Optikai elemek stabilitásvizsgálata kvantumkommunikációs laborméréseihez

Kobán Gergely
ELTE TTK Geofizikus MSc –
Űrkutató-Távérzékelő szakirány

Konzulens:
Dr. Imre Sándor
BME-HIT

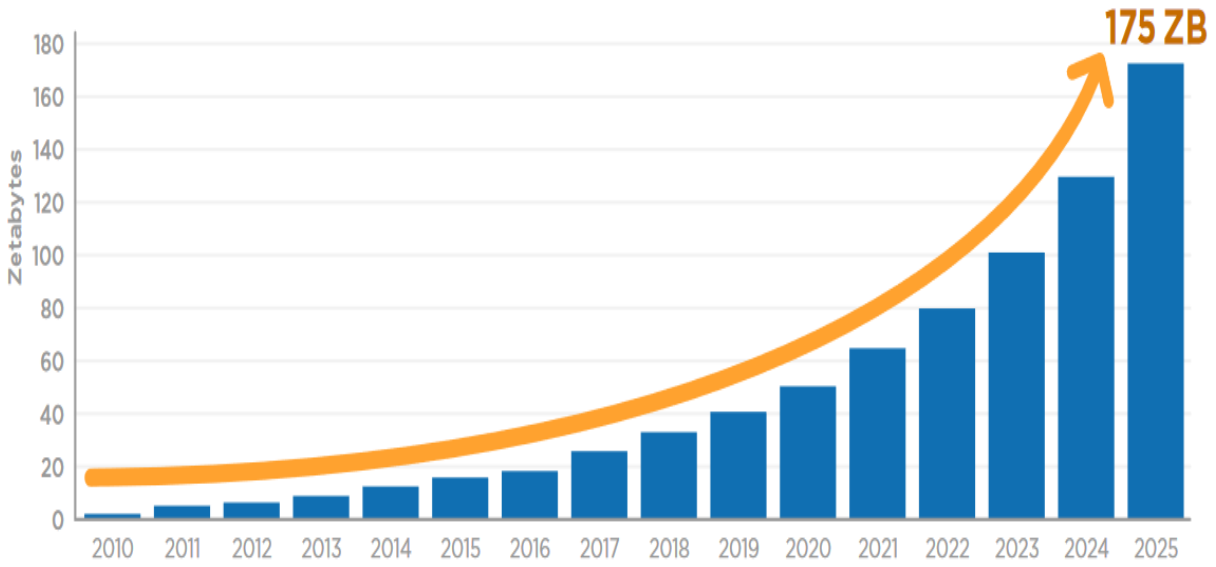
2020

A munka a Kvantumbitek előállítása, megosztása és kvantuminformációs hálózatok fejlesztése nevű, 2017-1.2.1-NKP-2017-00001 számú projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a "Nemzeti kiválósági program" pályázati program finanszírozásában valósult meg.

Tartalom

1. Bevezetés

A világban hihetetlen mennyiségű adat keletkezik minden egyes nap, többek között személyes fotók, beszélgetések, MRI- és műholdképek, vagy tudományos eredmények formájában. A gazdaság, az ipar nem tudna ezen adatok nélkül működni. Ám önmagában nem elég előállítani az adatot, muszáj feldolgozni és az esetek többségében továbbítani is. A klasszikus számítógépek számítási kapacitása drasztikus ütemben növekedett, hogy lépést tudjon tartani a növekvő igényekkel, azonban ez egyre nehezebb. Ezenkívül az adatot lemásolhatják, ellophatják, ha nincs megfelelő védelemmel ellátva. Ezen problémákra megoldást találhatunk a kvantuminformáció-elmélet (alkalmazása) segítségével.



1. ábra: Globálisan, évente megtermelt adatmennyiség (forrás: IDC)[1]

Jelenleg az adataink és kommunikációnk védelmét ellátó kriptográfiai algoritmusok három matematikai problémára épülnek: integer faktorizációja, diszkrét logaritmus probléma, illetve elliptikus görbe kriptográfia. Az alapja ezeknek a módszereknek az, hogy klasszikus számítógépekkel az említett problémák matematikai megoldása nehézkes és lassú, még a mindenkori legfejlettebb hardverrel is, így elég bizonyos időközönként a kulcs hosszát megnövelni. Ez azonban a kvantumszámítógépek megjelenésével már nem igaz [2]. Bár a jelenlegi, működő, a nyilvánosság számára ismert kvantumszámítógépek kapacitása kevés hozzá, hogy a ma használatos algoritmusokat feltörjék, azonban a technológia maga hatalmas veszélyt jelent. A jelenleg nagymértékben használatos RSA-algoritmus 2048 bites kulcsot használ [3]. Ezt klasszikus számítógépeknek több száz trillió évbe telne feltörni [4], ezért mondjuk azt rá, hogy biztonságos. Ezzel szemben egy 4099 stabil qubitet számláló kvantumszámítógép 10 másodperc alatt képes feltörni (persze érdemes megjegyezni, hogy a jelenlegi legnagyobb kvantumszámítógép is csak 72 qubites) [5].

A legnagyobb veszélyt a jelenlegi kriptográfiai algoritmusokra a Shor-algoritmus és a Grover-algoritmus jelenti. Előbbi nagy számok faktorizálását végzi hatékonyan, míg utóbbi egy rendezetlen adatbázisban lévő keresést gyorsít nagymértékben. Az utóbbi években kifejlődött egy olyan kutatási irány, a poszt-kvantum kriptográfia, amely ezen kvantum algoritmusok, illetve maga a kvantum-számítógépek által jelentett fenyegetésnek is ellenálló kriptográfiai algoritmusok fejlesztését tűzte ki célul.

2. ábra: Az IBM 53 qubites kvantumszámítógépe

A 2. ábrán látható IBM Q hardveren 2019-ben a Shor-algoritmus használatával sikerült faktorizálni három számot, a 15-öt, 21-et, és a 35-öt [6]. Ez utóbbi máig a legnagyobb szám, amit sikerült faktorizálni kvantumszámítógépen.

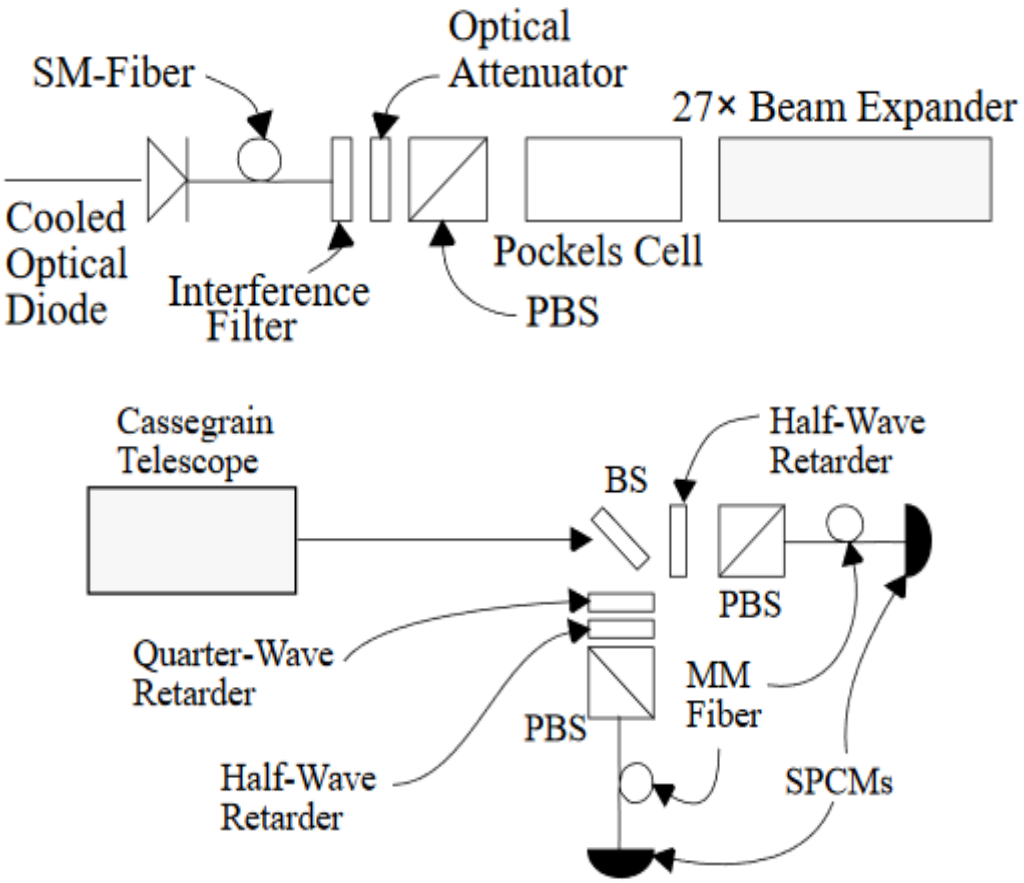
Ahogy korábban említettem, a jelenlegi kriptográfiai algoritmusaink arra épülnek, hogy a számítógépek kapacitása nem elegendő bizonyos számítási feladatok elvégzéséhez. Ezzel szemben a kvantum kriptográfia olyan biztonságot kínál, amit még egy elméletileg végtelen számítási kapacitású lehallgató számára is lehetetlen kijátszani. A biztonságot maga a kvantummechanika klasszikustól merőben eltérő tulajdonságai adják.

A kvantumkriptográfia fő irányvonala a kvantum-kulcsszétosztás. Klasszikusan háttérbe szorultak a szimmetrikus kulcsú algoritmusok, ugyanis a kulcs eljuttatása a másik félhez biztonságosan olyan probléma, amit klasszikus módon nehéz megoldani. Ezzel szemben manapság már több olyan kvantumalgoritmus is létezik, amely biztonságosan képes kulcsot kiosztani. Ennek elméletét a 2. fejezetben tárgyalom

részletesen, itt az ilyen irányú projektekről értekezem, ezek közül is a szabadlégköri alkalmazásokat előtérbe helyezve.

Az első szabadlégköri kulcsszétosztó rendszert 1991-ben készítették Bennett és Brassard [7]. Ez még beltéri volt, 32 cm hosszú csatornával. A fotonforrás egy zöld LED volt (550±20 nm), amit 25 mm-es fókusztávolságú lencsével és 25 μm-es lyukkal kollimáltak. Kollimálás, szűrés és polarizáció után az intenzitás 0.1 foton volt impulzusonként.

Köszönhetően a légköri elnyelésnek és az alacsony hatékonyságú detektoroknak, 715000 impulzusból csak nagyjából 4000-et detektáltak. Lehallgató nélkül ez egy 754 bites titkos kulcsra volt elég, míg lehallgatóval 105 bites kulcsot tudtak készíteni. Ez az intenzitás ilyen kicsi távolságon elég volt ahhoz, hogy demonstrálják a rendszer működőképességét, de nagyobb távolságú kommunikációra a légkörben alkalmatlan. 1998-ban a Los Alamos laboratórium dolgozói 772 nm-es lézert használva már 950 m-es távolságon tudtak kulcsot kiosztani [8]. A fotonok száma pulzusonként <0.1 volt. A cikkben amellett is érveltek, hogy mivel a légköri turbulencia az atmoszféra alsó 2 km-ében jelentős, így egy földi állomás és egy alacsonypályás műhold között is lehetséges a kulcsszétosztás.

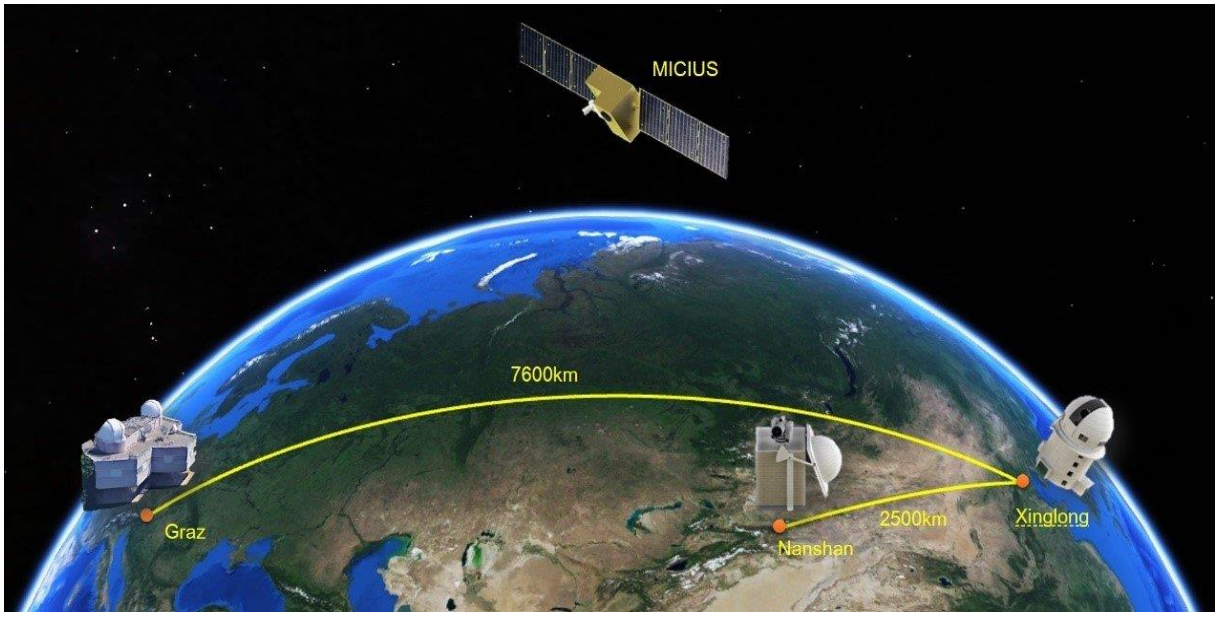


3. ábra: Az 1998-as kísérlet műszerei, felül az adó, alul a vevő

Megfigyelhetünk hasonlóságokat a két rendszer között, például az alacsony fotonszámot impulzusonként. Erre azért van szükség, hogy a lehallgató ne tudja tovább hasítani az impulzust több fotonra. Az optikai frekvenciák használata pedig a légköri depolarizációs hatások csökkentése érdekében ajánlatos. A mérőrendszer elrendezéséről bővebben a 3.5.-ös alfejezetben írok.

