Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

Csizmadia Géza Gergő

ÚJGENERÁCIÓS VEZETÉKES KVANTUMKOMMUNIKÁCIÓS HÁLÓZATOK VIZSGÁLATA

KONZULENS

Dr. Bacsárdi László

BUDAPEST, 2021

Tartalomjegyzék

Összefoglaló

Napjainkban jelentős volumenű kutatások irányulnak a kvantumkommunikáció felé, mely fizikai alapokra helyezve garantál megbízható kommunikációt. Ezen technológia segítségével nagy távolságú szuperbiztonságos hálózatok építhetőek ki olyan intézmények és infrastruktúrák között, ahol a lehallgathatatlanság egy kritikus szempont. Továbbá lehetőségünk van összeköttetést létrehozni – akár nagy távolságra lévő – kvantumszámítógépek között, melynek segítségével a számítási kapacitásuk a korábbi érték akár többszörösére is nőhet, ezáltal hatékonyabban tudnak komplexebb feladatokat elvégezni. Szerte a világon vannak kísérleti jellegű projektek, ahol kvantumkommunikációs hálózatokat próbálnak meg egyre nagyobb távolságokban kiépíteni, és ezeket egyre eredményesebbé tenni.

Vezetékes kvantumkommunikáció esetén használt optikai szálakon lézerimpulzusokkal kommunikálunk, azonban az ebben haladó jel nagy távolságra való közvetítése során csillapítást szenved, melynek kiküszöbölésére köztes csomópontokra van szükségünk, amik a korábban beérkezett gyenge jelet felerősítve továbbküldik. Sajnos jelenleg nem léteznek ilyen egységek, mivel ismeretlen állapotú kvantumbitről nem tudunk identikus másolatot létrehozni, illetve a kvantumbitek mérése esetén a kommunikáció biztonsága sérülhet. Azonban elméletben tegyük fel, hogy ezek léteznek. Ezek a csomópontok lehetnek megbízhatóak, illetve nem megbízhatóak, utóbbi esetben feltételezzük, hogy a csomópont hardveres rendszere bármikor kompromittálódhat, így ez alapján kell tervezzük a protokollunkat. A köztes kommunikációra használt csatornákat optimalizálhatjuk különféle kvantum alapú protokollokra a hatékonyság növelése érdekében.

Munkám során kvantumkommunikációs hálózatok szimulációjával foglalkoztam. Nagy távolságú, nem megbízható csomópontokon alapuló és kvantumkulcsszétosztásra optimalizált hálózatokat vettem alapul, melyeket több aspektusból is megvizsgáltam. Először is, hogy más kvantumösszefonódáson alapuló protokoll – kvantumteleportáció, szupersűrű tömörítés – használható-e, és ezek milyen hatékonysággal működnek a megadott környezetben. Továbbá, amennyiben más protokoll nem kompatibilis a hálózattal, akkor milyen változtatások mellett van lehetőség ezek hatékony használatára.

Abstract

Nowadays, a significant amount of research is directed towards quantum communication, which guarantees reliable communication on a physical basis. This technology can be used to build long-range super-secure networks between institutions and infrastructures where interception is a critical concern. We also have the possibility to create interconnections between quantum computers, even over long distances, which can increase their computing power by several times, enabling them to perform more complex tasks more efficiently. Experimental projects are underway around the world to build quantum communication networks at ever greater distances and make them more efficient.

In fiber based quantum communications, information is coded into laser pulses. The signal travelling over the fibres suffers attenuation during transmission over long distances, and to overcome this we need intermediate nodes that amplify the weak signal received earlier and send it on. Unfortunately, such units do not currently exist since we cannot create an identical copy of a quantum bit in an unknown state, and the security of communication may be compromised if quantum bits are measured. However, imperfect copies can be created and based on these copies, we might be able to build quantum repeaters and quantum memories in the near future. These nodes can be trusted or untrusted, in the latter case we assume that the hardware of the node can be compromised at any time, so we must design our protocol based on this. The channels used for intermediate communication can be optimized for different quantum-based protocols to increase efficiency.

My work has involved simulation of quantum communication networks. I have considered networks based on long distance, untrusted nodes and optimized for quantum key distribution, which I have investigated from several aspects. Firstly, whether other protocols based on quantum entanglement – quantum teleportation, superdense coding – can be used and their efficiency in the given environment. Also, if other protocols are not compatible with the network, what changes can be made to make them effective.

1 Bevezetés

A kvantumkommunikáció már az első félévemben felkeltette az érdeklődésemet, köszönhetően tankörvezetőmnek. A nyár folyamán kezdtem el aktívan foglalkozni a kvantumkommunikáció rejtelmeivel, illetve ennek alapjaival. Szimulációkkal kezdtem el foglalkozni, melyet az alapjaitól tanultam.

Kvantumhálózatokat különböző célokra használhatunk. Először is, szuperbiztonságos kommunikáció vihető vele végbe, ami fizikai alapokon nyújt védelmet. Egy lehallgató könnyedén észrevehető a rendszerben, mely elősegíti a biztonságot. Továbbá összekapcsolhatóak különböző kvantumszámítógépek. Ez a felhasználás különösen érdekes, ugyanis ennek a segítségével megsokszorozhatjuk a számítógépek számítási kapacitását, melyet felhasználhatunk kutatási célokra. Az előbbieken kívül a jelenlegi kommunikációs rendszereink biztonságának növelésére is használható, ugyanis kvantumkulcsszétosztással biztonságos módon történhet a kulcscsere két kommunikáló fél között.

Különböző protokollokat használhatunk a kommunikáció során, melyek mindazonáltal, hogy biztonságosak, akár csökkenthetik is az átvitt bitek számát a kommunikáció sérülése nélkül. Munkám során összevetettem egy kvantumkulcsszétosztó protokollt, nevezetesen a BB84-et [1], illetve a kvantumteleportációt [2].

A fő célom az újgenerációs kvantumhálózatok vizsgálatával, hogy összevessem a jelenleg használatos kvantumhálózatokkal. Több aspektusból is vizsgáltam ezeket, melyek rávilágítottak, hogy kisebb változtatásokkal ugyan, de a későbbiekben egyéb protokollok használatára szintén használhatóak a jelenlegi felépítések.

A második fejezetben egy rövid áttekintést adok a kvantummechanika és a kvantumkommunikáció alapjairól, külön kitérve az általam használt jelenségekre, mint például a kvantumösszefonódás. A harmadik fejezetben ismertetem a NetSquid szimulátor felépítését és működését. A negyedik fejezetben bemutatom az általam készített szimulációt, illetve az eredményeket, amiket a kutatásommal értem el.

2 A kvantumkommunikáció alapjai

2.1 Kvantummechanikai alapok

A kvantumkommunikáció és kvantumszámítástechnika napjaink egyik leggyorsabban fejlődő és legkecsegtetőbb újításokat felmutató ága. A legtöbb előrehaladás a kvantumkommunikáció és a titkosítás terén történt. A kvantumszámítógépek ugrásszerű fejlődése következtében, ugyanis a korábbi matematikai alapokra helyezett titkosítási algoritmusaink kiszolgáltatottá váltak a kvantumalgoritmusok számára. Ennek következtében egyre nagyobb teret nyer magának a kvantumkulcsszétosztás, mely fizikai alapokra helyezve garantál megbízható kommunikációt a két fél között. Azonban ennek a műveletnek a megértéséhez szükséges a kvantummechanikai egyszerűsített modellje.

A kvantummechanika a fizika azon ága, mely a nanoszkopikus jelenségek működését és a látható világgal való kapcsolatát írja le. Alapjának a következő 4 posztulátumot tekintjük:

I. Zárt fizikai rendszer aktuális állapota egy olyan állapotvektorral írható le, amely komplex együtthatókkal rendelkezik, egységnyi hosszú a *H* Hilbert-térben

II. A zárt rendszer időbeli fejlődése unitér transzformációval írható le, amely csak a kezdő és végállapottól függ

III. Legyen {m} a mérés lehetséges eredményeinek a halmaza. Egy mérés a mérési operátorok halmazával adható meg { M_m }, ahol m mérés lehetséges eredményei.

Ha a megmérendő rendszer állapota $|\varphi\rangle$, akkor annak a valószínűsége, hogy a mérés az m eredményt adja $P(m|\ |\varphi\ \rangle) = \langle\varphi|\ M_m^{\dagger}\ M_m\ |\varphi\rangle$

A mérés után a rendszer állapot $|\ \varphi'\ \rangle = \frac{M_m|\rho\rangle}{\sqrt{\langle\rho|M_m^{\dagger}Mm|\rho\rangle}}$

IV. Ha V és Y a két kvantumrendszerhez rendelt Hilbert-tér, akkor az ebből a két rendszerből álló összetett rendszerhez a $W = V \otimes Y$ Hilbert-tér rendelhető.

A négy posztulátum szolgál alapjául a kvantummechanikának, illetve ezeket felhasználó tudományágaknak, ezáltal a kvantumkommunikációnak is. A mi megközelítésünkből megtudjuk ezeket feleltetni a következőeknek:

I. posztulátum – kvantumbitek

II. posztulátum – logikai kapuk

III. posztulátum – kvantum/klasszikus átalakítások, azaz mérések

IV. posztulátum – kvantumregiszterek

A kvantumkulcsszétosztás működésének megértéséhez meg kell ismerkednünk egy nagyon fontos jelenséggel, ami a kvantumösszefonódás. Vegyük a következő kvantumbitet: $|\varphi\rangle = a|0\rangle + b|1\rangle$, ahol φ a kvantumbit, 'a' és 'b' pedig az egyes valószínűségi amplitudók, vagyis ezek jelölik, hogy mekkora valószínűséggel mérjük ezt az állapotot. Különböző kvantumbiteknek vehetjük a tenzorszorzatát, azonban kvantumösszefonódás esetén nem tudjuk megfeleltetni a végső állapotot kvantumbitek tenzorszorzataként. Továbbá egy különös jelenség is életbe lép, miszerint az egyik kvantumbit mérése során a hozzáfonódott kvantumbit is felvesz egy értéket – mely függ az összefonódott állapottól –, a távolságtól függetlenül. Ezt Einsten csak „spooky action at a distance"-ként jellemezte.

Összefonódást a gyakorlatban CNOT (Controlled NOT Gate) kapuk segítségével érhetünk el. A kvantumkommunikáció során fontos, hogy olyan bázisokat válasszunk a mérésünkhöz, melyek ortogonálisak és ezáltal megkülönböztethetőek. Fontos kiemelni a Bell párokat, melyekre a korábban említett bázis tulajdonságok teljesülnek:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\beta_{00}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Az összefonódást több kvantumkommunikációs protokoll esetén is kihasználjuk – például a kvantumteleportációban -, melyeket a dolgozat későbbi fejezetében tárgyalok.

