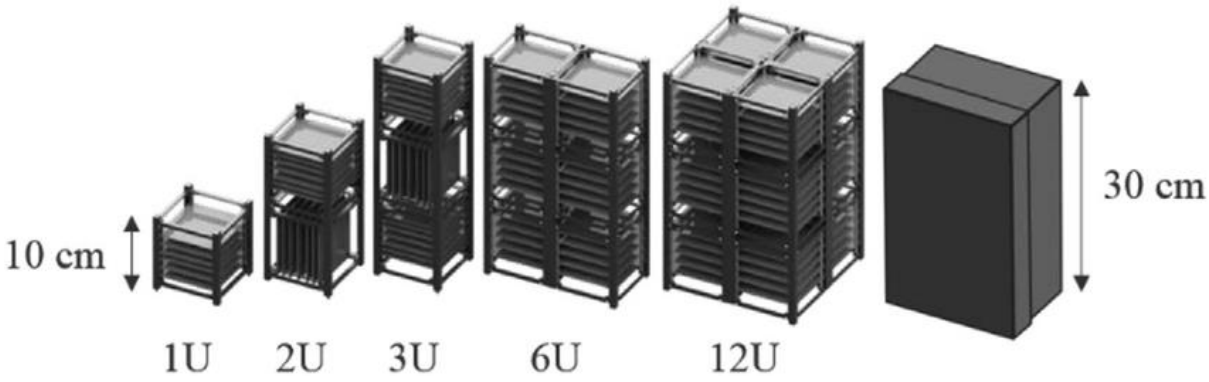

Figure 2 – A CubeSat szabvány méretei Unit alapján növekvő sorrendben.

1.2. BB84 protokoll

A QKD protokolljához a BB84-et választottam, mert ez egy könnyen megérthető technika, és technológiai elvárásai is alacsonyabbak. A titkosításhoz két csatornára lesz szükség: egy klasszikus, rádióhullámmal működő; és egy kvantumos, amelyet fotonok közvetítenek. A kvantumbiteket fotonok polarizációja reprezentálja.

A BB84-ben két ortogonális bázis alapján határozzuk meg a fotonok polarizációját. Az egyik egy horizontális/merőleges, a másik pedig egy diagonális.

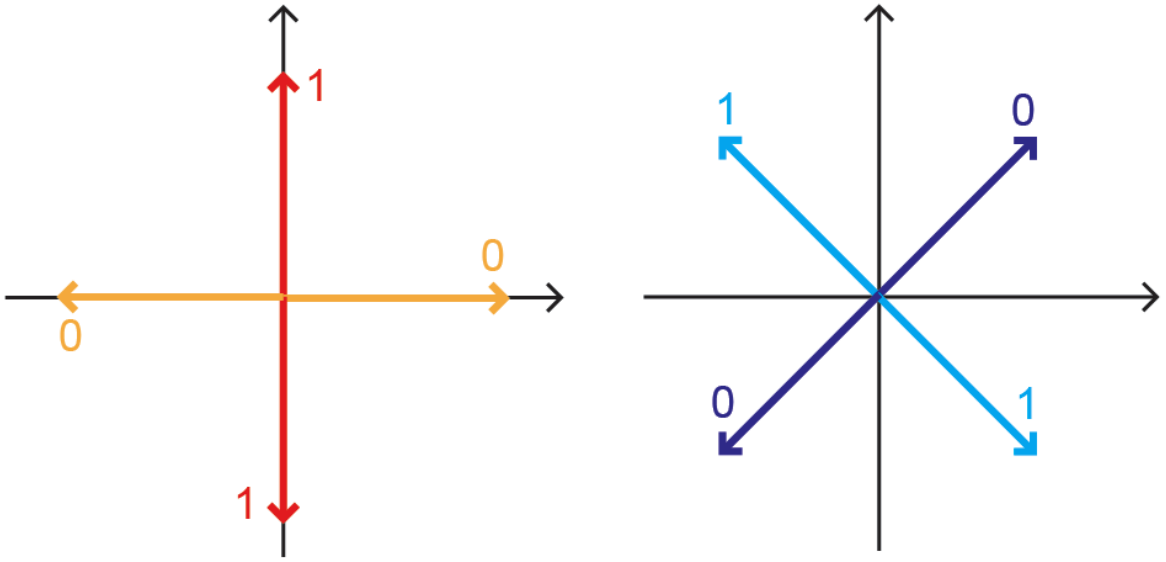

*Figure 3 - A BB84 protokollnál általánosan használt két bázis, a **horizontális/vertikális** és a **diagonális**.*

Ezekben a bázisokban lévő polarizációra képezzük le a 0 és 1 bitet. Az első bázisban az 1-et a függőleges, 0-át a vízszintes polarizáció jelöli. A másik bázisban is hasonlóan kódoljuk a biteket a képen látható módon. A biteket a kvantumos világban – összhangban a kvantummechanika posztulátumával - 0 helyett $|\mathbf{0}\rangle$ (*ketnull*) és 1 helyett $|\mathbf{1}\rangle$ (*ketegy*)-ként említjük.

De egy foton polarizációja nem csak ez a két állapot lehet. Ha ábrázoljuk a fotont egy ilyen koordinátarendszeren, egy véletlenszerű pozícióba mutató egységvektort kapunk. Legyen ezentúl a fotonunk $|\varphi\rangle$, a vízszintes tengely ábrázolja a $|\mathbf{0}\rangle$-át, a függőleges a $|\mathbf{1}\rangle$-et. Ekkor egy tetszőleges $|\varphi\rangle$, egységvektor felírható a következő alakban:

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

Ahol:

$$a, b \in \boldsymbol{C}$$
$$a^2 + b^2 = 1$$

Ezt az alábbi ábra szemlélteti:

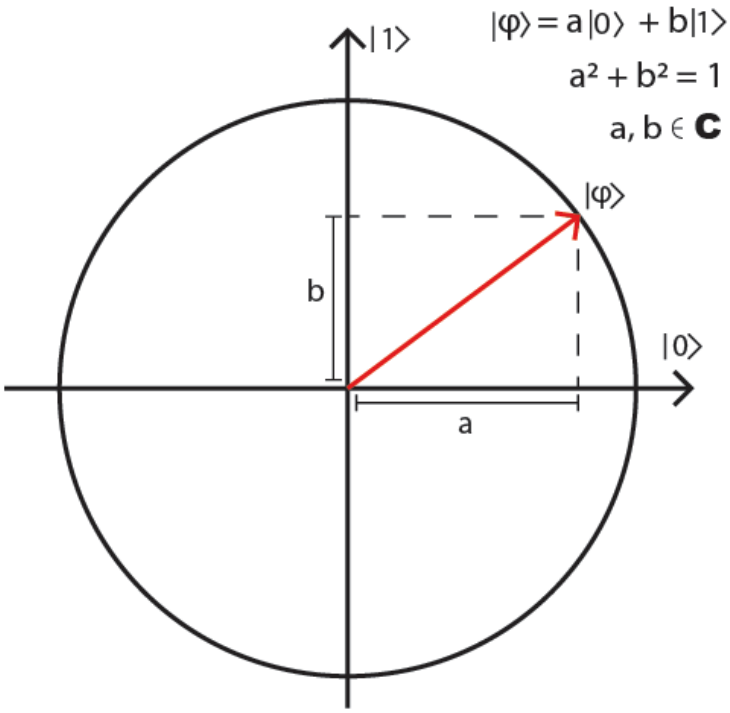

Figure 4 - Egy tetszőleges qubit reprezentálása egységkörön.

Ha egy ilyen fotonon mérést hajtunk végre, akkor **a^2 eséllyel $|0\rangle$-t, b^2 eséllyel $|1\rangle$-et** mérünk. Így ha a fotonunk polarizációjának iránya megegyezik a bázisunk valamelyik tengelyével, akkor 100% eséllyel meg tudjuk mondani a mérés eredményét. Ha viszont pont a két tengelytől egyenlő távolságra mutat a vektor, akkor 50% eséllyel mindkettőt mérhetjük.

Tehát ha abban a bázisban mérjük a fotont, amiben elküldték, akkor 100% valószínűséggel meg tudjuk mondani, mit küldtek. Ha a másik bázisban mérünk, véletlenszerű az eredmény, nem jutunk információhoz.

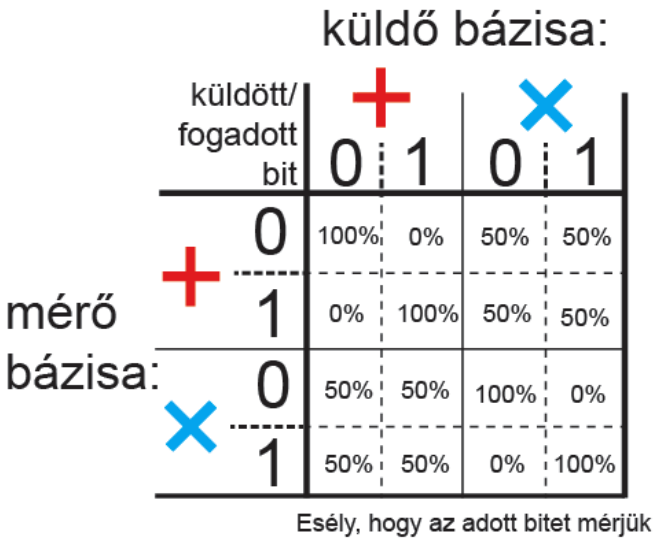

Figure 5 - Mérési valószínűségek megegyező és különböző bázisokban.

Térjünk vissza a műhold és a vevőállomás konfigurációjára. QKD-ben a kulcscserében résztvevő két felet Alicenek és Bobnak szokás hívni. A mi esetünkben Alice a műhold, Bob pedig a földi vevőállomás (OGS = Optical Ground Station).

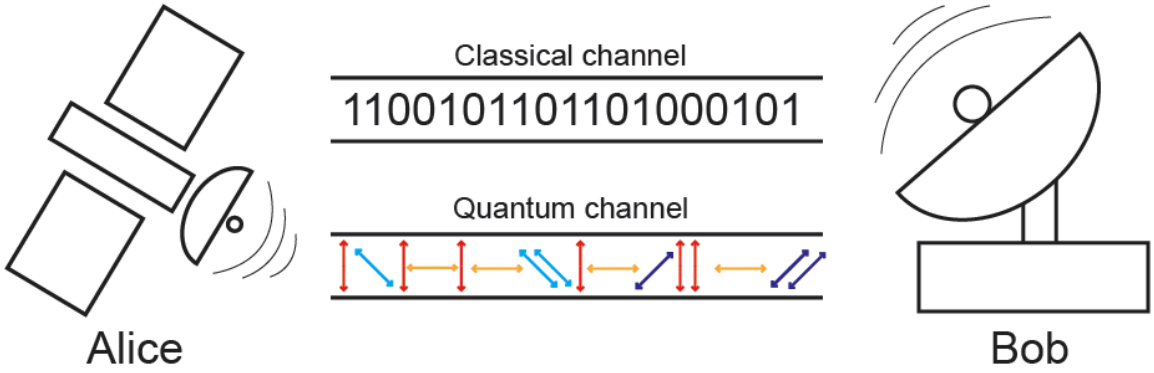

Figure 6 - A CubeSat és az OGS közötti csatornák

Első lépésként Alice a kvantumos csatornán elküld egy véletlen bitsorozatot. Minden bit küldése előtt véletlenszerűen választ egyet a két lehetséges bázis közül, és abban kódolja a bitet (kvantumbitté).

Figure 7 - Alice által küldött bitek és a bitekhez tartozó bázisok.

Bob megméri ezt a kvantumbit-sorozatot, minden méréskor véletlenszerűen választva a két bázis közül. Ha eltalálta a megfelelő bázist, jót fog mérni, ha nem, akkor ott véletlenszerűen mér 0-át vagy 1-et.

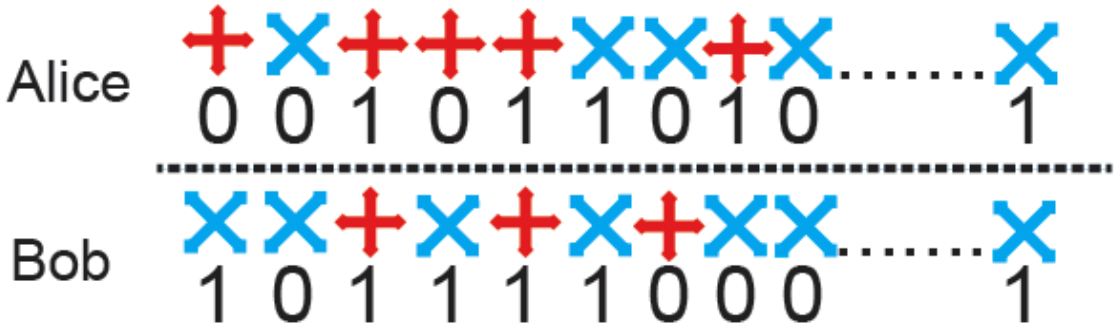

Figure 8 - Bob által mért bitek és a mérési bázisok. Látható, hogy ahol nem ugyanabban a bázisban mért, mint amiben Alice a fotont küldte, ott az eredmény véletlenszerű.