2006-ban egy nagyobb ugrás következett távolságban. Egy Rupert Ursin vezette nemzetközi csoport kísérletében polarizáció alapú kvantum-összefonódott fotonpárokat generáltak az adóoldalon, a pár egyik tagján mérést végeztek helyben, a másikat pedig továbbították a vevőoldalra, így generálva kulcsot [9]. Mindez 2400 méterrel a tengerszint felett, a forrás La Palma, a vevő pedig Tenerife szigetén, egymástól 144 km-re! Ilyen módon 75 másodperc alatt 178 bites kulcsot tudtak generálni. Ezekkel az eredményekkel egyre közelebb kerülünk a műholdas kvantumkommunikációhoz.

Végül 2016-ban a Micius műholddal elérkezett az idő erre is [10]. A műholdat a kínai QUESS (Quantum Experiments at Space Scale) kísérlet keretében lőtték fel, a földi vevőállomásait az Osztrák Tudományos Akadémia működteti. A 97.4 fokos inklinációjú napszikron pályán keringő műhold fő feladata demonstrálni a fedélzetén lévő kvantumoptikai eszközök képességeit. A műholdon összefont fotonpárokat állítanak elő, amikből egyet leküldenek a földi állomásra, így generálva a kulcsot.



4. ábra: A Micius műhold, és földi állomásainak távolsága

A műhold legkisebb távolsága a földi állomástól 507 km, míg a legnagyobb 1034 km volt. Előbbin 40.2 kbit/s volt az elérhető legnagyobb ráta, utóbbin 1.2 kbit/s. A kvantum bithiba-arány 1-3% között változott.

Természetesen vannak negatívumok is, ilyen például a nagyon kicsi napi lefedettség (273 másodperc naponta), illetve az, hogy megfelelő időjárási körülmények szükségesek a megfelelő kommunikációhoz.

Az alábbi táblázatban összefoglaltam az említett szabadlégköri projektek évét és távolságát:

Év	Típus	Távolság
1991	Légköri (beltér)	32 cm
1998	Légköri	950 m
2006	Légköri	144 km
2016	Műholdas	1034 km

Már az említett pár kísérlet alapján is egyértelmű a gyors fejlődés. Nem is annyira régen, 2020 júliusában az Egyesült Államok Energiügyi Minisztériuma kiadott egy jelentést [11], ami gyakorlatilag egy tervezet a „kvantum internet” fejlesztéséhez. Az Egyesült Államokban leginkább a vezetékes kvantumkommunikációt preferálják, de természetesen szabadlégköri és műholdas kutatások is folynak. Az ESA a műholdas programjain belül támogatja kvantumkommunikációs és kriptográfiás eszközök fejlesztését. Hatalmas mennyiségű kutatási idő és pénz ömlik a területbe, és ez évről-évre növekszik.

2. Alapfogalmak

Ebben a fejezetben azokat az alapvető fogalmakat tárgyaljuk, amelyek a kvantum-információelmélethez és a kvantum kommunikáció tárgyalásához nélkülözhetetlenek, illetőleg fontosak.

2.1. Qubit

A klasszikus információ alapeleme a bit. Ahogy a neve is mutatja, a bitnek két állapota van, a 0, illetve az 1. A klasszikus rendszer egyértelműen az egyik vagy a másik állapotban van. Ezzel szemben a kvantum információ alapeleme a kvantumbit, vagy röviden qubit. A qubit egyedi módon a két állapot szuperpozícióját is felveheti [12]. A rendszer így írható le:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.1}$$

ahol α és β az ún. valószínűségi amplitúdók, ezek komplex számok. A két bázisállapot vektoriálisan a következő alakot veszi fel:

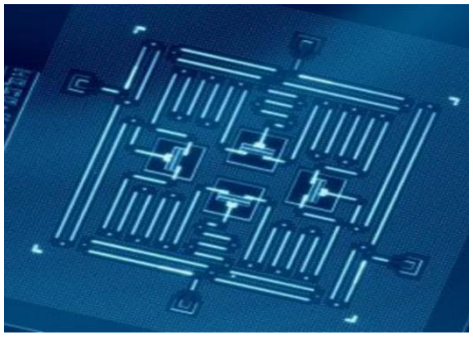
$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \tag{2.2}$$

$$|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}. \tag{2.3}$$

Fontos továbbá a normalizációs tulajdonság, vagyis, hogy a valószínűségi amplitúdók négyzetösszege 1:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.4}$$

Egy kvantumszámítógép qubitje kísérletileg elektron vagy atommag spinekkel, illetve szupravezető áramkörökkel valósítható meg.



3. ábra: Az IBM 4 transzmonból (szupravezető töltés-qubit) álló kísérleti eszköze [13]

2.2. Pauli-operátorok, logikai kapuk

Egy kvantummechanikai rendszer állapotát (hullámfüggvényét) a Schrödinger-egyenlet írja le [14], aminek legáltalánosabb alakja az időfüggő változat:

$$i\hbar \frac{d}{dt}|\Psi(t)\rangle = H(t)|\Psi(t)\rangle, \tag{2.5}$$

ahol ħ a redukált Planck állandó, *H(t)* pedig a Hamilton-operátor. Qubit esetén a Hamilton-operátor egy 2x2-es mátrix. Mint minden 2x2-es hermitikus mátrix, ez is kifejezhető a négy Pauli-operátor lineárkombinációjával:

$$H(t) = \sum_{j=0}^{3} c_j(t)\sigma_j, \tag{2.6}$$

ahol σ_j a j-edik Pauli operátort jelöli:

$$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{2.7) , (2.8}$$

$$\sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.9) , (2.10}$$

Az utóbbi három Pauli-operátort számok helyett betűkkel is szokták jelölni, vagyis létezik σ_X, σ_Y, σ_Z is. A Pauli operátorok alapvető fontosságúak és gyakran előkerülnek kvantum-információelméletben. Például a Pauli X-operátor a kvantum bit-flip kapu, mivel $|0\rangle$ állapotot $|1\rangle$-be képezi, illetve fordítva.

Qubitek állapotát a klasszikus számítógépekhez hasonlóan logikai kapukkal tudjuk befolyásolni. Minden kapu leírható unitér operátorokkal, és ezek, ellentétben a klasszikus esettel, reverzibilisek. Egy qubiten ható kapu például a már említett Pauli-operátorok, vagy a Hadamard-kapu [15]:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.11}$$

amely egy tökéletesen kevert állapotot csinál az eredeti állapotból. Természetesen léteznek több qubiten ható logikai kapuk is. Ilyen például az irányított negálás, a CNOT kapu:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{2.12}$$

Illetve akár három qubiten operáló kapu is, például a Toffoli-kapu, vagy más néven CCNOT, amelynek két kontroll bitje van:

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \quad (2.13)$$

A hullámfüggvény időfejlődését (dinamikáját) egy ún. propagátorral tudjuk kifejezni.

$$\Psi(t) = U(t)\Psi(0). \quad (2.13)$$

A propagátor, vagyis U(t) unitér mátrix vagyis transzponált konjugáltja egyben inverze is.

2.3. Bloch-gömb, mérés

A qubitek állapotát egy szemléletesebb képpel is le tudjuk írni, ez a Bloch-gömb. Tetszőleges qubit állapot felírható a következőképp:

$$|\Psi\rangle = e^{i\gamma}\left(cos\frac{\theta}{2}|0\rangle + e^{i\varphi}sin\frac{\theta}{2}|1\rangle\right). \quad (2.14)$$

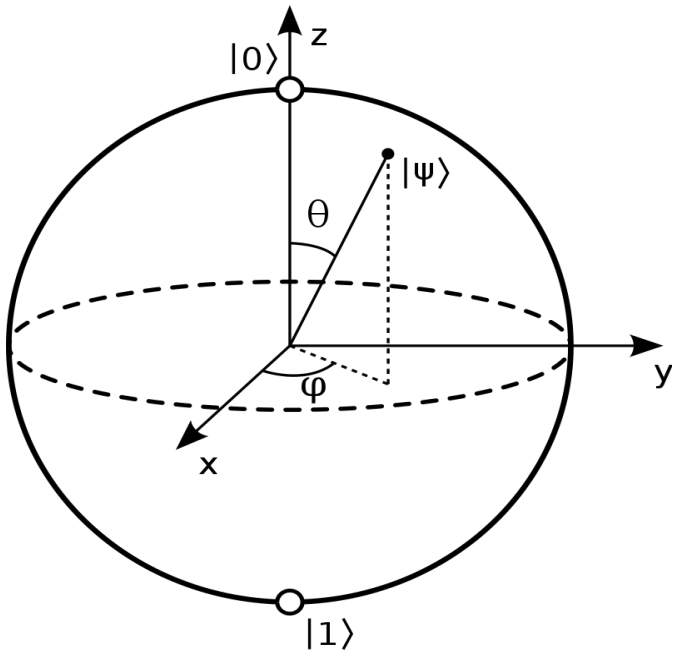
Valójában γ-nak nincs fizikai jelentése, így egyszerűsíthetünk:

$$|\Psi\rangle = \left(cos\frac{\theta}{2}|0\rangle + e^{i\varphi}sin\frac{\theta}{2}|1\rangle\right). \quad (2.15)$$

A $0<\theta<\pi$ és $0<\varphi<2\pi$ számpár meghatároz egy pontot az egységnyi sugarú háromdimenziós gömbön. Vagyis egy qubit állapot leképezhető ezen egységgömb felületére:

$$|\Psi\rangle \rightarrow (\theta, \varphi) \rightarrow (\sin\theta cos\varphi, sin\theta sin\varphi, cos\theta). \quad (2.16)$$

Ez a gömb a Bloch-gömb.



4. ábra: A Bloch-gömb

Egy qubitből az információt méréssel tudjuk kinyerni. Azt, hogy milyen eséllyel mérünk $|0\rangle$, illetve $|1\rangle$ állapotot, az amplitúdók abszolútértéknégyzete határozza meg. Tehát annak az esélye, hogy nullát, illetve egyet mérünk:

$$P_0 = |\alpha|^2, \tag{2.17}$$

$$P_1 = |\beta|^2. \tag{2.18}$$

Amennyiben 0-át mérünk, a qubit a $|0\rangle$ állapotba billen, míg ha 1-et, akkor az $|1\rangle$-be.