2.2 Kvantumkulcsszétosztás

A kvantumkriptográfia legismertebb és legfejlettebb alkalmazása a kvantumkulcsszétosztás (QKD – Quantum Key Distribution) [3], amely szimmetrikus kulcsok létrehozására alkalmas két fél között olyan módon, hogy egy harmadik személy, lehallgatás esetén se legyen képes megismerni a létrehozandó kulcsot. Ahhoz, hogy valóban teljesen biztonságos legyen ez a kommunikáció, egy kulcsot csak egy alkalommal használhatunk fel, ugyanis a kulcs felderítése klasszikus esetben jelentős kockázatot rejt magában.

A QKD protokollokat két-két csoportba sorolhatjuk. Az első generációs protokollok egyfoton forrásokon alapulnak, tehát egy időben mindössze csak egy fotont küld. Ennek az előállítása azonban nagyon nehéz. Második generációs protokollok esetén gyengített lézerjelekkel fotoncsomagokat küldünk, amelyek néhány tíz fotont tartalmaznak. Mindkettő esetén könnyedén észlelhető egy lehallgató fél, így teljesen biztonságosnak tekinthetőek. Továbbá lehetnek összefonódáson alapuló és összefonódást nem használó protokollok. Szimulációm során a BB84 protokollt valósítottam meg és vizsgáltam.

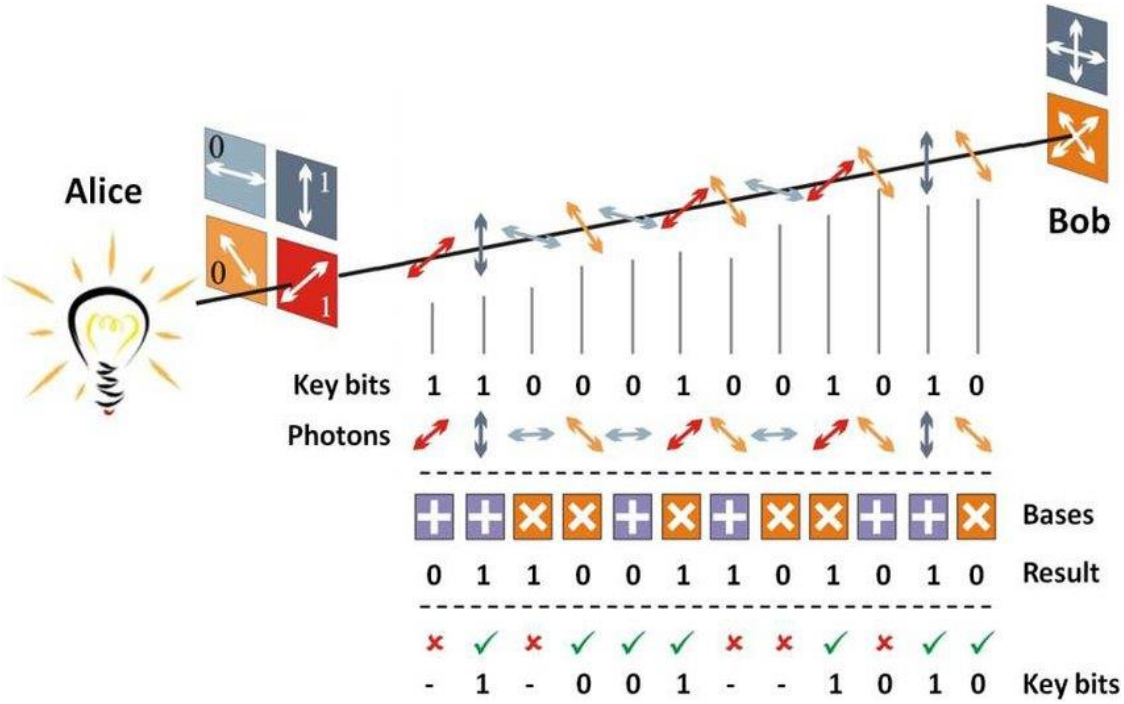
A csomópontok megbízhatóságát tekintve is alakíthatunk ki csoportokat. A megbízható csomópontokon alapuló kvantumkulcsszétosztás során feltételezzük, hogy egy csomópont fizikai rendszere rezisztens a támadásokkal szemben. Ezzel szemben nem megbízható csomópontok esetén a korábbi feltevést semmisnek tekintjük és számíthatunk arra, hogy a fizikai rendszer sérülékeny a támadásokra, ezáltal úgy kell megválasztanunk a protokolljainkat ebben az esetben, hogy ez ne jelentsen problémát.

2.2.1 BB84 protokoll

Ezt a protokollt Charles Benett és Gilless Brassard dolgozta ki 1984-ben. Lényegében ezt tekintjük az első kvantum kriptográfiai protokollnak. A protokoll biztonsága az NCT-n (No Cloning Theorem) [4] alapul, miszerint ismeretlen állapotú kvantumbitről nem tudunk identikus másolatot létrehozni. A protokoll lényege, hogy egy véletlenszám generátorral a küldő fél előállít egy 0 és 1-et tartalmazó számsorozatot, mely a bitek átvitele során alkalmazott kódolás módját határozza meg. A protokoll két féle bázist használ: $|0\rangle$ és $|1\rangle$, illetve $|+\rangle$ és $|-\rangle$. Utóbbi kettő a következőképpen írható fel:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

A fogadó fél a küldőhöz hasonlóan előállít egy véletlenszerű számsorozatot, a már korábban meghatározott módon, melyek a mérési bázisokat jelentik. Ezt követően a beérkezett fotonokat a fogadó egy detektorral, a már korábban generált bázisban megmér, majd így tesz az összes többi beérkezett fotonnal is. Ezt követően a fogadó egy publikus csatornán közli a küldővel, hogy sikeres volt a vétel. Ezután a publikus csatornán megbeszélik – a mérési bázisaik segítségével -, hogy melyek voltak azok a bázisok, amelyek mindkét félnél megegyeztek, az összes többi helyen pedig eltávolítják a mért biteket. A biztonság ellenőrzése érdekében, a küldő fél véletlenszerűen kiválaszt $\frac{k}{2}$ bitet, melyeket egy publikus csatornán elküld a fogadó fél számára és ellenőrzik, hogy egy megadott határértéknél kevesebb bit különbözik-e. A sikeres ellenőrzést követően további módszerek segítségével kidolgoznak egy szimmetrikus kulcsot, illetve felerősítik az adatvédelmet.



1. ábra: Alice (küldő) és Bob (fogadó) közötti kommunikáció. A képen jól látható a küldő által használt négy bázis, illetve a mérési eredmények.

2.2.1.1 Reconciliation – Információ-összeegyeztetés [5]

Az eljárás a csatornán való adatátvitel során keletkezett, illetve a mérőműszer tökéletlenségéből fakadó hibák javítására szolgál. Fontos, hogy ennek során mindössze minimális információt adjanak közzé a kulcsról, mivel a csatornát lehallgathatja egy harmadik fél. Az eljárás iterációkra osztott, ahol véletlenszerű permutációk és rostálás segítségével javítjuk a felmerülő hibákat. A permutált rostált kulcsot egyenlő blokkokra osztjuk, mely függ a kvantumbit hiba aránytól, és minden egyes új iteráció és permutáció során duplájára növeljük a blokkok méretét. A paritás tesztek minden blokk után összehasonlításra kerülnek, és bennük bináris kereséssel megkeressük a hibákat, majd javítjuk ezeket. Az algoritmus hatékonyságának növelése érdekében azonban ezt a műveletet többször is el kell végezzük, hogy biztosan kiküszöböljünk minden fennálló hibát.

2.2.1.2 Privacy Amplification – Titkosításfelerősítés [5]

Az információ-összeegyeztetést követően a kommunikáló feleknél nem teljesen privát kulcsok találhatóak, a korábbi algoritmus futtatásának köszönhetően. Azonban ennek a kiküszöböléséhez szükségünk van egy olyan hash függvényre, amely már a kapott adat minimális változása esetén is nagy változást idéz elő a kimeneti értékben. Erre a hash függvényre egy remek példa az SHA-512 [6].

2.3 Kvantumteleportáció

A kvantumteleportáció egy olyan eljárás, melynek a segítségével kvantum információt tudunk továbbítani. A küldőnek nem szükséges tudnia, hogy milyen információt továbbít, azonban a továbbításhoz meg kell mérnie a kapott kvantum bitet, majd ezt a fogadó félnek egy klasszikus csatornán továbbítani. Továbbá mindkét félnek rendelkeznie kell egy összefonódott fotonpár egyik tagjával.

Az eljárást már 1993-ban kidolgozták, olyan nagyszerű fizikusok, mint Bennett és Brassard. 1998-ban sikeresen véghez vitték az első kísérletet. A jelenlegi legnagyobb távolságú kvantumteleportálás rekordját egy kínai műhold segítségével vitték végbe, 1400 km távolságra.

2.3.1 Kihívások

Az egyik legnagyobb kihívás a no-cloning theorem, mely kimondja, hogy ismeretlen állapotú kvantumbitről nem tudunk identikus másolatot létrehozni. Ez önmagában kizárja egy tökéletesen működő kvantumjelismétlő létezését. Ugyanakkor a kvantum teleportációval képesek vagyunk egy ismeretlen állapotú kvantumbitet továbbítani, de ehhez meg kell mérnünk, majd klasszikus csatornán a vevő fél számára el kell küldenünk. Azonban ez az implementációja egy kvantumjelismétlőnek a biztonságot lecsökkenti. Amennyiben a hardverhez hozzáfér egy rosszindulatú támadó, a mérés eredményeivel és az összefonódott fotonpár másik tagjával könnyedén megszerezheti a számára érdekes információt. Továbbá természetes gondolat, hogy ennek az eljárásnak a segítségével a fénynél gyorsabb kommunikációt hajthatunk végre, azonban ez nem lehetséges. Az összefonódott fotonpárok módosítása esetén az összefonódás könnyedén megszűnhet, így nem tehetjük meg azt, hogy az összefonódott pár egyik tagját a számunkra szükséges állapotba hozzuk, majd a mérést követően a pár másik tagja is felveszi ezt.

A kommunikációhoz használt összefonódott fotonpár egyik tagját a fogadó oldalon tárolnunk kell mindaddig, ameddig a küldő oldalról nem érkeznek meg a megfelelő információk a klasszikus csatornán. Azonban nagy távolságok esetén ez a késleltetés, akár olyan mértékű is lehet, hogy a kommunikáció ebből fakadóan sikertelen. Ennek a kiküszöbölésére elméletben létező, azonban fizikailag egyelőre csak kezdetlegesen megvalósított kvantummemóriát terveztek, melyben lehetőségónk van egy kvantumbitet tárolni.

