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

Összefonódás megosztásának vizsgálata kvantum alapú hálózatokban

Szakdolgozat

Készítette
Solymos Balázs

Konzulens
dr. Bacsárdi László

2017. november 23.

Tartalomjegyzék

HALLGATÓI NYILATKOZAT

Alulírott *Solymos Balázs*, szigorló hallgató kijelentem, hogy ezt a szakdolgozatot meg nem engedett segítség nélkül, saját magam készítettem, csak a megadott forrásokat (szakirodalom, eszközök stb.) használtam fel. Minden olyan részt, melyet szó szerint, vagy azonos értelemben, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Hozzájárulok, hogy a jelen munkám alapadatait (szerző(k), cím, angol és magyar nyelvű tartalmi kivonat, készítés éve, konzulens(ek) neve) a BME VIK nyilvánosan hozzáférhető elektronikus formában, a munka teljes szövegét pedig az egyetem belső hálózatán keresztül (vagy autentikált felhasználók számára) közzétegye. Kijelentem, hogy a benyújtott munka és annak elektronikus verziója megegyezik. Dékáni engedéllyel titkosított diplomatervek esetén a dolgozat szövege csak 3 év eltelte után válik hozzáférhetővé.

Budapest, 2017. november 23.

Solymos Balázs
hallgató

1. fejezet

Bevezetés

1.1. Motiváció

A számítógépes rendszerek elterjedésének természtes következménye volt az őket összekötő hálózatok megjelenése és fejlődése. Napjainkban egyre kevesebb olyan eszközt találni, amely ne lenne alkalmas egy ilyen hálózatra való csatlakozásra, rengetek alkalmazás és funkció van, ami valamilyen hálózatból kapott információra támaszkodik működése során. Tekintve a kvantummechanikára építő technológiai megoldások fejlődését, kísérleti kvantumszámítógépek jelenlegi állását[1][2] , az ilyen kvantumos erőforrásokat használó eszközök összekötésére alkalmas hálózatokra is igény lesz. További motivációt jelent még, hogy ezen kvantumos információ továbbítására alkalmas hálózatok sok más felhasználási lehetőséget kínálnak a leendő kvantumszámítógépek összekapcsolásán túl. Ezek közül talán a legismertebb és legelterjedtebb a kvantum kulcsszétosztás, ahol kvantumos állapotokat használunk titkosított kulcsok bizonyítottan biztonságos megosztására.[3] Ezt a technológiát már a valós életben is használják, nem csak kutatási célokra.[4] Mindezek hatására egyre nő az egyre nagyobb ilyen hálózatokra való igény, egy jövőbeli kvantum internet[5] megvalósítára való törekvés. Ennek jelenleg a legnagyobb gátat a távolság jelenti. A klasszikus információval ellentétben a kvantumos infromáció nem másolható [6], emiatt a klasszikushoz hasonló erősítők sem alkalmazhatóak a kommunikációs csatorna által okozott veszteségek korrigálására. Ezt leküzdendő születtek meg különböző megvalósítások, az egyik ilyenek egy csoportja az ún. kvantum ismétlők. Itt a fő cél a küldő és a fogadó állomás között összefonódott párok megosztása. Ezután az összefonódás különös tulajdonságait felhasználva a felek már különböző kvantumos műveletekre képesek. Tetszőleges kvantumbit küldése például a párok és egy klasszikus kommunikációs csatorna valamint a kvantum teleportációs protokoll[7] segítségével már megvalósítható. A kvantum ismétlő protokollok ugyan működésük kvantumos alapokon nyugszik, a velük kapcsolatos megoldandó problémák jelentős része hasonlít a klasszikus hálózatokban felmerülőkhöz. Ezen protokollok hatékony megvalósításhoz is szükséges több elosztott erőforrás megfelelő együttműködése, itt is fontos szerepet kap például a hibakezelés, vagy éppen az adott lépések megfelelően összehangolt végrehajtási sorrendje.

1.2. Feladatkiírás

A feladatkiírás négy főbb pontot jelöl meg a dolgozat témáját tekintve, a következőképpen: (*idézve a feladatkiírásból*)

> A hallgató feladatának a következőkre kell kiterjednie:
>
> - A kapcsolódó szakirodalom áttekintésével mutassa be a kvantum alapú informatikát és kvantum alapú kommunikációt!
> - Mutassa be részletesen az összefonódás megosztásának elvét és ismertesse a különböző felhasználási lehetőségeket, valamint technológiai megoldásokat!
> - Válasszon alkalmas szoftverkörnyezetet és készítsen szimulációt az összefonódás megosztásának lehetőségeinek vizsgálatára kvantum alapú vezetékes és vezeték nélküli hálózatokban!
> - Értékelje a kapott eredményeket!

Ennek megfelelően a dolgozatot egy gyors történeti áttekintés, majd egy hosszabb elméleti bevezető nyitja. Ezek után a készített szimuláció leírása, majd végül a szimulációs eredmények és ezeken keresztül egyes technológiai megvalósítási lehetőségek áttekintésével zárul.

2. fejezet

Történeti áttekintés, Elméleti alapok

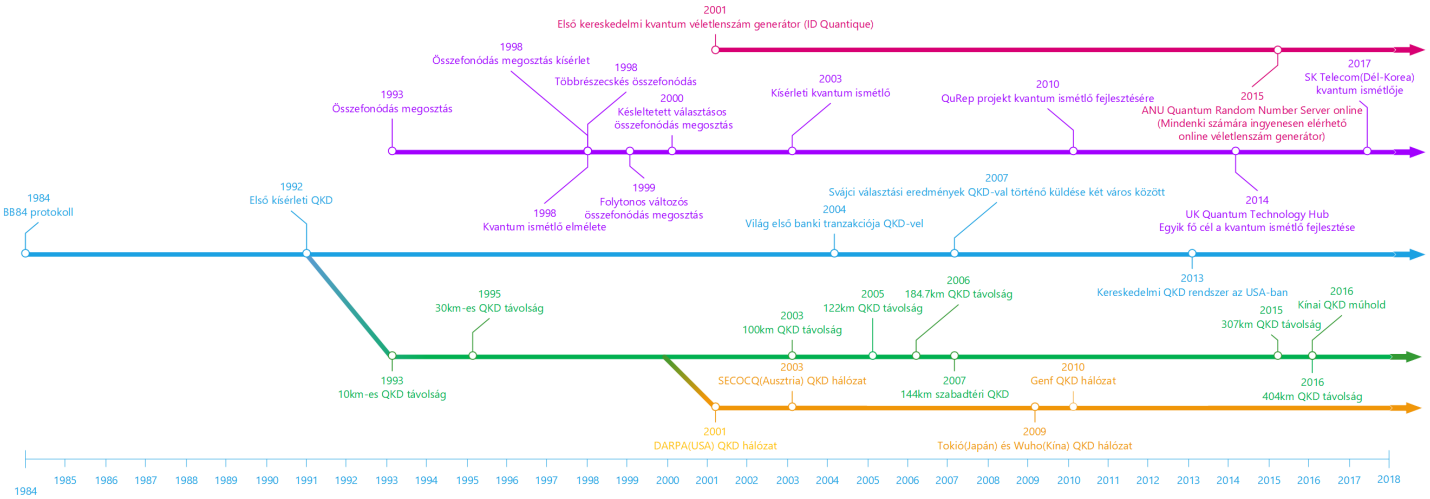
2.1. A kvantumkommunikáció napjainkig

A kvantumkommunikációról valamint kvantuminformatikáról mint kutatási terület, valamikor a 90-es évek eleje-közepe felőltől beszélhetünk, habár az általa vizsgált és használt főbb jelenséggekkel a fizika már az 1920-as években is foglalkozott. Elég csak azt tekinteni, hogy a kvantummechanika egyik mai meghatározó alapköve az 1926-ban publikált Schrödinger egyenlet.[8] Az azóta eltelt időben a témához kapcsolható talán leghíresebb történés az 1980-as évekig az 1935-ös ún. EPR paradox[9] valamint ennek kapcsán Bell 1964-es válasza[10]. Az EPR paradoxon-ban Einstein-ék összefonódott azt a különleges tulajdonságát vizsgálták, hogy az egyik részecskén elvégzett véletlen eredményű mérés,azonnal hatással van az összefonódott pár másik tagjára is, távolságtól függetlenül. Mivel az azonnali információterjedés lehetősége a relativitáselméletben megismertekkel ellenkezik, helyi rejtett, számunkra ismeretlen változók ötletével álltak elő ennek magyarázatára. Így ezekbe ismeretlen változókba lehetséges lehetne előre eltárolni információt, ami alapján a számunkra véletlennek tűnő méréseknél a pár mégis korreláló eredményeket mutathat. Mivel a kvantummechanikában ilyen rejtett változók nincsenek, ezért szerintük a kvantummechanikának hiányosnak kell lenni. Bell 1964-es irásában erre reflektál. Az általa levezetett egyenlőtlenség lehetővé tette ezen elméletek kísérleti tesztelését, melyek később a kvantummechanika jóslatait igazolták, a rejtett változós elképzeléssel szemben.
Az 1980-as években már kezdték vizsgálni ezen jelenségek későbbi lehetséges alkalmazásait, 1982-ben született a később meghatározó „No Cloning Theorem"[6] ami a tetszőleges kvantumbit másolhatatlanságát mondja ki, továbbá 1984-ben merült fel az első kvantumkriptográfia protokoll ötlete is.[3]. Az 1990-es évektők kezdődően pedig már kísérleti megvalósításokkal is találkozhatunk. További meghatározó eljárások, mint a kvantum teleportációs protokoll [7], majd ennek későbbi kísérleti megvalósítása[11], vagy akár az elméletben RSA titkosítás törésére is használható Shor-algoritmus.[12] Kvantumkommunikációs szempontból 1992-ben először hajtottak végre sikerrel kvantum kulcsszétosztást[13], valamint 1993-ban felmerült az összefonódás megosztás ötlete[14], amit 1998-ban kísérletileg is megvalósítottak.[15] Fontos előrelépés volt még az első összefonódás tisztító eljárások[16] megjelenése is, később ezen újítások segítségével vázolták fel a kvantum ismétlő ötletét

is[17].