2.4. Kvantum-összefonódás

A kvantuminformatika alapvető erőforrása, ami a kvantumkommunikáció egy sarokköve is, a kvantum-összefonódás [16]. Ennek matematikai leírásához nézzünk egy két kvantumállapotból (például két qubitből) álló rendszert:

$$|\Psi\rangle = |\Psi\rangle_A \otimes |\Psi\rangle_B, \tag{2.19}$$

ahol $|\Psi\rangle_A$ az első rendszer állapota, $|\Psi\rangle_B$ pedig a másodiké. Az ily módon leírható állapotokat nevezzük szeparábilisnek. Azonban vannak olyan kompozitrendszerek, amelyek nem írhatók fel tenzorszorzatként, vagyis nem szeparábilisek. Az ilyen rendszerek az összefonódott kvantumrendszerek. Az egyik legismertebb példa erre a Bell-állapotok, négy maximálisan összefonódott két-qubites állapot:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\right), \tag{2.20}$$

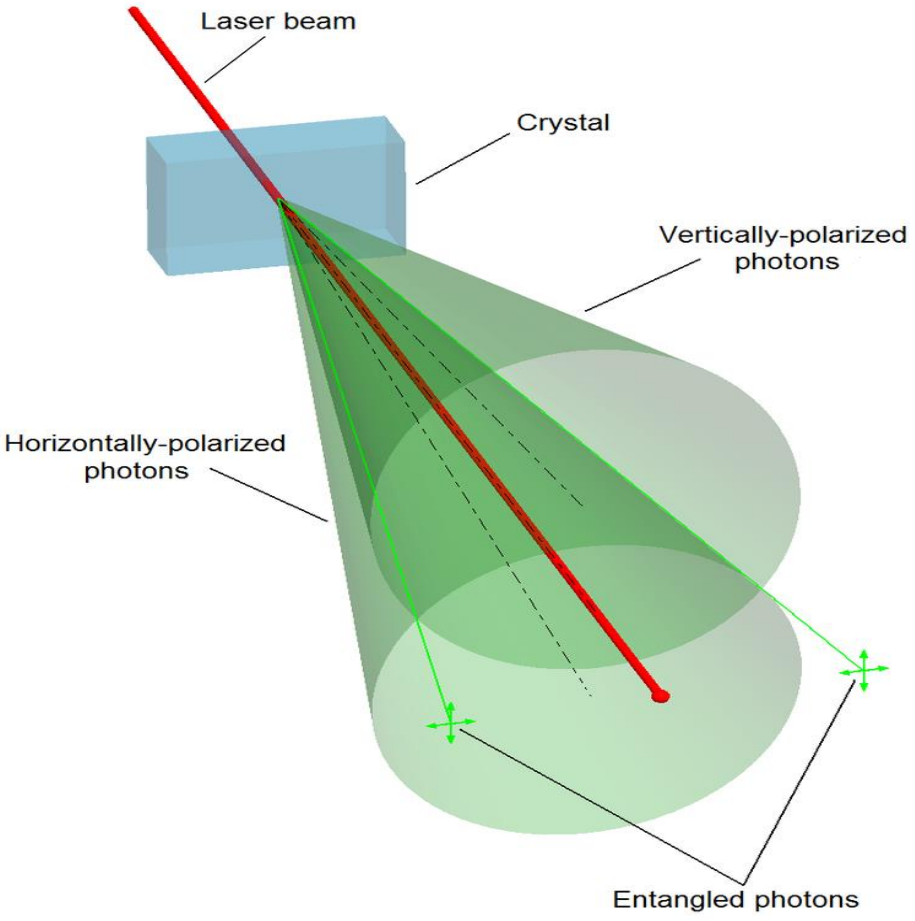
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B\right), \tag{2.21}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B\right), \tag{2.22}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right). \tag{2.23}$$

A négy állapotvektor együtt alkotja a Bell-bázist.

A gyakorlatban összefonódott fotonokat leggyakrabban egy SPDC-nek, vagyis Spontán Parametrikus Le-Konverzió nevezett eljárással állítanak elő [17]. Az eljárás lényege, hogy nemlineáris kristállyal felhasítanak egy fotonnyalábot két, kisebb energiájú fotonra. A bemenő fotont pump fotonnak, a kijövőket signal és idler fotonoknak hívják.



5. ábra: II-es tipusú SPDC működése

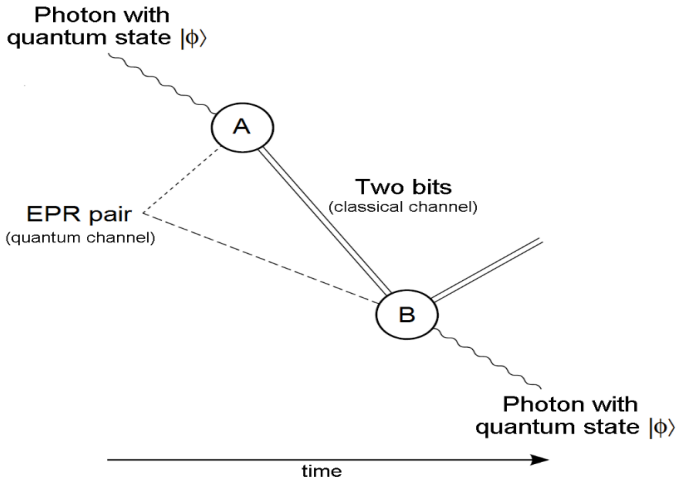
Az energia és impulzus megmaradása miatt a kimenő fotonoknak együtt ugyanakkora az energiájuk és az impulzusuk. Polarizáció alapján kétféle SPDC-t különböztetünk meg: Ha a signal és idler fotonok polarizációja azonos, I-es tipusú, míg ha ugyanezen fotonok körpolarizáltak, II-es tipusú SPDC-ről beszélünk.

Ha az output fotonpárokat nagyon messze eltávolítjuk egymástól, és az egyik polarizációját megmérjük egy adott bázisban, a másik polarizációja is egyből eldől. Vagyis hiába van a két foton nagyon messze egymástól, mégis világos kapcsolat van köztük, összefonódottak. Ez a klasszikus fizikában idegen és furcsa tulajdonság egy fontos erőforrása a kvantumszámítógépeknek és a kvantumkommunikációnak. Fontos viszont megjegyezni, hogy az összefonódás nem használható szuperluminális, vagyis fénynél gyorsabb kommunikációra. Ennek oka, hogy ahhoz, hogy információt tudjunk kinyerni a rendszerből, a feleknek kommunikálniuk kell egymással, például, hogy megfelelő bázist tudjanak választani a méréshez.

2.5. Kvantumteleportáció, szupersűrű kódolás

Két olyan folyamat is van kvantumkommunikációban, amely az összefonódásra épül. Az első a kvantumteleportáció, a második ennek bizonyos értelemben az ellentéte, a szupersűrű kódolás [18].

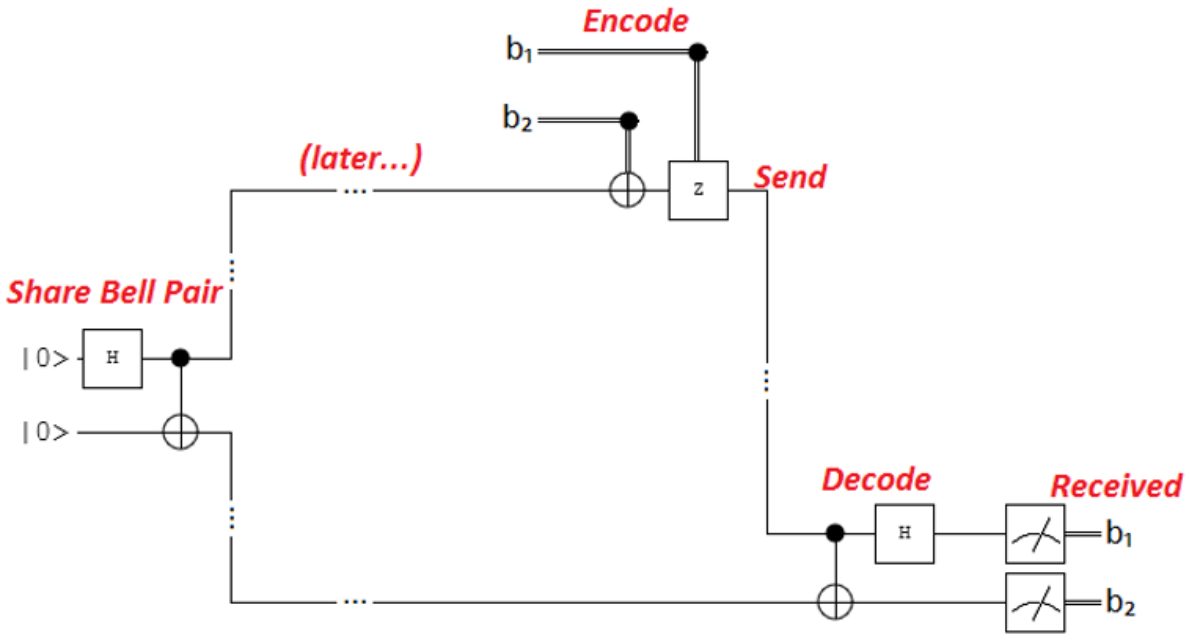
A kvantumteleportáció során kvantuminformáció, vagy állapot teleportálódik egyik helyről a másikra. Kezdetben a két kommunikáló fél, Alice, a küldő, és Bob, a fogadó, rendelkezik egy klasszikus csatornával, egy összefonódott részecskepár egy-egy tagjával, illetve egyiküknél ott van az átküldeni kívánt $|\Phi\rangle$ állapot. Az összefonódott részecskepárt akár egy harmadik személy is generálhatta, elküldve az egyik részecskét az egyik félhez, a másikat a másikhoz. Ezután a küldő fél közös mérést végez a küldendő állapoton és a pár nála lévő tagján, így nyerve két bitnyi klasszikus információt. Ezt a két bitet aztán a küldő fél a klasszikus csatornán továbbítja a fogadó félnek.



6. ábra: Kvantumteleportáció vázlata

Ekkor a pár fogadó félnél lévő tagja négy lehetséges állapotot vehet fel: vagy már $|\Phi\rangle$ állapotban van, vagy olyan állapotban, hogy a három Pauli-operátor valamelyikének alkalmazásával $|\Phi\rangle$-be forgatható. Azt, hogy melyik Pauli-operátort kell alkalmazni, a két mért bit határozza meg. A megfelelő operátor alkalmazása után a fogadó félnél lesz a kvantumállapot.

A szupersűrű kódolás során két klasszikus bitet továbbítunk oly módon, hogy csak egyetlen qubitet mozgatunk. Ennek előfeltétele, hogy legyen egy összefonódott állapotpárunk, aminek egyik tagja Alice-nél, a másik Bobnál van. Kezdetben tehát Alicenél van két továbbítandó bit, illetve egy összefonódott qubitpár egy tagja, Bobnál pedig a másik tag. Alice attól függően, melyik két bitet akarja továbbítani, a saját qubitjén alkalmazza egy valamelyik Pauli-operátort, beleértve az identitást. Ekkor ezen szinglet állapot a négy Bell-állapot valamelyikébe megy át. Az unitér művelet után Alice a saját qubitjét elküldi Bobnak. Az információ dekódolásához Bob projektív mérést végez a Bell-bázisban, amit a gyakorlatban a CNOT kapu (A kontrollal), majd a $H \otimes I$ művelet alkalmazásával valósít meg.



7. ábra: A szupersűrű kódolás vázlata

Ez alapján úgy tűnhet, 2 klasszikus bitnyi információt kódoltunk 1 qubitbe, innen a név. A valóságban viszont csak az összefonódást kihasználva elértük, hogy csak az egyik qubitet kelljen fizikailag mozgatnunk, a másik qubitet jóval a protokoll megkezdése előtt továbbíthatjuk a másik félnek.

A szupersűrű kódolás a kvantum teleportáció ellentétének is tekinthető abban az értelemben, hogy utóbbiban egy qubitet helyezünk át két klasszikus bit ssegítségével, míg előbbiben két klasszikus bitet küldünk egy qubit segítségével.

2.6. Nem-klónozhatósági tétel

Egy másik fontos tulajdonság kvantuminformáció-elméletben, amit kihasználunk, a Nem-klónozhatósági tétel (No-Cloning Theorem) [19]. Ez kimondja, hogy nem lehetséges tökéletes másolatot készíteni egy tetszőleges kvantumrendszerről. Szemléltetésképpen, vegyünk egy tetszőleges kvantumrendszert, illetve egy bármilyen állapotban, mondjuk $|0\rangle$-ban lévő regisztert. Ahhoz, hogy tökéletes másolatot készítsünk, olyan unitér operátorra van szükségünk, amely a regisztert feltölti az ismeretlen állapottal:

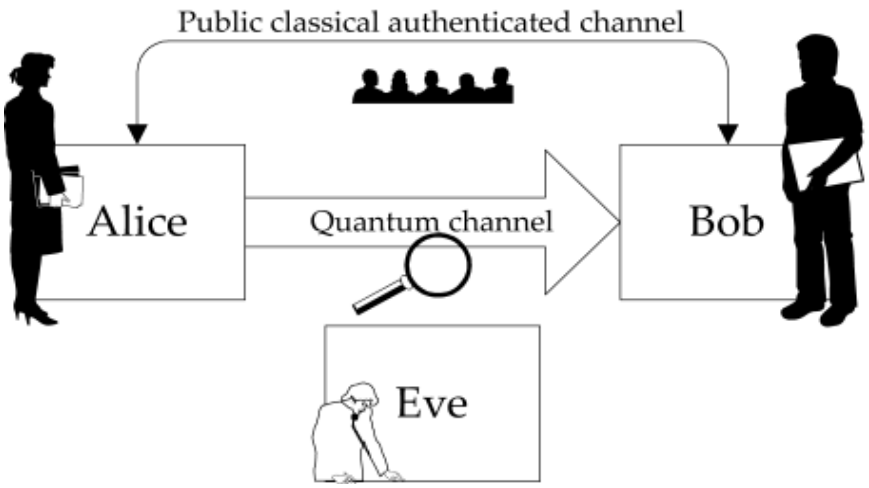
$$U|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle. \tag{2.24}$$

Könnyen bizonyítható, hogy tetszőleges rendszerre nem konstruálható ilyen unitér operátor. Ez a fundamentális eltérés a klasszikus rendszerektől akadályozó tényező is, hiszen emiatt a klasszikus hibajavító algoritmusok nem használhatók. Egy ideig ezen okból azt hitték, a kvantumszámítógép megvalósíthatatlan, azonban Peter Shor 1995-ben megalkotta az első kvantum hibajavító algoritmust, megkerülve a nem-klónozhatósági tételt. Ezzel szemben kvantum-kriptográfiában alapvető fontosságú, hiszen egy klasszikusan elérhetetlen biztonságot ad: megakadályozza az esetleges lehallgatót arról, hogy másolatot készítsen az információról.