Ezután Bob a klasszikus csatornán közzéteszi a bázisokat, amelyekkel mért. Ezt Alice összehasonlítja a saját bázisaival, és visszaküldi azokat az indexeket, ahol Bob eltalálta a bázist. Majd mindketten eldobják azokat az eredményeket, ahol a bázis nem stimmelt.

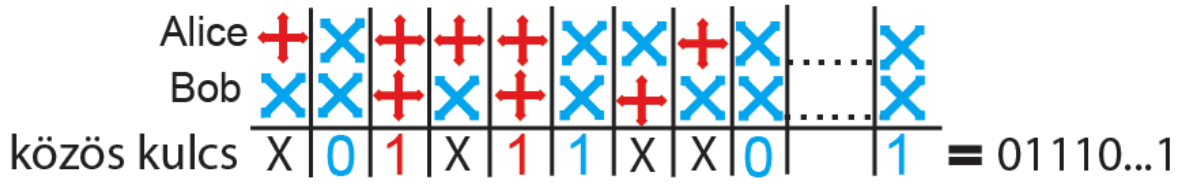

Figure 9 - A bázisok egyeztetése után előállítható a közös bitsorozat.

Ebből ki fog alakulni a közös kulcs, mert ahol stimmeltek a bázisok, ott biztosan egyezik a küldött és fogadott kvantumbit. Ezt a kulcsot már használhatjuk teljes biztonsággal szimmetrikus kulcsú titkosításhoz.

A bázisok megosztása nem jár a titkosítás szempontjából rizikóval, mert egy potenciális támadónak nincs semmi tudomása arról, hogy a mérés eredménye mi volt.

A protokoll feltörthetetlensége két dologban rejlik. Az első, hogy nem lehet passzívan lehallgatni. Passzív lehallgatás az, amikor a támadó a csatorna módosítása nélkül “belehallgat” az adásba. Ez itt azért nem lehetséges, mert a közvetítő közeg egy darab foton/qubit, és ezt a fotont lemérni csak úgy lehet, ha elnyeletjük egy detektorral. Tehát ha valaki belehallgatna, megakadályozná, hogy Bob-hoz eljusson a fotonsorozat.

Így csak az az opció maradt, hogy aktívan támadjuk meg a rendszert, azaz belekontárkodunk a két fél közötti kommunikációba (man-in-the-middle attack). Ha ezt megtesszük, úgy tudnánk megelőzni a lebukást, hogy lemérjük a küldött fotont, majd továbbküldünk egy ugyanolyat. Itt jön a képbe a kvantumfizika. Egy nagyon fontos posztulátum tartozik ide, a **No-Cloning**

Theorem. [3] Ez kimondja, hogy tetszőleges ismeretlen kvantumállapot nem másolható le (a foton polarizációja is egyfajta kvantumállapot). Tehát a támadó nem tudja lemásolni a fotont, így csak annyit tehet, hogy ő is leméri valamilyen bázisban a fotont. Még ha ismeri is a két bázist, melyet Alice és Bob használ, ő is csak véletlenszerűen választhat a kettő közül. Majd az így mért értéket továbbküldi Bobnak.

Ekkor két eset fordulhat elő: a támadó eltalálta a bázist, és a megfelelő qubitet küldte Bobnak. De ha nem találta el a bázist, akkor véletlenszerűen küld tovább 0-át vagy 1-et. Ez azt jelenti, hogy 50% eséllyel nem találja el a bázist, és ekkor 50% eséllyel tudja csak a jó qubitet küldeni. Ez 50% * 50% = **25% extra zajt okoz a rendszerben**. Alice és Bob ezt fogja észrevenni.

Amikor előállt a közös kulcs, még egy lépést végre fog hajtani a két fél: a lehallgatás ellenőrzését. Ekkor Bob a közös kulcs egy előre megadott részét levágja, és klasszikus csatornán megosztja Alice-el. A mi esetünkben ez a kulcs első X bitje lesz (általában X a kulcs felének hosszával egyezik meg), de valós esetben ezt egy sokkal bonyolultabb algoritmussal oldják meg. A kulcs megosztott részét persze a két fél eldobja, mert publikussá tétele kompromittálta azt.

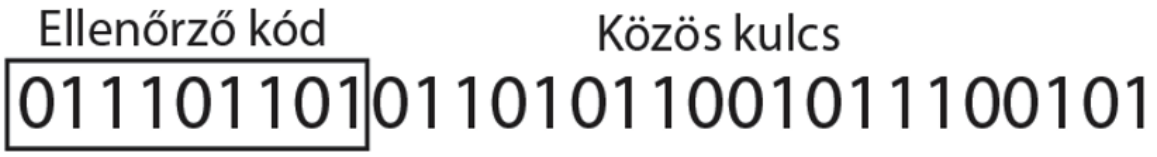

Figure 10 - Az ellenőrző kulcs kiválasztása. Ez a való életben nem ilyen egyszerű algoritmussal történik, és általában a bitek fele elveszik.

Ezt az ellenőrző kódot Alice összehasonlítja a sajátjával, és megméri a zajt (QBER = Quantum Bit Error Rate). A zaj alapján észrevehető, hogyha támadó van a rendszerben, mert ez a QBER érték jelentősen megnövekszik. A protokollban meghatároztak egy küszöbértéket, amely felett a két fél eldobja a kulcsot, mert nem garantálható annak biztonsága. Ha ez megtörténne, újbóli kulcscserét hajtanak végre, amíg nem sikerül biztonságos kulcsot kialakítani. A BB84 protokollnál a QBER küszöbértéke 0.11, azaz 11%. Ha a mért zaj efölé megy, akkor lehetséges, hogy valaki lehallgatja az adást. Ilyenkor mindkét fél azonnal abbahagyja a titkosítást és eldobja az eddig megalkotott biteket/kulcsot, és újrakezdik a protokollt.

1.3. A szimuláció ismertetése

Kutatásom során egy kisműholdat fogok vizsgálni, mely egy, de akár több földi vevőállomással kommunikálva kvantumos titkosítást hajt végre optikai csatornán keresztül. A szimuláció során különböző ideig tartó keringést fogok modellezni, mely során állítható finomsággal mintavételezek,s ezeket az eredményeket felhasználva egy becslést adok arra, hogy mennyi ideig működött a titkosítás, azaz mennyi volt az effektív idő. Emellett az átvitt bitek mennyiségére és a bitsebességre is adok egy becslést. Elsőként a műhold pályájának modellezését fogom bemutatni, majd az optikai csatornát. Végezetül a szimuláció felépítését taglalom, és ezek eredményeit elemzem.

A szimulációban 6 U-os méretű műholdat feltételezek, melynek a méretkövetelményekből adódóan teleszkópmérete 0 és 0.2m között mozoghat. A cubesat SSO-n (Sun Synchronous Orbit, napszinkron pálya), azaz napszinkron pályán kering, melynek magassága 500 km. Méréseim során feltételezem, hogy a műhold mindig éjszaka halad át a földi vevőállomás felett. Ez elérhető megfelelően paraméteretett napszinkron pályával, mert ennek speciális tulajdonsága, hogy a műhold mindig azonos szöget zár be a nappal. A műholdon (két) lézer fogja a fotonokat előállítani és elküldeni a vevőállomás felé 1 MHz-s frekvenciával. Feltételezem, hogy csak minden 10-ik pulzus tartalmaz fotont, ez a használt technológiából adódik.

Az modellben a földi vevőállomást Budapesten helyeztem el, a többi vevőállomás Tenerifén és Grazban található meg. Ezek teleszkópmérete 1 méter. A detektorok hatásfokát és egyéb paramétereit a mai készülékek adataihoz hasonló értékre állítottam.

A programomban megadható a szimuláció hossza és a mintavételezési időtartam. A szimuláció végén eredményként megkapom vevőállomásonként az effektív időt, az átvitt bitek mennyiségét és a sebességet byte/s-ként. Ezekből az adatokból a legkedvezőbbet és egyben valósághűbbet kiválasztva egy elméleti becslést teszek a megvalósíthatóságra, majd ezután a technológia jövőjét fogom elemezni.

2. Napszinkron pálya modellezése

2.1. Pályamagasság

A műholdpályákról való kutatásaim során a napszinkron pálya mellett döntöttem, több okból is. Egyértelműen csak alacsony Föld körüli pálya (LEO), azaz Low Earth Orbit pályák jöhettek szóba, mert egy kisműholdra nem tudunk elég nagy teljesítményű fotonforrást telepíteni ahhoz, hogy ennél magasabbra is tehessük a kisműholdat. Ezen pályák kb. 300 km-től egészen 2000 km-ig tartanak. Számunkra célszerű volt minél alacsonyabb pályát választani, mert így csökkenthetőek a távolság miatt jelentkező veszteségek. Két dolgot fontos figyelembe venni a pálya megválasztásakor, melyek közt meg kell találni a számunkra optimális opciót. Ez a két érték a várható minimális és maximális élettartam.

A minimális élettartam annál kisebb, minél alacsonyabban száll a műhold. Ahogy telik az idő, a műholdunk pályamagassága lassan csökkeni kezd, elkezd beesni a föld irányába. Amint eléri az atmoszférát, a műhold elég, és így vége a missziónak. Emiatt a kutatás szempontjából meg kell határozni egy minimális élettartamot, mely a mi esetünkben 1 év. A maximális élettartamra viszont szabályok vonatkoznak, melyek szerint maximálisan 25 éven belül be kell esnie a légkörbe és megsemmisülnie.

A ténylegesen pályamagasság megállapítását egy hazai űripari céggel, a C3S kft.-vel [4] közösen végeztem. Több modellel is ki kell számolni a várható élettartamot, melyekből a legrosszabbat kell figyelembe venni a szabályok szerint. Ezek alapján egy 6 U-os CubeSat-et modellezve egy **500 km-es** pályán a várható élettartam minimálisan 1-2 év, a maximális 24.99 év, így ez tökéletes számunkra.

2.2. SSO paraméterezése

Ahhoz, hogy meghatározzuk egy tetszőleges műhold pályáját, bizonyos paramétereket ismernünk kell. Ezek az adatok jelen dolgozatban nem mindenhol tükrözik egy esetlegesen a jövőben elkészülő kisműhold valós pályáját, de számunkra ebben a kutatásban a pontos pályaadatok nem szükségesek. A kutatás eredménye függetlenül a paraméterektől közelítőleg ugyan azt az eredményt fogja adni elég hosszú időtartam szimulálásakor, ha maga a pályamodell helyes.

A napszinkron pálya egyik nagyon nagy előnye, hogy cirkuláris, azaz nagyon közel kör alakú, így képletei egyszerűsödhetnek egy-két helyen. Munkám során be fogom mutatni a teljes képleteket, majd az általam használt egyszerűsített alakot is. Bár emiatt szimulációm jelenleg csak napszinkron pályák szimulálására alkalmas, de kevés bővítéssel használható lehet tetszőleges LEO pályákra is.

Fő célunk, hogy a keringési adatokból és az aktuális időből meg tudjuk határozni a műhold pontos pozícióját. A műhold aktuális helyzetét hosszúsági és szélességi fokban kezelem, így ezeket az adatokat kell előállítani. A számolások során a következő paraméterekre lesz

szükség: **pályamagasság, inklináció, eccentricity (excentricitás), semi-major axis, longitude of the ascending node, argument of periapsis.**

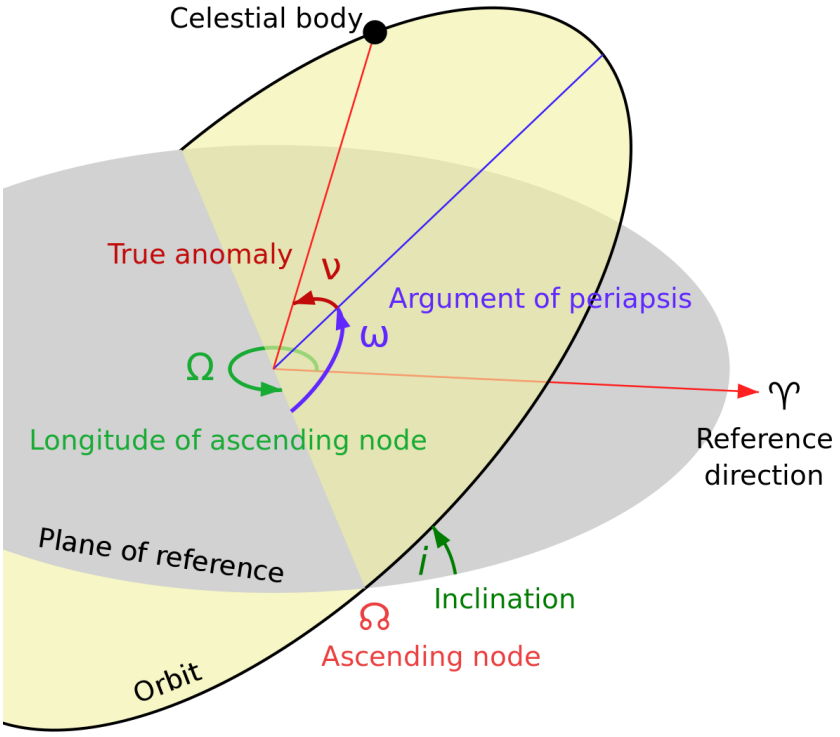

Figure 11 - Egy tetszőleges pálya paramétereinek szemléltetése. - Wikipedia

Az inklináció a pályamagasságból kiszámolható. Először a periódust fogjuk meghatározni hozzá, melyet Kepler 3. törvényének segítségével írunk fel:

$$T = 2\pi\sqrt{\frac{a^3}{\mu}}$$

ahol

T = periódusidő
a = semimajor axis ≈ 6,835,439.3 m ≈ (R + h)
R = a föld sugara az egyenlítőnél
h = pályamagasság
μ = standard gravitational parameter = G*M ≈ 398,589,405,760,000 m^3s^{-2}