Az elkövetkezendő években egyre hatékonyabb eljárások, valamint az új technológiák segítségével pontosabb és megbízhatóbb kísérletek készültek. Ezt bizonyítja, hogy a 2000-es évek közepétől kezdtek elérhetővé válni (főleg kvantumkriptográfiában) a nagyközönség számára is használható kvantumos termékek. A folyamatos fejlődés megfigyelhető a kapcsolódó kutatások növekedésén is, idővel egyre több helyen alakultak a témába vágó kutatóközpontok, valamint kísérleti kvantumhálózatok. Egyre közeledünk az előzetes kutatások iparban való felhasználhatóságához, ezt mutatják a közelmúltban a témában elért eredmények is. Ezek közül az egyik talán legjelentősebb a kínaiak által 2016-ben fellőt műhold[18] kvantum kulcsszétosztás tesztelésére, melyről már kísérleti eredmények is származnak[19]. Megemlítendő még, hogy felismerve a területben rejlő lehetőségeket, a kvantumos kutatások támogatása bekerült az Európai Unió fejlesztési tervébe is, amiben 1 milliárd eurót terveznek támogatásként szétosztani.[20]

A „kvantum internet”[5][21] megvalósításához azonban még mindig le kell küzdeni a hoz-



2.1. ábra. *Kvantumkommunikáció fejlődése 1984-től*

záférési pontok közti távolságból adódó problémákat. Habár a kapcsolódó technológiák fokozatosan javultak az évek során, olyan megbízható, hibatűrő rendszer ami ehhez kéne még nincs. A közeljövőben erre két kutatási terület is kínálhat megoldást: egyes kvantum hibajavító kódok[22] melyek alkalmazhatóak hálózatokra is [23], valamint a kvantum ismétlők[24][25][26][27]. A dolgozat a továbbiakban ezek közül a kvantum ismétlőkkel foglalkozik.

2.2. Elméleti alapok

A dolgozatban használt terminológia, valamint a vizsgált rendszerek megértéséhez szükséges a kvantuminformatikában használt alapvető jelölések, valamint a kvantumos állapotok alapvető tulajdonságainak és a rajtuk végzett mérések, műveletek hatásainak ismerete. Ehhez nyújt egy gyors áttekintést a következő rész.Megjegyzendő, hogy jelen esetben a rendszereket csak diszkrét időben vizsgáljuk, mivel a későbbiekben vizsgált események leírásához ez elégséges, valamint a bevezető megfelelő lineáris algebrai előismeretekre is épít.

2.2.1. Posztulátumok:

[28]

1.állapotteres leírás: Egy zárt fizikai rendszer éppen aktuális állapota leírható egy **V** Hilbert tér-beli egységhosszú, komplex együtthatós állapotvektorral. Hilbert tér például egy komplex lineáris vektortér, amire értelmezve van a belső szorzat(skalárszorzat). Vegyünk példának egy két dimenziós Hilbert teret, ami egy egyszerű zárt fizikai rendszer jelképez. A rendszer állapotát le lehet írni egy /textbfv két dimenziós vektorral, ahol:

$$v = \begin{bmatrix} a \\ b \end{bmatrix} = a\mathbf{0} + b\mathbf{1} \text{ ,ahol } \mathbf{0} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{1} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, a, b \in C$$

Itt **0** és **1** az orthonormális(ortgonális és egységhosszú) bázisvektorok. Mivel az állapotvektor egységhosszú,ezért ki kell még kötni, hogy $|a|^2 + |b|^2 = 1$. Az együtthatókra szokás még valószínűségi amplitúdóként is hivatkozni(a Schrödinger hullámfüggvényben amplitúdóként jelennek meg).

2.Rendszerek időbeli fejlődése:Zárt fizikai rendszer időbeli fejlődése leírható csak változás kezdő- és végpontjától függő unitér transzformációval. Az előbbi jelölésrendszer segítségével leírva:

$$v'(t_2) = U(t_1, t_2)v(t_2), v' \in V$$

U unitér operátor lineáris algebrai reprezentációja egy **U** kvadratikus mátrix, melynek U_{ij} elemei a bemeneti **j** orthonormális bázisvektor **i** vektorral való kapcsolatát jelképező valószínűségi amplitúdókat jelölik.

3.Mérés: Méréseket leírhatunkM_m mérési operátorokkal, ahol m a lehetséges mérési eredményeket jelöli. m mérésének a valószínűsége, ha a rendszer **v** állapotban van:

$$P(m|\mathbf{v}) = \mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v}$$

A rendszer állapota mérés után:

$$\mathbf{v}' = \frac{M_m \mathbf{v}}{\sqrt{\mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v}}}$$

Mivel a kimenetek összesített valószínűsége 1-el egyenlő.(a lehetséges kimenetek lefedik a teljes eseményteret):

$$\sum_m P(m|\mathbf{v}) = \sum_m \mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v} \equiv 1$$

ami alapján:

$$\sum_m M_m^\dagger M_m \equiv I$$

A mérések nem visszafordíthatóak és viszonylag durvának tekinthetőek abból a szempontból, hogy befolyásolják a mért rendszer állapotát a fentebb már leírt módon. Ugyanakkor velük teremthetjük meg a kapcsolatot a klasszikus és a kvantum világ között, mivel ők azok az eszközök, amikkel megfigyelhetjük mégiscsak mi történik a kvantum világban.
4.Összetett rendszerek: Egy W összetett fizikai rendszer állapota leírható az őt összetevő rendszerek tenzorszorzataként: $W = V \otimes Y$ .Továbbá ha $\mathbf{v} \in V$ és $\mathbf{y} \in Y$ akkor a belőlük alkotott állapot: $\mathbf{w} = \mathbf{v} \otimes \mathbf{y}$. A kvantummechanikában a legkisebb információt hordozó elem a bit, amit kvantumbitnek, vagy röviden qubitnek szokás hívni. Egy qubit szokványos leírása:

$$|\psi\rangle = a|0\rangle + b|1\rangle = a\begin{bmatrix}1\\0\end{bmatrix} + b\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}a\\b\end{bmatrix}$$

A klasszikus számítástechnikához hasonlóan n qubit felhasználásával építhetünk n bites kvantumregisztereket. Vizsgáljunk például egy két qubitből alkotott kvantumregisztert. Ekkor a teljes két qubites rendszer állapota:

$$|\psi\rangle \equiv |\psi_1\rangle|\psi_2\rangle \equiv |\psi_1, \psi_2\rangle \equiv |\psi_1\psi_2\rangle$$

Ami például hogyha:

$$|\psi_1\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |\psi_2\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}},$$

akkor:

$$|\psi\rangle = \frac{|0\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle+|1\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle}{2} = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$$

látszik, hogy az előbbi rendszer a 00,01,10,11 állapotok(ők mellesleg ortogonálisak egymásra,itt az állapottér bázisának tekinthetőek) súlyozott(most itt mindegyik $1/2$ -el de ez lehet bármilyen más komplex szám is, sőt akár 0 is.) összege, ezeket mind tartalmazza és jól látszik, hogy felbontható $|\psi_1\rangle$ és $|\psi_2\rangle$ tenzorszorzatára. Az ilyen állapotokat hívjuk szorzat állapotoknak.
Most vizsgáljuk a következő állapotot:

$$|\psi\rangle = a|00\rangle + b|11\rangle$$

Ezt nem tudjuk felbontani két qubit tenzorszorzatára. Az ilyen állapotokat hívjuk összefonódott állapotnak. Vegyük észre ennek az állapotnak egy érdekes tulajdonságát. Ha megmérjük az egyik bitjét, akkor akkor valamilyen valószínűséggel 0-át vagy 1-et kapunk. Viszont ha ezután megmérjük a másik bitet is, ha az első mérésünk eredménye 0 volt, akkor itt már csak 0 mérhetünk és ehhez hasonlóan 1-es eredmény esetén pedig csak 1-et. Továbbá kísérletileg bizonyított, hogy ez a jelenség akkor is fenn marad, ha a rendszer két qubitjét helyileg egymástól eltávolítjuk. Néhány nevezetes összefonódott állapot, amelyeket Bell-állapotoknak szokás nevezni:

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle - |1_A 1_A\rangle)$$
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_A\rangle)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_A\rangle)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle + |1_A 0_A\rangle)$$

Figyeljük meg, hogy ezek az állapotok egymásra merőlegesek, az állapotérnek bázisaiként szolgálhatnak. Ennek segítségével definiálhatjuk az ún. Bell mérést ami egy 2 qubites rendszer projektív mérése ezekben a bázisokban. Megjegyzendő még, hogy a mérés után a mérési posztulátumnak megfelelően a két qubit a négy Bell állapot egyikébe kerül.
Ezeken felül, bár a továbbiakhoz nem feltétlen szükséges, viszont a hivatkozások olvasásához igen, ismerjünk meg a rendszerek egy másik lehetséges leírási módját a teljesség igénye nélkül, a sűrűségmátrixos leírást[29]. Ebben az esetben a rendszert a lehetséges állapotainak valószínűségeinek összegével jellemezzük:

$$p = \sum_i p_i |\phi\rangle \langle\phi_i|$$

ahol $|\phi_i\rangle$ az i-edik rendszer állapot, melynek előfordulási valószínűsége p_i a sűrűségmátrixos leírás ilyen ún. tiszta állapotok valószínűségi elegyeként írja le a rendszert.Ezek alapján például a

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

rendszer sűrűségmátrixa a következőképpen számolható:

$$p = |\phi\rangle \langle\phi| = \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a^* b^* \end{bmatrix} = \begin{bmatrix} aa^* & ab^* \\ a^* b & bb^* \end{bmatrix} = \begin{bmatrix} |a|^2 & ab^* \\ a^* b & |b|^2 \end{bmatrix}$$

Ezen felül definiáljük még a “trace” (magyarul nyom) operátort a következőképpen. Egy n-szer n-es A mátrixra:

$$Tr(A) = a_{11} + a_{22} + ... + a_n n = \sum_{i=1}^{n} a_{ii}$$

Továbbá említésre méltó még, hogy Tr(A) egyenlő A sajátértékeinek összegével.