2.7. Kvantum-kulcsszétosztás

A 2.6-os fejezet következménye, hogy a lehallgatót tudjuk detektálni. Nézzünk meg egy zajos kvantumcsatornát, amin $|0\rangle$ vagy $|1\rangle$ állapotba kódolt fotonokat küldünk! A zaj valamennyire természetesen összezavarja a fotonok állapotát, így nem mindig pontosan a kódolt állapotot mérjük a fogadó oldalon. A nemklónozhatósági tétel miatt, ha a lehallgató szeretne információt nyerni a „beszélgetésről”, akkor mérést kell végeznie a fotonok egy részén. Ez természetesen megnöveli a bit-hiba arányt. Ha egy határt túllépne a BER, akkor a kommunikáció az adott csatornán leállítható, így megakadályozva a lehallgatást.

1984-ben Charles Bennett és Gilles Brassard kifejlesztette a BB84 protokollt, ami az első kvantum-kulcsszétosztó (QKD) protokoll [20]. Két fél, Alice, a küldő, és Bob, a fogadó fél szeretne kommunikálni. Pontosabban, Alice egy kulcsot szeretne eljuttatni Bobhoz úgy, hogy a kulcs biztonságos legyen, és fel lehessen használni titkosításra.
Ehhez rendelkezésükre áll egy kvantumcsatorna, és egy publikus, mindenki számára látható klasszikus csatorna is. Az átküldeni kívánt információt fotonok polarizációjába kódolják. Két állapotpárt használnak, mindkettő merőleges állapot, például a vertikális-horizontális, illetve a 45°-os és 135°-os polarizáció.



8. ábra: A BB84 összeállítása

Első lépésként Alice random bázisokban kódolt random biteket küld Bobnak a kvantum csatornán keresztül. Bob ezeket szintén random választott bázisokban megméri. Ezután a klasszikus csatornán megosztják egymással, Alice milyen bázisokban kódolt, Bob pedig milyen bázisokban mért. Elvetik azokat a biteket, amiket Bob nem a megfelelő bázisban mért. Ezek után a megmaradt bitek egy részét veszik, és meghatározzák belőlük a bit-hiba arányt. Természetesen az így megosztott bitek később nem használhatóak fel a kulcsba, hiszen, ezek publikussá válnak.

A lépések elvégzése után, ha a bit-hiba arány a küszöbszint alatt maradt, Alice és Bob rendelkeznek egy adott hosszúságú bitsorozattal.

Alice bázis	+	X	X	X	+	+	X	+
Alice bit	1	0	0	1	0	1	1	0
Alice polarizáció	→	↗	↗	↖	↑	→	↖	↑
Bob bázis	+	+	X	+	+	X	X	X
Bob mért polarizáció	→	→	↗	→	↑	↗	↖	↗
Bázisegyeztetés								
Közös kulcs	1		0		0		1	

A fenti táblázatban egy példát látunk a BB84 algoritmus lépéseire. A + a V-H bázist, míg az X az ehhez képest 45 fokban elforgatott bázist jelenti.

Természetesen két oldalon a mérési bizonytalanság, illetve a zajos csatorna miatt nem biztos, hogy adott helyen ugyanaz a bit áll. Ezek a hibás bitek javíthatóak információ-egyeztető algoritmusokkal, amilyen például a Cascade. Így az eljárás végén mindkét fél rendelkezik a közös kulccsal, és biztosak lehetnek benne, hogy harmadik fél nem szerzett elégséges információt erről a kulcsról.

Természetesen léteznek összefonódás alapú kvantum-kulcsszétosztó protokollok is, például az E91 [21].

3. Szabadlégköri kvantumkommunikáció

A vezetékes kvantumkommunikáció nagy hátránya, hogy bizonyos helyeken, térségekben nehezen telepíthető a környezet adottságai miatt. Egy ideális kvantumkommunikációs hálózatnak vezetékes és szabadlégköri részei is kell, hogy legyenek.

Szabadlégköri kvantumkommunikáció során a fotonok, amelyek polarizációjába az információt kódoltuk, valamilyen tulajdonságú légköri rétegen haladnak keresztül. Az út során az intenzitás veszteség mellett a polarizációjuk is megváltozik a légkör hatásai miatt. Ez a fogadó oldalon bithibaként jelentkezik, vagyis, ha mérést végzünk a qubiteken, a vártnál rosszabb arányban fogjuk eltalálni a qubitbe kódolt állapotot.
Természetesen az, hogy a légkör milyen mértékű bithiba-arány romlást okoz, nagyban függ a tulajdonságaitól, összetételétől. Ebben a fejezetben az ehhez kapcsolódó fogalmakat, jelenségeket járjuk körül.

3.1. Beer-Lambert törvény

A közegen keresztül haladó fény csillapítását, vagyis intenzításveszteségét a Beer-Lambert-törvénnyel [22] jellemezhetjük:

$$\tau = \frac{I}{I_0} = e^{-\gamma x}, \tag{3.1}$$

ahol x a megtett út, γ pedig a csillapítási együttható. Ez az együttható összegzi a molekulák és az aeroszolok abszorpciós és szórási képességét azon a szakaszon, amelyen a nyaláb keresztülhalad. Ez az abszorpciós és szórási együtthatók segítségével kifejezve:

$$\gamma = \alpha_a + \alpha_m + \beta_a + \beta_m. \tag{3.2}$$

3.2. Stokes-paraméterek

George G. Stokes 1852-ben négy paramétert definiált, amivel jellemezhető a fény polarizációja [23]. Az első elem az intenzitás, a második egy síkpolarizáció, a harmadik egy a másodikhoz képest 45 fokkal elforgatott síkpolarizáció, míg a negyedik a körpolarizáció. A 4 paramétert vektorként szokás megadni, a következő jelöléssel:

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} I \\ Q \\ U \\ V \end{bmatrix}. \tag{3.3}$$

Ahhoz, hogy az egyes elemek jelentését szemléltessük, írjuk le egy elektromágneses sugárzás elektromos komponensét két inkoherens, ortogonális polarizációjú nyalábbal [24]:

$$E = a_1 E_1 + a_2 E_2, \tag{3.4}$$

ahol E_1 és E_2 ortogonális egységvektorok, a_1 és a_2 pedig a fázist és amplitúdót leíró komplex számok. Ezekkel az együtthatókkal képezhetjük a nyaláb sűrűségmátrixát, amely polarizált esetben így néz ki:

$$\rho = \begin{bmatrix} a_1 a_1^* & a_1 a_2^* \\ a_2 a_1^* & a_2 a_2^* \end{bmatrix}, \tag{3.5}$$

míg nem polarizált nyalábra így:

$$\rho_{np} = \tfrac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{3.6}$$

Teljesen általános esetben számba kell vennünk a polarizált és a nem polarizált részt is:

$$\rho = U\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + P\begin{bmatrix} a_1 a_1^* & a_1 a_2^* \\ a_2 a_1^* & a_2 a_2^* \end{bmatrix}, \tag{3.7}$$

ahol P egy 0 és 1 közötti szám, a polarizáció mértéke.
Láthatjuk, hogy a P=0 esetben U értéke ½, míg a P=1 esetben U értéke 0. Vagyis:

$$U = \frac{1}{2}(1 - P). \tag{3.8}$$

A 3.5-ös és a 3.6-os egyenlet kombinálásával a következőt kapjuk:

$$\rho = \frac{1}{2}(1 - P)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + P\begin{bmatrix} a_1 a_1^* & a_1 a_2^* \\ a_2 a_1^* & a_2 a_2^* \end{bmatrix}. \tag{3.9}$$

Ezen egyenlet elemeivel kifejezve a Stokes-paraméterek a következők:

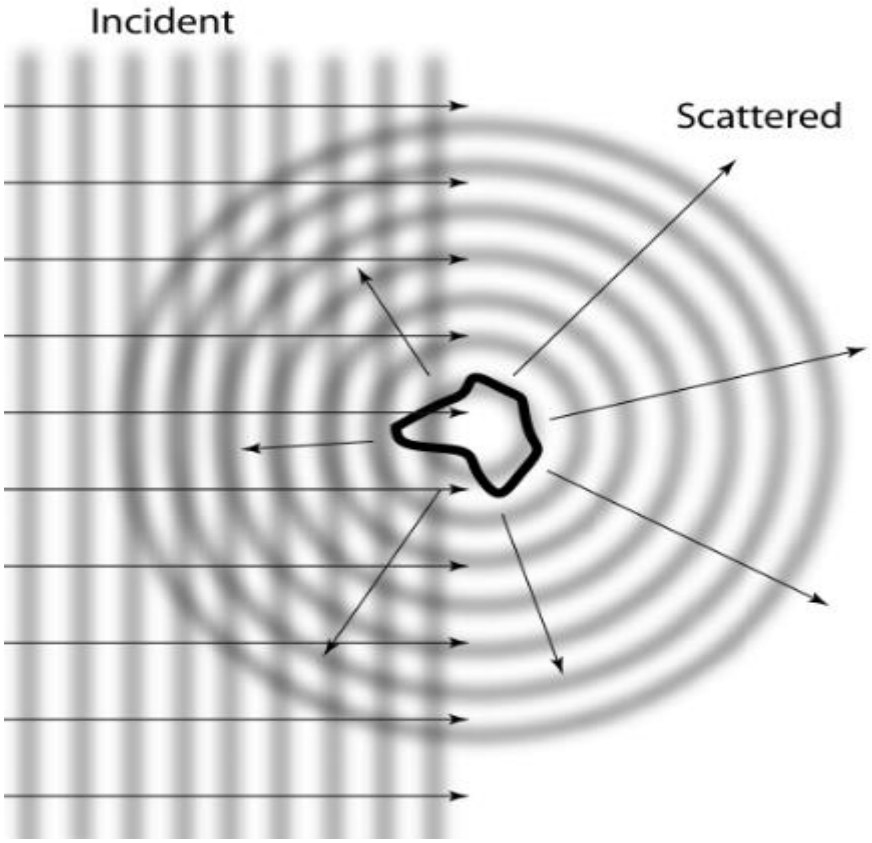
$$\begin{bmatrix} I \\ Q \\ U \\ V \end{bmatrix} = \begin{bmatrix} \rho_{11} + \rho_{22} \\ \rho_{11} - \rho_{22} \\ \rho_{12} + \rho_{21} \\ i(\rho_{21} - \rho_{12}) \end{bmatrix}. \tag{3.10}$$

A következő táblázatban összefoglaltam néhány polarizációs állapot Stokes-paramétereit:

Polarizációs állapot	*I*	*Q*	*U*	*V*
Nem polarizált	1	0	0	0
Horizontális pol.	1	1	0	0
Vertikális pol.	1	-1	0	0
Lineáris $+45^0$ pol.	1	0	1	0
Lineáris -45^0 pol	1	0	-1	0
Bal cirkuláris pol.	1	0	0	-1
Jobb cirkuláris pol.	1	0	0	1

3.3. Légköri elemek szórása

A szórás olyan jelenség, mely során az elektromágneses sugárzás (foton) kölcsönhat egy részecskével. A kölcsönhatás során a részecske elnyeli a fotont, gerjesztődik, majd kibocsát egy hasonló tulajdonságokkal rendelkező fotont. Ez a jelenség a légkörben gyakori, számos tudományterület és technológiai alkalmazás során előkerül. Számunkra azért fontos, mivel a foton polarizációs tulajdonságait és irányát is megváltoztatja.