2.3.2 Menete

Kvantumteleportációhoz szükségünk van egy klasszikus csatornára, amely két klasszikus bit továbbítására képes, egy külső forrásra, aki a két kommunikáló fél között szétoszt egy összefonódott fotonpárt. A kommunikáció lépései:

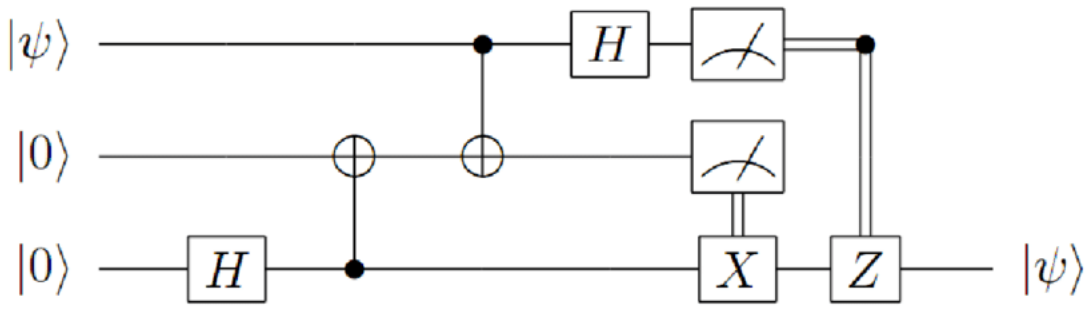
1. Egy Bell állapot generálódik, amelynek egyik tagját a küldő fél, a másik tagját pedig a fogadó fél kapja
2. Egy Bell mérés történik a küldő oldalon a teleportálásra szánt ($|\varphi\rangle$) és a kapott Bell állapotú kvantumbiten. Ennek kimeneteleként négy féle érték kapható, amely két biten leírható. Mindkét kvantumbit eldobásra kerül.

3. A klasszikus csatorna használatával, a két bit elküldésre kerül a fogadó számára.
4. A küldő oldalon végzett mérést követően a Bell állapotú kvantumbit a fogadó oldalon a négy lehetséges állapot valamelyikében van. Ezek közül az egyik megegyezik az eredeti kvantum állapottal |φ⟩. A másik három állapotot a kapott klasszikus bitek segítségével az eredeti állapotba transzformálhatjuk. Ehhez kvantumkapukra van szükségünk:

Kapott bitek	Használandó kvantumkapu
00	I |φ⟩
01	X |φ⟩
10	Z |φ⟩
11	ZX |φ⟩

1. Táblázat: A kvantumteleportációs eljárás során a fogadó oldalon történő kvantumkapuk használatának esetei.

Ezt követően egy |φ⟩-vel identikus kvantumbitet kapunk a fogadó oldalon.



2. ábra: A kvantumteleportáció fizikai megvalósítása. Az ábrán látható a klasszikus csatorna, amely a fogadó oldalon mért bitek továbbítására szolgál (dupla vonallal jelölve).

2.4 Kvantumhálózatok [7]

A kvantumhálózatok fontos elemét képezik a kvantum-számítástechnikának és a kvantumkommunikációnak. Ezek segítségével kvantumbitek segítségével

kommunikálhatunk a hálózaton, különböző, fizikailag elkülönülő kvantum processzorok között. Kvantum processzor alatt egy olyan egységet értünk, amely képes kvantum logikai kapukat végrehajtani megadott számú kvantumbiten.

Különböző felhasználási módjai vannak a kvantumhálózatoknak:

- Kvantumszámítások hatékonyságának növelésére: Ekkor különböző kvantumprocesszorokat kötünk össze, kvantumhálózatok segítségével. Segítségével a különálló processzorok számítási kapacitását összeadva, sok gyengébb helyett, egy erős, nagy számítási kapacitású, azonban elosztott processzort kapunk.
- Kvantumkommunikációra: Ebben az esetben valósíthatunk meg szuperbiztonságos kommunikációt két fél között. Ugyanis a kvantumcsatornákon való kommunikáció fizikai alapokra helyezi a biztonságot, a már megszokott matematikai modell helyett. Kvantumkulcsszétosztás során a már meglévő klasszikus kommunikációnkat egészítjük ki, a kettő együttműködik. Szupersűrű tömörítés segítségével egy megadott bitsorozatot feleannyi kvantumbit segítségével juttathatunk el a másik fél számára.

2.4.1 Hálózatok elemei

- **End nodes (végpontok):** A végpontok egyaránt képesek információ adására és vételére. Kvantumprocesszorok segítségével tudunk kvantuminformációkat előállítani és értelmezni, így ezek szerves részét képezik ennek az elemnek.
- **Kommunikációs csatornák:** Ebben az esetben beszélhetünk vezetékes, illetve szabadtéri hálózatokról. Előbbi esetben egy optikai szálat használunk lézerimpulzusokkal a kommunikációra, amely azonban nem tökéletes, így ezen a fotonok csillapítást és depolarizációt szenvednek el. Utóbbi esetben a levegőt használjuk közvetítő közegként, melynek következtében az átvitt információ sokkal jobban kiszolgáltatott a zajoknak, mint a vezetékes kommunikáció.
- **Jelismétlők [8]:** Jelenleg még csak elméleti alapon léteznek, a No Cloning Theorem miatt azonban kétséges a megvalósítása. Fizikai

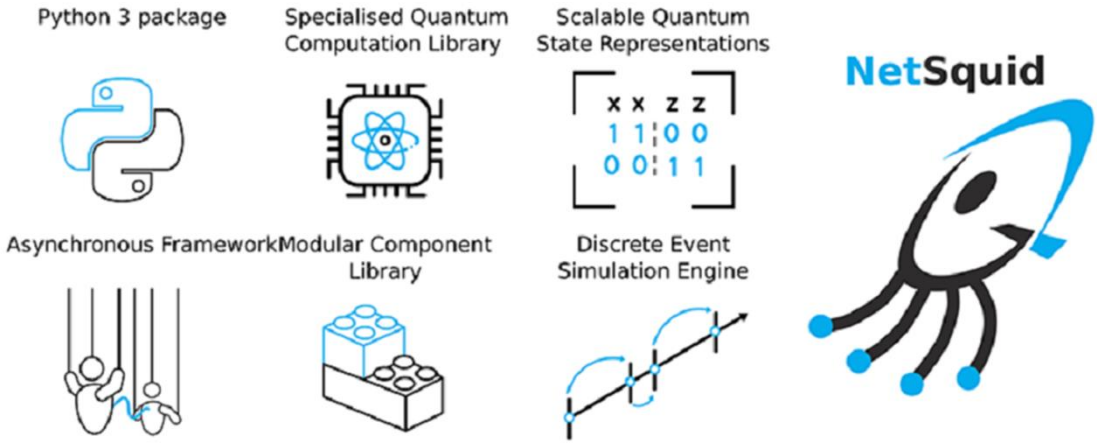
megvalósítása jelentős áttörést eredményezne a nagy távolságú kvantumkommunikációban. A vezetékekben jellemzően 0.25dB/km a csillapítás, amely nagy távolságok esetén meghiúsítja a kommunikációt.

3 Kvantum hálózati szimulátor

Dolgozatom elkészítése során megismerkedtem egy kvantum hálózati szimulátorral, a NetSquid-del. Az alapját a Python nyelv képezi, így könnyedén készíthetőek vele kvantum hálózati szimulációk. A következőkben ismertetem a felépítését és működését.

3.1 NetSquid [9]

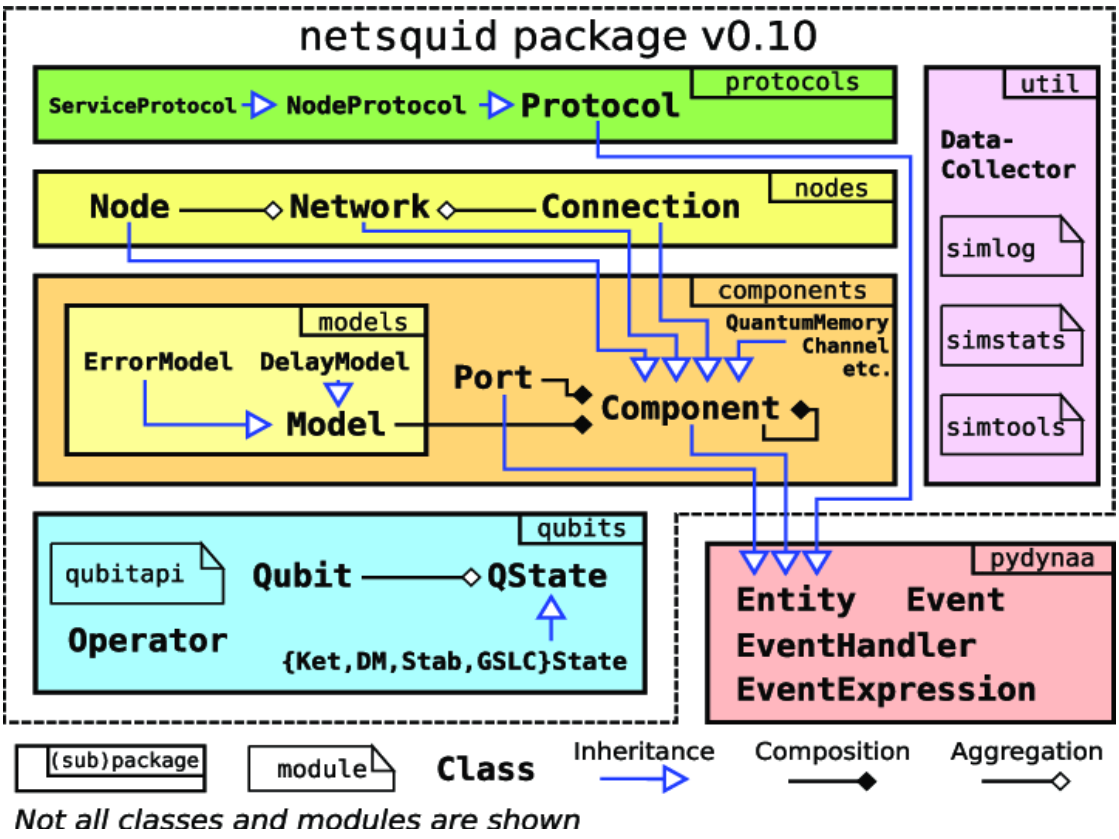
A NetSquid egy mozaikszó, melynek a feloldása Network Simulator for Quantum Information using Discrete events. A QuTech által fejlesztett szimulációs és modellező eszköz skálázható kvantumhálózatokhoz. A NetSquid egyik kulcs jellegzetessége, hogy könnyen és pontosan képes modellezni az idő hatását a kvantumrendszerben. Az eszköz moduláris megközelítése lehetővé teszi számunkra, hogy részletes fizikai modellt készítsünk a rendszerről és felhasználjuk komplex szimulációk készítésére, nagy méretű rendszerekhez.



3. ábra: A NetSquid kvantum hálózati szimulátor kulcs jellegzetességei, mely a versenytársakkal szemben előnybe helyezi.

3.2 Felépítése és működése

A NetSquid egy diszkrét esemény vezérelt szimulátor, amely a pyDynAA motort használja. Az eseményeket előre ütemezi, tehát egy szimuláció elindítása után a valós környezethez hasonlóan láncreakcióként mennek végbe a megfelelő események.



4. ábra: A NetSquid kvantum hálózati szimulátor moduláris felépítése, melyen jól láthatóak a különböző, egymással együttműködő modulok.