2.3. Összefonódás megosztás

(entanglement swapping)

2.3.1. A jelenség bemutatása

Az összefonódott állapotok érdekes tulajdonságait, természetesen igyekszünk kihasználni a kvantuminformatikában is, nem véletlen tehát, hogy magára az összefonódásra is mint egy fontos erőforrásként tekinthetünk. Elég csak olyan, protokollokra gondolni, mint a szupersűrűségű kódolás, vagy a kvantumteleportáció, melyek mind összefonódott állapotok “használnak el” a működésük során.Nem csoda tehát,hogy egy adott helyen(vagy helyek között) való összefonódás létrehozásának képessége különös jelentőséggel bír. Ezzel kapcsolatban

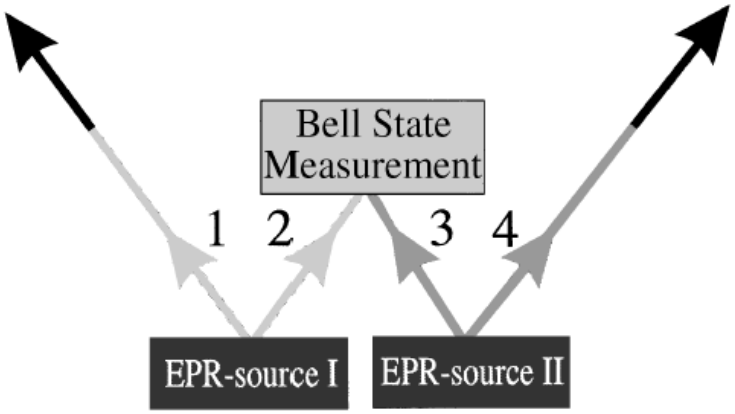
létezik szerencsére egy számunkra igen hasznos és viszonylag sokszor hasznosított jelenség, az összefonódás megosztás(entanglement swapping), mellyel egy összefonódott párok közötti érdekes interakciót írunk le. A már 1993-ban felvetett koncepció szerint[14] 2 összefonódott pár interakcióját vizsgáljuk egymással a következő módon.A példában tekintsünk kvantum információ hordozóira fotonokként hivatkozunk, de természetesen minden fotonhoz hasonló kvantum információ hordozására hasznos módszerre is az alábbiak szerinti a jelenség. Az összefonódott párjaink közül az egyik kezdetben legyen Alíznál, a másik pedig Bobnál. Legyen a rendszerünk kezdő állapota:

$$\left|\Psi^-_{kezd}\right\rangle = |\Psi^-\rangle_{AB} \otimes |\Psi^-\rangle_{CD}$$

ahol Ψ^- a már fentebb említett Bell állapot,AB fotonpár van Alíznál és CB fotonpár pedig Bobnál.A teljes állapot felírható:

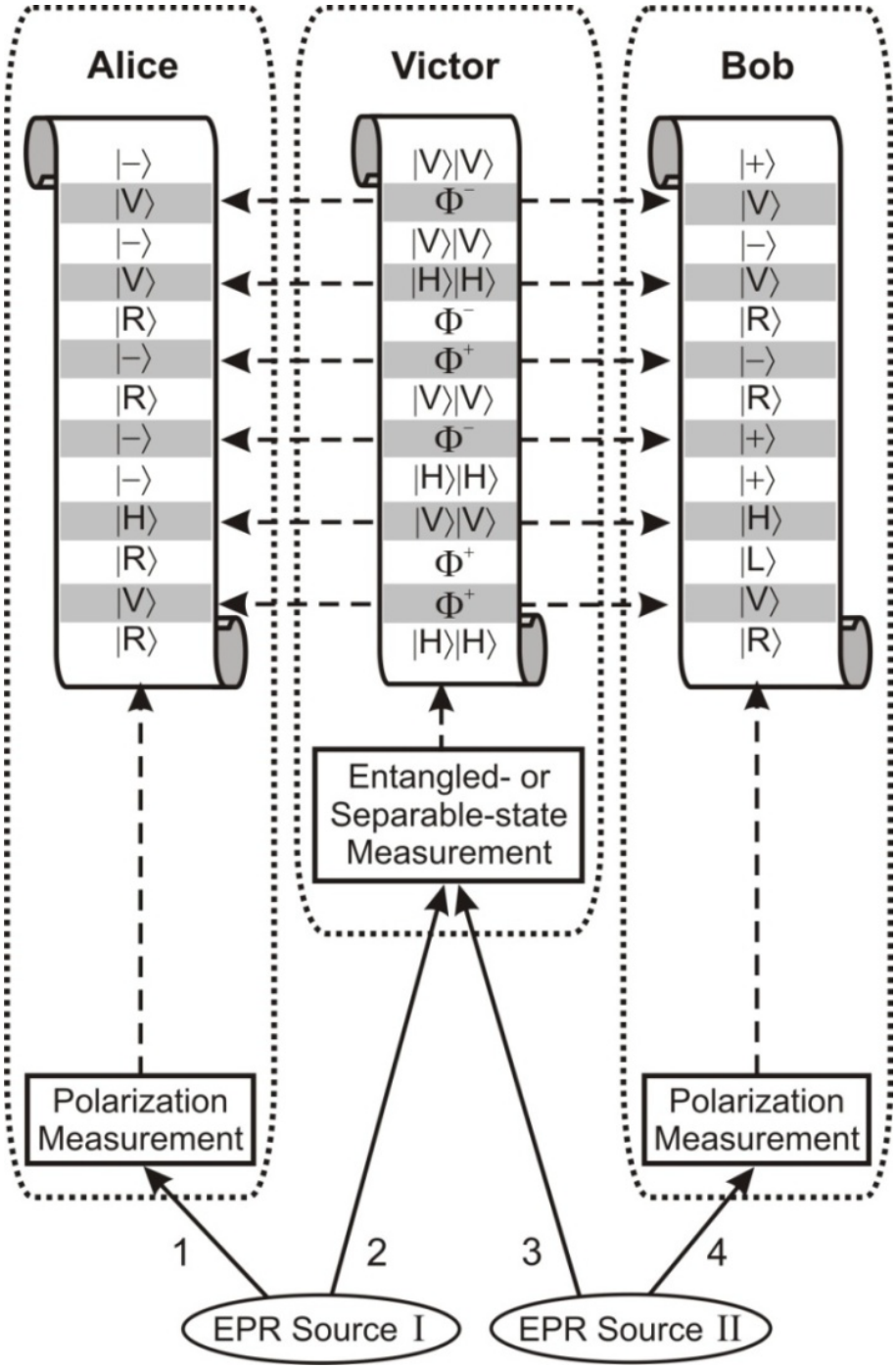
$$\left|\Psi^-_{kezd}\right\rangle = \frac{1}{2}\Big(|\Psi^+\rangle_{AD}|\Psi^+\rangle_{BC} - |\Psi^-\rangle_{AD}|\Psi^-\rangle_{BC} - |\Phi^+\rangle_{AD}|\Phi^+\rangle_{BC} + |\Phi^-\rangle_{AD}|\Phi^-\rangle_{BC}\Big)$$

Alíz elküldi A fotont Bobnak, Bob pedig C fotont Alíznak, tehát Alíznál lesz B és C, míg Bobnál A és D. Ha Alíz Bell mérést hajt végre BC fotonpárján és $|\Psi^-\rangle_{BC}$ állapotban találja, akkor ha Bob is megméri a saját párját $|\Psi^-\rangle_{AD}$ állapotot fog találni. Ha Alíz a mérése során a maradék három állapot közül találja valamelyiket, akkor Bob ennek megfelelő állapotokat fog találni az ő fotonpárja mérésénél is. Látszik, hogy a Bobnál előfordulható állapotok mind tiszta összefonódott állapotok, emiatt ha Alíz Bell mérést végez, tudhatjuk, hogy a Bobnál lévő fotonpár össze van fonódva Alíz mérési eredményének pontos ismerete nélkül. Érdemes megfigyelni, hogy a Bobnál lévő fotonok semmilyen közös múlttal nem rendelkeznek, mégis szert tettek egy közös tulajdonságra, összefonódott állapotba kerültek. A folyamatot lehet úgy is tekinteni, mintha a kvantumteleportációs protokoll[7] segítségével egy már kezdetben is összefonódott állapot egyik kvantumbitjét teleportáltuk volna, csak ebben az esetben nem a kiválasztott kvantumbit pontos átvitele a fontos, hanem csak az összefonódás, mint a két kvantumbites rendszerre jellemző állapot, továbbítása az. Alíz mérési eredményének pontos ismerete és a feltételes visszaállító transzformációk, továbbá az ehhez szükséges 2 klasszikus bitnyi információ itt nem is része a folyamatnak, mivel fentebb már megmutattuk, hogy az összefonódás léte(ami most minket érdekel) ezek nélkül is belátható.