9. ábra: A szórás folyamata

Azonban a szórásnak is léteznek egymástól markánsan eltérő típusai. A szórás utáni részecske tulajdonságai függnek a részecske a fény hullámhosszához viszonyított méretétől. Ennek karakterizálására bevezették a méretparamétert:

$$x = \frac{2\pi r}{\lambda}. \tag{3.11}$$

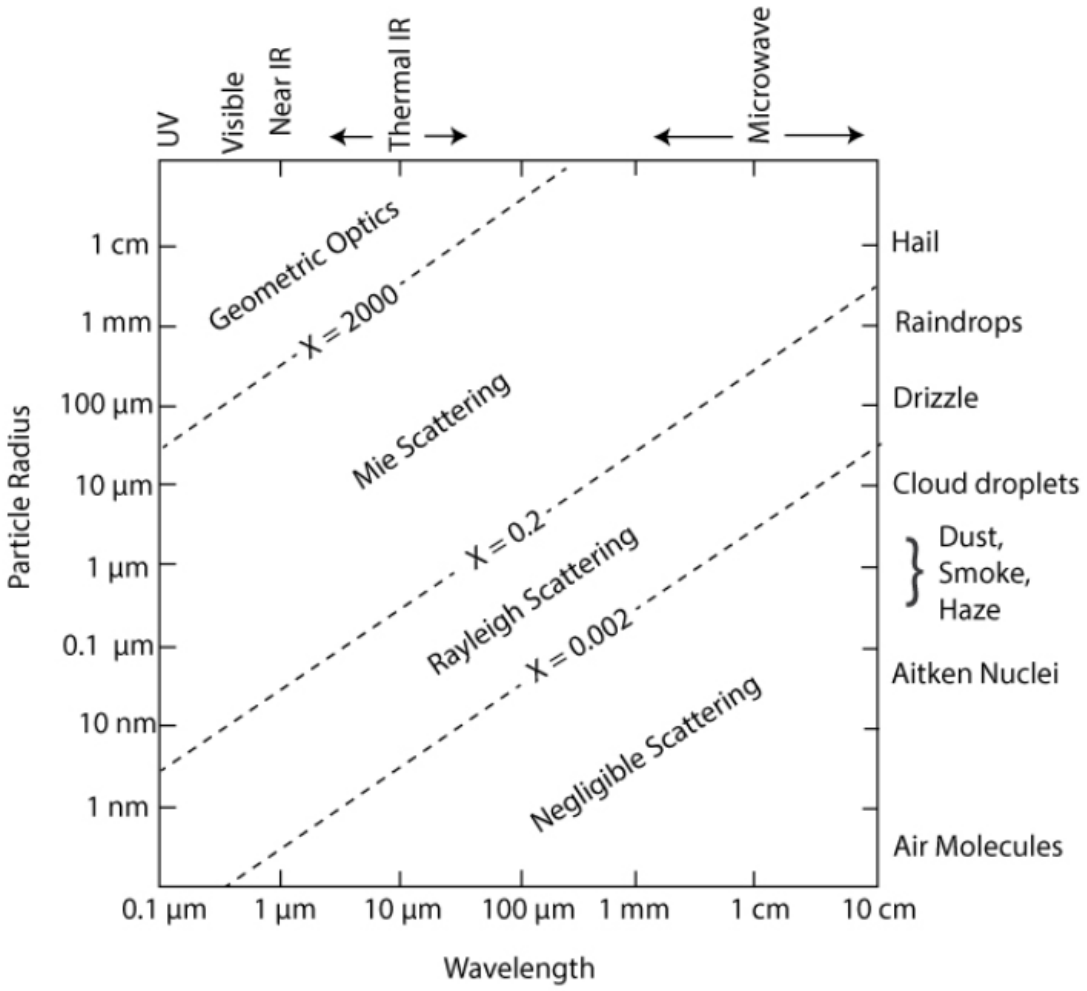
ahol r a részecskék karakterisztikus mérete (sugara), λ pedig a sugárzás hullámhossza [25]. Ezen méretparaméter alapján három különböző szórást is megkülönböztethetünk:

- Ha $x<<1$, a részecske mérete kicsi a hullámhosszhoz képest. Ez a Rayleigh-szórás.
- Ha $x\sim1$, A részecske mérete és a hullámhossz összemérhető. Ez a Mie-szórás
- Amennyiben $x>>1$, a részecske jóval nagyobb, mint a sugárzás hullámhossza. Ez a típus a geometrikus szórás.

Számunkra az első kettő lesz a fontos.
Az alábbi táblázatban összeszedtem a földi atmoszféra főbb elemeit [26]:

Név	Kémiai jel	Térfogatszázalék
Nitrogén	N_2	78.084%
Oxigén	O_2	20.95%
Vízpára	H_2O	1-3%
Széndioxid	CO_2	0.0397%
Hélium	He	0.000524%
Metán	CH_4	0.000179%

A két fő összetevő a Nitrogén és az Oxigén, amelyek mérete 150 pm körüli. Ezzel ők a Rayleigh-szórók közé tartoznak, a többi molekulával együtt. Azonban a légkörben nem csak ezen elemek vannak. Bár relatíve nagyon kis részét teszik ki a légkörnek, nem tekinthetünk el az aeroszoloktól. Az aeroszolok olyan cseppek vagy szilárd részecskék, amik a levegőben szuszpenzióban vannak. Ezek mérete nagyon nagy skálán mozog, de a legtöbben Mie-szórónak tekinthetők a kvantumkommunikációra jellemző hullámhosszokon.



10. ábra: A szórás típusa a részecske mérete és a sugárzás hullámhossza függvényében [27].

Az aeroszoloknak jellemzően két fajtáját különböztetjük meg: természetes aeroszol például a köd, a por, a vulkáni hamu vagy a pollen, míg antropogén (mesterséges) a füst, a korom, vagy más légszennyezők. Az aeroszolok tulajdonságairól részletes leírás található a HITRAN online adatbázisban. Manapság ezek a légköri összetevők felkapottak a globális klímaváltozással kapcsolatos kutatások okán.

Ami még bonyolítja a dolgokat, az az aeroszolok azon tulajdonsága, hogy mind térben, mind időben nagyon dinamikusan változik az arányuk egymáshoz és a légkör többi eleméhez képest is. Az évszakonkénti változás és az egyik napról a másikra kialakuló köd vagy esős idő mellett a szemmel nem látható, érzékelhető változások is komoly hatással lehetnek a szabadlégköri csatornára.

3.4. Rayleigh- és Mie-szórás

A fentiek alapján kijelenthetjük, hogy mindkét típusú szórással foglalkoznunk kell. Érdemes tehát megnézni, hogy milyen különbségek vannak a kettő között.

Ahogy a polarizációs állapotot egy vektorral, úgy a szórást egy mátrix-szal írhatjuk le. Ez az ún. szórási mátrix, amely a kezdeti állapot és szórás utáni állapot között teremt kapcsolatot. A mátrix elemeit Gustav Mie (és tőle függetlenül Ludvig Lorent) vezette le elektromágneses síkhullámra, amely egy homogén gömbön szóródik, ezért ezt a megoldást Mie-ről nevezték el. Természetesen légköri részecskékre nézve a homogén gömb egy közelítés. Maga a megoldás gömbfüggvények végtelen sorösszegeként áll elő. Mie-szórás esetén a mátrix következő alakot veszi fel [28]:

$$P = \begin{pmatrix} P_{11} & P_{12} & 0 & 0 \\ P_{12} & P_{11} & 0 & 0 \\ 0 & 0 & P_{33} & P_{34} \\ 0 & 0 & -P_{34} & P_{33} \end{pmatrix}. \tag{3.12}$$

A mátrixelemeket a (szórási szögtől függő) szórásfüggvényekkel, illetve a k hullámszámmal lehet kifejezni [29]:

$$P_{11}(\theta) = \frac{2\pi}{k^2}[|S_1(\theta) * S_1^*(\theta)| + |S_2(\theta) * S_2^*(\theta)|], \tag{3.13}$$

$$P_{12}(\theta) = \frac{2\pi}{k^2}[|S_1(\theta) * S_1^*(\theta)| - |S_2(\theta) * S_2^*(\theta)|], \tag{3.14}$$

$$P_{33}(\theta) = \frac{2\pi}{k^2}[S_2(\theta)S_1^*(\theta) + S_1(\theta)S_2^*(\theta)], \tag{3.15}$$

$$P_{34}(\theta) = \frac{2\pi}{k^2}[S_2(\theta)S_1^*(\theta) - S_1(\theta)S_2^*(\theta)]. \tag{3.16}$$

A szórásfüggvények pedig a következő alakot veszik fel:

$$S_1(\theta) = \sum_{n=1}^{\infty} \frac{2n+1}{n(n+1)}[a_n\pi_n(cos\theta) + b_n\tau_n(cos\theta)], \tag{3.17}$$

$$S_2(\theta) = \sum_{n=1}^{\infty} \frac{2n+1}{n(n+1)}[b_n\pi_n(cos\theta) + a_n\tau_n(cos\theta)], \tag{3.18}$$

ahol a_n, b_n együtthatók a gömbi Bessel-függvényeket, a π_n, τ_n együtthatók pedig a Legendre polinomokat tartalmazzák különböző formában. Ahogy az egyenletekből kitűnik, a Mie-szórás mátrixának kiszámolása általában numerikusan történik.

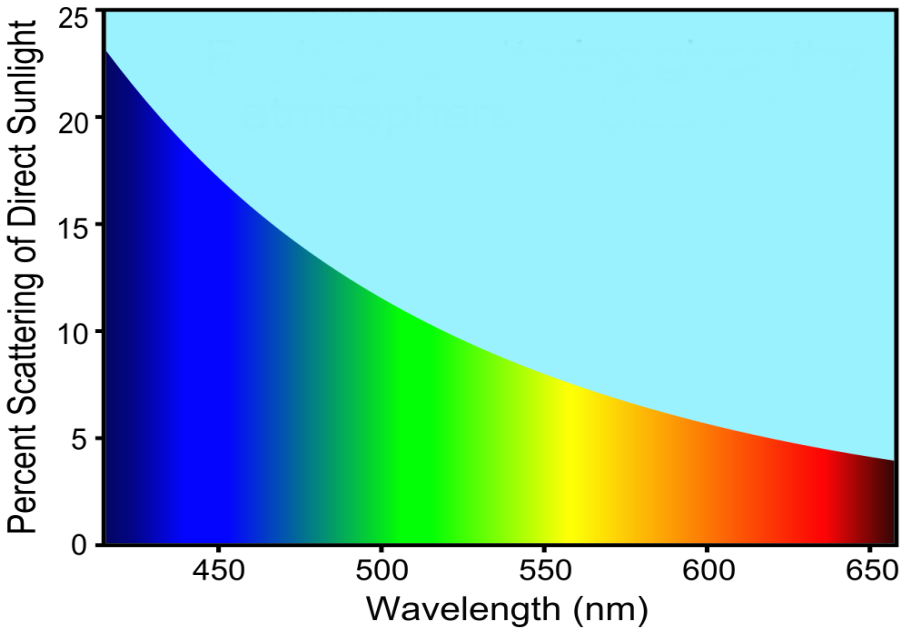
A Rayleigh-szórás esetén, figyelembe véve az $x \ll 1$ limitációt, egy jóval egyszerűbb mátrixot kapunk:

$$P = \frac{3}{4}\begin{pmatrix} 1+cos^2\theta & -sin^2\theta & 0 & 0 \\ -sin^2\theta & 1+cos^2\theta & 0 & 0 \\ 0 & 0 & 2cos\theta & 0 \\ 0 & 0 & 0 & 2cos\theta \end{pmatrix}. \tag{3.19}$$

A Rayleigh szórás egy érdekes tulajdonsága az erős hullámhosszfüggése. A Rayleigh-szórás szórási keresztmetszete [30]:

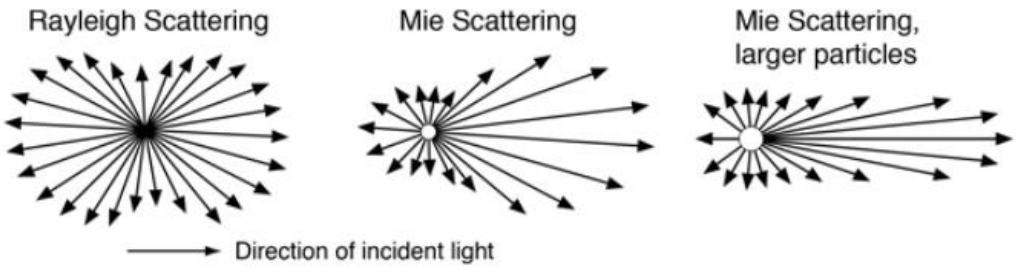
$$\sigma_{Rayleigh} = \frac{2\pi^5}{5}\frac{d^6(n^2-1)^2}{\lambda^4(n^2+2)^2}, \tag{3.20}$$

ahol d a részecske átmérője, n a törésmutató, λ pedig a hullámhossz. Ez a bizonyos negyedik hatványú függés okozza az ég kék színét, hiszen így a kék színt sokkal jobban szórja a légkör, és ez a szórt fény jut a szemünkbe.



11. ábra: A kisebb hullámhosszú fény nagyobb mértékben szenved Rayleigh-szórást

A Mie-szórásnak van még egy fontos tulajdonsága, méghozzá, hogy erősen előre szór, aminek mértéke ráadásul a méretparaméter növekedésével nő.