Ezekből az adatokból kiszámolva:

$$T \approx 5624.3s$$

Mely 1,56 órával egyenlő körülbelül. Ebből az inklinációt a következőképp számolhatjuk ki SSO pályáknál [5].

$$\Delta\Omega = -3\pi \frac{J_2 R_E^2}{p^2} \cos i$$

ahol

Ω = angular precession = precesszió
J_2 = coefficient of second zonal term
R_E = a Föld sugara
p = semi-latus rectum of orbit - SSO pályáknál p ≈ a
i = inklináció

Ha felírjuk a precesszió képletét:

$$\rho = \frac{\Delta\Omega}{T}$$

Ezt felhasználhatjuk az előző képletben:

$$\rho \approx -\frac{3J_2 R_E^2 \sqrt{\mu} \cos i}{2a^{\frac{7}{2}}}$$

A napszinkron pálya fő jellemzője, hogy a precesszió (ρ) egyenlő a Föld Nap körül való mozgásával, amely jelen esetben 360° évente ($1.99096871 \times 10^{-7}$ rad/s). Ezt felhasználva rendezzük cos(i)-re:

$$\cos i \approx -\frac{2\rho}{3J_2 R_E^2 \sqrt{\mu}} a^{\frac{7}{2}} = -\left(\frac{a}{12352km}\right)^{\frac{7}{2}} = -\left(\frac{T}{3.795h}\right)^{\frac{7}{3}}$$

melyből már könnyen kiszámolható i, azaz az inklináció. Elvégezve a számolásokat:

$$\cos i \approx -0.126073$$

$$i \approx 1.6972\, rad \approx 97.2427^o$$

Az inklináció után a következő feladat az excentricitásból a mean anomaly (M), majd az eccentric anomaly (E) meghatározása. Ehhez szükségünk less az úgynevezett "average rate of sweep"-re (n), amely azt fejezi ki, hogy mennyi idő kell egy testnek egy teljes keringéshez. [6]

$$n = \frac{2\pi}{T}$$

ahol:

n = sweep
T = a pálya periódusa

Ebből meghatározhatjuk a mean anomalyt:

$$M = n(t - \tau)$$

ahol:

M = mean anomaly
N = sweep
t = idő az adott pillanatban, amelyben meg szeretnénk határozni az értéket
τ = pericenter passage, ez egy offset, melyet az egyszerűség kedvéért 0-nak veszünk.

Innen a eccentric anomaly:

$$M = E - e \sin E$$

ahol:

E = eccentric anomaly
M = mean anomaly
e = eccentricity

Ez egy nem lineáris egyenlet, emiatt az E értékét csak közelíteni tudnánk. Szerencsére az egyenletből a második tag kiesik, mert az excentricitás körpályákon 0, így e ≈ 0.

$$M = E$$

A következő paramétereket az egyszerűség kedvéért nullának tekintjük, az eredmény nem befolyásolják:

Ω = longitude of the ascending node = 0
ω = argument of perihelion = 0

2.3. Aktuális pozíció számolása

Az előző bekezdésben meghatározott és kiszámolt adatokat használva megkaphatjuk a műhold aktuális helyzetét szélességi és hosszúsági koordinátákban. Ehhez szükséges lesz először a Cartesian koordinátákat kiszámolni, majd ezeket J2000-es ("Celestial")- koordinátákra váltani [7, 8].

Először számoljuk ki a Cartesian koordinátákat:

$$X_o = a(\cos E - e) \approx a \cos E$$

$$Y_o = a\sqrt{1 - e^2} \sin E \approx a \sin E$$

$$Z_o = 0$$

mert e ≈ 0. Ezt, hogy J2000-be váltsuk, egy transzformációs mátrixot kell használnunk, melyből az alábbi koordinátákat kapjuk:

$$x = X_o(\cos\omega \cos\Omega - \sin\omega \cos i \sin\Omega) - Y_o(\sin\omega \cos\Omega + \cos\omega \cos i \sin\Omega)$$

$$y = X_o(\cos\omega \sin\Omega + \sin\omega \cos i \cos\Omega) + Y_o(\cos\omega \cos i \cos\Omega - \sin\omega \sin\Omega)$$

$$z = X_o(\sin\omega \sin i) + Y_o(\cos\omega \sin i)$$

ahol

Ω = longitude of the ascending node = 0
ω = argument of perihelion = 0
i = inclination ≈ 1.6972 rad

Ebből a hosszúsági és szélességi adatok a következőképp számolhatók ki:

$$latitude = \sin^{-1} z$$

$$longitude = \tan^{-1}\frac{y}{x}$$

Ezek alapján minden pillanatban ki tudjuk számolni a kisműhold helyzetét. Felhasználva ezeket az adatokat a következő fejezetben kiszámolom az OGS (optikai vevőállomás, Optical Ground Station) és a műhold közötti azimut és zenit szögeket.

A Föld forgásából adódó pozícióváltozást könnyű bevezetni. Elég, ha a műhold pozíciójának kiszámolása után egyszerűen elforgatjuk a műhold alatt a Földet, mely a Föld szempontjából a műhold ellentétes irányban való azonos mértékű elforgatásával egyenlő.

A Föld adott t másodperc alatt végzett forgása:

$$\Delta\alpha = 2\pi\frac{eltelt\ idő}{1\ nap} \approx 2\pi\frac{t}{86{,}400}$$

Ezt levetítjük a [0, 2π[tartományra, és a kapott szöget egyszerűen kivonjuk a hosszúsági szögből (longitude), majd az új értéket visszavetítjük a [0, 2π[tartományra.

2.4. Azimut és zenit szög meghatározása

A *zenit* és *azimut* szög jelöli a földi vevőállomás, azaz az OGS és a műhold által bezárt szögeket a hosszúsági és szélességi körök tengelyén, ezek alatt "látszik" a műhold. Ezen szögek szükségesek a későbbi optikai csatorna kiszámolásánál, ezért ezeket is pontosan meg kell tudnunk adni. A korábban kiszámolt pályaadatokból ez már nem jelent problémát.

Itt látható az OGS, a kisműhold, és a Föld középpontja ábrázolva, melyek egy háromszöget alkotnak:

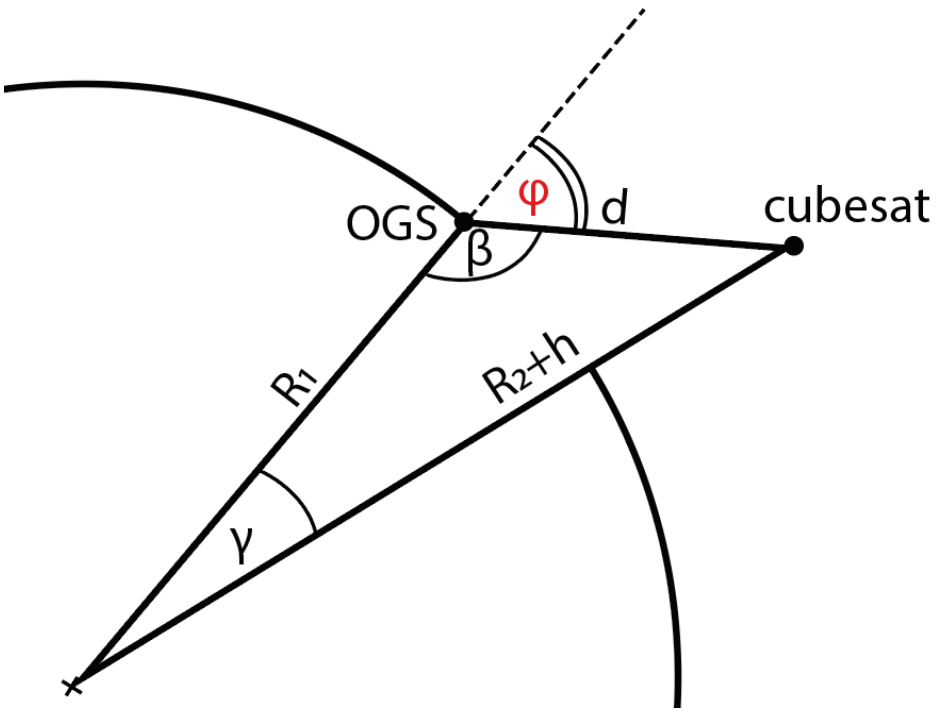

Figure 12 - Zenit és azimut szög számolása trigonometrikus azonosságokkal.

ahol:

R_1 = a Föld sugara az OGS-nél	h = a pályamagasság
R_2 = a Föld sugara a kisműholdnál	γ = szélességi vagy hosszúsági különbség szöge
β = 180 – φ	φ = a keresett szög

Külön meg fogjuk határozni az *azimut* és a *zenit* szöget. Ugyanazt a képletet használhatjuk mindkettőre, csupán a hosszanti (*longitude*) és szélességi (*latitude*) szög értékét kell cserélni. Fontos, hogy γ **nem** a műhold hosszúsági/szélességi szöge, hanem az OGS és a műhold közötti szög, azaz:

$$\gamma = |lat_{OGS} - lat_{CubeSat}|$$

Szeretnénk kiszámolni β-t, mert abból φ már könnyen megadható. Ahhoz, hogy ezt megtegyük, felírhatjuk a cosinus tételt az R_2+h oldalra.

$$(R_2 + h)^2 = R_1^2 + d^2 - 2R_1 d \cos\beta$$

Ebből R_1 és R_2 ismert, de szükségünk van "d" meghatározására. Ehhez felírjuk d-re is a cosinus tételt.

$$d^2 = R_1^2 + (R_2 + h)^2 - 2R_1^2(R_2 + h)\cos\gamma$$

Ezt a képletet a *zenit* szögnél γ = *latitude*-ként, az *azimutnál* pedig γ = *longitude*-ként írjuk fel. Így megkapjuk "d" értékét mindkét esetben. Így már megoldható az előbbi képlet, melyet β-ra felírva az alábbi egyenletet kapjuk:

$$\cos\beta = \frac{R_1^2 + d^2 - (R_2 + h)^2}{2R_1 d}$$

Ezt a *latitude* és *longitude*-ból kapott 2 különböző "d"-vel behelyettesítve kapjuk meg a kívánt szögeket. Így tökéletesen meghatároztunk minden szükséget adatot, mely az OGS és a CubeSat helyzetét megadja.

Sok helyen használjuk a föld sugarát, ennek értéke viszont nem egy állandó. A Föld nem tökéletes gömb alakjából adódóan a pontos szimuláció érdekében minden vizsgált pontban szükséges kiszámolni a sugarat. Ehhez a következő képlet áll rendelkezésre: [9]

$$R_c = \frac{1}{\frac{cos^2\alpha}{M} + \frac{sin^2\alpha}{N}}$$

ahol

R_c = a Föld sugara a vizsgált pontban
α = azimuth szög, az északi sarktól mérve
M = meridional radius
N = prime vertical radius

Ehhez szükséges a meridional radius és a prime vertical radius meghatározása. A meridional radiust a következőképp számolhatjuk ki:

$$M(\varphi) = \frac{(ab)^2}{[(a\cos\varphi)^2 + (b\sin\varphi)^2]^{\frac{3}{2}}}$$

ahol

a = egyenlítői sugár = semi-major axis = 6,378,137 m
b = sarkokon mért sugár = semi-minor axis = 6,356,752.3 m
φ = szélességi fok = latitude

A prime vertical radius pedig a következő képlet alapján adhatjuk meg:

$$N(\varphi) = \frac{a^2}{\sqrt{(a\cos\varphi)^2 + (b\sin\varphi)^2}}$$

ahol

a = egyenlítői sugár = semi-major axis = 6,378,137 m
b = sarkokon mért sugár = semi-minor axis = 6,356,752.3 m
φ = szélességi fok = latitude

Ezeket a képleteket használva megfelelő pontossággal tudjuk megadni a Föld sugarát.