2.2. ábra. *Összefonódás megosztás elvi rajza: Két összefonódott pár forrás (EPR source I és II) összefonódott fotonpárokat bocsájt ki(1-2 és 3-4). Mindegyik párból 1-1 fotonnal (2 és 3) végrehajtunk egy közös Bell mérést, aminek hatására a maradék két foton(1 és 4) is összefonódott állapotba kerül.*

Megjegyzendő még érdekességként, hogy Peres elméletének megfelelően[30] az összefonódás megosztás akkor is végbemehet, ha a (jelen esetben Alíznál) Bell mérést csak azután hajtjuk végre, hogy Bobnál már megmértük a másik két(jelen példánál A és D) állapotokat. Ezt igazolja például egy 2012-es kísérlet is[31].



2.3. ábra. *Elvi kísérleti összeállítás delayed choice(késleltetett döntéses) összefonódás megosztás vizsgálatára. Az előzőekhez hasonlóan itt is két összefonódott pár forrás szolgáltatja a fotonpárokat, viszont a korábbiakkal ellentétben itt először az 1-es és 4-es foton állapotait nézzük meg, utána véletlenszerűen döntünk, hogy Bell mérést, vagy valamilyen szétválasztható állapot szerinti mérést végzünk el. Ezek után Alice és Bob rendezni és vizsgálni tudja a már meglévő mérési adatait Victor döntése ismeretében. Azt kapjuk, hogy Alice és Bob fotonjai vagy összefonódott vagy szétválasztható állapotokként viselkednek, Victor mérési eredményeinek megfelelően.*

2.3.2. Összefonódás megosztások összefűzése

Tekintve, hogy milyen fontos szerepe van az összefonódásnak a kvantumkommunikáció területén, az összefonódás megosztás is egy fontos eljárása, építőeleme számos kvantumkommunikációs protokollnak. Ezek közül talán az egyik legfontosabb ilyen felhasználási terület a kvantum ismétlők. A kvantumkommunikációs csatornák a valóságban nem tekinthetőek tökéletesnek, hasonlóan a klasszikus összeköttetésekhez, itt is számolni kell például csillapítással(hosszabb távon komoly probléma például a fotonok elnyelődése, detektálásuk nehézsége), a környezet hatásaival, mint például dekoherencia,zaj. Ebből adódóan nem élhetünk azzal a feltételezéssel, hogy hosszabb kapcsolatoknál az elküldött információnk a fogadó oldalra eredet formájában jut el. A kvantum csatorna átvitelére jellemző exponenciális csökkenés pedig gyakorlatilag ellehetetleníti a hosszabb távokon át történő információátvitelt. Erre lehetne az egyik megoldás, a klasszikus kommunikációhoz hasonlóan, ha megfelelően nem túl nagy távolságonként ismételnénk, eredeti állapotában mindig újra küldenénk tisztábban. A klasszikus kommunikációban ez könnyedén megoldható, azonban a kvantumos másolási tétel (No Cloning Theory) miatt nem lehet azt a megoldást teljes egészében lemásolni.Vegyük észre viszont, hogy a kvantum teleportációs protokoll segítségével tetszőleges állapotot tudunk elvinni egyik helyről a másikra, feltéve hogy a cél és a forrás rendelkezik egy összefonódott párral amin már előzőleg megosztottak.A problémát ily módon vissza tudjuk vezetni összefonódott párok szétosztására(mert klasszikus információt már tudunk nagy távolságokra is szállítani).Összefonódott párokat különben sem csak a teleportációs protokoll használ működése során, két hely közötti összefonódásra tekinthetünk egy általában is értékes erőforrásként. Itt lehet segítségünkre az összefonódás megosztás jelentősége.

Természetesen az összefonódott párokat akarunk szétosztani ugyanúgy fennállnak az előzőleg említett problémák a csatornával, viszont tekintsük a következő esetet[32]: Ha az összefonódott párok közül az egyiket előzőleg összefonódás megosztásával hozzuk létre, könnyen elképzelhető, egy szabadon bővíthet séma, ahol a nagy átviteli távolságot, többszöri összefonódás megosztásával több kisebb szakaszra lehet bontani. Vizsgáljuk meg azt az esetet amikor ezt a hosszabb távot két részre osztjuk fel. Ilyenkor kétszer kell összefonódást megosztani, három összefonódás forrásunk van, és két Bell mérést hajtunk végre a párjaink. Ha a párjaink kezdetben 1-2 3-4 és 5-6, akkor a Bell méréseket hajtunk végre 2-3-on és 4-5-ön. Ennek eredményeként 1 és 6 kerül összefonódott állapotba.

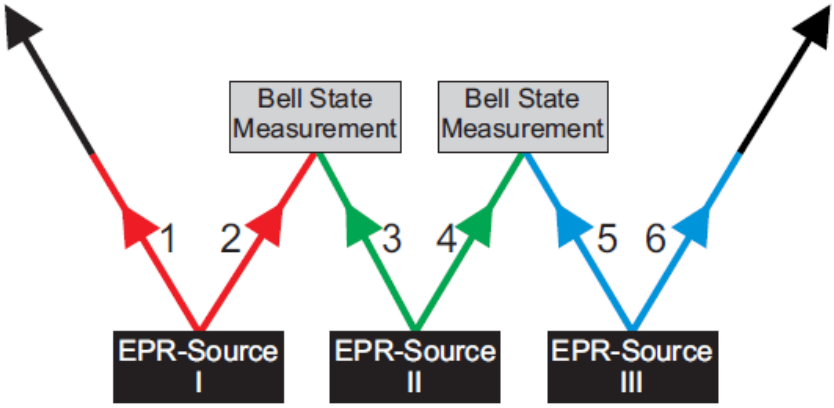
Felírva a rendszer állapotát:

$$|\Psi\rangle_{123456} = |\Psi^-\rangle_{12} \otimes |\Psi^-\rangle_{34} \otimes |\Psi^-\rangle_{56}$$

Ez átírható a következő alakra:

$$|\Psi\rangle_{123456} = \frac{1}{2}\Big[\, |\Psi^+\rangle_{14}|\Psi^+\rangle_{23} - |\Psi^-\rangle_{14}|\Psi^-\rangle_{23} - |\Phi^+\rangle_{14}|\Phi^+\rangle_{23} + |\Phi^-\rangle_{14}|\Phi^-\rangle_{23} \Big] \otimes |\Psi^-\rangle_{56}$$

A korábbi két fotonpáros esethez hasonlóan itt is megfigyelhető, hogy az 1-es és 4-es fotonok a Bell mérés után összefonódott állapotban lesznek a mérés eredményétől függetlenül. Az eredmény csak arról szolgáltat információt, hogy melyik összefonódott állapotban vannak„



2.4. ábra. *Többlépcsős összefonódás megosztás elvi felépítése: A források által(EPR-Source I-II-III) kiadott kezdeti összefonódott párok: 1-2, 3-4, 5-6. 2 és 3-on majd 4 és 5-ön elvégezzük a Bell mérést. A két Bell mérés hatására végül 1 és 6 kerül összefonódott állapotba.*

mivel az most is egyezik 2-3 közös mért állapotával. Ha feltesszük, hogy 2-3-as fotonpárnál $|\Phi^-\rangle$ állapotot mértünk, a fennmaradó 4 fotonos rendszer a továbbiakban a következő formában írható fel:

$$|\Psi\rangle_{1456} = \frac{1}{2}\Big[\,|\Psi^+\rangle_{16}|\Phi^-\rangle_{45} + |\Psi^-\rangle_{16}|\Phi^+\rangle_{45} - |\Phi^+\rangle_{16}|\Psi^-\rangle_{45} - |\Phi^-\rangle_{16}|\Psi^+\rangle_{45}\,\Big]$$

Hasonlóan az előzőekhez, elvégezzük a Bell mérést 4-5-ön, aminek hatására 1 és 6 összefonódott állapotba kerül. A mérési eredménynek megfelelően például, ha a Bell mérésnél $|\Phi^-\rangle$ állapotot mérünk, akkor 1-6-nak az állapota: $|\Psi^+\rangle$.
A folyamat a fentiekből kiindulva általánosítható több tetszőleges számú összefonódott párral, tetszőleges számú Bell-méréssel, amivel az áthidalni kívánt távolság is tetszőleges számú szakaszra bontható fel.
A itt ábrázolt módszer is még idealizált csatornákkal dolgozik, magában nem oldja az előzőleg említett problémákat, mégis egy fontos építőeleme a későbbi ismétlő létrehozására irányuló modelleknek.

2.3.3. A kvantum ismétlő

A kvantum ismétlő megvalósítására törekvő modellek túlnyomó része három fő építőelemből áll, és jellemzően e három építőelem más és más megvalósításában tér el egymástól.Egy jellemző általános megvalósítás az alábbi: A nagy távolságon jelentkező romlás elkerülése végett, ezt a távolságot felosztjuk több kisebbre, amik között a fentebb részletezett módon összefonódás megosztással teremtünk kapcsolatot. A felosztott kis távolságok között állomásokat alakítunk ki(ismétlőket), itt végezzük el az összefonódás megosztáshoz szükséges Bell méréseket. Továbbá minden szakaszhoz(minden összefonódás megosztási lépcsőhöz) létre kell hoznunk plusz összefonódott párokat amiket a folyamat során elhasználunk.
Ehhez szükségünk van egy összefonódott pár forrásra, ami manapság már igen sokféle lehet.