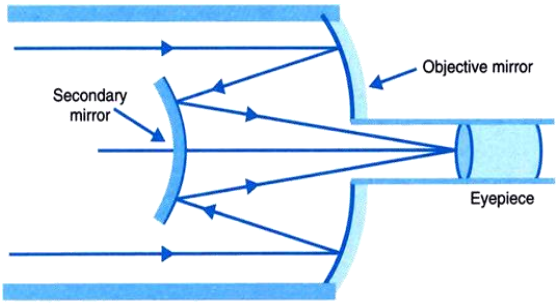


12. ábra: Rayleigh és Mie szórás a részecske méretének függvényében [31]

3.5. Mérési eszköz

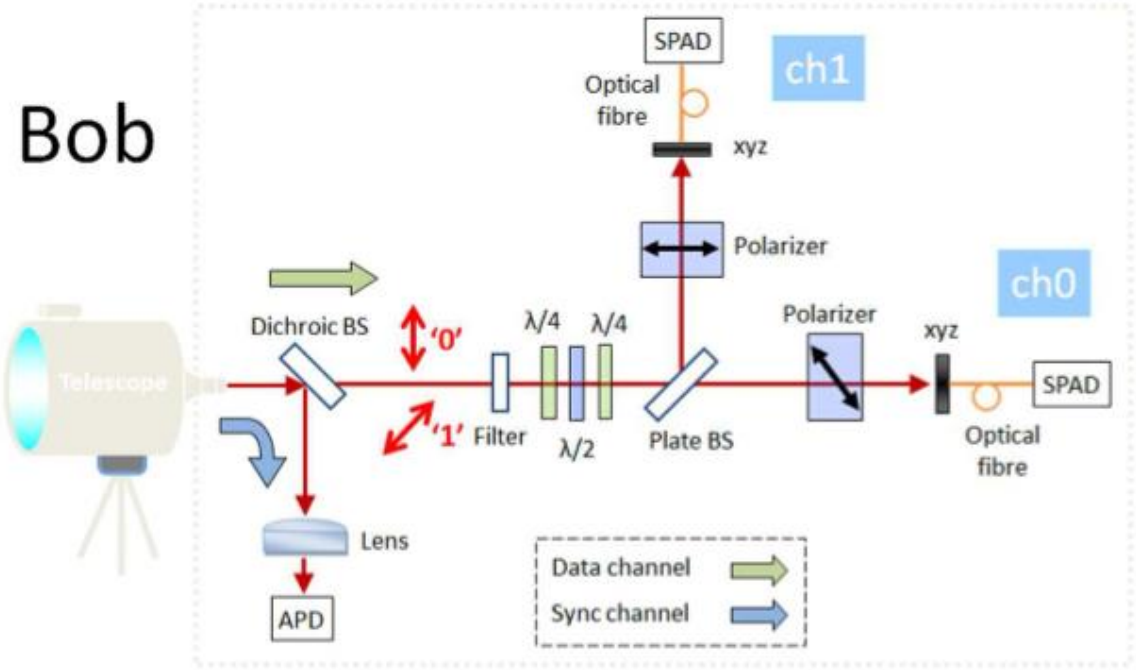
Ebben az alfejezetben egy tipikus mérési elrendezést mutatok be röviden szabadlégköri kvantumkommunikáció esetére [32]. A leírás során a 13. ábrán látható elrendezésre fogok hivatkozni.

Először azon fotonok, amelyek megérkeznek a vevőhöz, egy teleszkópban gyűjtődnek össze. Ez gyakran Cassegrain elrendezésű, hogy a lehető legtöbb fényt gyűjtse be és fókuszálja.



13. ábra: Cassegrain teleszkóp

A dichroic szűrő célja, hogy leválassza a kommunikációra használt fotonokat az időzítéshez vagy a célkövetéshez használt, a kommunikációtól eltérő hullámhosszú fényt. Emellett szükség van még egy szűrőre, amely a Napból, illetve más forrásból beérkező fotonokat szűri ki.



14. ábra: Egy tipikus mérési elrendezés szabadlégköri kvantumkommunikációra

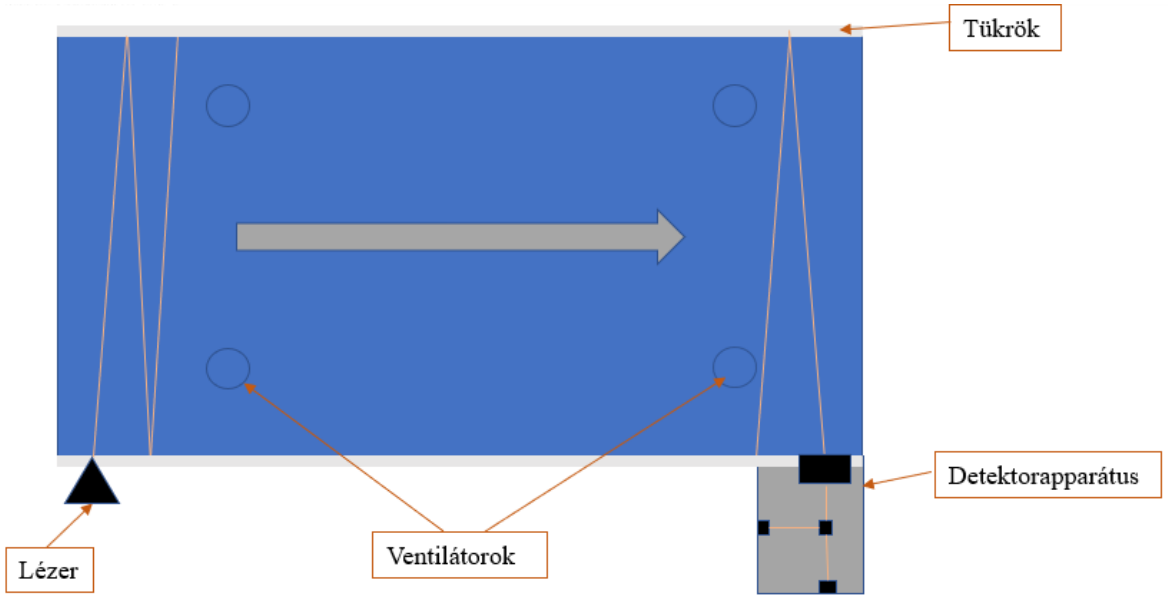
A következő elem egy nyalábosztó, amely a különböző bázisban mérő eszközök között osztja szét a fotonokat. Az egyesével beérkező fotonokat a magas hatásfok, alacsony zaj, és viszonylagos olcsóságuk miatt gyakran SPAD-ekkel (single photon avalanche diode – egyfoton lavinadióda) detektálják. Ez a fotodiódák egy különleges fajtája, melyben a záróirányú előfeszültség akkora, hogy az ún. Geiger-mód régióban van. Ekkor egyetlen foton érkezése is lavinaáramot generál, ami könnyen mérhető.

4. Légköremuláció laboratóriumi körülmények között

A korábbi fejezetekben rávilágítottam, hogy a kvantumkommunikáció és a kvantum-kulcsszétosztás során mennyire fontos a bithiba-arány, illetve ennek előrejelzése, és hogy ez a légkör dinamikája miatt nehézkes feladat. Emiatt érdemes jobban megvizsgálni ezeket a jelenségeket és ajánlásokat, szabványokat kidolgozni. A laborban történő vizsgálat előnyei közé tartozik az, hogy jóval olcsóbb, és igény szerinti környezetben elvégezhető. Ebben a fejezetben egy olyan lehetséges kísérleti elrendezést mutatok be, amely alkalmas lehet vizsgálatok végzésére, illetve bemutatok néhány, a gyakorlati alkalmazás során jelentkező problémát és megoldásaikat.

A laborban történő vizsgálathoz megfelelő méretű, környezetétől légmentesen elzárt dobozra van szükség. Ennek két oldalán, egymással szemben tükröket helyezünk el. A sugarat ezeken reflektálva elérhető megfelelő hosszúságú fényút. A rendszerbe belépő preparált foton a tükrökön visszaverődik, majd elegendő számú reflexió után a detektorba kerül, ahol mérést végzünk rajta. Elegendő számú fotonból a preparált állapot ismeretében meghatározható a bit-hiba arány.

Első lépésként a dobozon belül a lehető legjobb vákuumot hozzuk létre, és így végzünk mérést, ez lesz a referencia. Erre azért van szükség, hogy felmérjük az optikai elemek hatását, hiszen például a tükrök hatása a légkörben nem lesz jelen. Ezután tiszta levegőt, vagyis oxigén és nitrogén megfelelő arányú keverékét juttatjuk be. Ezzel a Rayleigh-szórás hatását tudjuk vizsgálni. Végül bejuttatjuk a szennyezőket (főképp vízpárát, aeroszolokat (füst, por)). Ezek koncentrációját esetlegesen változtatva is végezhetünk méréseket.



15. ábra: Egy lehetséges kísérleti elrendezés sematikus rajza

A rendszernek mindenképpen tartalmaznia kell pár darab ventilátort. Ez egyrészt az aeroszolok megfelelő eloszlatása érdekében fontos, másrészt pedig a ventilátorokkal még egy fontos légköri tulajdonság modellezhető: a turbulencia. A turbulencia befolyásoló képessége alapvetően abból ered, hogy a turbulens áramlás térben és időben inhomogenitást okoz a közegben, ami miatt változik a lokális törésmutató. A jelenséget, főleg a csillagászok, (atmoszférikus) szcintillációnak nevezik. Természetesen figyelni kell, hiszen a túl nagy sebességű ventilátorok teljesen tönkretehetik a kísérletet, olyan mértékben eltérítve a nyalábot, amely már nem detektálható.

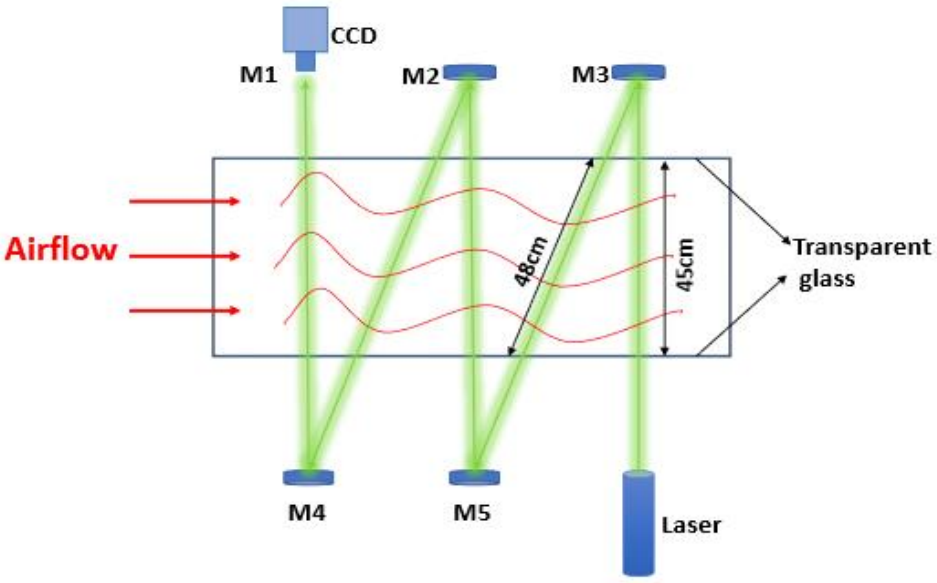
Szerencsére a szabadlégköri optikai kommunikáció fontossága miatt ez egy aktívan kutatott terület. Például [33]-ban egy elméleti modellt láthatunk, amit kísérlettel validáltak, az eredmények pedig felhasználhatóak a saját rendszerünk tervezésénél.
Az elméleti modell a következőképpen írja le a propagációt random turbulens környezetben:

$$i\frac{\partial A(x,y,z)}{\partial z}+\frac{1}{2k}\nabla_{\perp}^{2}A(x,y,z)+kn_{1}A(x,y,z)=0, \tag{4.1}$$

ahol k a hullámszám, n_1 a szél által okozott törésmutató, A(x,y,z) pedig az ún. light field, egy olyan vektor függvény, amely fény terjedését fejezi ki. Valamint:

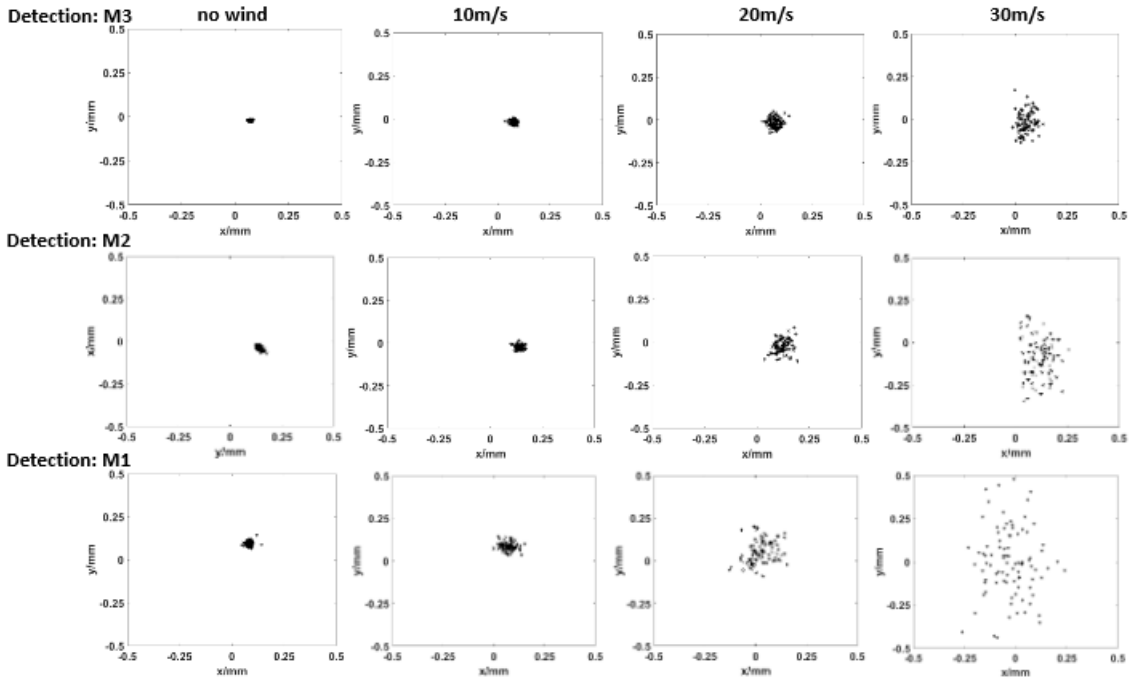
$$\nabla_{\perp}^{2}=\frac{\partial^{2}}{\partial x^{2}}+\frac{\partial^{2}}{\partial y^{2}}. \tag{4.2}$$

A tesztelésre létrehozott rendszer sematikus rajza a 15-ös ábrán látható:



16. ábra: A szél nyalábra gyakorolt hatásának mérése

A szélcsatorna szélessége 45 cm. Az 532 nm-es forrás által generált nyalábot 4 alkalommal reflektálják, illetve 3 ponton mérik.