Az eszköz 6 almodulból épül fel, melyek a következők:

- **protocols**
- **nodes**
- **components**
- **qubits**
- **util**
- **pydynaa**

A különböző modulok használhatóak külön-külön egyenként is, azonban felhasználhatóak komplex rendszerek leírására is. Moduláris felépítésének köszönhetően

mindössze a megfelelő modulokat kell felhasználnunk, figyelembevéve a közöttük lévő logikai függőségeket. Amennyiben változtatni szeretnénk a rendszeren, mindössze a megfelelő modul cseréjére van szükség a többi réteg zavarása nélkül.

A szimulátorban kiválóan modellezhető egy közvetítő közeg tökéletlensége. Beépítetten tartalmazza a különböző depolarizációs és közvetítés során fellépő hibák modelljeit. Ezek figyelembe veszik, hogy az adott kvantumbit mennyi időt töltött egy adott elemben – kvantummemória, közvetítő közeg- vagy egy kapun áthaladva. A modellek által használt egyenlet egy valószínűséget ad vissza, amely megadja, hogy a kvantumbit mekkora eséllyel depolarizálódik vagy veszik el. A depolarizációs valószínűség kiszámításának módja a következő:

$P_{\text{depolarizáció}} = 1 - \exp(-\text{késleltetés [ns]} * \text{depolarizációs ráta [Hz]} * 10^{-9})$, ahol a depolarizációs ráta egy nemnegatív, változó érték.

4 Újgenerációs kvantumhálózatok modellezése

A dolgozatom témájának kiválasztásánál fontos szerepet játszott, hogy olyan kutatást végezzek, amely a későbbiekben felhasználhatóvá válik. Ennek érdekében témavezetőm ajánlásával a jelenleg használatban lévő kvantumhálózatok tulajdonságainak vizsgálatát tűztem ki célul. Mindezt tettem azért, hogy a későbbiekben megállapításokat tehessek az újgenerációs kvantumhálózatok kiépítésével kapcsolatban. A jelenlegi generációban a kvantumkulcsszétosztásra optimalizált hálózatok kerülnek kiépítésre, ebben a környezetben vizsgáltam a BB84 protokoll működését és tulajdonságait. Ugyanezt a rendszert felhasználva kvantumteleportációt hajtottam végre, majd megvizsgáltam, hogy ez milyen kihatással van a rendszeren átvitt kvantumbitre, illetve milyen módosítások szükségesek a rendszer megfelelő működéséhez nem kvantumkulcsszétosztó protokoll esetén.

4.1 Szimulátor működése

A két protokoll szimulációja jelentősen eltérő. Azonban a hálózatok felépítése, amelyekkel dolgoztam mindkét esetben megegyeznek. A szimulációk a kezdeti paraméterek kézzel történő megadását követően automatizáltan futnak.

4.1.1 BB84 protokoll

A protokoll segítségével szimuláltam két pont közötti kvantumkulcsszétosztást. Kezdetben változó paraméterekkel próbáltam megtalálni a protokoll megvalósításához optimális hálózati tulajdonságokat, majd ezeket felhasználva futtattam a további szimulációimat, ahol a távolság növelése mellett, a hálózatban található végpontok számát is növeltem.

Az átviteli közeg csillapításából és depolarizációjából adódóan egy hibajavító kódolásra volt szükségem, hogy a két végpont közötti kulcs kommunikáció titkosítására alkalmas legyen.

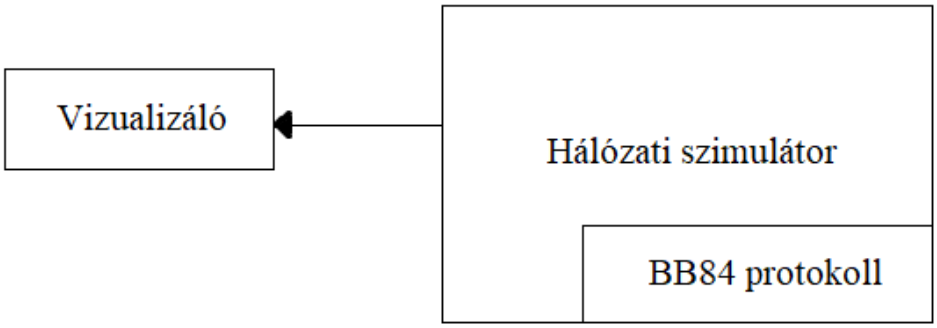
4.1.2 Kvantumteleportáció

A protokoll segítségével szimuláltam két pont közötti kvantumteleportációt. A korábban már BB84 protokoll során használt, kvantumkulcsszétosztásra optimalizált hálózat paramétereit használtam fel ennél a szimulációnál is.

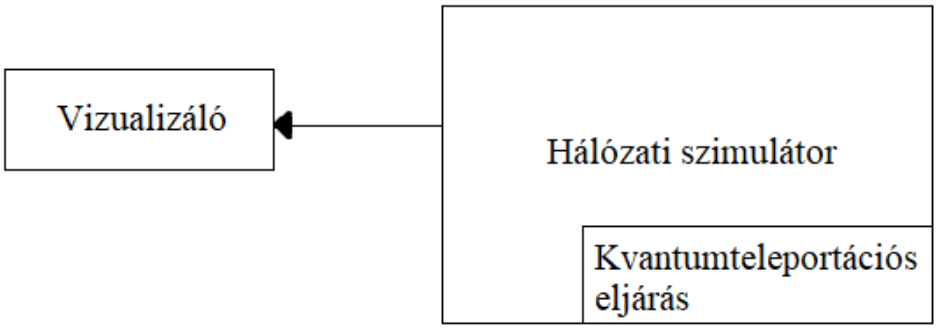
Az átviteli közeg csillapításából és depolarizációjából adódóan könnyedén megfigyelhetővé vált, hogy a jelenleg használatos kvantum hálózati paraméterekkel mennyire hatékony a protokoll működése.

4.2 A szimulációm felépítése

A szimulációimat a megadott protokollok működési leírása alapján implementáltam. Ezekhez felhasználtam a NetSquid-ben már megtalálható elemeket, illetve a NetSquid által biztosított alapvető funkciókat. A szimulátorom egyenlő távolságokra lévő végpontok közötti kommunikáció szimulációjára képes. Az átviteli közegekhez egyaránt használtam kvantum- és klasszikus csatornát.



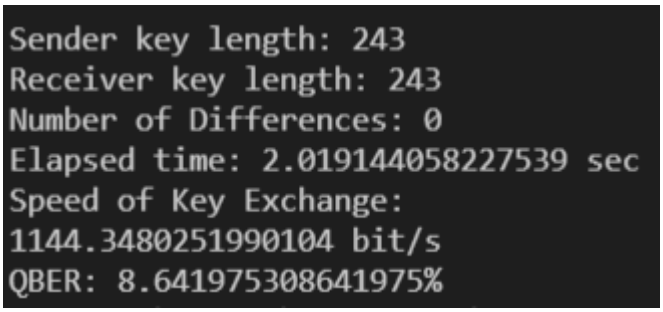
5. ábra: A BB84 protokollt használó szimuláció moduljai és azok közötti kapcsolatok



6. ábra: A kvantumteleportációs eljárást használó szimuláció moduljai és azok közötti kapcsolatok

4.2.1 BB84 protokoll modul

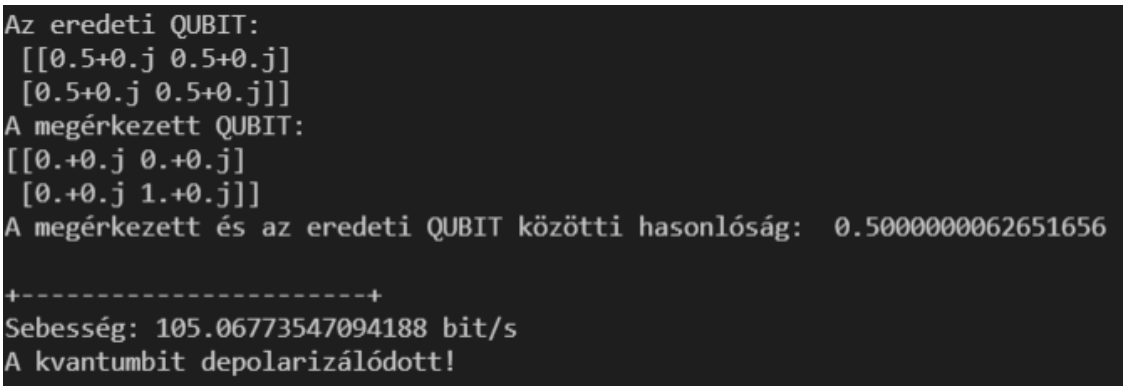
Ez a modul a BB84 protokoll eljárásait hajtja végre. A küldő és vevőoldalon generál egy véletlenszerű 0 és 1-et tartalmazó számsorozatot, amelyek a kódolási, illetve mérési bázisokat adják. Továbbá elvégzi a már korábban említett információösszeegyeztetést, amivel a szimmetrikus kulcsok előállnak. A végpontban eltárolt kulcsot egy hash függvénnyel, egészen pontosan SHA512-vel állítottam elő, melynek bemeneteként a már egyeztetett szimmetrikus kulcs szolgált. A modul erősen épít a hálózati modulra, hiszen ezen keresztül kommunikál a hálózatban található többi végponttal.



7. ábra: BB84 protokoll futásának adatai. A mezők fentről lefelé: A küldő kulcsának hossza, a fogadó kulcsának a hossza, a kulcsok közötti különbségek száma az információegyeztetést követően, a kulcsszétosztás ideje másodpercben, a kulcsszétosztás sebessége bit/s-ban, Kvantum bit hiba arány

4.2.2 Kvantumteleportációs modul

Ez a modul felelős a kvantumteleportáció eljárásainak végrehajtásáért. A végpontban, amely végrehajtja ezt az eljárást létrehozza az összefonódott foton párt, majd elküldi a vevő félnek, illetve kiolvassa és a hálózati modul segítségével a másik végpont számára továbbítja a klasszikus biteket, melyek a vevő oldalon az eredeti kvantumbit előállításához szükségesek. Ez a modul erősen épít a hálózati modul funkcionalitására.



8. ábra: Kvantumteleportáció futásának adatai. A mezők fentről lefelé: Az eredeti Qubit sűrűségmátrixa, a megérkezett Qubit sűrűségmátrixa, az eredeti és a megérkezett Qubit közötti hasonlóság, az átvitel sebessége, a következő mérés eredményeként kapott hibaüzenet

4.2.3 Hálózati modul

Ez a modul felelős a kvantumhálózatban található végpontok összeköttetéséért. Ebben találhatók meg azok az eljárások, amikkel a végpontok közötti átviteli közegek előállításra kerülnek – kvantum és klasszikus csatornák -, itt kerülnek előállításra a végpontok, illetve itt veszik fel a hálózati elemek a megfelelő paramétereket. Továbbá amikor egy végpont egy másikkal kommunikálni szeretne, akkor az ebben a modulban található eljárások segítségével kerülnek továbbításra a megfelelő adatok.