Ez az egyik fő hasonlóság és egyben különbség is a legtöbb megvalósításban. A források maguk is sokféle karakterisztikával rendelkezhetnek. Adhat ki egy forrás kis sebességgel, nagy hibaszázalékkal közel teljesen tiszta állapotokat, vagy akár nagyobb sebességgel kisebb hibaszázalékkal több kevésbé tiszta állapotot is egyszerre.
A csatorna nem ideális átvitelével is foglalkozni kell, látható, hogy az továbbra is exponenciálisan fog romlani a csomópontok és a hossz növelésével. Ennek kiküszöbölésére használhatunk valamilyen összefonódás tisztító eljárást.
Ezek jellemzően több nem teljesen tiszta összefonódott állapotból állítanak elő kevesebb, tisztább, jobban összefonódott állapotok.Tipikusan van egy tisztasági határérték a felhasznált "koszos" összefonódott állapotokra ami fölött alkalmazhatóak, emiatt akár ezek paraméterei támaszthatnak határokat a csatornaszakaszok hossza felé. Segítségükkel az átviteli sebesség kárára ugyan, de az átviteli folyamatok közé megfelelően beiktatva, kompenzálhatóak a csatornából származó veszteségek. Ennek szemléltetésére vizsgáljunk egy egyszerűbb ilyen eljárást.
Példa egy tisztító protokollra:
Egy lehetséges ilyen tisztító protokoll például a Bennett által javasolt[16] aminek folyamán helyben végzett transzformációk segítségével több nem teljesen "tiszta" összefonódott párból kevesebb jobban összefonódott állapot hozható létre. (Megemlítendő, hogy eredetileg elektronspinekre írták le, de természetesen megvalósítható más hordozók esetén is.) Legyen M egy "kevert"(nem tiszta) állapot amiből tisztább, jobban összefonódott állapotokat szeretnénk létrehozni. (Ilyen lehet például egy zajos csatornán megosztott $|\Psi^-\rangle$ pár.) Ilyenkor M tisztaságát az eredeti teljesen összefonódott állapothoz képest $F = \langle\Psi^-| M |\Psi^-\rangle$ (?fidelty?)-vel fejezhetjük ki. Ezt akár értelmezhetjük azzal is ebben az esetben, hogy egy véletlenszerű bázisban végzett mérésnél mekkora valószínűséggel mérjük a két bit állapotát párhuzamosnak($P_{||}$). Ezzel kifejezve: $F = 1 - 3P_{||}/2$.
A protokoll lépései leegyszerűsítve:
Először végrehajtunk egy véletlenszerű bilaterális forgatást minden megosztott páron külön, aminek hatására következő forgásszimmetrikus állapothoz jutunk:
$W_F = F \cdot \langle\Psi^-| + \frac{1-F}{3} \langle\Psi^+|\Psi^+\rangle + \frac{1-F}{3} \langle\Phi^+|\Phi^+\rangle + \frac{1-F}{3} \langle\Phi^-|\Phi^-\rangle$
Az így kapott W_F Werner-állapot ugyanolyan F tisztaságú, mint a kiinduló M. A továbbiakban a következő műveletekre lesz szükségünk.:
-Unilaterális Pauli forgatások.:az összefonódott párban egy részecske π radiánnal való elforgatása az x,y, vagy z tengely körül. Ennek hatására a Bell állapotok egymásba mennek át:

$$\sigma_x : \Psi^\pm \leftrightarrow \Phi^\pm$$
$$\sigma_z : \Psi^\pm \leftrightarrow \Psi^\mp s \Phi^\pm \leftrightarrow \Phi^\mp$$
$$\sigma_y : \Psi^\pm \leftrightarrow \Phi^\mp$$

-Bilaterális $\pi/2$ forgatások B_x , B_y és B_z a pár mindkét tagjára megfelelően x,y és z szerint. Hatása:

$$B_x : \Phi^+ \leftrightarrow \Psi^+$$
$$B_y : \Phi^- \leftrightarrow \Psi^+$$
$$B_y : \Phi^+ \leftrightarrow \Phi^-$$

-Kvantum XOR vagy CNOT bilaterálisan végrehajtva a mindkét megfigyelő által két megosztott pár megfelelő bitjein.A bilaterális XOR az hagyományos XOR-hoz hasonlóan működik.Alíz és Bob osztozzon 2 páron, Alíznál van 1 és 3, Bobnál 2 és 4. Ekkor egy 1, 2 forrású és 3,4 célú BXOR feltételesen fordítja a 3-as bitet, akkor és csak akkor, ha 1-es 1(például elektronspinek esetében felfele áll, de ez hordozónként szabadon változhat.) és ehhez hasonlóan feltétetlesen fordítja a 4-es bitet, akkor és csak akkor, ha 2-es 1.A BXOR hatása Bell állapotokra:

Before		After (n.c. = no change)	
Source	Target	Source	Target
$\Phi^{\pm}$	Φ^+	n.c.	n.c.
$\Psi^{\pm}$	Φ^+	n.c.	Ψ^+
$\Psi^{\pm}$	Ψ^+	n.c.	Φ^+
$\Phi^{\pm}$	Ψ^+	n.c.	n.c.
$\Phi^{\pm}$	Φ^-	$\Phi^{\mp}$	n.c.
$\Psi^{\pm}$	Φ^-	$\Psi^{\mp}$	Ψ^-
$\Psi^{\pm}$	Ψ^-	$\Psi^{\mp}$	Φ^-
$\Phi^{\pm}$	Ψ^-	$\Phi^{\mp}$	n.c.

2.5. ábra. *BXOR hatása Bell állapotokra.*

-Az előző unitér transzformációkon kívül alkalmazunk még egy mérést is, melyben Alíz és Bob a z tengely mentén mér(elektronok spinjeit), amivel megbízhatóan meg tudjuk különböztetni a Φ és Ψ állapotokat, viszont a „-” és „+” -t nem. Természetesen a mérés után a mért pár már nincs összefonódott állapotban. Ezen műveletek birtokában tekintsük az alábbi protokollt, melynek bemenetei valamilyen F tisztaságú Werner állapotok:

1. Egy unilateláris σ_y forgatást hajtunk végre mind a két páron, aminek hatására a többnyire Ψ^- Werner állapotból a többnyire Φ^+ Werner állapotba kerülnek.

2. Végrehajtunk egy BXOR-t a két nem tiszta Φ^+ állapoton és utána a célpárt megmérjük a z tengely mentén.Ha a mérési eredmények párhuzamosak, ami a Φ^+ állapotnak megfelelő, akkor a meg nem mért forráspárt megtartjuk, ellenkező esetben nem.

3. Végül, ha a forráspárt megtartottuk, egy többnyire Ψ^- állapotba visszaalakítjuk egy unilaterális σ_y forgatással, majd forgásszimmetrikussá tesszük egy véletlen bilaterális forgatással.

Ezen egyszerű protokoll ismétlésével lépésenként $\frac{1}{4}$-ed valószínűséggel növekvő F tisztaságot lehet elérni, amennyiben a felhasznált M párokra igaz, hogy $F_m > 1/2$. Továbbá a

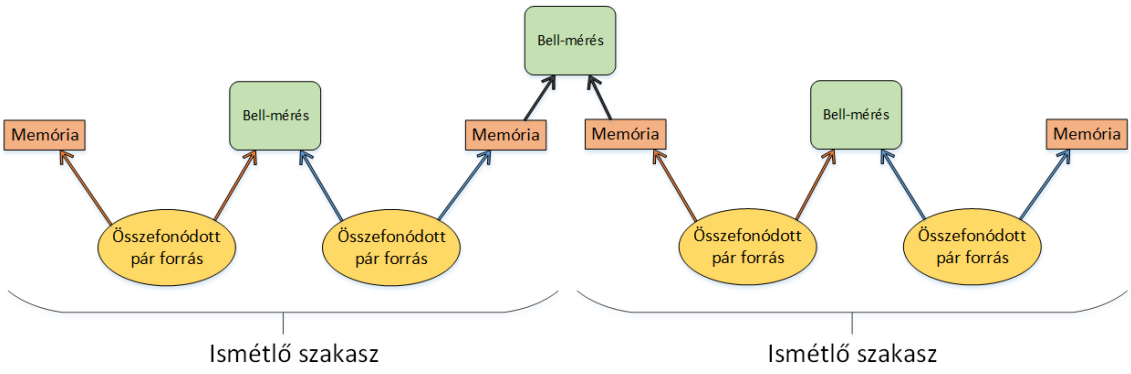
lépésenként így elért $F' > F$ kielégíti a következő egyenletet:

$$F' = \frac{F^2+\frac{1}{9}(1-F)^2}{F^2+\frac{2}{3}F(1-F)+\frac{5}{9}(1-F)^2}$$

A módszer ismételt elvégzésével a tiszta állapotot tetszőlegesen megközelítő állapot állítható elő, viszont a hatékonyság(nem tiszta bemenet/tiszta kimenet) a teljesen tiszta kimenet közelítésével a 0-hoz tart. Ennek a javítására szerencsére vannak módszerek, egy ilyen lehetőség például, ha nem egy forrást párt BXOR-olunk egy célpárral, hanem többet. Ennek az ötletnek egy továbbfejlesztése, amikor tiszta Φ^+ állapotokat használunk a BXOR céljaként a több nem tiszta forráspárhoz. Ezután megmérjük a célt. A fenti tábla alapján minden Ψ^+ vagy Ψ^- forráspár váltja a célt Φ^+ és Ψ^+ között, a forrásra való hatás nélkül. Ennek alapján a BXOR-t egyfajta paritás tesztként használva meg tudjuk állapítani, hogy a mért halmazban páratlan vagy páros számú Ψ állapot van. Ezután további BXOR-ok elvégzésével a részhalmazokon, kiválasztható az összes Ψ állapot és Φ állapotra javítható, majd hasonló módszerrel meg lehet találni a Φ^- állapotokat is és javítani a kívánt Φ^+-ra. Természetesen léteznek más tisztítóprotokollok is más tulajdonságokkal, viszont a továbbiakhoz nem szükséges ezen terület mélyebb ismerete.