3. Az optikai csatorna modellezése

3.1. A csatorna felépítése

Az optikai vevőállomást (OGS) és a műholdat egy optikai csatorna köti össze, azaz egy fotonsugár. Így szükségünk van egy olyan fotonforrásra, mely "egyfoton" forrás, azaz ideálisan egyetlen fotont sugároz ki egy impulzusra. Két különböző konfiguráció jöhet szóba: a lézer a OGS-en, vagy a CubeSat-en van elhelyezve. Számunkra a műholdon elhelyezett fotonforrás a kedvezőbb, mert ilyenkor később jelentkezik a földi atmoszféra által létrejövő veszteség, pl.: nyalábszélesedés, elnyelődés, stb… Ezáltal erősebb lesz az optikai kapcsolat, mely számunkra nagyon fontos.

Sok tényezőt kell számításba vennünk, amelyek befolyásolják az optikai kapcsolatot. Bár a szabadtéren haladó fotonok polaritásukat nagy eséllyel megtartják, viszont sok más zavar léphet fel. Az alapvető nyalábszélesedés, elnyelődés a légkörben, turbulancia, az időjárás okozta zavarok, illetve a napból érkező fotonok, melyeket fals pozitívként érzékel a detektor, és még sok más. Ezek modellezésére a BME-n már megalkotott csatornamodellt használom [10] [11] [12] [13].

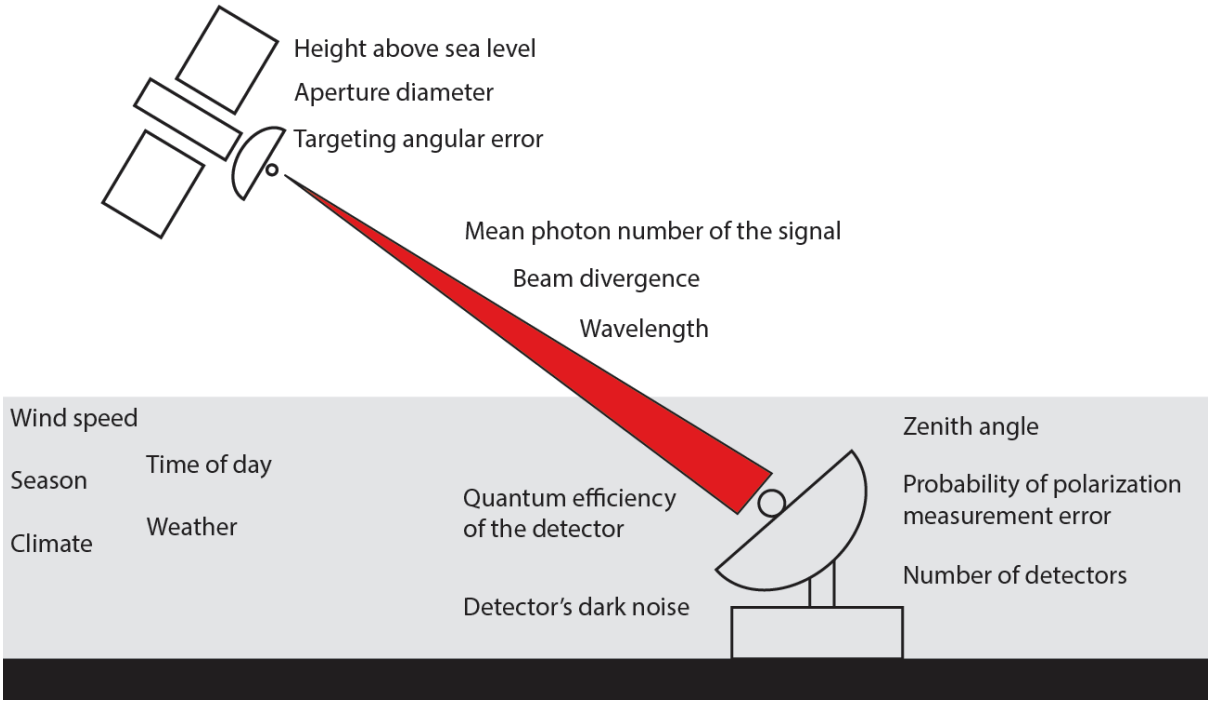

Figure 13 - Az optikai kapcsolatot befolyásoló tényezők.

3.2. A csatornamodell

A szabadtéri fotonnyalábok teljesítménye csökken az optikai út során fellépő csillapítások és fizikai jelenségek által. Először a nyalábszélesedést fogjuk meghatározni. Ha a lézersugarunkat egy Gauss-nyalábbal közelítjuk, akkor a diffrakció általi nyalábszéledését a következőképp írhatjuk fel:

$$\rho = \sqrt{\frac{4L^2}{k^2D^2} + \frac{D^2}{4}\left(1 - \frac{L}{F}\right)^2 + \frac{4L^2}{(k\rho_o)^2}}$$

ahol

ρ = nyalábszélesedés
L = az optikai csatorna hossza
k = a lézer hullámszáma
F = a fókusztávolság, a mi esetünkben végtelennek tekinthető
D = a kezdeti nyalábátmérő = Alice teleszkópjának átmérője
ρ_o = koherenciahossz

A hullámszám könnyen megadható:

$$k = \frac{2\pi}{\lambda}$$

ahol

λ = a fotonsugár hullámhossza = $8.08 \cdot 10^{-9}$ m

Ebből a koherenciahosszat a következő képpen írhatjuk fel:

$$\rho_o = \left[1.46k^2 \int_0^L C_n^2(z)\left(1 - \frac{z}{L}\right)^{\frac{5}{3}}\right]^{-\frac{3}{5}}$$

ahol

ρ_o = koherenciahossz
k = a lézer hullámszáma
z = optikai csatorna hossza km-ben
$C_n(z)$ = turbulencia

Ezt az integrált egy szummával tudjuk közelíteni. Ehhez bizonyos magasságonként rétegekre osztjuk az atmoszférát, és ezeket a rétegeket fogjuk összegezni. Tehát a gyakorlatban az alábbi képlettel közelítjük a koherenciahosszt:

$$\rho_o = \left[1.46k^2 \sum_i \frac{C_n^2(h_i)\left(1-\frac{z_i}{L}\right)^{\frac{5}{3}} + C_n^2(h_{i+1})\left(1-\frac{z_{i+1}}{L}\right)^{\frac{5}{3}}}{2} |z_{i+1} - z_i| \right]^{-\frac{3}{5}}$$

ahol

h = a vizsgált magasság km-ben

Innen h-t a vizsgált rétegből megkapjuk, z-t pedig a következőképp számoljuk:

$$z_i = L - \frac{h_i}{\cos\varphi}$$

Már csak a C_n turbulanciát kell megadnunk, melyet a *Hufnagel-Valley 5/7* modellből számolhatunk ki az alábbi képlettel:

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

$$+ 2.7\cdot 10^{-16} exp\left(-\frac{h}{1500}\right) + A\, exp\left(-\frac{h}{100}\right)$$

ahol

h = magasság km-ben
W = szélsebesség = 21 m/s
A = turbulanciaerősség a földhöz közel = $1.7 * 10^{-14}$ $m^{-2/3}$

Így a nyalábszélesedést már pontosan ki tudjuk számolni. Ezt fel tudjuk használni annak meghatározására, hogy mekkora eséllyel érkezik meg egy foton a detektorra Bob oldalán. Ennek valószínűségi sűrűségfüggvénye egy Gauss függvény, aminek varianciája a következő:

$$\sigma_{spread}^2 = \rho^2 + \sigma_{point}^2$$

ahol

σ_{point} = célzási veszteség
ρ = nyalábszélesedés

A célzási veszteség a kisműholdon lévő ADCS-n, azaz Attitude Determination and Control System-en múlik, illetve az egyéb célzást segítő berendezéseken. Ennek értékét a következőképp adhatjuk meg:

$$\sigma_{point} = L \cdot \sigma_{angular}$$

ahol

L = az optikai út hossza
$\sigma_{angular}$ = a célzási szöghiba = 5

A célzási szög hibáját $5 \cdot 10^{-7}$ rad.-nak választottam, mert a mai CubeSat-en használatos technológiák kb. ilyen pontosságot biztosítanak.

Az esély, hogy egy foton eltalálja Bob detektorát megkapható, ha integráljuk a sűrűségfüggvényt a detektor felületére, mely a mi esetünkben egy kör alakú antenna. Ebből a következő összefüggést kapjuk:

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

ahol

τ_{spread} = transmittance (spread)
R_B = Bob detektorának sugara
σ_{spread} = veszteség/variancia

Ezt másnéven dinamikus veszteségnek is nevezzük.

Szabadtéri fotonsugaraknál nem elhanyagolható a levegőben lévő molekulák, anyagok általi elnyelődés illetve szóródás. Két esetet különböztetünk meg itt: molekuláris és aeroszol elnyelődést és szóródást. Ezen részecskék és anyagok a légkör adott magasságaiban különböző mértékben vannak jelen, így célszerű itt is rétegre bontani az atmoszférát. Így megint egy szummával tudjuk közelíteni ezen csillapítások értékét:

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

ahol

τ_{air} = levegő csillapítása (statikus veszteség)
s_i = i-edik réteg szórási együtthatója
a_i = i-edik réteg elnyelési együtthatója
ΔL_i = optikai út hossza az i-edik rétegben

A két együttható kiszámolására egy táblázatot [10] használok. A szórási együttható úgy áll elő, hogy összeadjuk a molekuláris és aeroszol szórást, az elnyelési együtthatóhoz pedig a molekuláris és aeroszol elnyelést kell összegeznünk. Ezen értékek függnek az adott időjárástól és évszaktól. A táblázatban időjárás szerint külön oszlopban szerepelnek. Az itt megkapott veszteséget statikus veszteségnek is nevezzük.

Most már meg tudjuk adni az átbocsátó képességet (transmittance), mely egyszerűen csak a két résztranszmittancia szorzata.

$$\tau_{link} = \tau_{air} \cdot \tau_{spread}$$

3.3. QBER és bitrate

A BB84 protokoll egyik legfontosabb eleme, hogy megadjuk az átvitelhez tartozó QBER-t, azaz Quantum Bit Error Rate-et. Ezen érték reprezentálja, hogy mennyire zajos a csatorna, és egyben megadja, hogy működőképes lehet-e a csatorna kvantumos titkosítás szempontjából. Ahhoz, hogy egy támadót észlelhessünk a rendszerben, a **QBER szintet 11% alatt kell tartanunk**, így a szimulációk során is ezt a küszöbértéket használom.

A QBER értékének meghatározására a következő képletet használhatjuk:

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

ahol

p_{pol} = rossz detektorra való érkezés, azaz hibás polarizáció esélye = 10^{-4}
p_{dark} = egy "dark count" beütés
n = detektorok száma = 4
τ_{link} = transmittance
η = fotont tartalmazó pulzusok aránya = 0.1
μ = a detector kvantumos hatásfoka = 0.7

Ehhez szükségünk van p_{dark} értékére. Ez az érték annak az esélyét határozza meg, hogy hány olyan foton becsapódását érzékeljük, mely nem a műholdról származik, és így zajnak minősül. Ezen háttérzaj meghatározásával sok tudományos kutatás is foglalkozott, de ezek által becsült értéke elég széles tartományban mozog. A kutatások közül kiválasztottam egy olyan eredményt, mely inkább nagyobb zajt feltételez, ezzel felkészülve a "worst case scenario"-ra. Így a szimuláció során **$2.104 \cdot 10^4$ beütés/másodpercre** állítottam ezt az értéket. Erre felírhatjuk a következőt egy Poisson eloszlást feltételezve:

$$E = R_{beüt} \cdot T_{ablak}$$

ahol

$R_{beüt}$ = beütések száma másodpercenként
T_{ablak} = a detektorra jellemző időablak = 10^{-8} másodperc
E = az eloszlás várható értéke

Ezt a várható értéket valószínűséggé alakítani szerencsére a mi esetünkben könnyű, mert olyan esetekkel foglalkozunk, ahol E << 1, mert csak ilyenkor végezhető mérés. Ilyen esetekben a P_{dark} valószínűség kb. megegyezik a várható értékkel, azaz:

$$p_{dark} = E$$

Így a szimuláció során $\mathbf{p_{dark} = 2.104 \cdot 10^{-4}}$ értékkel fogok számolni.

A QBER mellett szükség van a bitsebesség kiszámolására is. Ezt a következő képlet adja meg:

$$R_{distilled} = \frac{1}{2} \cdot f_{pulse} \cdot \mu \cdot \tau_{link} \cdot \eta$$

ahol

$R_{distilled}$ = bitrate (bit/s)

Az átvitt bitek még nem konkrét titkosítási kulcsot jelentenek. A BB84 protokoll ezeken a biteket több módosítást is elvégez, melyeket a bevezetésben részleteztem, egyet kivéve. A polarizációk egyeztetése és az ellenőrzőbitek eldobása után szükség van még egy privacy amplification-nek nevezett lépésre is. Ennek lényege, hogy a biteket elhasheljük, így tovább csökkentve az információt, amit egy támadó megszerezhetett. Ez általában 4n bitből n + delta bitet állít elő, ahol delta a hashfüggvénytől függ. Delta értéktől most eltekintünk. Összességében ezen transzformációk miatt **az előállított kulcs hossza az átvitt bitek hosszának kb. 16-a lesz.**

A következő fejezetben ezen eredmények pontos kiszámolását és elemzését fogom elvégezni különböző konfigurációkkal.