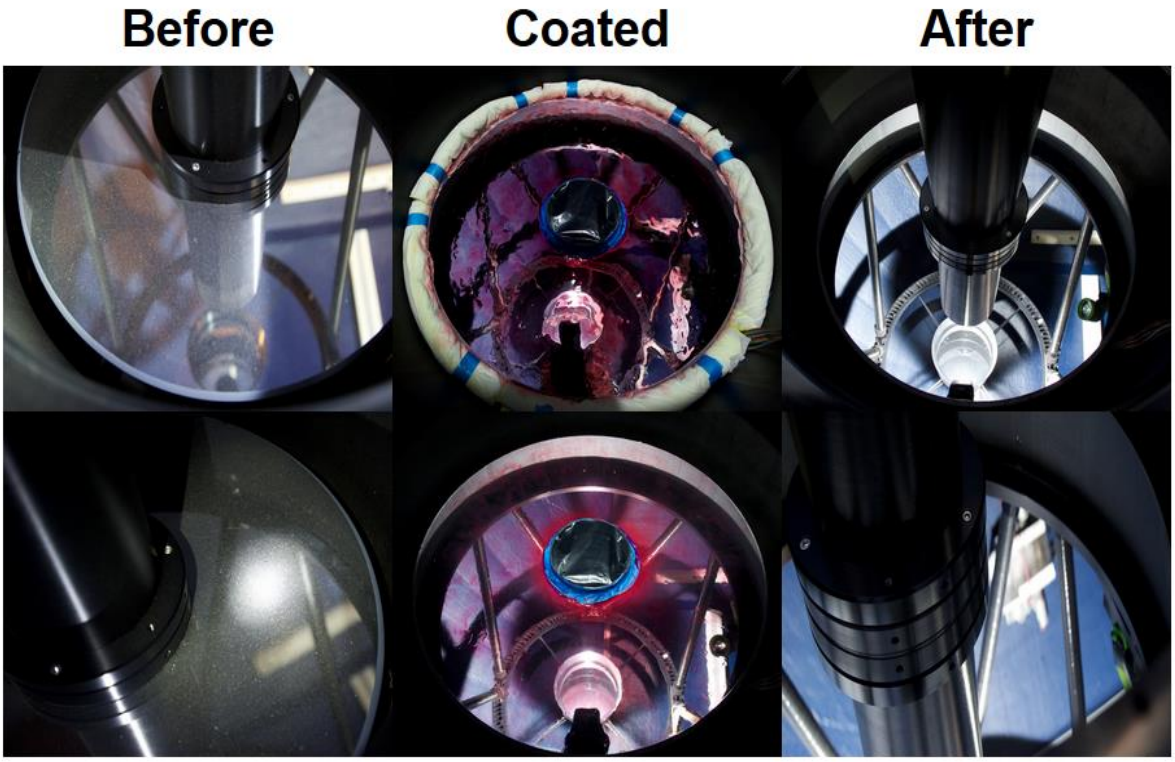
17. ábra: Szélcsatornában történt mérések eredményei

A mérési eredmények alapján a saját rendszerünk paraméterei ismeretében meg tudjuk határozni a ventilátorok ideális sebességét, illetve ezen sebesség mellett a nyaláb propagációját.

Emellett felvetődik a problémaként a tükrök védelme. A zárt rendszerbe bevezetett aeroszolok könnyedén megtapadhatnak az optikai elemek felületein, befolyásolva ezzel a későbbi méréseket, illetve csökkentve az élettartamot. Tekintve, hogy egy ilyen rendszer egyik legdrágább elemei a tükrök, ez nem szerencsés.

Optikai elemek tisztítására többféle megoldást alkalmaznak az iparban. A legegyszerűbbek a valamilyen tisztítófejjel, vagy nagynyomású vízzel, illetve levegővel való tisztogatás a használat után. Sajnos ezek sokszor megkarcolhatják, vagy megsérthetik a felületet, ami ugyanúgy befolyásolja a mérést és csökkenti a tükrök élettartamát. Másik esetleges megoldás az elektrosztatikus védelem. Amikor nincs lehetőség időről-időre tisztítani, akkor a felület mögé, vagy közvetlenül rá kötött elektronikával lehetséges valamilyen mértékben taszítani a port, és tisztítani is a már lerakódott réteget. Ilyen alkalmazások legfőképp a nagyon magas épületeket ablakain fordulnak elő (főleg Kína, Dubai), de például a NASA-nál is felvetődött roverek napelemeinek tisztítására [34]. Ezek azonban drága és számunkra szükségtelenül bonyolult rendszerek.

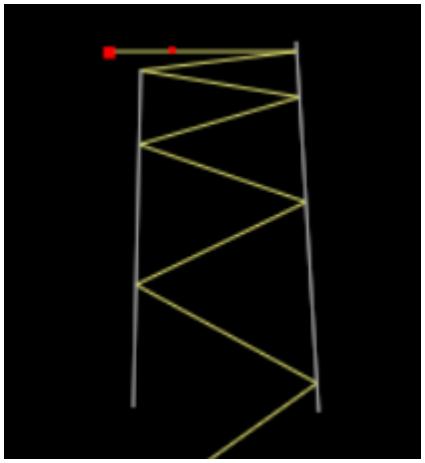
Az általam javasolt egy köztes megoldás, a First Contact Polymer [35]. Ez tulajdonképpen egy spray, amivel be kell fújni a felületet. Némi várakozás után megszilárdul, és egy alkalmas segédeszközzel (ami szintén van a csomagban) el lehet távolítani. Nem sérti fel az anyagot, és eltávolítja a megtapadt szennyeződést. Nem kell hozzá tisztítófej, vagy törlőkendő. Ugyanezt a terméket használják például a Keck Obszervatóriumban, Mauna Keán. Természetesen éles használat előtt érdemes rendelni egy csomagot és kipróbálni, hogyan működik, és milyen mértékben befolyásolja az optikai elemeket.



18. ábra: First Contact Polymer használat közben

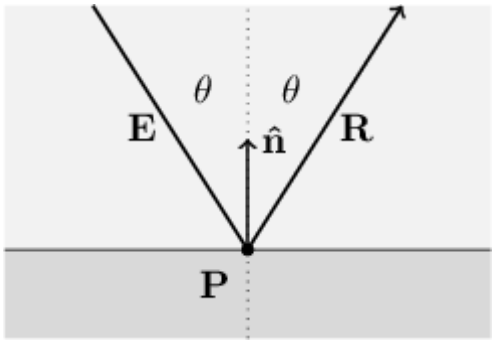
A tükrök elrendezése és alakja is fontos. Szeretnénk a lehető leghosszabb fényutat, vagyis a lehető legtöbb reflexiót elérni. Ehhez a legkézenfekvőbb elrendezés a két, egymással szemben felállított síktükör, így jelen dolgozatban ezt fogjuk vizsgálni.

A két síktükör elhelyezésében három módon állhat elő hiba: ha párhuzamosan állnak, de el vannak csúszva; ha párhuzamosan állnak, de a mérttől távolabb; illetve, ha nem párhuzamosan állnak, egymással valamekkora szöget zárnak be. Az első két eset a könnyebben kizárható, illetve nem is okoz nagyobb hibát. A harmadik eset azonban nagyon is reális: tökéletesen párhuzamosan beállítani két tükröt mérnökileg is nehéz feladat. Természetesen az effektus pici, azonban elég sok reflexió esetén komolyan befolyásolja a rendszer képességeit. Ekkor ugyanis a beesési szög, és ezzel a visszaverődés szöge folyamatosan nőni fog, míg a nyaláb egyszer csak „lecsúszik” a tükörről, jóval kevesebb reflexiót elérve, mint ideális esetben.



19. ábra: Két, egymással nem teljesen párhuzamos tükör esete

A probléma vizsgálatára egy egyszerű sugárkövető (Ray-Tracing) programot írtam, amely kiszámolja a reflexiók szögét. Vegyünk egy egyszerű síktükröt, amire érkezik egy fénysugár:



20. ábra: Visszaverődés síktükörről

Az ábrán E vektor jelöli a beérkező sugarat, R a reflektált sugarat, $\hat{n}$ pedig a felület normálvektorát. A beérkezés szöge a normálishoz képest θ, és a tükörtörvényből tudjuk, hogy ez lesz a visszaverődés szöge is. E és $\hat{n}$ ismeretében R a következőképpen határozható meg [36]:

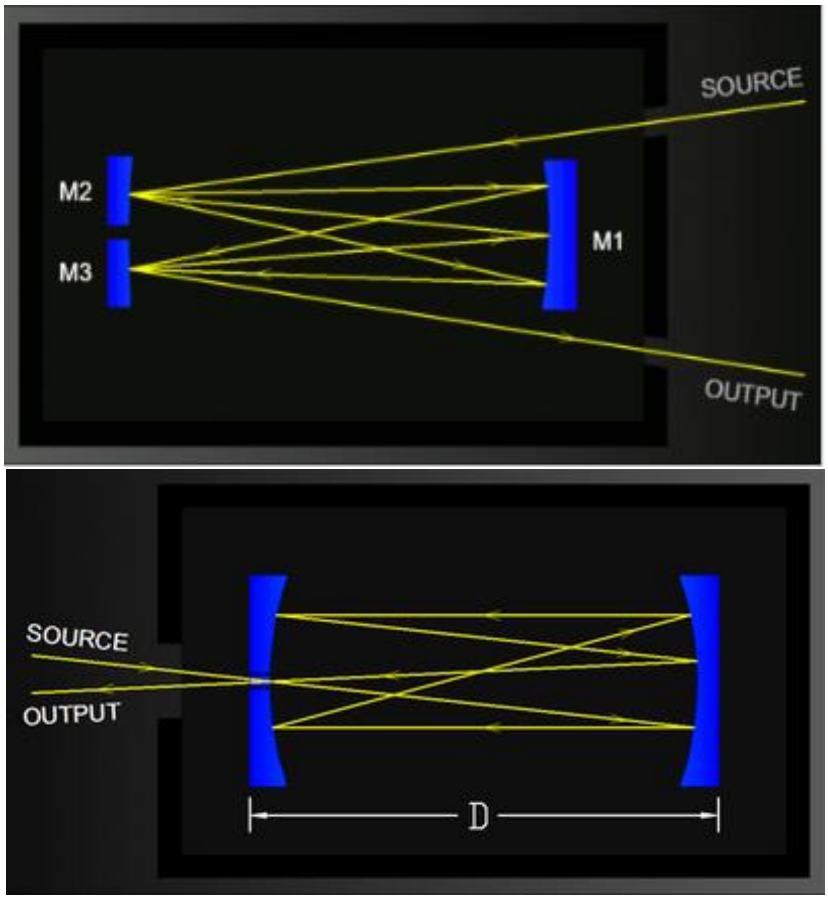
$$R = E - 2(E * \hat{n}\,)\hat{n}. \qquad (4.3)$$

Mivel E-t ismerjük, $\hat{n}$ síktükör esetén triviálisan meghatározható, ezért R számolható.
A programban a következő geometriát alkalmaztam: a két tükör egymással szemben áll, 1 méter hosszúak, és a legközelebbi pontjuk egymástól 1 méterre van. az egyik tükör α fokkal el van fordítva a párhuzamostól. Ez egy valamilyen beállítási pontatlanság, 3 különböző értéket próbáltam ki. A kezdeti fénysugár merőleges a megfelelően beállított tükörre. A program addig fut, amíg a fénysugár le nem csúszik a tükörről, majd ezután megnézzük az elért reflexiók számát. Az eredmények az alábbi táblázatban láthatók:

α	reflexiók száma
0.1	32
0.01	106
0.001	338

Figyelembe véve, hogy a tükrök közötti távolság egy méter, a fényút nagyjából a reflexiók száma méterben. Természetesen a már megépített rendszerben a fényút könnyedén mérhető lesz a fénysebesség segítségével.
A jövőben a programot tervezem módosítani bonyolultabb geometriák vizsgálatához.

Itt még érdemes megemlíteni az iparban főleg spektroszkópiára használt multipass cellákat. Ezek vékony hengerek, amiknek két végébe szférikus tükröket helyeztek úgy, hogy reflektálják a fényt a túloldalra. A nyaláb egyik oldalon bemegy, a másikon pedig távozik, miután adott távolságot beutazott a hengerben. A két legismertebb típusa ezeknek a White cella [37] és a Herriot cella [38].