Az ismétlő következő eleme maga a Bell-mérés aminek következtében maga az „összefonódás megosztás" nevű jelenség a párokon ténylegesen végbe megy. Megemlítendő, hogy amennyiben nem teljesen tiszta állapotokat mérünk ennek hatására a létrejövő új pár tisztasága is romlani fog, valamint magának a mérésnek is lehet egy hibaszázaléka[33], amiket a későbbi lépésekben ugyanúgy javítani kell.

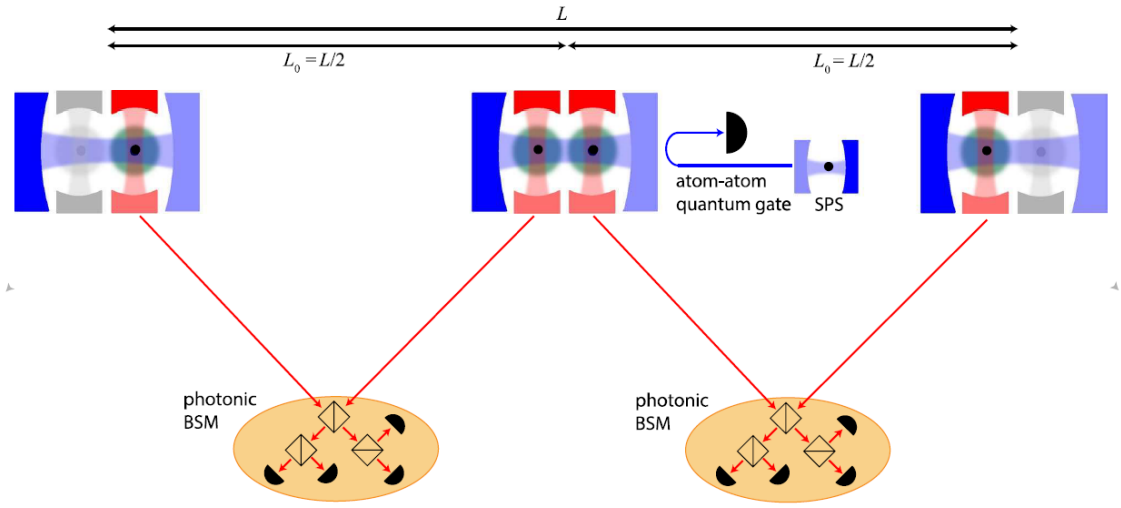
Fontos elemek még az állomásokon található kvantumos állapotok tárolására képes memóriaegységek. Mivel a végső cél az ismétlő két végén található memóriában tárolt qubit közötti összefonóds létrehozása, természetes feltétel az állapothú tároláson túl, hogy ezek a memóriák képesek legyen megtartani a qubit állapotát a protokoll végigfutási ideje alatt. Az alkalmazható hibajavítási stratégiáknak ez is egyfajta gátat szab mint az összes rendszerben tölthető idő felső határa



2.6. ábra. *Általános ismétlő elvi rajza*
A tisztító protokoll a képen nincs feltüntetve, tipikusan a Bell-mérések előtt alkalmazzák, habár ettől eltérő stratégiák is létezhetnek.

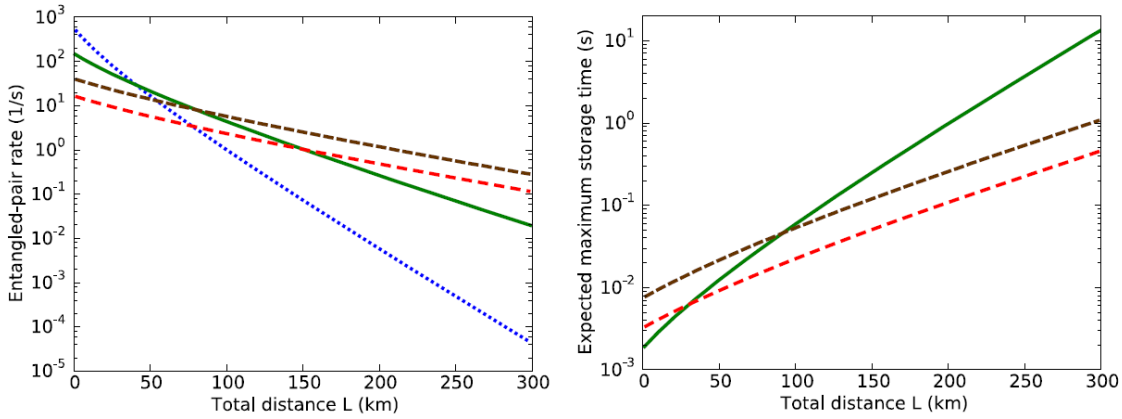
2.3.4. Néhány megvalóstás

A továbbiakban vizsgáljunk néhány mostani megvalósítást, ahol már láthatóak a technológia alkalmazásából származó előnyök valamint kihívások is.
Egy 2016-os német tanulmányban[24] atom-foton összefonódott párokat használnak, melyeket optikai mikroüregekben található magányos atomok segítségével hoznak létre. Az összefonódás közvetlen az atomi kvantummemória és a foton között jön létre. További előny még, hogy ennek létrejöttét egy másik ún. "bejelentő" foton is jelzi és az összefonódást szállító foton olyan előnyös tulajdonságokkal rendelkezik(spektrum stb), hogy az egész elrendezés a szokványos telekommunikációs hullámhossztartományban használható. A további lépések az általános modellt követik, maga az összefonódás megosztás, fotonok közötti Bell mérésekkel, és atom-atom kapuk alkalmazásával történik.



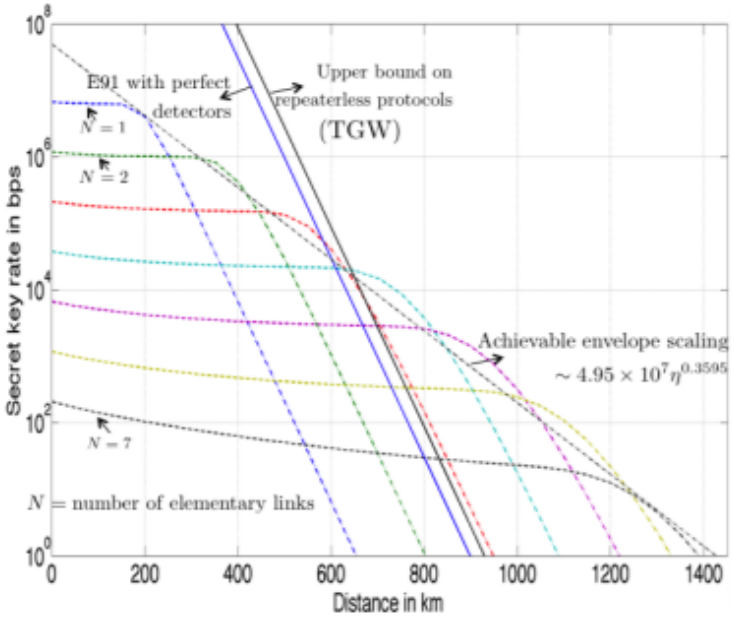
2.7. ábra. *A 2016-os német tanulmány elvi rajza.*
Egy ismétlő csomópont a "bejelentő" üregből(kék) és telekommunikációs hullámhosszú összefonó üregekből áll. Az atomokat(fekete pont) lézersugarakkal irányítjuk. Az L/2 távolságra lévő csomópontokat először összefonódott állapotba juttatjuk a fotonokon elvégzett(L/4 távolságnál) Bell mérések segítségével. A csomópont párok között összefonódás megosztást a központi csomópontban elvégzett(atom-atom) művelettel valósítjuk meg.

A tanulmány szépen szemlélteti még a távolságból és a hibajavításból adódó problémák hatását.



2.8. ábra. *A várható átviteli sebesség és tárolási idő alakulása az áthidalni kívánt távolság függvényében.*
Kék pontozott vonal-> ismétlő nélküli eset; zöld folytonos vonal->2 szakasz esetén
piros szaggatott vonal->4 szakasz esetén, hibánál teljes újrakezdéssel
barna szaggatott vonal->4 szakasz hibánál a már összefonódott állapotok megtartásával

Látszik, hogy kis távolságoknál a közvetlen összeköttetés a legjobb egyszerűsége miatt, viszont 100km fölött már számottevően jobbak az ismétlős megoldások. A tárolási idő szempontjából látszik, hogy nagy távolságoknál a több részre felosztott rendszerek teljesítenek jobban.(Továbbá az is, hogy a hiba teljes újrakezdéssel való javítása is meglehetősen csökkenti a szükséges tárolási időt.)
Egy másik 2016-os tanulmány[25] az ún. parametric down conversion jelenséget és két foton interferenciát hasznosító összefonódott pár forrásokat használó jelen/közeli jövőbeli ismétlők lehetséges korlátjait vizsgálta, különös tekintettel,az egyszerű megvalósíthatóságra a mai technológiákkal.Az ő szimulációjukból is látszik, az ismétlők előnye nagyobb távolságok esetén:



2.9. ábra. *A különböző számú kapcsolatokból álló ismétlőrendszerek átvitele és összehasonlításuk más ismétlő nélküli protokollok határaival(TGW vonal ezek felső határa).*

Különböző ismétlő protokollok akár ionokkal való megvalósítási lehetőségét is vizsgálták[26] ugyancsak 2016-ban. Az általuk használt kísérleti összeállításban $^{40}Ca^{+}$ ionok segítségével már F>0.95 esetén 100 állapot/s sebességet is elértek bizonyos protokollok esetén, azonban megfelelő változtatásokkal a több mint 750 állapot/s sebességet is elérhetőnek találták, az ionos megvalósítások esetében.