4. Szimuláció

4.1. Konfiguráció

A szimuláció során számos olyan paraméter van, mely nagyban befolyásolja az eredményeket, és értéke nem egy állandó. Ide tartozik az adó és vevő teleszkópjának átmérője, a célzási szöghiba, az aktuális időjárás okozta csillapítás, illetve a földi vevőállomás helye. Ezen paraméterek több szóbajöhető értékét fogom most taglalni, ezek függését bemutatni, és ezután kiválasztani a legmegfelelőbbet, mellyet majd a végleges szimuláció során használok.

Az időjárás egy nagyon fontos tényező a szabadtéri optikai csatornáknál. A levegő összetétele nagy mértékben befolyásolja annak csillapító hatását. A kísérlet során két időjárástípust fogok megkülönböztetni, a tiszta (*clear)* és a számunkra nagyon kedvezőtlen ködös *(hazy)* időjárást. Emellett három évszakot is megkülönböztetek, a lehetséges opciók pedig a nyár (*summer*), a tél (*winter),* és bár nem évszak, de a trópust (*tropical*) is elkülönítem.

Az évszakok nagyon keveset befolyásolnak az eredményen. Lefuttatva a szimulációt a három különböző esetre (tropical, summer, winter) 1 éves időtartammal:

Tropical	= 183,996,968 átvitt bit	= 11.5 Mb-nyi kulcs
Summer	= 183,941,401 átvitt bit	= 11.5 Mb-nyi kulcs
Winter	= 183,928,538 átvitt bit	= 11.5 Mb-nyi kulcs

Mint látható, összesen **1 év alatt 68,430 bitet** változik az eredmény. Ez az érték olyan kevés, hogy a **szimuláció további részében ezen paramétert egyszerűen nyárra (summer) állítom**, mert nem befolyásolja nagyban az eredményeket.

Sokkal inkább számít számunkra az időjárás. Ezen értékeket szemléltetve egy grafikonon látható, hogy a QBER számottevően csökken, ezzel együtt az átvitt bitek értéke, ha az időjárás ködös (*hazy*).

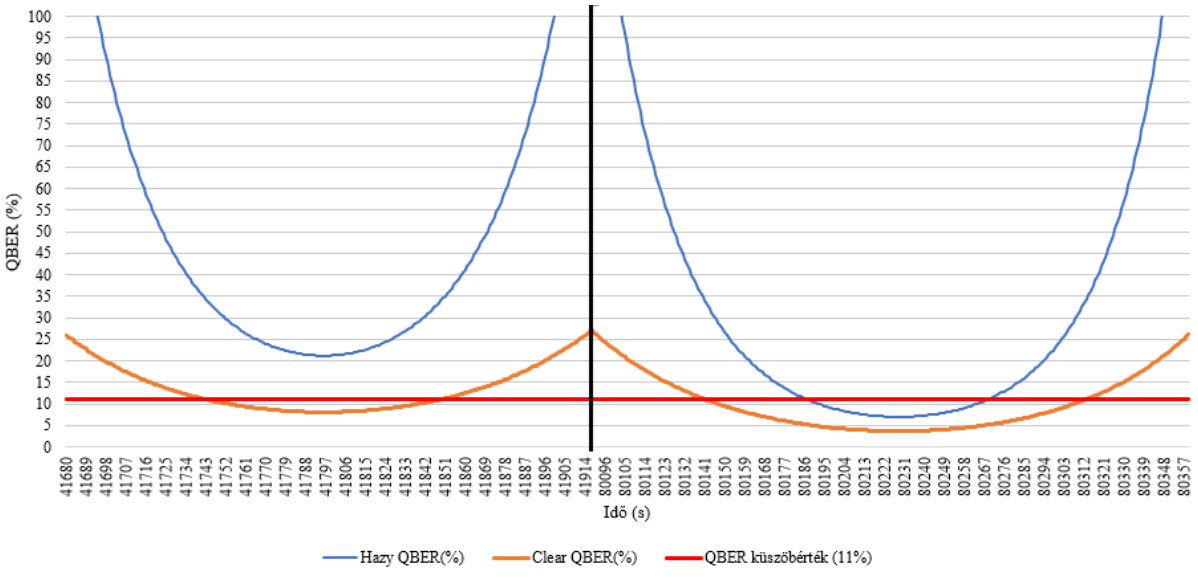

Figure 14 - QBER alakulása tiszta és ködös időjárás esetén egy nap alatt.

A grafikon egy napnyi (86400 másodperc) szimulációt ábrázol. **Csak azon eredmények láthatók az ábrán, melyeknél a műhold maximum 70°-os zenith szöget zárt be a vevőállomással**. Ez kétszer történt meg, a 41800-adik másodperc (kb. 11 óra 36 perc) és a 80250-adik másodperc (22 óra 20 perc körül) körül. Megemlítendő, hogy a rossz időjárási körülmények mellett az első időszaknál nem csökkent le annyira a QBER (11% alá, ezt a piros vonal jelzi), hogy megbízható kapcsolat jöhessen létre. Egyértelműen leolvasható a grafikonról, hogy nagy mértékben függ a kulcsszétosztás az időjárástól:

Clear (tiszta):
Legjobb QBER = 3.73932%
átvitt bitek száma = 912.4 Kb

Hazy (ködös):
Legjobb QBER = 7.04113%
átvitt bitek száma = 209,2 Kb

Az itt 1 nap alatt mért 700 Kb különbség egy év alatt 146 Mb fölé emelkedik. Ekkor kb. 184 Mb helyett csak kb. 37 Mb-ot tudunk átküldeni. Ez 9 Mb-os végleges kulcshossz különbséget jelent. Ezek alapján egyértelműen megállapítható, hogy az időjárás fontos befolyásoló tényező. **Későbbi szimulációim során tiszta (*clear*) időjárást feltételezek**, mely egy optimista becslés, de megvalósíthatóság szempontjából megengedhető.

A teleszkópméret szintén hatalmas befolyással bír a kulcsszétosztás sikerességére. Három földi vevőállomást feltételezek és használok a szimuláció során: egyet Budapesten, egyet Grazban és egyet Tenerifén. Ebből az utóbbi kettő állomás létezik, Budapesten csak feltételezem, hogy van egy ilyen állomás a BME E épület tetején.

Tenerifén található az ESA Optical Ground Station [14], melynek átmérője 1 méter. Grázban pedig az ASA Astro Systeme Austria található, ahova egy 0.8 méter átmérőjű optikai vevőállomást telepítettek. [15] [16] Magyarországon elméletben egy 0.5 méter átmérőjű teleszkópot terveznek, de ez még nagyon gyerekcipőben jár. Ezeket az értékeket nem az adott országban lévő vevőállomás koordinátáival fogom kiszámolni, ehelyett Budapesten fogok feltételezni egy 1, egy 0.8, és egy 0.5 méteres optikai vevőállomást. Ezáltal a OGS elhelyezkedése nem szól bele az eredményekbe.

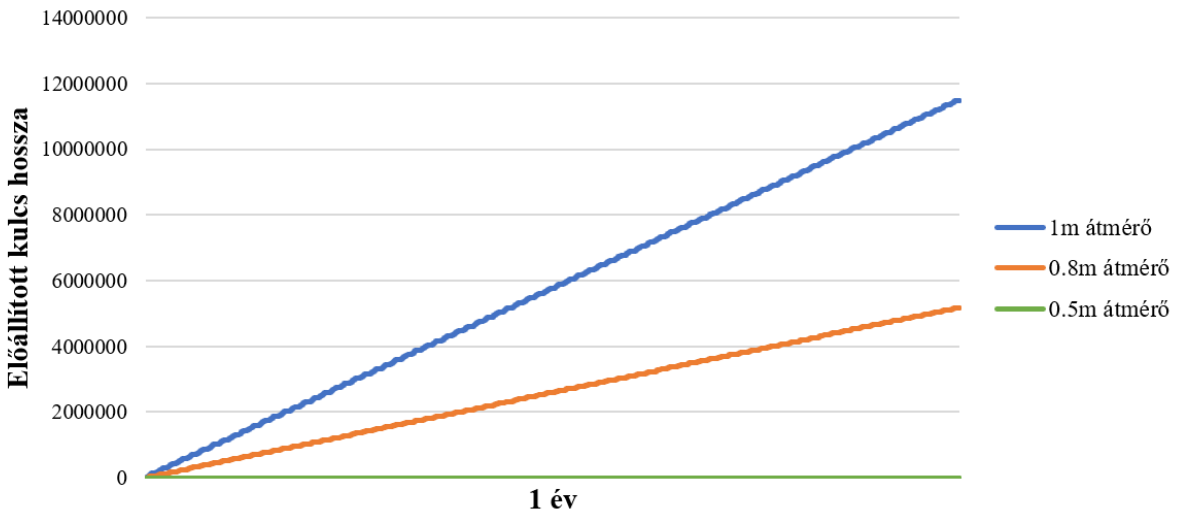

Figure 15 – Az 1 év alatt előállított kulcs hosszúsága az OGS teleszkópátmérőjének függvényében.

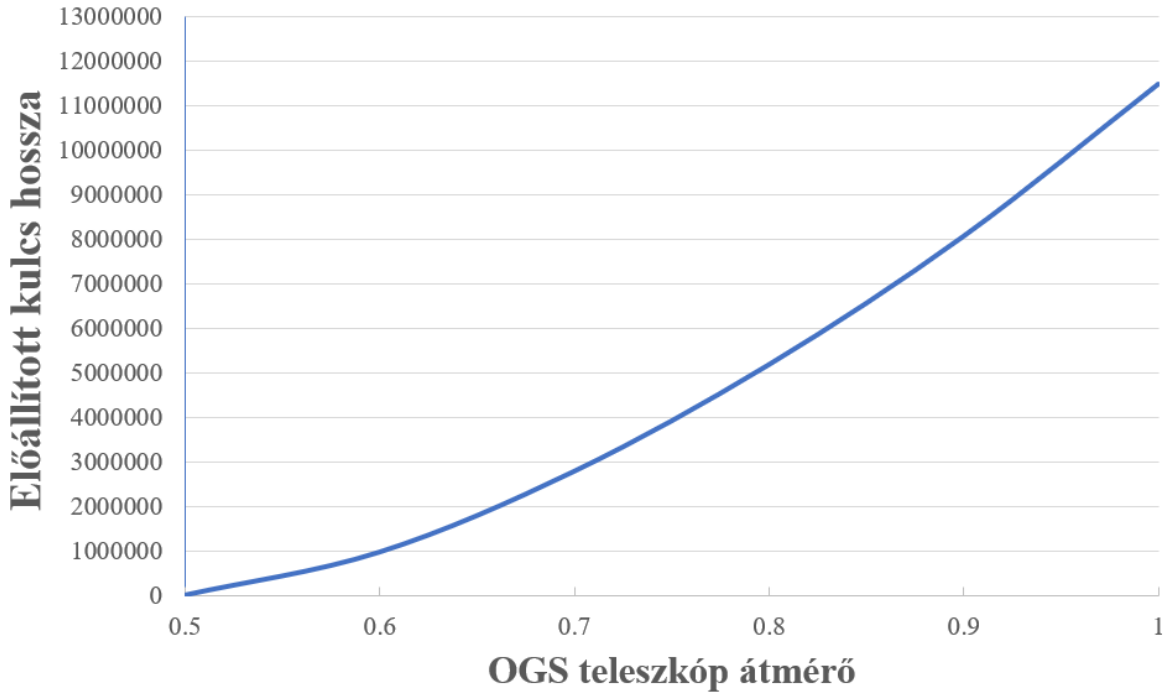

Figure 16 – Az előállított kulcs hosszának függése az OGS-en található teleszkóp átmérőjétől, 1 évre levetítve.

Bár most az átvitt kulcs hosszát jelenítettem meg, természetesen ez is a QBER értékétől függ (igazából a tranzmittanciától, amitől a QBER is függ), de ezt egy évre ábrázolni nem igazán lehetséges, ezért választottam az előállított kulcs hosszát.

Látható, hogy egy év alatt 1 méteres teleszkópméreten majdnem 12 Mb-et tudunk átvinni, amíg 0.8 méteresnél ez az érték már épp csak 5 Mb körül van, és 0-ra csökken, ha az átmérő 0.5 méteres.

Ahogy az időjárásnál is kiválasztottam egy alapértelmezett értéket, itt is megteszem: **ezentúl a szimuláció során 1 méteres teleszkópot fogok feltételezni minden vevőállomáson**. Ezt Tenerife mutatja, hogy létezhet ilyen OGS, és ez számomra elég megvalósíthatóság szempontjából.