4.3 Eredmények

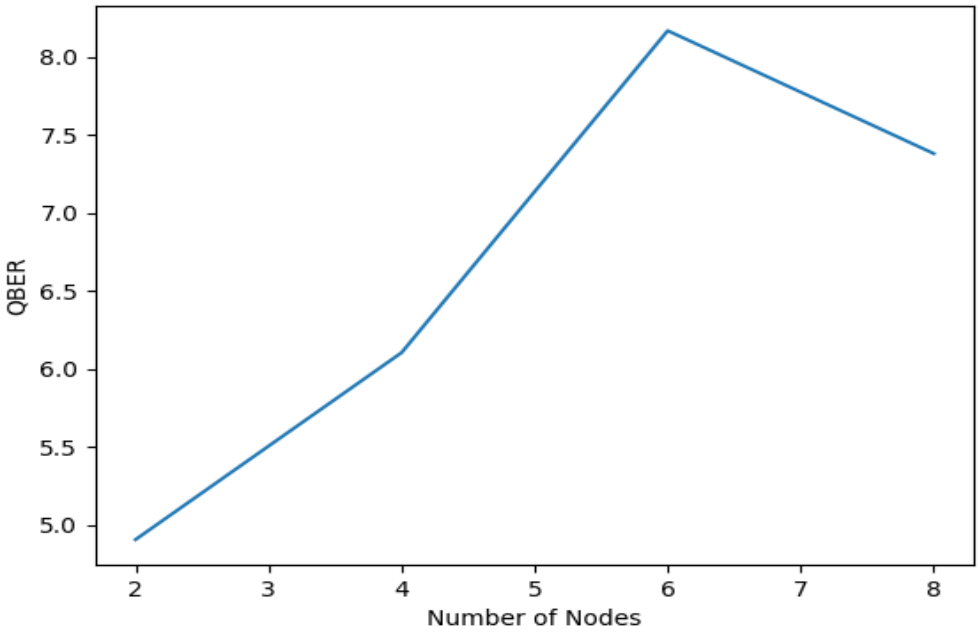
4.3.1 BB84

A BB84 szimulációt több paraméterrel is lefuttattam, változó végpontok közötti távolsággal – melyek továbbra is egyenlőek -, illetve a hálózatban található végpontok számának változtatásával. Az átviteli közeg egyéb paramétereit – késleltetés, depolarizációs ráta, csillapítás – nem változtattam.

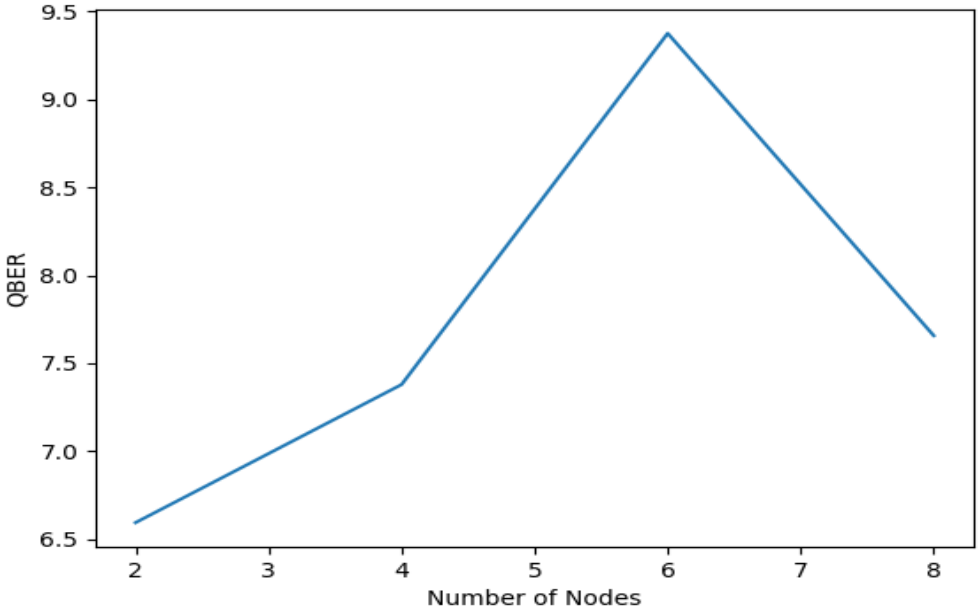
Paraméter neve	**Értéke**
Végpontok száma	2 – 8 db
Végpontok távolsága	10 – 70 km
Depolarizációs ráta	0.2
Csillapítás	0.25 db/km
Kulcs hossza	1024 bit

2. Táblázat: A BB84 szimuláció futása során használt hálózati paraméterek

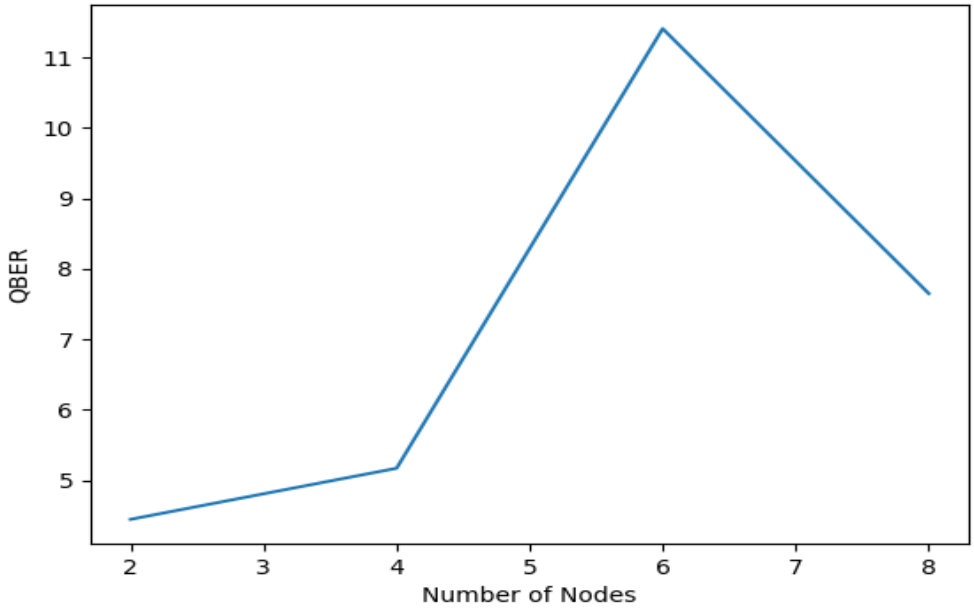
4.3.1.1 QBER a végpontok számának arányában



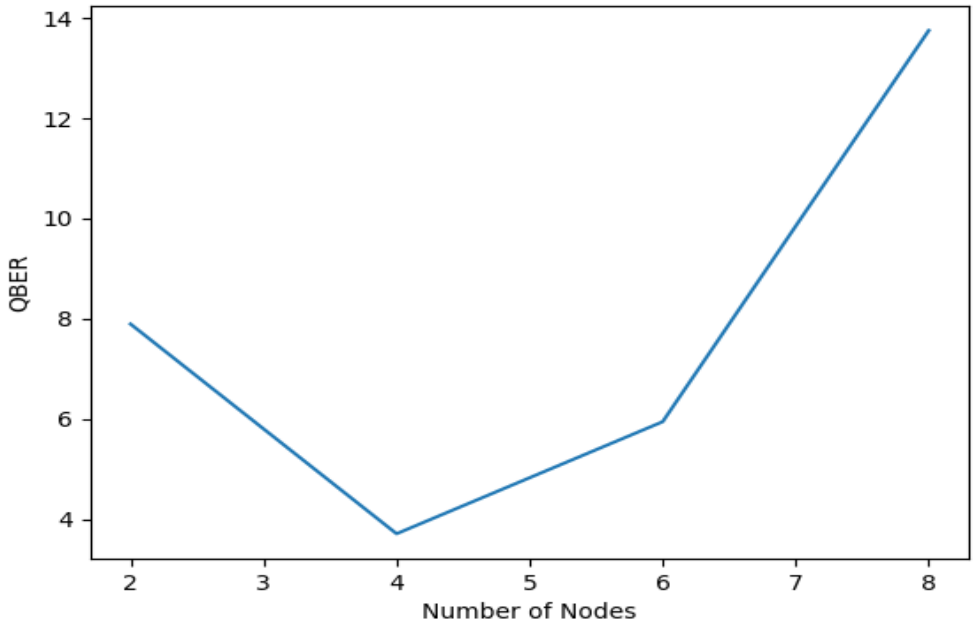
9. ábra: Kvantum bit hiba arány (%) a végpontok számának arányában, 10 km-es végpontok közötti távolsággal



10. ábra: Kvantum bit hiba arány (%) a végpontok számának arányában, 30 km-es végpontok közötti távolsággal



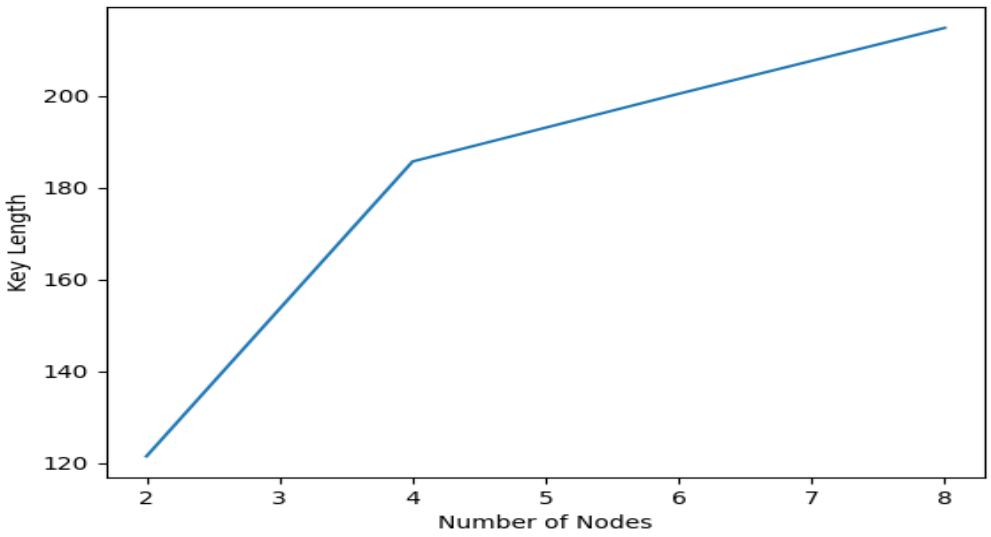
11. ábra: Kvantum bit hiba arány (%) a végpontok számának arányában, 50 km-es végpontok közötti távolsággal