Egy negyedik, kínai tanulmány[27] pedig a kvantum pontok és optikai üregek használatával való megvalósítással foglalkozik. Ennek egyik érdekessége, hogy itt úgynevezett time-bin összefonódást hoznak létre, aminek folyamán a fotonoknak az időbeli szabadságfokát használják fel információtárolásra. A tanulmányban továbbá megmutatják, egy N többfelhasználós kvantum ismétlő rendszer felépítését is.

2.4. Összefoglaló

Már az említett megvalósításokból is látszik, hogy a kísérleti kvantuminformációs megvalósítások, hatékonysága, erőforrásigénye és megbízhatósága egyre inkább közelíti a gyakorlatban való eredményes használhatósághoz szükséges feltételek teljesítését az információszétosztás területén is. Tekintve a terület gyors fejlődését, különösen, hogy a kvantum titkosítás és kulcsszétosztás már a jelenben is gyakorlati jelentőséggel bír, a kvantum ismétlők ipari megvalósítása nagy valószínűséggel már a közeljövőben is egy megoldandó mérnöki feladatot fog jelenteni. A fentebb szemléltetett tervezésnél megfontolandó nehézségek fényében döntöttem egy szimuláció elkészítése mellett, ahol a továbbiakban ezek hatását szemléltetetem illetve vizsgálom.

3. fejezet

Szimuláció

A szimuláció elsődleges célja egy általános kvantum ismétlő protokoll működésének vizsgálata. Ennek megfelően a különböző fizikai megvalósítások pontos szimulációjától ezek sokszínűsége miatt a továbbiakban eltekintettem, helyette egy általánosított modellen vizsgáltem az egyes paraméterek hatását. A modell elemei a bevezetőnek megfelelően ismétlő állomások és csatornák. Az állomások rendelkeznek kvantum memóriákkal, képesek mérések, és helyi műveletek elvégzésére a memóriájukban tárolt qubitjeiken, valamint egy speciális állomásfajtának tekinthetjük az összefonódott pár forrásokat is. A csatornák az állomásokat összekötő kommunikációs összeköttetések, amelyeken keresztül a qubitjeinket az állomásonak szétküldjük. Továbbá feltételezzük, hogy az egyes állomások képesek egymásközt hagyományos kommunikációra is.

3.1. Választott környezet, eszközök

A szimuláció c++ nyelven íródott(c++11-et használ),valamint az Eigen [34] lináris algebra könyvtárt használja. Az elkészítésnél cél volt sokféle szimulációs elrendezés támogatása, emiatt használata a legtöbb esetben egy c++ könyvtáréhoz hasonló. A legegyszerűbb esetben egy előre megírt függvény egyszeri meghívásával akár egy teljes szimuláció is futtatható, viszont a rendelkezésre álló eszközökkel lehetőség van teljesen egyedi szimulációs elrendezés készítésére is. Az egyes elemek 4 fő csoportba sorolhatók, melynek megfelelően az egyes funkciók 4 header fájlba kerültek szétosztásra. Ezek: a kvantumos elemek reprezentációit tartalmazó, az ismétlő protokoll elemeit tartalmazó, a szimuláció vezérléséért felelős, valamint az előre megírt teszteseteket tartalmazó fájlok.

3.2. A szimuláió vezérlése

A szimuláció vezérlése egy végrehajtási lista alapján történik, melynek kezelését a `SimRoot` és `SimItem` osztályok végzik. A lista `SimItem` típusú elemekből áll. Ebben az osztályban találhatók infromációk az egyes elemek egymáshoz képesti viszonyáról a sorban, valamint a végrehajtandó lépéseket is itt tárolódnak. Egy ilyen lépést egy itt tárolt függvény (std::function) jelképez ami végrehajtáskor meghívódik. Ilyen függvény lehet például egy Bell-mérés végrehajtása, vagy egy qubit átküldése egy csatornán. Ezen felül tárolva van

még a végrehajtás tervezett ideje is. A listát kezelő `SimRoot` osztály ennek alapján új elem felvételénél a megfelelő helyre tudja rakni a tagokat ezzel egy idő szerint rendezett struktúrát hozva létre. A végrehajtásnál így már mindig csak a soron következő elemmel kell foglalkozni. Az objektumba felelős még a sor megfelelő ürítéséért is törlésnél, valamint itt található a szimuláció aktuális órája is. E két osztály a `Simulation.h` fájlnak része.

3.3. A kvantumos elemek reprezentációja

A szimuláció során elemi kvantumos egységnek nem a kvantum bitet, hanem mivel minden esetben egy vagy több párral kell dolgozni a kvantum bitpárt választottam. Ennek leírására `qrep.h` fájlban található `QPair` osztály szolgál. Párt választani alapelemnek abból a szempontból is nagy könnyebség, hogy a két részecske közti lehetséges összefonódást a bitek együttes állapota már tartalmazza, ezért annak külön kezelésével nem kell foglalkozni. Az együttes állapot leírására ennek megfelelően egy 4 dimenziós komplex vektor szolgál(a 2 bit egy 4 dimenziós állapotteret feszít ki). Ide sorolató továbbá még az egybites kvantumos memóriát reprezentáló `QMem` osztály. Az egy qubitre való hivatkozáshoz itt tárolva van a pár címe, aminek a tárolt qubit a része, valamint egy index aminek segítségével a összetett páros állapotból ki tudjuk nyerni a számunkra érdekes qubitet. Az objektum tárolni tudja még ezen kívül egy adott qubit beérkezési idejét is, amiből így később számítható a bit teljes memóriában töltött ideje. A két osztál az említetteken túl egyéb szimulációt segítő segédváltozókat tartalmaz még.

3.4. Az ismétlő protokoll elemei

Az ismétlő protokoll működéséhez szükséges elemeket az `elements.h` fájl tartalmazza. Itt vannak meghatározva a csomópontok, csatornák, valamint az általuk használt eszközök, eljárások. Ezek közül egyik másik erősen épít egymásra. Az itt található fontosabb dolgok ezt is figyelembe véve:
`Pair2Measure` osztály ami párokon elvégzendő mérések megvalósítására szolgál. Jelen esetben csak a Bell-mérés megvalósítására szolgál, viszont megfelelő paraméterekkel más mérések is elvégezhetőek. Mérést tud végezni 2 páron. Ehhez mivel a párok közötti összefonódással számolni is számolni kell létrehozza az így kialakuló minde a két párra kibővített teret és a továbbiakban azon dolgozik. Magát a mérést a bevezetőben leírtak szerint el lehet végezni. Továbbá tartalmaz állítható kisegítő mátrixokat is, amivel például egyszerűbb bázisváltás is végezhető, megfelelő beállításukkal a mérési folyamat tovább egyszerűsíthető. A beépített Bell-mérés(`.bmeasure()`) ezeket használja, emiatt a beállításuk fontos, viszont ez egyszerűen megtehető egy másik beépített függvénnyel(`.SetBellMeasure()`).
`EPR` osztály, ami összefonódott párok előállításáért felel. Benne állítható a létrehozni kívánt pár(ez bármilyen lehet) állapota, amit itt is egy 4 dimenziós komplex vektor ír le, valamint a kiadott pár ehhez képesti tisztasága, amivel egy ismeretlen zaj hatását lehet imitálni. Beállítható még a pár generálások közt eltelt idő, ami később a szimulációban kerül felhasználásra.
`Channel` osztály az egyes csomopontokat összekötő kvantumos kommunikációs csatornák

leírására. Az egyes csatornákat a hosszukkal, valamint csillapításukkal, amit itt egy „csillapítási hosszal" jellemzünk. A csatorna által okozott zavar/veszteség egy bit egyszeri átküldésénél a legtöbb esetben átviteli valószínűségként nyilvánul meg. Ennek értéke az előző jellemzőkkel leírva:

$$p = e^{-\frac{L}{L_{cs}}}, \text{ ahol } L \text{ a teljes hossz } L_{cs} \text{ pedig a „csillapítási hossz".}$$

Ezeken felül az osztály tartalmaz még a szimulációt segítő egyéb változókat(pl.: melyik két csomópontot köti össze), valamint egy a szimulációs sorban végrehajtandó lépést is. A `SendThrough` függvény írja le azt, hogy mi történik a qubittel a csatornán való áthaladás során. A csatorna jellemzőinek megfelelően módosítja a qubitet tartalmazó pár állapotat, valamint lépteti tovább a szimulációt azáltal, hogy a végrehajtási sorba beütemezi a következő lépést.
`Node` osztály felelős a használt csomópontok leírásáért. El vannak benne tárolva a csomópont működéséhez szükséges információk: a csomópont helye a felépített kísérleti rendszerben(a többi csomóponthoz képest), a működése során felhasznált eszközök(Bell-mérés, pár létrehozás, pár tisztítás). Ezeken felül minden ilyen csomópont rendelkezik valamennyi memóriával is(`QMem` tömb) amiken keresztül működése során az egyes qubiteket manipuláln tudja. Az összefonódott párokat létrehozó egységeknél állítható plusz változó még az egyszerre létrehozandó párok száma, valamint a mérést végző egységek esetében a tisztító protokoll által elérendő tisztaság. Az osztályban van még definiálva a végrehajtási sorban fellelhető szimulációs lépések nagy része is.