Még egy fontos tényező a kisműholdon található teleszkóp átmérője, mely a kiküldött fotonnyaláb kezdeti átmérője is egyben. Ennek minimális és maximális értékét maga a CubeSat szabvány adja meg. A legkisebb ilyen pikoműholdak is legalább 10x10x10 centiméteresek, így a teleszkóp mérete legrosszabb esetben is 0.1 méter lehet. A maximumot 12 U-nál tudjuk elérni, mely egy 30x20x20 cm-es méretet határoz meg. Ezen egy 20x20-as oldalt kihasználva ide már egy 0.2 méter átmérőjű teleszkópot is használhatunk, és ezt a szimuláció során feltételezett 6 U-os mérettel is megtehetjük.

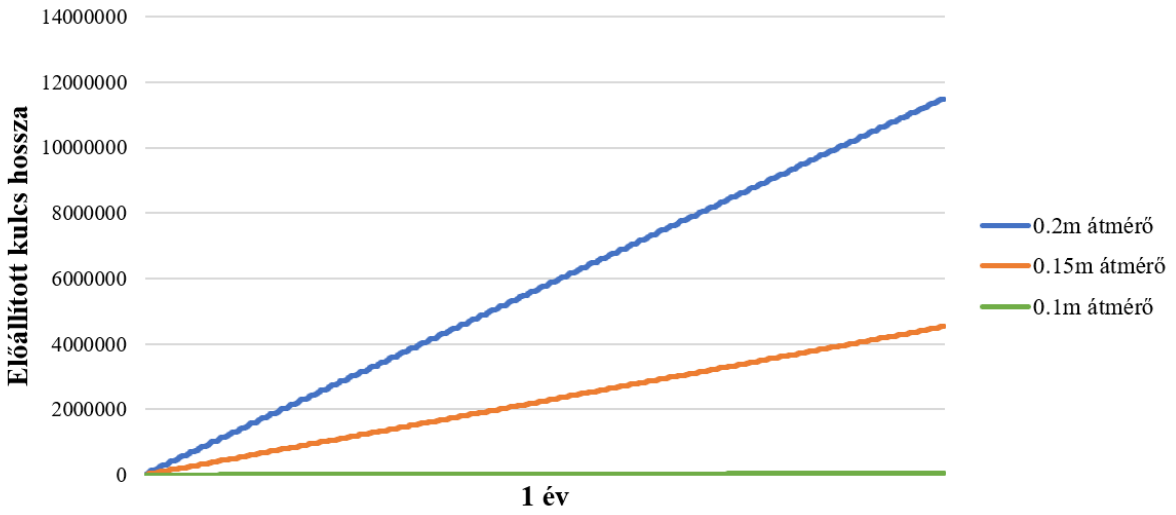

Figure 17 – Az 1 év alatt előállított kulcs hosszúsága a CubeSat-en található teleszkóp átmérőjének függvényében.

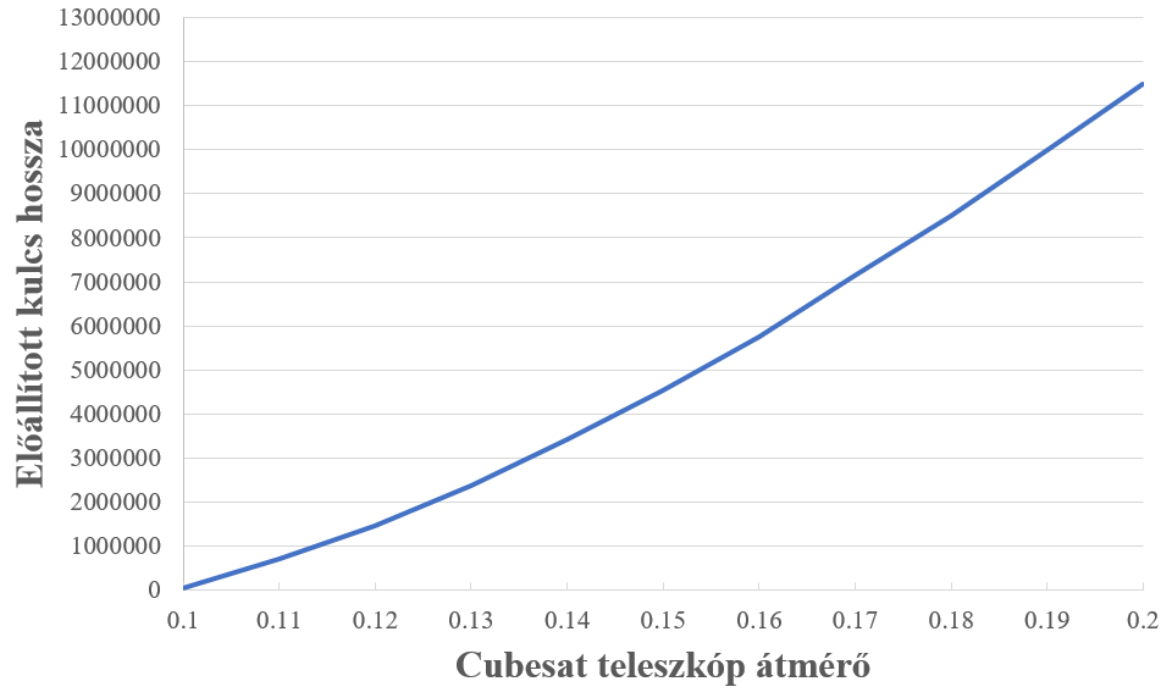

Figure 18 – Az előállított kulcs hosszának függése a CubeSat-en található teleszkóp átmérőjétől, 1 évre levetítve.

Itt is hasonló eredményeket láthatunk, mint az OGS-eknél. A legkisebb átmérőjű teleszkóp ebben az esetben sikeresen átvitt biteket, de több nagyságrenddel is elmarad a nagyobb teleszkóptól.

Itt is követem az eddigi eljárást, **és a szimuláció során a legjobb, 0.2 méteres antennával** fogok számolni.

Az utolsó paraméter, mellyel külön foglalkozom, a célzási veszteség. Ennek értékét egyrészt a CubeSat-en használt ADCS, azaz Attitude Determination and Control System pontossága határozza meg, melyek fizikai paraméterei egyre nagyobb ütemben fejlődnek. Jelenleg az elérhető ilyen eszközök pontossága szögmásodperces tartományban mozog (µrad tartomány). Ráadásul értéke tovább csökkenthető, ha a pikoműholdra egy nagyobb teljesítményű lézert telepítünk, amely adott időrésekben pozíciómeghatározást és iránykorrektálást, illetve szinkronizációt végez.

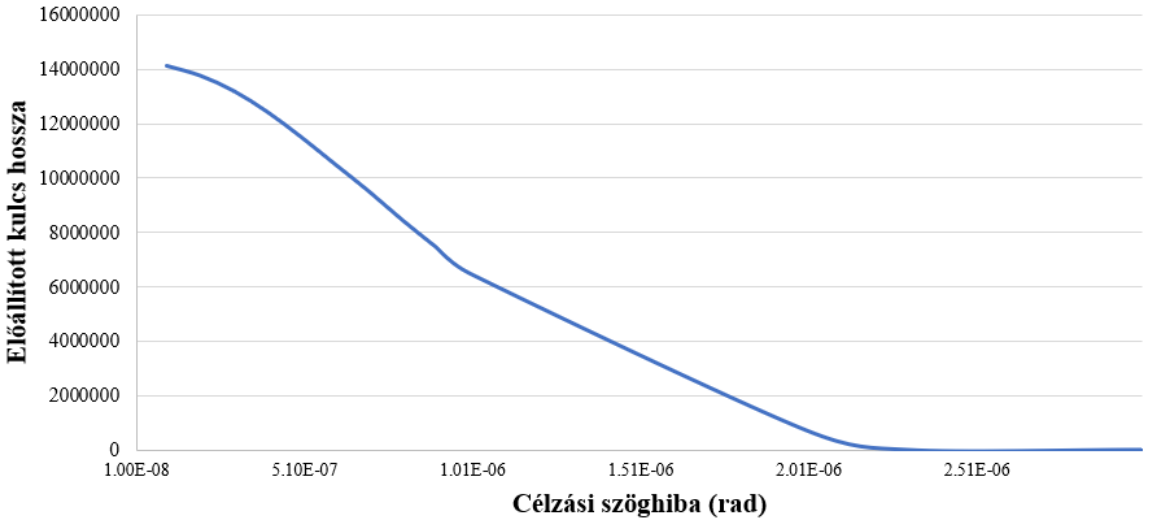

Figure 19 – Az előállított kulcs hosszának függése a célzási szöghibától, 1 évre levetítve.

A grafikonról is leolvasható, hogy ha a célzási szöghiba $2 \cdot 10^{-6}$ fölé megy, akkor már nem létesíthető olyan jó kapcsolat a vevőállomás és a műhold közt, amely alkalmas lenne a kvantumos kulcsszétosztásra. **Ezen kísérlet további részében $5 \cdot 10^{-7}$-es szöghibát fogok használni**, mely biztosan elérhető lesz a közeljövőben, mire esetlegesen elkezdődne egy ilyen pikoműhold fizikai megvalósítása.

Fontos, hogy a paraméterek függésének szimulációja során a többi függő paraméter értékét arra állítottam, amit később a szimulációban is használni fogok.

4.2. A szimulátor bemutatása

Az modellt egy C++ nyelven írt programmal szimulálom. Azért választottam ezt a nyelvet, mert így hatékony és gyors kódot írhattam, mellyel képes vagyok pár másodperc alatt leszimulálni egy egész éves műholdkeringést, másodperces mintavételezési idővel. A program a C++ 17-es szabványával készült, és csak a Standard Libraryt használja.

A program konzolos felülettel rendelkezik, és két helyen képes kimenetet generálni. Alapvetően a konzolablakban figyelhető a szimuláció menete, és az, hogy éppen hol tart. Amikor végez, leolvasható a hasznos idő, mely azt jelöli, hogy mennyi ideig volt a QBER 11% alatt, azaz mennyi ideig történt kulcsszétosztás. Emellett látható az átvitt bitek mennyisége, az adatátvitel sebessége byte/s-ben, illetve az előállított kulcs hossza bit-ben.

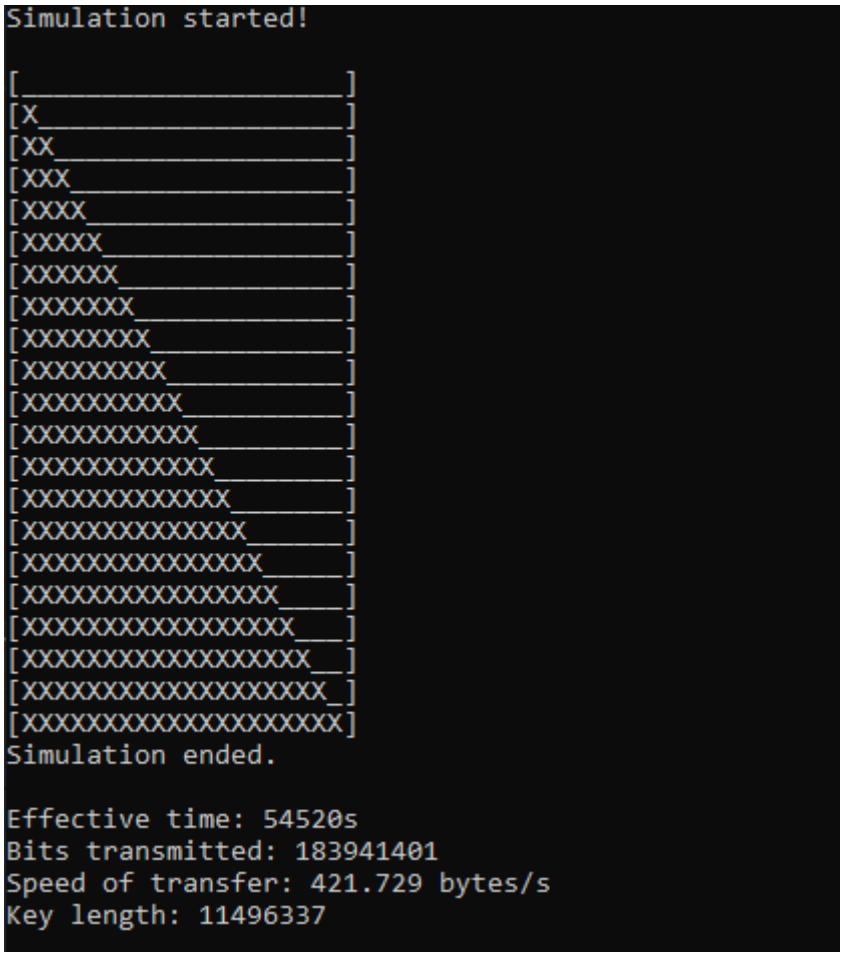

Figure 20 – A szimulátor kimenete egy éves szimuláció után.

Beállítható, hogy a konzolablakban a szimuláció során írja ki az aktuális értékeket minden időintervallumban. Ez segít a köztes események és részeredmények vizsgálatában.