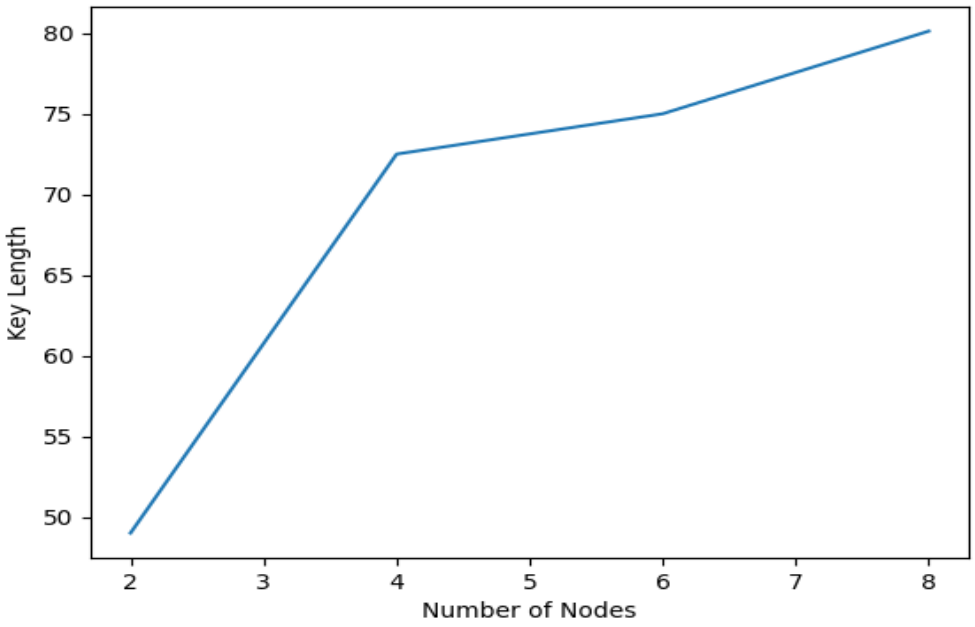
12. ábra: Kvantum bit hiba arány (%) a végpontok számának arányában, 70 km-es végpontok közötti távolsággal

Jól látható, hogy néhány kiugró érték következtében a grafikonok helyenként kilengéseket mutatnak. Azonban észrevehető, hogy a távolság és a végpontok számának növelésével a kvantum bit hiba arány egyenesen arányosan növekszik.

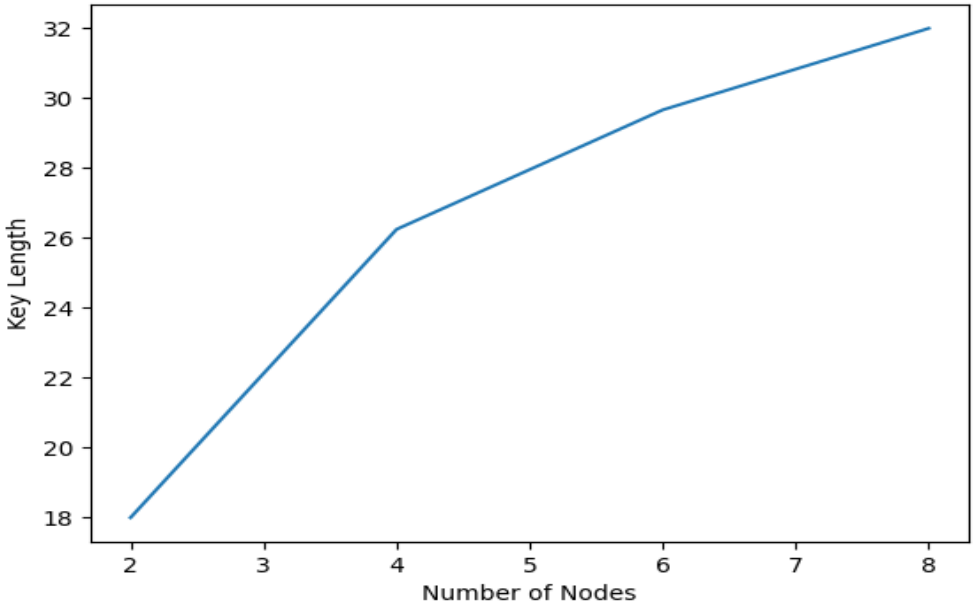
4.3.1.2 Kulcsok hossza a végpontok számának és távolság arányában



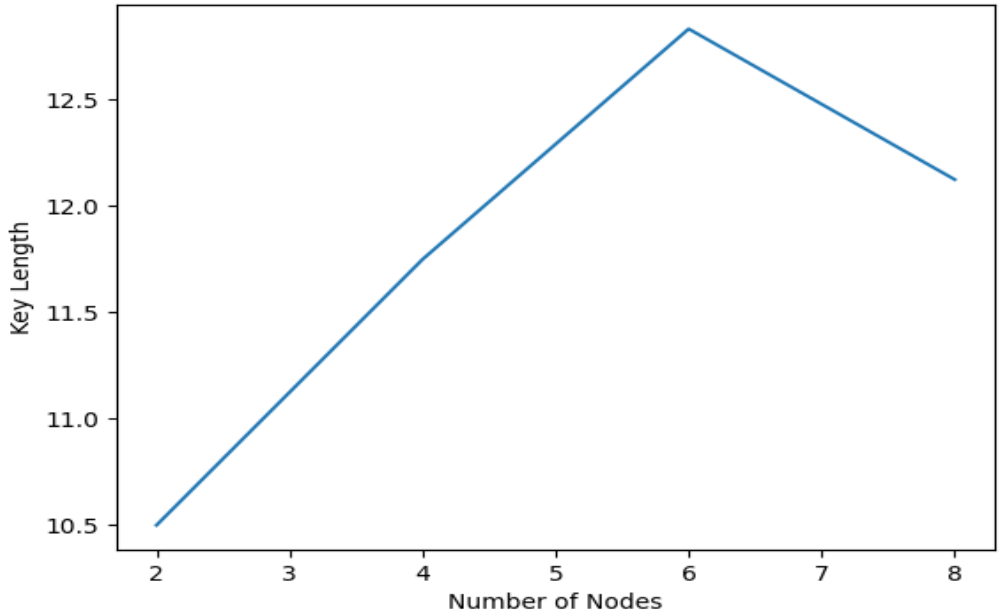
13. ábra: Kulcsok hossza (bit) a végpontok számának és a távolság arányában, 10 km-es végpontok közötti távolságnál



14. ábra: Kulcsok hossza (bit) a végpontok számának és a távolság arányában, 30 km-es végpontok közötti távolságnál



15. ábra: Kulcsok hossza (bit) a végpontok számának és a távolság arányában, 50 km-es végpontok közötti távolságnál

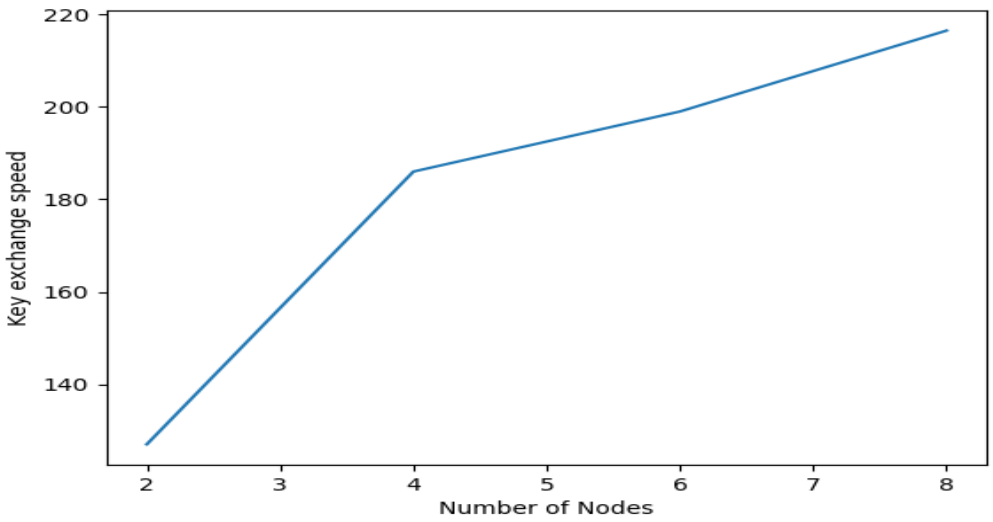


16. ábra: Kulcsok hossza (bit) a végpontok számának és a távolság arányában, 70 km-es végpontok közötti távolságnál

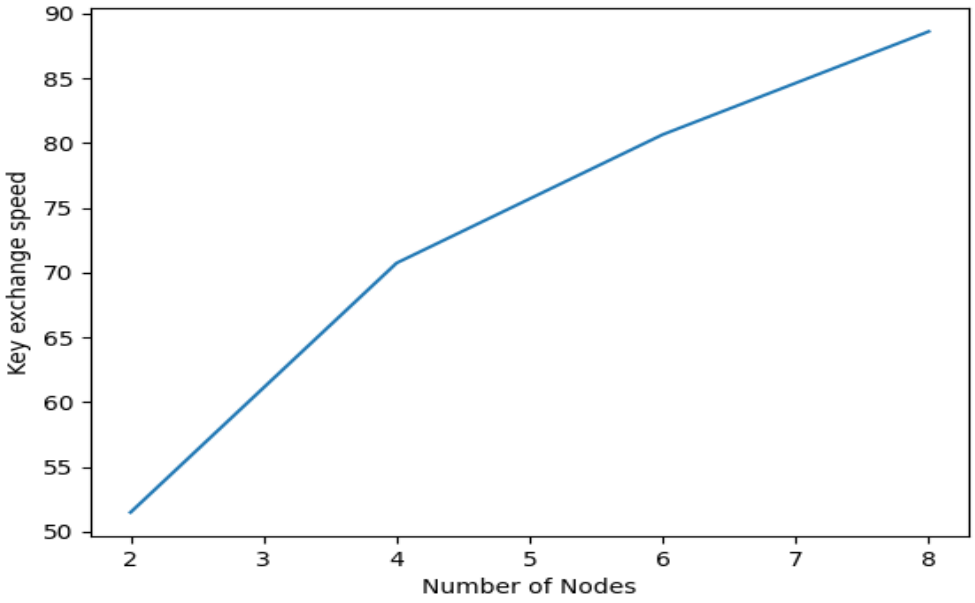
Jól megfigyelhető az ábrákon, hogy a kulcsok hossza a távolság növekedésével egyenesen arányosan csökken. Ugyanakkor a végpontok számával ez a szám növekszik,

köszönhetően, annak, hogy ezekben az esetekben átlagokat mérek, tehát egy-egy kiugró adat akár a teljes eredményt falssá teheti.