3.5. Szimuláció működése

A szimuláció és az alkalmazott modell működésének bemutatásához tekntsük a következő egyszerű esetet. A vizsgált rendszerben két végpont között egy csomópont, valamint két összefonódott pár forrás segítségével szeretnénk összefonódott állapotokat megosztani. Így összesen 5 egységünk és 4 csatornánk van:3 hagyományos csomópont és 2 párt generáló, valamint az őket összekötő csatornák. A továbbiakban egy pár útját vizsgáljuk ahogy halad és változik a rendszerben. Ehhez kiindulásak feltételezzük, hogy már vannak más párok is a rendszerben, viszont a vizsgált párunk számára is van még szabad memória.
FIG
A vizsgált párt az egyik párokat generáló csomópont hozza létre a `GenEPR` lépés segítségével, ami végrehajtása során a pár létrehozásán túl másik két lépést is ütemez a végrehajtási sorba. Ez a két lépés ez egyes összekötő csatornák által tárolt `SendThrough`, a pár megfelelő indexeivel meghívva. Amennyiben a pár átjut a csatornán, a csatorna típusának és hosszának megfelelő késleltetéssel ütemezve lesz a következő lépés ami az egyes csatornák végpontjaihoz tartozó hagyományos csomópontokon végrehajtott `ReceiveFromCh`. Itt kizárólag azt vizsgáljuk, hogy az éppen beérkező qubit számára van-e hely az egység memóriájában. Amennyiben nincs, a párt megfelelően törli, ha van, akkor pedig berakja az üres memóriába, és ütemezi a következő teendőt, valamint a csomópont struktúrában elfoglalt helyének megfelelően állítja a memória szimulációs állapotát. Mivel a párral csak akkor tudunk a

továbbiakban dolgozni, ha mind a két bitjét sikerrel fogadtuk, ezért a két fogadó csomópontnak ezt a tényt le kell kommunikálniuk klasszikus kommunikációs csatornák segítségével. Ezt a folyamatot jelképezi a megfelelő késleltetéssel ütemezett `ReceiveFromChSuccess`. Ha mindkét bit sikeresen bekerült a hozzá tartozó memóriába, állít a memória szimulációs állapotán, valamint ütemezi a következő lépést. Ez az `Updateformeasure` ami egy a csomópontot elvégzett frissítés. Azt nézi, hogy memóriákon végrehajtható-e már a Bell-mérés, valamint hogy mely tárolt párokon szükséges tisztítóprotokollt végrehajtani. Ennek megfelelően Bell-mérés elvégzést ütemez, vagy tisztítóprotokoll elvégzést ütemez. A Bell-mérés elvégzését a `Bellmeasure` lépéssel lehet elvégezni. Ennek során a bevezetőben leírtak alapján két páron megtörténik a Bell-mérés. Végeredményül az egyik új pár(a mért bitekből keletkezett) törlődik, míg a két távoli állomás bitjei között új pár keletkezk. A mérésnek 4 eredménye lehet, de mivel a protokoll során mi egy bizonyos állapotot szeretnénk szétosztani szükség van egy mérés utáni korrekcióra. Ehhez szükség van a mérés eredményére, valamint az új pár qubitjein kell elvégezni, ezért itt is fellép a csomópontok között szükséges klasszikus kommunikációból adódó késleltetés. Ez a `CorrectAfterMeasure` megfelelő időre történő ütemezésével szimulálható. Maga a korrekció elvégezhető a qubiteken történő helyi műveletek végrehajtásával a teleportációs protokoll idevágó lépéséhez hasonlóan [7] Pauli X és Z kapuk segítségével. Legyen a cél állapotunk $|\Phi^+\rangle$, ekkor a mérés után lehetséges 4 Bell állapotból csupán az első biten végrehajtott műveletekkel a következő módon előállítható:

$$|\Phi^+\rangle \to |\Phi^+\rangle$$
$$Z|\Phi^-\rangle \to |\Phi^+\rangle$$
$$X|\Psi^+\rangle \to |\Phi^+\rangle$$
$$ZX|\Psi^-\rangle \to |\Phi^+\rangle$$

4. fejezet

Szimulációs eredmények

Insert stuff and nice graphs here

Irodalomjegyzék

[1] IBM, „Ibm announces advances to ibm quantum systems & ecosystem." `http://www-03.ibm.com/press/us/en/pressrelease/53374.wss`, 2017.

[2] C. Neill, P. Roushan, K. Kechedzhi, S. Boixo, S. Isakov, V. Smelyanskiy, R. Barends, B. Burkett, Y. Chen, Z. Chen, *et al.*, „A blueprint for demonstrating quantum supremacy with superconducting qubits," *arXiv preprint arXiv:1709.06678*, 2017.

[3] C. H. Bennett and G. Brassard, „Quantum cryptography:public-key distribution and coin tossing„" *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.

[4] P. Marks, „Quantum cryptography to protect swiss election." `https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/`, 2007.

[5] H. J. Kimble, „The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[6] W. K. Wootters and W. H. Zurek, „A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, „Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.

[8] E. Schrödinger, „An undulatory theory of the mechanics of atoms and molecules," *Physical Review*, vol. 28, no. 6, p. 1049, 1926.

[9] A. Einstein, B. Podolsky, and N. Rosen, „Can quantum-mechanical description of physical reality be considered complete?," *Physical review*, vol. 47, no. 10, p. 777, 1935.

[10] J. Bellt, „On the einstein podolsky rosen paradox," 1964.

[11] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, „Experimental quantum teleportation," *Nature*, vol. 390, no. 6660, pp. 575–579, 1997.

[12] P. W. Shor, „Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[13] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, „Experimental quantum cryptography," *Journal of cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[14] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, „" event-ready-detectors" bell experiment via entanglement swapping," *Physical Review Letters*, vol. 71, no. 26, pp. 4287–4290, 1993.

[15] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, „Experimental entanglement swapping: entangling photons that never interacted," *Physical Review Letters*, vol. 80, no. 18, p. 3891, 1998.

[16] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, „Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical review letters*, vol. 76, no. 5, p. 722, 1996.

[17] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, „Quantum repeaters: the role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.

[18] R. Brandom, „China's new satellite would create the world's largest quantum network." `https://www.theverge.com/2016/8/15/12489914/china-satellite-quantum-encryption-network-launch`, 2017.

[19] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, *et al.*, „Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[20] „Quantum manifesto endorsement." `http://qurope.eu/manifesto`, 2016.

[21] S. Pirandola and S. L. Braunstein, „Unite to build a quantum internet," *Nature*, pp. 169–171, 2016.

[22] D. A. Lidar and T. A. Brun, *Quantum error correction*. Cambridge University Press, 2013.

[23] J. Zhang, Y.-x. Liu, Ş. K. Özdemir, R.-B. Wu, F. Gao, X.-B. Wang, L. Yang, and F. Nori, „Quantum internet using code division multiple access," *Scientific reports*, vol. 3, 2013.

[24] M. Uphoff, M. Brekenfeld, G. Rempe, and S. Ritter, „An integrated quantum repeater at telecom wavelength with single atoms in optical fiber cavities," *Applied Physics B*, vol. 122, no. 3, p. 46, 2016.

[25] H. Krovi, S. Guha, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, „Practical quantum repeaters with parametric down-conversion sources," *Applied Physics B*, vol. 122, no. 3, p. 52, 2016.

[26] A. D. Pfister, M. Salz, M. Hettrich, U. G. Poschinger, and F. Schmidt-Kaler, „A quantum repeater node with trapped ions: a realistic case example," *Applied Physics B*, vol. 122, no. 4, p. 89, 2016.

[27] T. Li, G.-J. Yang, and F.-G. Deng, „Heralded quantum repeater for a quantum communication network based on quantum dots embedded in optical microcavities," *Physical Review A*, vol. 93, no. 1, p. 012302, 2016.

[28] I. Sándor and F. Balázs, *Quantum Computing and Communications: an engineering approach.* John Wiley & Sons, 2005.

[29] S. Imre and L. Gyongyosi, *Advanced quantum communications: an engineering approach.* John Wiley & Sons, 2012.

[30] A. Peres, „Delayed choice for entanglement swapping," *Journal of Modern Optics*, vol. 47, no. 2-3, pp. 139–143, 2000.

[31] X.-s. Ma, S. Zotter, J. Kofler, R. Ursin, T. Jennewein, Č. Brukner, and A. Zeilinger, „Experimental delayed-choice entanglement swapping," *Nature Physics*, vol. 8, no. 6, pp. 479–484, 2012.

[32] A. M. Goebel, C. Wagenknecht, Q. Zhang, Y.-A. Chen, K. Chen, J. Schmiedmayer, and J.-W. Pan, „Multistage entanglement swapping," *Physical Review Letters*, vol. 101, no. 8, p. 080403, 2008.

[33] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, „Bell measurements for teleportation," *Physical Review A*, vol. 59, no. 5, p. 3295, 1999.

[34] „Eigen c++ library." `eigen.tuxfamily.org/`.