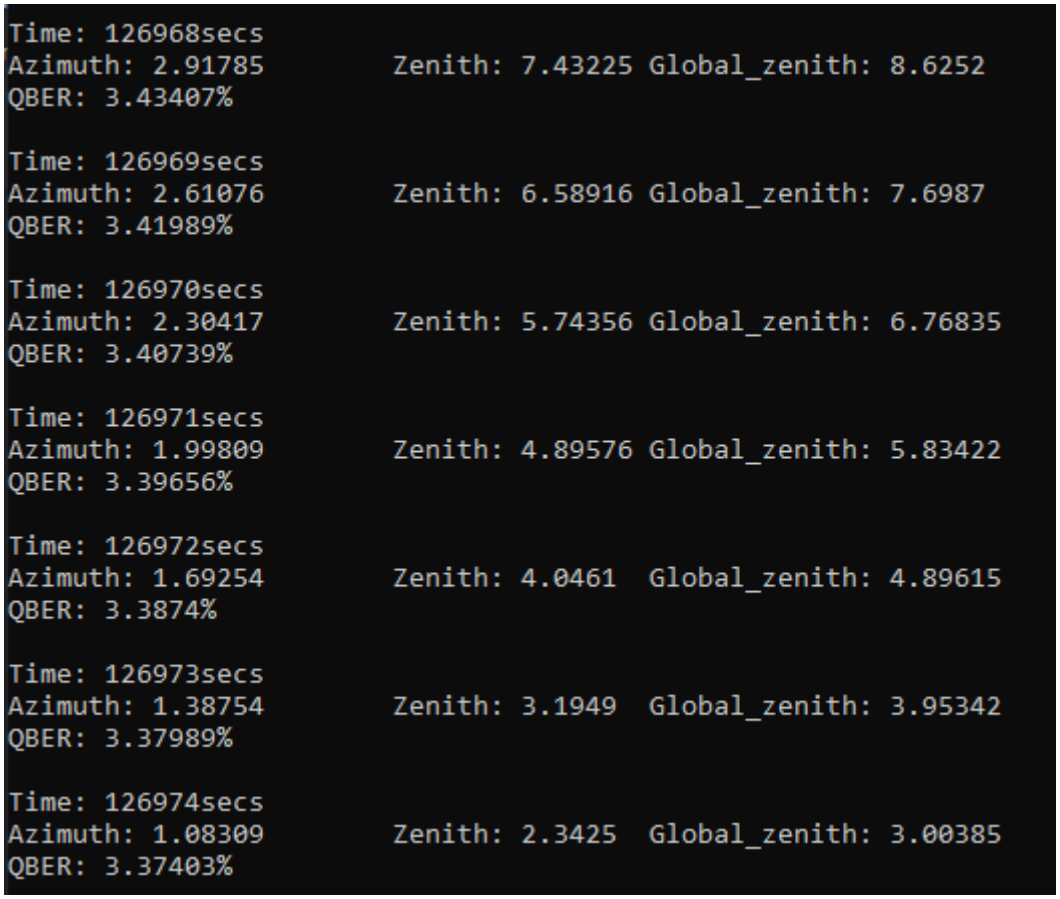

Figure 21 – Egy pillanatkép a szimulációról. A kisműhold éppen elhalad majdnem tökéletesen a vevőállomás fölött. A valódi zenit szög itt Global_zenith néven szerepel.

Fontos, hogy a program csak akkor ír ki részeredményt, ha a zenit szög kisebb, mint 70º. Ezen érték felett nincs értélme elvégezni a számolásokat, mert a műhold nem lát rá a földi vevőállomásra. Ha az elkövetkező adatok közt egy ugrás található az időben, az emiatt történt.

Ezen a képen látható, ahogy másodpercenként változik a bezárt szög, azaz változik a műhold pozíciója. Megtévesztő lehet, de itt az azimut és zenit szögek igazából a hosszanti és szélességi körök tengelyén az OGS-el bezárt szöget jelölik. Az "igazi" zenit szög a Global_zenith, melyet az előző két komponensből számolok.

Emellett leolvasható az aktuális QBER, mely kedvező, 3.4%-os érték. Ez azt jelenti, hogy ebben az esetben a szimuláció kezdete után kb. 35 órával éppen működőképes a titkosítás.

Ez még mindig nehezen kezelhető lenne modellezés és kiértékelés szempontjából, ezért a szimulátor képes egy szöveges file-ba írni egy részletesebb kimenetet is. Ezt használtam a kutatás során az adatok megjelenítésére is, Excellel feldolgozva.

Elapsed Time (secs)	Zenith (degrees)	Transmittance	QBER (%)	Transmitted Bits	Key length
41848	57.4729	0.0547622	10.9873	241199	15074
41849	57.6641	0.0541947	11.1023	243115	15194
41850	57.8562	0.0536264	11.2198	243115	15194
41851	58.049	0.0530576	11.34	243115	15194
41852	58.2425	0.0524886	11.4628	243115	15194
41853	58.4367	0.0519197	11.5883	243115	15194
41854	58.6315	0.0513512	11.7165	243115	15194
41855	58.8267	0.0507832	11.8474	243115	15194
41856	59.0223	0.0502161	11.9811	243115	15194
41857	59.2182	0.04965	12.1176	243115	15194
41858	59.4145	0.0490853	12.2569	243115	15194
41859	59.6109	0.0485221	12.3991	243115	15194
41860	59.8075	0.0479606	12.5441	243115	15194
41861	60.0042	0.047401	12.6921	243115	15194
41862	60.2009	0.0468436	12.843	243115	15194
41863	60.3976	0.0462884	12.9969	243115	15194
41864	60.5942	0.0457358	13.1538	243115	15194
41865	60.7907	0.0451857	13.3138	243115	15194
41866	60.987	0.0446385	13.4769	243115	15194
41867	61.1831	0.0440942	13.6431	243115	15194
41868	61.3789	0.043553	13.8126	243115	15194
41869	61.5745	0.043015	13.9852	243115	15194
41870	61.7697	0.0424804	14.1611	243115	15194
41871	61.9644	0.0419492	14.3403	243115	15194

Figure 22 – A szimuláció kimenete Excel-ben.

Emellett még egy fontos funkciója van a programnak. Képes egyszerre bárhány földi vevőállomás párhuzamos kezelésére. Koordinátákkal megadható a föld bármely részén saját paraméterekkel rendelkező OGS, melyet módosítás nélkül tud használni. Több vevőállomás esetében a szimulátor kiszámolja, a műhold melyik állomással tudja a legjobb optikai csatornát kialakítani, és ezzel fog csak kommunikálni. Ezáltal modellezhető egy kvantumos kisműhold, mely három különböző állomással is kommikálhat priorizálásos alapon, és a végén megkapjuk állomásonként az előállított kulcs hosszát.

Elapsed Time (secs)	OGS Name	Zenith (degrees)	Transmittance	QBER (%)	Transmitted Bits	Key length
20850	Budapest	68.2431	0.0268996	22.3576	0	0
20860	Budapest	64.5479	0.0358657	16.7709	0	0
20870	Budapest	60.563	0.0465619	12.9206	0	0
20880	Budapest	56.5906	0.0580572	10.3643	20320	1270
20890	Budapest	53.2652	0.0681075	8.83638	44157	2759
20900	Budapest	51.4822	0.0735211	8.18646	69889	4368
20910	Budapest	51.8864	0.0720732	8.35072	95114	5944
20920	Budapest	54.2902	0.0644547	9.33659	117673	7354
20930	Budapest	57.8562	0.0536264	11.2198	117673	7354
20940	Budapest	61.7697	0.0424804	14.1611	117673	7354
20950	Budapest	65.5523	0.0326234	18.4367	117673	7354
20960	Budapest	69.0067	0.0245513	24.4952	117673	7354
23840	Tenerife	68.5827	0.0260808	23.0592	0	0
23850	Tenerife	64.019	0.0371261	16.2019	0	0
23860	Tenerife	58.2982	0.0528689	11.3805	0	0
23870	Tenerife	50.9777	0.0750638	8.01843	26272	1642
23880	Tenerife	41.5776	0.104522	5.76138	62854	3928
23890	Tenerife	30.1215	0.137435	4.38402	110956	6934
23900	Tenerife	19.4987	0.160954	3.74488	167289	10455
23910	Tenerife	19.7939	0.159958	3.76812	223274	13954
23920	Tenerife	30.4099	0.135521	4.44579	270706	16919
23930	Tenerife	41.5662	0.103072	5.84227	306781	19173
23940	Tenerife	50.7142	0.0743886	8.09111	332817	20801
23950	Tenerife	57.8694	0.0527664	11.4025	332817	20801
23960	Tenerife	63.4854	0.0373686	16.0968	332817	20801
23970	Tenerife	67.9801	0.0265198	22.6777	332817	20801
40050	Budapest	69.9065	0.0222232	27.0603	117673	7354

Figure 23 – Két OGS-el (Budapest és Tenerife) felváltva kommunikáló műhold szimulációjának részlete.

Ezen a szimuláción látható, hogy a 20850-edik percben a műholdnak sikerült közel kerülnie a budapesti vevőállomáshoz, majd sikeresen átvitt 7354 bitnyi kulcsot. Ezután kb. 3000 másodperccel később közel ért a tenerifei állomáshoz, és ezzel 20801 bit kulcsot állított elő. Jelen esetben az állomások feletti áthaladások közt sok idő telt el, de elméletben előfordulhat, hogy egy adott időrés után egyből átvált a másik állomásra, mert erősebb lett a jel.

A végleges szimuláció során a most említett konfigurációt fogom használni, azaz Budapest és Tenerife közt zajló kvantumos kulcsszétosztást, illetve modellezek egy OGS-ek közti versenyhelyzetet is Graz bevezetésével.

4.3. Eredmények

A végleges szimulációban Budapest és Tenerife között fogok modellezni egy 500 km magas SSO pályán keringő 6 Unitos CubeSat-et egy éves keringési idővel. Meghatározom az előállított bitek mennyiségét, a kulcs hosszát, modellezem a QBER-t, és a pályát. Később Grazot is beveszem a vevőállomások közé. **A szimuláció során a mintavételezési frekvencia 1 minta/másodperc.**

SSO pályán mozgó kisműhold hosszúsági (longitude) és szélességi (latitude) szögeinek változását mutatja be az alábbi ábra. Ezen egy periódust ábrázolok csak, mert egy év alatt ezen értékek túl sokat változnának.

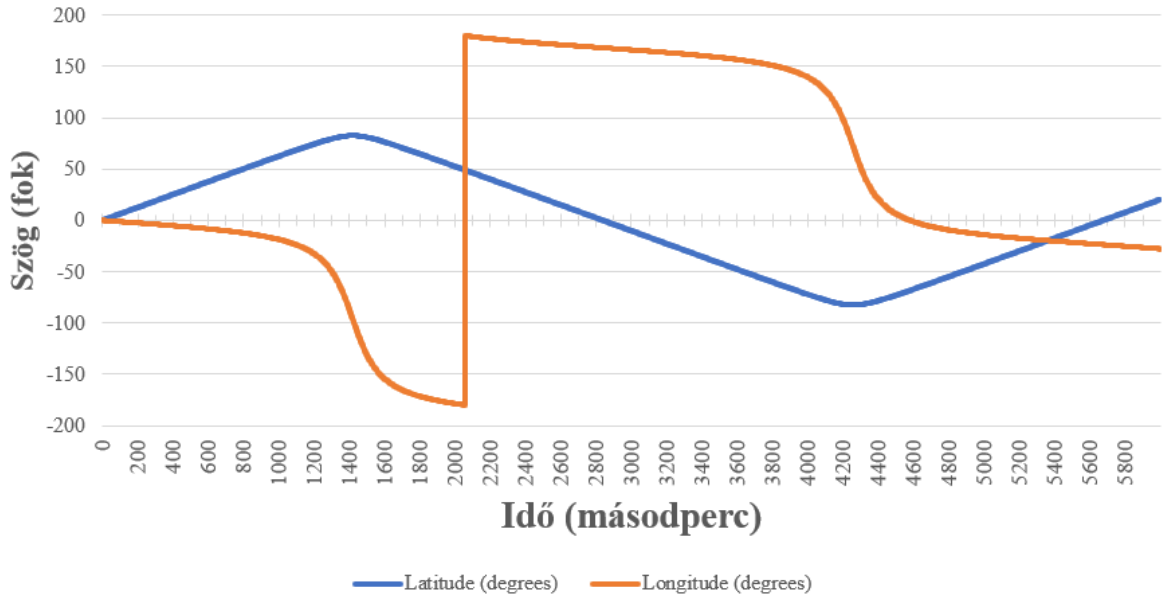

Figure 24 - Egy periódus alatt a kisműhold hosszúsági és szélességi koordinátáinak változása.

Látható, hogy a hosszúsági és a szélességi fok nem a 0-ban metszi egymást egy periódus után. Ez a föld forgásának tudható be. A periódusidő a korábbi számolásaim alapján 5624.3s, és ennél az időpillanatnál kb. -25° olvasható le a grafikonról. A föld ennyi idő alatt 360° / (5624s / 86400s) = 23.43°-ot forgott, ami egyezik az ábrán látottakkal. Az ugrás a narancssárga vonalban -180°-ról +180°-ra azért történik, mert hosszúsági koordinátáknál a -180° és a +180° ugyanazt a sávot jelöli, csak az változik, melyik irányból "kerüljük" a Földet. Ennek az ugrásnak alapvetően a periódus felénél kellene megtörténnie és a Föld forgása miatt tolódott el balra.