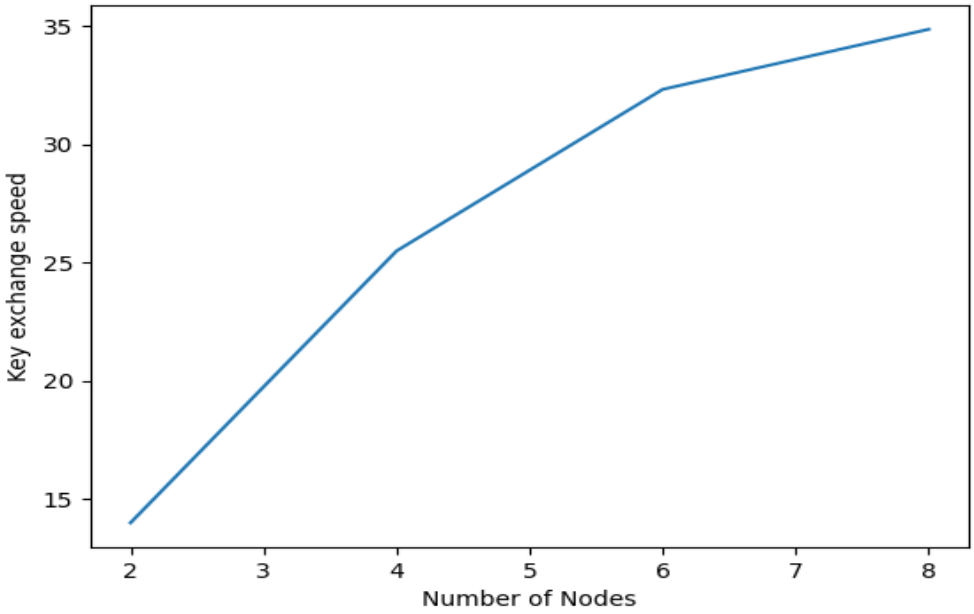
4.3.1.3 Átviteli sebesség a végpontok számának és távolság arányában



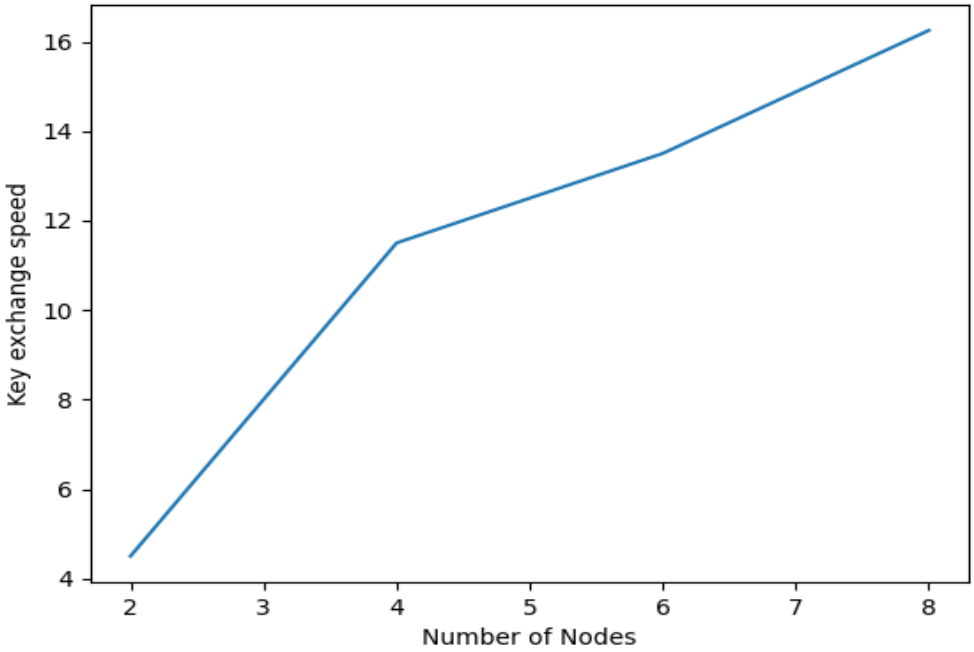
18. ábra: Átviteli sebesség (bit/s) a végpontok számának és a távolság arányában, 10 km-es végpontok közötti távolságnál



17. ábra: Átviteli sebesség (bit/s) a végpontok számának és a távolság arányában, 30 km-es végpontok közötti távolságnál



19. ábra: Átviteli sebesség (bit/s) a végpontok számának és a távolság arányában, 50 km-es végpontok közötti távolságnál



20. ábra: Átviteli sebesség (bit/s) a végpontok számának és a távolság arányában, 70 km-es végpontok közötti távolságnál

Jól látható a fenti grafikonokon, hogy a távolság növekedésével egyenesen arányosan csökken az adatátviteli sebesség, ugyanakkor az átlagolás miatt a végpontok számának növekedésével az adatátviteli sebesség is nő.

4.3.2 Kvantumteleportáció

A kvantumteleportációs szimulációt többféle paraméterrel is lefuttattam. Egyrészt növeltem a kvantumhálózatban található végpontok számát, másrészt pedig növeltem a végpontok közötti távolságot. A szimulációkat a BB84 szimuláció futásához használatos paraméterekkel futtattam, melyek a következők:

Paraméter neve	**Értéke**
Végpontok száma	2 – 8 db
Végpontok távolsága	10 – 70 km
Depolarizációs ráta	0.2
Csillapítás	0.25 db/km
Kulcs hossza	1024 bit

3. Táblázat: A kvantumteleportációs szimuláció futása során használt hálózati paraméterek

4.3.2.1 Kihívások

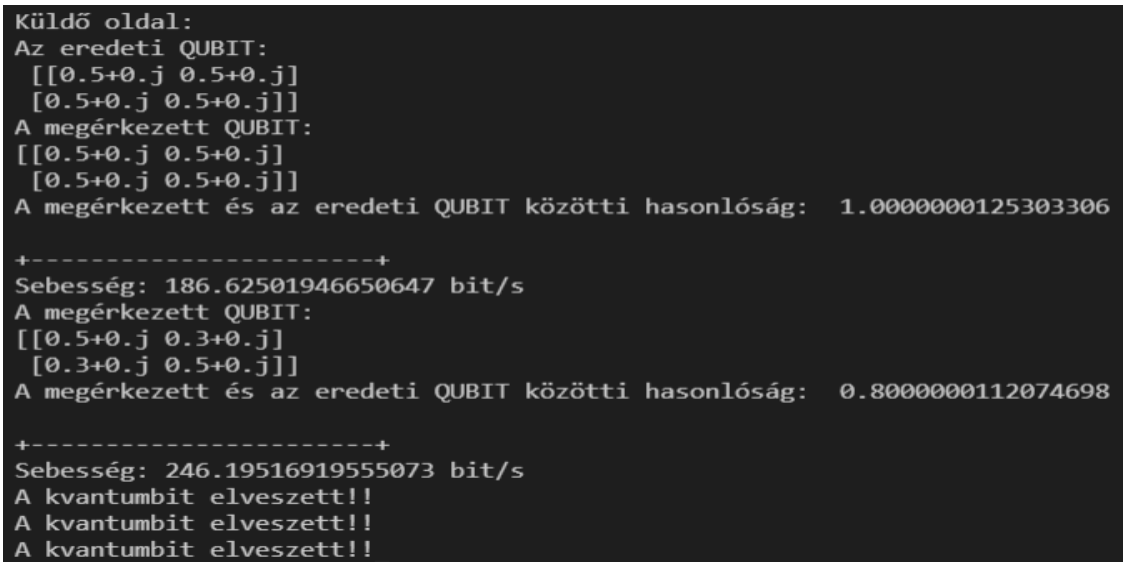
A kvantumteleportáció során minden átvitt kvantumbit jelentős szerepet tölt be az elküldött adatban, így ezeknek az elvesztése nem megengedett. Azonban a megadott hálózati paraméterekkel, sajnálatos módon mindössze néhány esetben sikerült adatot átvinnem a teljes rendszeren anélkül, hogy a küldött kvantumbit depolarizálódótt vagy elveszett volna. Azonban ennek a kiküszöbölésére használható lenne, hogyha az átvitt adatot a küldő oldalon megtöbbszöröznénk, majd átküldenénk a fogadó számára a megtöbbszörözött értéket. Ekkor a fogadó oldalon lévő végpont a méréseket követően kiválasztaná azt az értéket, amely a mérések során túlsúlyba került, ez adná az átvitt bitet.

További lehetőség egy kvantum hiba korrekciós eljárás implementálása, melynek segítségével a zaj okozta hatásokat tudjuk csökkenteni. Létezik már ilyen implementáció, amit Shor Code-nak neveznek Azonban ez az eljárás sem tudja garantálni, hogy az

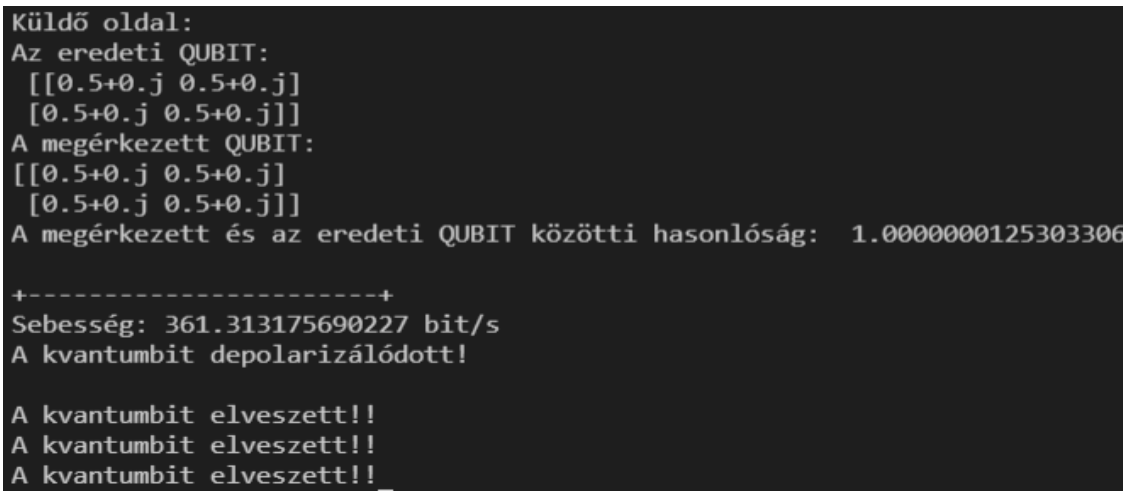
elküldött adat nem depolarizálódik vagy veszik el az átvitel során, így ez sem megoldás a problémára.

4.3.2.2 Mérési eredmények

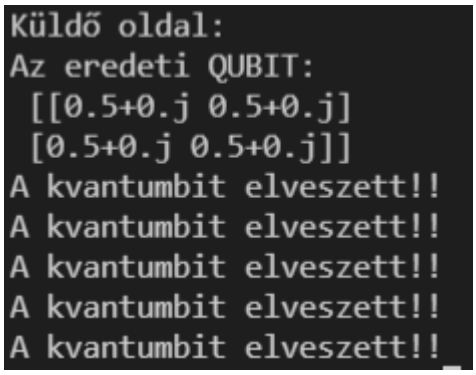
A már korábban említett hálózati paramétereket felhasználva a következőkben néhány mérésem eredményét mutatom be.