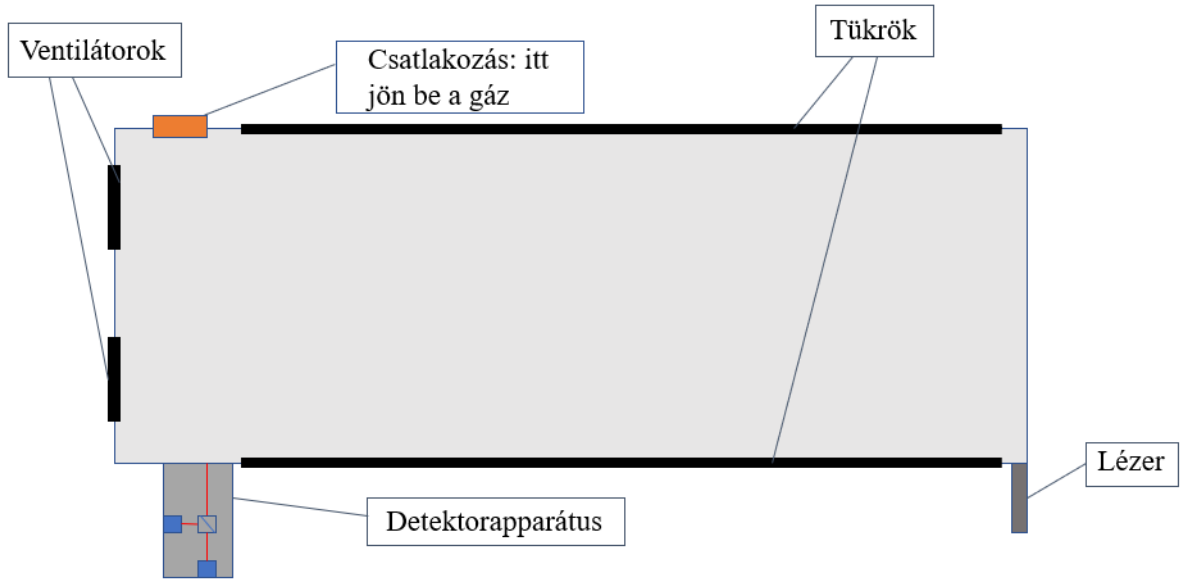


21. ábra: Multipass cellák elrendezése. Felül a White cella, alul a Herriot cella

Azonban ezen rendszerekben az optikai úthossz tipikusan 16-32 méter között mozog [39]. Emellett ezek a rendszerek nem alkalmasak arra, hogy utólag hozzáadott

alkotóelemeket keverjenek el, egyetlen nyílás van gáz bevezetésére, és nem tartalmaznak semmilyen ventillátort. Emiatt szükség van saját, testreszabott rendszer tervezésére és építésére, amellyel hosszabb úthosszon vizsgálódhatunk, és tetszőlegesen tudunk hozzáadni és elkeverni aeroszolokat.

Végül egy előzetes javaslatot teszek az emulátor rendszer felépítésére. Ennek sematikus rajza látható a 22.-ik ábrán.



22. ábra: A légköremulátor rendszer sematikus rajza

A rendszer teljes mérete körülbelül 1x1.1 m. A tükrök egy méter hosszú síktükrök. a plusz tíz centi a detektorapparátus és a lézer, illetve a szelep helye. A szélcsatornás mérés azt mutatja, hogy a függőleges deviancia elhanyagolható nagyságú, bár ilyen sok reflexiónál a felületi hibák ezt növelhetik, így a tükrök magasságát 10-15 cm-nek hagynám. A rendszer bal oldalán a tükrök mellett kap helyet a detektorapparátus, illetve az a szelep, amin a gázkomponenseket bevezetjük. Ezen csatlakozásra a másik alkalmas méretű hely a ventilátorokkal szemben lenne, de akkor félő, hogy a ventilátorok visszanyomnák a gázt, és több időbe telne eloszlatni. Így a beérkező komponenst nyomják előre, és az meglehetősen gyorsan szétterül.

Ami a ventilátorok sebességét illeti: háromfajta mérést javaslok. Az első szélcsendes idő, amikor egyáltalán, vagy alig működnek mérés közben. A második 10 m/s-os sebesség. Ez a Beaufort-skálán élénk szél [40], de nem viharos. A harmadik a 20 m/s-os sebesség, amely már viharos szélnek számít. Skálázva a [39]-es adatait a saját rendszerünkre, a nyaláb várható devianciája 0.51 mm, illetve 1.55 mm. Természetesen turbulens esetekről beszélünk, így pontos értéket lehetetlen mondani, de a trend alapján ekkora értékekre lehet számítani.

Ahogy korábban megmutattam, ezzel az elrendezéssel várhatóan 106 méteres optikai úthossz érhető el, szemben például a Herriott-cella 31.2 méterével. Azonban a rendszer mérete is nyilván nagyobb. A későbbiekben megpróbálok más tükörgeometriákat, ugyanis mindenképpen érdemes megvizsgálni, hogy egy ugyanekkora méretű rendszer más típusú tükrökkel, vagy más elrendezésben (például sokszögek esetén) milyen optikai úthosszra képes. Ez alapján az emulátorrendszer később még módosulhat.

5. Összefoglalás és továbblépési lehetőségek

A jelenleg alkalmazott kriptográfiai megoldásaink arra támaszkodnak, hogy nincs olyan elérhető számítógépes kapacitás, ami elég gyorsan képes lenne feltörni ezeket. Ez azonban a kvantumszámítógépek küszöbön álló megjelenésével megváltozik. Szükség van a kvantumkriptográfiára, amely valódi biztonságot nyújthat a lehallgatók ellen. Azonban ezen biztonság eléréséhez szükséges minél biztosabban meghatározni a várható bithiba-arányt.

Ez szabadlégköri kvantumkommunikáció esetén bonyolult feladat. A légkör nagyon dinamikus, hirtelen változhat, illetve évszakonként is van egy nyomon követhető változás. A kétfajta szórás, amely befolyásolja a bithiba-arányt, a Rayleigh- és a Mie-szórás. Utóbbi az aeroszolokra jellemző, így ezek koncentrációja a légkörben egy fontos mérték.

A légköri hatások modellezése laborban egy olcsóbb megoldás, illetve, mivel a paramétereket mi tudjuk beállítani, ezért kézenfekvőbb is, mint a szabadban mérni, és megfelelő környezeti tulajdonságokat várni, keresni. Azonban egy ilyen rendszer építése során több probléma is felmerül. Jelen dolgozatban a tükrök élettartamára, illetve a ventilátorok sebességének beállítására kínáltam megoldást, ezen kívül a tükrök geometriájával foglalkoztam. Felvázoltam egy lehetséges elrendezést ezek alapján.

A továbbiakban érdemes megvizsgálni más elrendezéseket és az ezek által kínált optikai úthosszt. Lehetséges ugyanis, hogy érdemi méret- és költségnövekedés nélkül nagyobb optikai úthossz érhető el hasonló rendszerrel, amellyel közelíteni lehetne a valós kommunikációs távolságokat. Ezen kívül érdemes megvizsgálni a hőmérsékleti viszonyokat egy ilyen cellán belül, ugyanis az esetleges páralecsapódás szintén nagyban befolyásolhatja a mérési eredményeket. A későbbiekben ezen kérdések vizsgálatát fogom elvégezni.

Források

[1] David Reinsel, John Gantz, John Rydning: The Digitization of the World From Edge to Core, IDC White Paper – #US44413318
[2] Peter W. Shor: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal on Computing. 26 (5), *doi*:*10.1137/S0097539795293172*
[3] Burt Kaliski: Twirl and RSA Key size, 2003, Corpus ID: 53855699
[4] Martin Giles: Explainer: What is post-quantum cryptography?, 2019, MIT Technology Review
[5] Craig Gidney, Martin Ekera: How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, 2019, arXiv:1905.09749 [quant-ph]
[6] Mirko Amico, Zain H. Saleem, Muir Kumph: An Experimental Study of Shor's Factoring Algorithm on IBM Q, 2019, DOI: 10.1103/PhysRevA.100.012305
[7] Charles H. Bennett, Gilles Brassard et al: Experimental Quantum Cryptography, 1992, J. Cryptology (1992) 5:3-28
[8] 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, 1998, [S0031-9007(98)07299-8]
[9] R. Ursin et al: Free-Space distribution of entanglement and single photons over 144 km, 2006, Nature Physics 3, 481 - 486 (2007)
[10] SK. Liao et al: Satellite-to-ground quantum key distribution, 2018, DOI: 10.1038/nature23655
[11] https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet
[12] Imre S. Quantum computing and communications – Introduction and challenges. Comput. Electr. Eng. (2013))
[13] J. M. Gambetta, J. M. Chow and M. Steffen, "Building logical qubits in a superconducting quantum computing system", *npj Quantum Information* 3, 2 (2017), doi:10.1038/s41534-016-0004-0
[14] Shankar, R. (1943). Principles of Quantum Mechanics (2nd ed.). Kluwer Academic/Plenum Publishers. *ISBN 978-0-306-44790-7*
[15] Nielsen, Michael A.*;* Chuang, Isaac (2000). Quantum Computation and Quantum Information. Cambridge: Cambridge University Press. ISBN 0521632358
[16] Matson, John (13 August 2012). "Quantum teleportation achieved over record distances". Nature News. doi*:*10.1038/nature.2012.11163. S2CID 124852641
[17] Boyd, Robert (2008). Nonlinear Optics, Third Edition. New York: Academic Press. pp. *79*–88. *ISBN 978-0-12-369470-6*.
[18] Diósi Lajos: Bevezetés a kvantuminformációelméletbe, ISBN 978 963 279 978 0
[19] W. H. Zurek, W. K. Wootters: A Single Quantum Cannot Be Cloned, Nature vol. 299, (1982)
[20] Bennett, Charles H.; Brassard, Gilles (2014-12-04). *"Quantum cryptography: Public key distribution and coin tossing"*. Theoretical Computer Science. Theoretical

Aspects of Quantum Cryptography – celebrating 30 years of BB84. 560, Part 1: 7–11. *doi*:*10.1016/j.tcs.2014.05.025*
[21] Ekert, Artur K. (5 August 1991). *"Quantum cryptography based on Bell's theorem"*. Physical Review Letters. 67 (6): 661–663. *Bibcode*:*1991PhRvL..67..661E*. *doi*:*10.1103/PhysRevLett.67.661*. *PMID 10044956*
[22] Beer (1852). *"Bestimmung der Absorption des rothen Lichts in farbigen Flüssigkeiten"* [Determination of the absorption of red light in colored liquids]. Annalen der Physik und Chemie (in German). 86 (5): 78–88. *doi*:*10.1002/andp.18521620505*
[23] Stokes, G. G. (1852). On the composition and resolution of streams of polarized light from different sources. Transactions of the Cambridge Philosophical Society, 9, 399.
[24] W. H. McMaster: Polarization and the Stokes Parameters, American Journal of Physics, Vol. 22, Number 6, 1954 September
[25] Bohren, Craig F. and Donald R. Huffman, Absorption and scattering of light by small particles, New York : Wiley, 1998, 530 p., ISBN 0-471-29340-7, ISBN 978-0-471-29340-8
[26] Lide, David R. *Handbook of Chemistry and Physics*. Boca Raton, FL: CRC, 1996: 14–17
[27] Simon A. Carn: Fundamentals of Remote Sensing, Michigan Tech - Dept. of Geological and Mining Engineering and Sciences, Lecture
[28] L. D. Travis, J. E. Hansen: Light Scattering in Planetary Atmospheres, Goddard Institutes for Space Studies, New York, NY 10025 USA, 1974.
[29] Chris Mclinden: Radiative Transfer, 1999.
[30] Cox, A.J. (2002). *"An experiment to measure Mie and Rayleigh total scattering cross sections"*. American Journal of Physics. 70 (6): 620. *Bibcode*: *2002AmJPh..70..620C*., *doi*:*10.1119/1.1466815*
[31] George Mathew: CHARACTERIZATION OF STIMULATED RAMAN SCATTERING IN DIFFERENTMATERIALS, 2015, DOI: 10.13140/RG.2.2.35363.25
[32] Alberto Carrasco-Casado; Verónica Fernández; Natalia Denisenko: Optical Wireless Communication, Springer 2016, pp. 589-607 doi: 10.1007/978-3-319-30201-0_27
[33] Huang et al: Investigation on the behavior of a laserpropagating through a random environmentinduced by wind, 2019, OSA, https://doi.org/10.1364/OE.27.009420
[34] C. I: Calle et al: Particle Removal by Electrostatic and Dielectrophoretic Forces for Dust Control During Lunar Exploration Missions, 11th International Conference on Electrostatics 2009
[35] https://www.photoniccleaning.com/
[36] Don Cross: Fundamentals of Ray-Tracing, 2013
[37] *White, John (1942). "Long Optical Paths of Large Aperture". Journal of the Optical Society of America. 32 (5): 285. Bibcode:1942JOSA...32..285W. doi:10.1364/josa.32.000285*

[38] *Herriott, Donald; Schulte, Harry (1965). "Folded Optical Delay Lines". Applied Optics. 4 (8): 883–891. Bibcode:1965ApOpt...4..883H. doi:10.1364/AO.4.000883*
[39] https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=12671
[40] https://www.met.hu/ismertetok/Beaufort-skala.pdf