A transzmittancia alakulását, csak úgy mint az előbbi adatokat, egy éves viszonylatban nem lehetne reprezentálni, mert nagyon gyorsan változik az értéke, Ennek alakulását ezért egy áthaladás alatt fogom bemutatni. Mivel a QBER és a bitsebesség is erőteljesen függ a transzmittanciától, így ezeket is bemutatom egy tetszőleges áthaladás alkalmával.

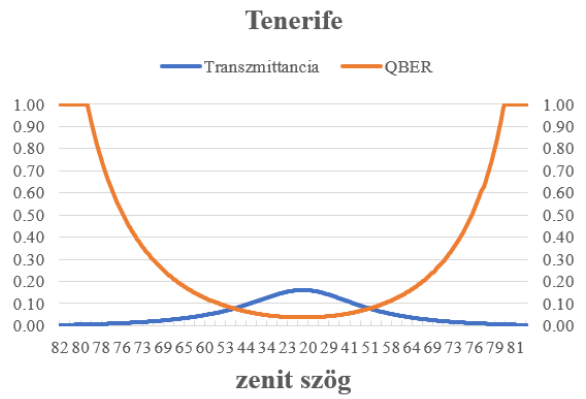

Figure 25 - A transzmittancia és QBER alakulása a zenit szög függvényében egy áthaladás során Tenerifén.

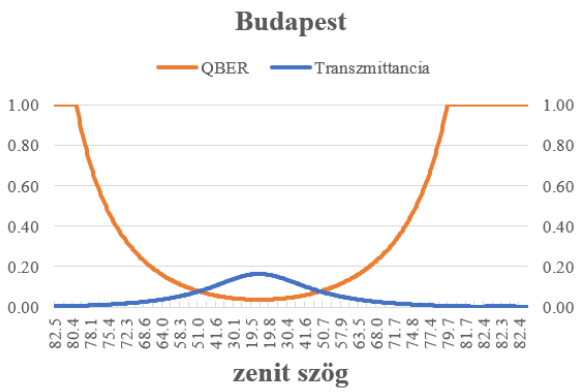

Figure 26 - A transzmittancia és QBER alakulása a zenit szög függvényében egy áthaladás során Budapesten.

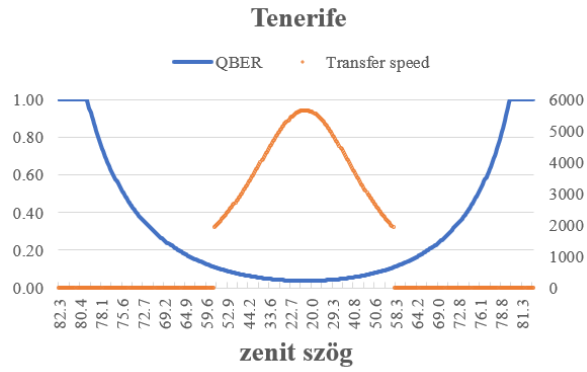

Figure 27 - A bitsebesség (bit/s) és QBER alakulása a zenit szög függvényében egy áthaladás során Tenerifén.

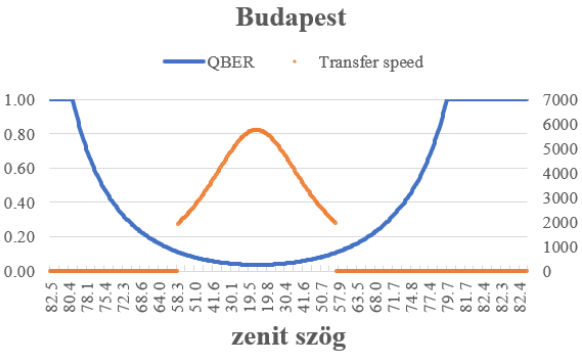

Figure 28 - A bitsebesség (bit/s) és QBER alakulása a zenit szög függvényében egy áthaladás során Budapesten.

A szimulált áthaladás zenit szöge jelen esetben nem csak 70°-ig, hanem magasabb értékekig is jelölve van, mert így látható a QBER 100%-ra növekedése. Az utóbbi kettő grafikonon látható, hogy kb. 59°-os zenit szögnél kezdődik meg a bitek megosztása. Ez stimmel a 11%-os QBER küszöbértékhez. A konfiguráció a zenit szögtől függően jelen esetben 2000 és 5800 bit/másodperc sebességgel ment, de tökéletes áthaladás (0-ás zenitszög) esetén ez az érték még magasabb.

A teljes, 1 éves szimuláció adatait nehéz reprezentálni, mert az idő nagyrészében nem történik kvantumos kulcsszétosztás, ezért erről grafikonok helyett csak konkrét eredményeket fogok adni. Lefuttatva a szimulációt 2 vevőállomásra a következő adatokat kaptam:

1. Szimuláció - Budapest, Tenerife

Eltelt idő = 31,536,000 másodperc = 1 év
Hasznos idő = 108,740 másodperc ≈ 30.2 óra
Átlagos kulcsbitsebesség ≈ 210.7 bit/s

Előállított kulcs hossza
Tenerife = 11,415,961 bit ≈ 11,4 Mb
Budapest = 11,498,612 bit ≈ 11,5 Mb

Ez alapján látható, hogy a két OGS-en kb. ugyanakkora kulcs állt elő. Ez leginkább annak köszönhető, hogy nem volt versenyhelyzet a két vevőállomás között, azaz nem létezik olyan pontja a műholdpályának, ahol a kisműhold mindkét állomással egyszerre tudna kommunikálni.

Amiatt, hogy olyan helyzet is előállhasson, hogy a kisműholdnak választania kelljen a vevőállomások közt, hozzáadtam az OGS-ek közé az Ausztriában található grazi vevőállomást is. Ekkor lefuttatva a szimulációt feltűnő a változás az eredményekben:

2. Szimuláció - Budapest, Graz, Tenerife

Eltelt idő = 31,536,000 másodperc = 1 év
Hasznos idő = 135,052 másodperc ≈ 37.5 óra
Átlagos kulcsbitsebesség ≈ 218 bit/s

Előállított kulcs hossza
Tenerife = 11,415,961 bit ≈ 11,4 Mb
Graz = 9,008,654 bit ≈ 9 Mb
Budapest = 9,008,008 bit ≈ 9 Mb

Látható, hogy Tenerifén sikerült ugyanakkora kulcsot előállítani, ebbe nem szólt bele a grazi vevőállomás, de Budapesten 2.5 Mb-el kisebb kulcs állt elő, mely egyértelműen a versenyhelyzet miatt van.

Ezen eredményeket a következő fejezetben összegzem.

5.Konklúzió

A szimuláció eredményei alapján biztonsággal kimondható, hogy a felhasznált kvantumtitkosítási modellel és az említett paraméterekkel a **kulcsszétosztás egy kisműhold és egy optikai vevőállomás között megvalósítható.** A mai technológia állása szerint olyan paraméterekkel rendelkező eszközök, mint amilyeneket feltételeztem a szimuláció alatt, már léteznek, vagy nagyon közel állnak a kívánt értékekhez. Bár nem végeztem méret, súly és energia (SwaP: Size, Weight and Power) analízist, ehhez hasonló kutatások [17, 18] alapján kijelenthető, hogy egy ilyen, vagy eggyel nagyobb (12 Unitos) kisműhold megtervezhető a CubeSat szabvány által felállított követelmények mellett.

Az eredmények alapján egy év alatt három vevőállomást használva majdnem 30 Mb-nyi kulcs előállítható. Bár ez kevés lenne a hétköznapi beszélgetéseink és böngészéseink titkosítására, de vannak területek, ahol ekkora kulcs is elegendő. Például bankok bizonyos összegű tranzakció felett kínálhatnak teljesen biztonságos átvitelt, így a nagy értékű utalásoknak elméletben nem lehet rizikófaktora a titkosítás miatt. Emellett használható fontos állami, katonai, stb.. információk kódolására, melyek kiszivárgása és feltörése hatalmas problémát és veszélyt jelenthetne egy egész országra vagy államra.

Beláttuk, hogy akár egy szomszédos országban való OGS sem rontja nagy mértékben a kulcs hosszát. Ez alapján "saját költség" nélkül beiktatható a titkosításba új vevőállomás, mellyel a hasznos időt növeljük, de más állomások nem szenvedek kárt. Ezt persze csak addig lehet, amíg az állomás távolsága megengedi, hogy minden OGS felett éjszaka haladjon át a műhold, mely limitálja az elérhető SSO pályák számát. Emellett lehetséges több kisműholdat is használni, melyek mindig máskor haladnak át az adott OGS-ek felett. Így létrehozható pl. egész Európa területén egy kvantumos titkosító hálózat, mely több vevőállomásból és műholdból áll. Ezekkel az előállított kulcsmennyiség nagy mértékben növelhető, és akár kereskedelmi használatba is kerülhet egy ilyen hálózat. A technológia rugalmasságának és bővíthetőségének köszönhetően elképzelhető, hogy a jövőben már az átlagemberek eszközei is ilyen titkosítást fognak használni, ezáltal elérhetővé téve mindenkinek a tökéletes adatbiztonságot.

Jelenleg is több kvantumos kulcsszétosztást megvalósító kisműhold van bejegyezve 2020 utáni indításra [19], ebből is látható, hogy ez a technológia éppen most kezd beindulni. Fejlődésének üteme rendkívül gyors, és egyre több egyetem és kutatócsoport dolgozik ilyen projekteken. Egyértelműen kijelenthető, hogy a kvantumos kulcsszétosztás egy meghatározó technológia lesz a kriptográfia terén, és emiatt a kvantumos műholdak használata is.

Irodalomjegyzék

[1] A. Dash, D. Sarmah, B. K. Behera and P. K. Panigrahi, “Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer,” 2018.

[2] U. o. S. a. T. o. China, “phys.org,” 19 01 2018. [Online]. Available: https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html. [Accessed 18 10 2019].

[3] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature,* vol. 299, pp. 802-803, 1982.

[4] “www.c3s.hu/,” C3S Kft, [Online]. Available: https://www.c3s.hu/hu/rolunk/. [Accessed 23 10 2019].

[5] R. J. Boain, “A-B-Cs of sun-synchronous orbit mission design,” 2005.

[6] J. B.-y. Tsui, Fundamentals of Global Positioning System Receivers: A Software Approach, 2000, pp. 46-50.

[7] K. E. f. A. P. o. t. M. Planets, “NASA,” 17 07 2018. [Online]. Available: https://ssd.jpl.nasa.gov/txt/aprx_pos_planets.pdf. [Accessed 23 10 2019].

[8] M. R. Schwarz, “Memorandum No. 1: Keplerian Orbit Elements −→ Cartesian State Vectors,” 5 10 2017. [Online]. Available: https://downloads.rene-schwarz.com/download/M001-Keplerian_Orbit_Elements_to_Cartesian_State_Vectors.pdf. [Accessed 23 10 2019].

[9] W. Torge, Geodesy, 2001, pp. 95-97.

[10] M. Galambos, L. Bacsardi and S. Imre, “Modeling and Analyzing the Quantum Based Earth-Satellite and Satellite-Satellite Communications,” in *International Astronautical Congress*, 2010.

[11] M. Galambos and L. Bacsárdi, “Comparing Calculated and Measured Losses in a Satellite-Earth Quantum Channel,” *INFOCOMMUNICATIONS JOURNAL,* vol. 3, pp. 14-19.

[12] L. Bacsardi, “On the Way to Quantum-Based Satellite Communication,” *51 : 8*, pp. 50-55, 2013.

[13] A. Kiss, M. Galambos and L. Bacsardi, “Refined computer simulation of loss in quantum-based satellite channel,” in *Proc. of 69th International Astronautical Congress*, 2018.

[14] Z. Sodnik, B. Furch and H. Lutz, “The ESA Optical Ground Station – Ten Years Since First Light,” *ESA bulletin,* vol. 132, pp. 34-40, 2007.

[15] ASA, “astrosysteme.com,” First ASA OGS installed, [Online]. Available: https://www.astrosysteme.com/experience/news/brand-new-ground-station. [Accessed 21 10 2019].

[16] ASA, “astrosysteme.com,” ASA AZ800 Ritchey-Chrétien optics, [Online]. Available: https://www.astrosysteme.com/products/telescopes/asa-az800. [Accessed 21 10 2019].

[17] E. Kerstel, A. Gardelein, M. Barthelemy, T. C. Team, M. Fink, S. K. Joshi and R. Ursin, “Nanobob: a CubeSat mission concept for quantum communication experiments in an uplink configuration,” 2018.

[18] R. Haber, D. Garbe, S. Busch, W. Rosenfeld and K. Schilling, “QUBE - A CubeSat for Quantum Key Distribution Experiments,” 2018.

[19] E. Kulu, “NANOSATELLITE & CUBESAT DATABASE,” 2014. [Online]. Available: https://www.nanosats.eu/database. [Accessed 23 10 2019].