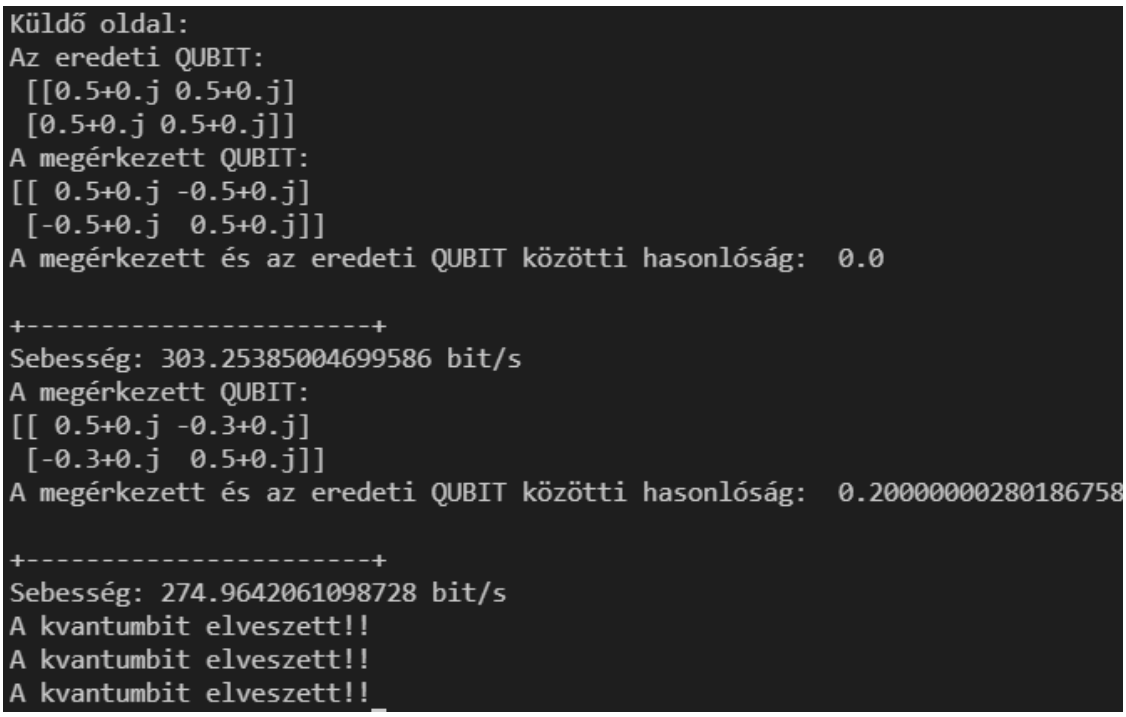
22. ábra: Kvantumteleportáció szimuláció futásának eredménye. Jól látható, hogy az első 3 végpont során még sikeres az adatátvitel, bár a 3. végponthoz már egy zaj által torzított adat érkezik, azonban a 3. és a 4. végpont közötti átvitel során a küldött adat elveszett, így sosem ért célba.



21. ábra: Kvantumteleportáció szimuláció futásának eredménye. Jól látható, hogy már az első küldést követően elveszett a kvantumbit, amelynek következtében a rendszer nem tudta átvinni a kódolt adatot.



23. ábra: Kvantumteleportáció szimuláció futásának eredménye. Jól látható, hogy az első két végpont között az adatátvitel rendben lezajlott, azonban a 3. végpont elérése előtt a kvantumbit depolarizálódott, melynek következtében ezt a rendszer eldobta.



24. ábra: Kvantumteleportáció szimuláció futásának eredménye. A képen egy viszonylag sikeresnek mondható szimulációs eset látható, hiszen a küldött kvantumbit két végponton keresztül a rendszerben volt. Azonban jól látható, hogy az elküldött kvantumbit jelentős zajnak volt kitéve, melynek hatására teljesen elvesztette az eredeti állapotát.

A kvantumteleportáció valós sebessége jelen esetben nem állapítható meg igazán. Kevés kvantumbitet küldtem át a rendszeren, melynek következtében a mért értékek eltérnek egy valós környezettől. Továbbá miután elveszett a küldeni kívánt kvantumbit nem tudtam átviteli sebességet mérni, ezáltal nem sikerült egy, a teljes rendszert átfogó képet kapni arról, hogy valójában mekkora sebesség érhető el.

4.3.2.3 Következtetések

A mérések eredményeiből jól látható, hogy a jelenleg használt kvantumkommunikációs hálózatok kiépítése nem támogatja más, nem kvantumkulcsszétosztásra optimalizált protokoll / kvantumkommunikációs eljárás használatát. Az átviteli csatornák javításával, illetve az átviteli mód megváltoztatásával azonban ezeket könnyedén kiküszöbölhetjük. Megtöbbszörözött adat átvitele megoldás lehet a problémára, mivel ekkor az átvitel rezisztensé válhat egy megadott mértékű adatvesztésre, sőt ebben az esetben egy átvitt kvantumbit is képes a kommunikációra, ugyanakkor nem szabad elfeledkeznünk arról, hogy az átvitel során a kvantumbit depolarizálódhat, melynek következtében továbbra is fontos, hogy hibajavítást végezzünk [10].

A jelenleg használt kvantummemória mentes végpontok nem támogatják a kvantumteleportációt, ugyanis a fogadó félnek a kapott összefonódott foton pár tagját meg kell tartania mindaddig, amíg a küldő oldaláról nem érkezik meg a klasszikus csatornán a mérések eredménye. Enélkül csak kis távolságokra tudunk teleportálni vezetékes rendszerben, hiszen nagy távolság esetén az átviteli idő is jelentősen nő, melynek hatására a polarizált fotont az idővel depolarizálódik.

Jól mutatják az eredményeim, hogy egy következő generációs kvantumhálózat építése során oda kell figyelnünk arra, hogy az átviteli közeg képes legyen más kvantumkommunikációs eljárások támogatására is, hiszen a későbbiekben akár egy remek, az eddigieknél jelentősen gyorsabb hálózatot is kaphatunk.

5 Összefoglalás

Elsősorban szeretnék köszönetet mondani Dr. Bacsárdi Lászlónak, aki már egyetemi éveim első félévében felkeltette az érdeklődésem egy ilyen nagy volumenű és jelentőségű terület felé, továbbá rendszeres konzultációkkal segítette a dolgozat előrehaladását.

Munkám során összehasonlítottam a jelenleg használatos kvantumkommunikációs hálózatok paraméterei mellett, hogy milyen eredményekkel járna, hogy ha kvantumkulcsszétosztás helyett más kvantumkommunikációs eljárást, illetve protokollt használunk.

Kezdetben megvizsgáltam egy kvantumkulcsszétosztó protokollt, egészen pontosan a BB84-et. Jól látható a mérések eredményén, hogy ez egy kiváló eljárás szimmetrikus kulcsok készítésére. A garantált biztonság és a jelentős sebesség hatására másodpercek alatt akár 70km-re is megtörténhet a kulcsok előállítása, alacsony kvantum bit hiba arány mellett, amely a távolság növekedésével egyenesen arányosan minimálisan nőtt.

Ezt követően egy másik kvantumkommunikációs eljárást, a kvantumteleportációt vizsgáltam meg. A mérések eredményei alapján, sajnálatos módon ez a kísérlet kevés sikerrel járt. A nagy mértékű depolarizáció, illetve a vezetékek jelentős csillapítása együttesen egy olyan tényező, amellyel az eljárás nem tudott megbirkózni. Ennek következtében azonban kijelenthetem, hogy a jelenleg használatos kvantumkommunikációs hálózati paraméterek mellett, ez az eljárás alacsony – szinte nulla – hatékonysággal működik. Továbbá a fogadó oldalon megkapott összefonódott foton tárolása sem megoldott egyelőre, amely nehézzé teszi ezt a fajta eljárás lebonyolítását.

Köszönetnyilvánítás

A kutatást az Innovációs és Technológiai Minisztérium és a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal támogatta a Kvantuminformatikai Nemzeti Laboratórium keretében.

6 Irodalomjegyzék

[1] B. Archana and S. Krithika, "Implementation of BB84 quantum key distribution using OptSim," *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, 2015, pp. 457-460, doi: 10.1109/ECS.2015.7124946. [Hozzáférés dátuma: 2021.10.25.]

[2] H. Prakash, "Quantum Teleportation," *2009 International Conference on Emerging Trends in Electronic and Photonic Devices & Systems*, 2009, pp. 18-23, doi: 10.1109/ELECTRO.2009.5441182. [Hozzáférés dátuma: 2021.10.25.]

[3] Laszlo Gyongyosi, Laszlo Bacsardi and Sandor Imre, "A Survey on Quantum Key Distribution", Infocommunications Journal, Vol. XI, No 2, June 2019, pp. 14-21. DOI: 10.36244/ICJ.2019.2.2 [Hozzáférés dátuma: 2021.10.25.]

[4] S. Epstein, "Algorithmic No-Cloning Theorem," in *IEEE Transactions on Information Theory*, vol. 65, no. 9, pp. 5925-5930, Sept. 2019, doi: 10.1109/TIT.2019.2910562. [Hozzáférés dátuma: 2021.10.25.]

[5] Sharon Goldwater, „Quantum Cryptograpgy and Privacy Amplification". Available: http://www.ai.sri.com/~goldwate/quantum [Hozzáférés dátuma: 2021.10.25.]

[6] S. Gueron, S. Johnson, J. Walker, „SHA-512/256", Available: https://ieeexplore.ieee.org/document/5945260 [Hozzáférés dátuma: 2021.10.25.]

[7] A.S. Cacciapuoti, M. Caleffi, F. Tafuri, F.S. Cataliotti „Quantum Internet: Networking Challenges in Distributed Quantum Computing", Available: https://www.researchgate.net/publication/337454545_Quantum_Internet_Networking_Challenges_in_Distributed_Quantum_Computing [Hozzáférés dátuma: 2021.10.26]

[8] Quantum Flagship: *Quantum Repeaters*, https://qt.eu/discover-quantum/underlying-principles/quantum-repeaters/ [Hozzáférés dátuma: 2021.10.26]

[9] Coopmans, T., Knegjens, R., Dahlberg, A. *et al.* NetSquid, a NETwork Simulator for QUantum Information using Discrete events. *Commun Phys* **4,** 164 (2021). https://doi.org/10.1038/s42005-021-00647-8 [Hozzáférés dátuma: 2021.10.26]

[10] H.P. Nautrup, N.Delfosse, V.Dunjko, H.J. Briegel, N. Friis, „Optimizing Quantum Error Correction Codes with Reinforcement Learning", Available: https://arxiv.org/abs/1812.08451 [Hozzáférés dátuma: 2021.10.26.]

[11] S. Imre, B. Ferenc, „Quantum Computing and Communications: An Engineering Approach", Wiley, 2005 [Hozzáférés dátuma: 2021.10.25]

[12] Bacsárdi László „Biztonságos kommunikáció kvantumalapú hálózatokban" http://www.hit.bme.hu/~bacsardi/pub/TermVil_Halozatkutatas_BacsardiL_2015aug.pdf [Hozzáférés dátuma: 2021.10.25]

[13] András Mihály and László Bacsárdi, "Effects of selected noises on the quantum memory satellite based quantum repeaters", Infocommunications Journal, Vol. XIII, No 2, July 2021, p. 19-24., https://www.doi.org/10.36244/ICJ.2021.2.3 [Hozzáférés dátuma: 2021.10.25.]