

gyongyosi@hit.bme.hu_209_24

Kvantuminformatikai protokollok

MTA doktori értekezés tézisei

Gyöngyösi László
PhD

Budapesti Műszaki és Gazdaságtudományi Egyetem
Hálózati Rendszerek és Szolgáltatások Tanszék
2024

© Gyöngyösi László, 2024.

gyongyosi@hit.bme.hu_209_24

Kivonat

A kvantuminformatika a kvantummechanika jelenségeire épülve fejlett számítástechnikai és telekommunikációs lehetőségeket biztosít. A hagyományos számítógép-architektúrák fizikai határaihoz érve, a kvantuminformatikai eljárások és protokollok kialakítása egyre inkább előtérbe kerül. A disszertáció újszerű kvantuminformatikai protokollokat definiál: egy többvívós kvantumkulcs-elosztási protokollt, egy kvantumáramkör-optimalizációs protokollt kvantumszámítógépekhez, valamint egy elosztott kvantumszámítási protokollt. A protokollok célja a kvantumszámítások, valamint a kvantumkommunikációs hálózatok teljesítményének és hatékonyságának növelése.

gyongyosi@hit.bme.hu_209_24

Téziscsoportok

1. Téziscsoport. Többvivős CVQKD kvantumkulcselosztási protokoll

1.1. Propozíció. *A protokoll az $\mathcal{N}$ fizikai Gaussi-kvantumcsatornát n Gaussi-alkvantum-csatornára osztja, $\mathcal{N}_i, i = \{0, \dots, n-1\}$, $\sigma_{\mathcal{N}_i}^2$ független zajvarianciákkal, ahol $\frac{1}{n} \sum_{i=0}^{n-1} \sigma_{\mathcal{N}_i}^2 = \sigma_{\mathcal{N}}^2$.*

1.1. Tézis. *Az $\nu_i = \sigma_{\mathcal{N}}^2 / |F(T_i(\mathcal{N}_i))|^2$ paraméter szerint, ahol $|F(T_i(\mathcal{N}_i))|^2 = \left| \sum_{k=0}^{n-1} T_k e^{\frac{-i2\pi i k}{n}} \right|^2$, $i = 0 \dots n-1$, meghatározható az $\sigma_{\omega}^2 = \nu_{Eve} - \min(\nu_i)$ optimális modulációs variancia az alkvantumcsatornák részére, ahol ν_{Eve} az optimális lehallgatáshoz tartozó biztonsági korlát paraméter.*

1.2. Tézis. *A protokoll abszolút biztonságos tetszőleges véges méretű koherens támadások esetén.*

1.3. Tézis. *A protokoll abszolút biztonságos tetszőleges optimális kollektív támadásokra.*

1.1. Lemma. *Adott $|T(\mathcal{N})|^2$ transzmissziós együttható mellett, $N_{tol,AMQD} \geq N_{tol,single}$, ahol $N_{tol,single}$ az egyvivős, $N_{tol,AMQD}$ pedig a többvivős CVQKD protokoll tolerálható zajmennysége.*

2. Téziscsoport. Kvantumáramkör-optimalizációs protokoll

2.1. Tézis. *A $\mathcal{P}$ előfeldolgozással meghatározhatóak a redukált komplexitású QG^* kapustruktúra $U(\vec{\theta}_i)$ kapuparaméterei, $i = 1, \dots, n$, valamint a $|\tilde{X}\rangle$ redukált bemeneti kvantumállapot, tetszőleges nem-redukált QG_0 kapustruktúra és $|X\rangle$ bemeneti állapot esetén.*

2.2. Tézis. *Az U_R operátorral a nem-redukált QG_0 struktúra $|Y\rangle$ kimeneti kvantumállapota előállítható a QG^* redukált struktúra $|Z\rangle$ kimeneti kvantumállapotából.*

2.3. Tézis. *A U_R operátor $\mathcal{O}(\sqrt{n})$ komplexitással implementálható tetszőleges L kapuszámú, nem-redukált QG_0 struktúra esetén.*

2.1. Lemma. Adott $\partial \geq 1$ redukciós arány mellett, a $G \in [0, 1]$ redukciós nyereség $G = 1 - \frac{1}{\partial}$.

3. Téziscsoport. Elosztott kvantumszámítási protokoll

3.1. Tézis. Egy tetszőleges N kvantumrendszer skálázható az összefonódott kapcsolatok összefonódási szintje, a kvantumcsomópontok lokális műveleteinek kapuparaméterei, valamint a csomópontokban végzett lokális mérések segítségével. Az N elosztott rendszer kapumodell kvantumszámításokat valósít meg skálázható, elosztott módon.

3.1. Propozíció. Egy adott V_x csomópontban, a j lokális qubit összefonódott kapcsolatban áll a lokális k qubittel, $\langle jk \rangle$, valamint Γ_j nem-lokális qubittel, $n_1, \dots, n_{\Gamma_j}$. A nem-lokális qubitek nem szomszédosak k qubittel (Γ_j és k között nincs kapcsolat). Azon qubitek száma, amelyek kapcsolatban állnak j qubittel, de k -val nem, összesen $\Gamma_j + 1$.

3.2. Propozíció. Az A_i forráscsomópontban a $\mathcal{L}_U(|+\rangle_i)$ feltöltési folyamat megvalósítható az $\mathcal{M}_B$ Bell-méréssel, amely a $|+\rangle_i$ bemeneti állapotban, valamint $|\Phi\rangle_i$ első állapotán kerül végrehajtásra, ahol $|\Phi\rangle_i$ a $\mathcal{P}(A_i \rightarrow B_i)$ számítási útvonalhoz rendelt hálózati rendszerállapot.

3.2. Tézis. Tetszőleges optimalizálási probléma C célfüggvénye maximalizálható N segítségével, elosztott és skálázható módon, az F függvény segítségével, $F = \sum_{\langle jk \rangle \in N} F_{\langle jk \rangle} = \max_{\forall \theta} \langle \phi^* | C | \phi^* \rangle$, ahol $\langle jk \rangle$ l -szintű, $l \geq 1$, összefonódottságot azonosít j és k qubitek között.

3.1. Lemma. Az N hálózat $\mathcal{D}(N)$ elosztott számítási tere egy kiterjesztett korrelációs tér, n összefonódott $\mathcal{P}(A_i \rightarrow B_i)$, $i = 1, \dots, n$ számítási útvonallal.

3.3. Tézis. A $\mathcal{P}(A \rightarrow B)$ számítási útvonalhoz tartozó $F_{\mathcal{P}(A \rightarrow B)}$ függvény, adott $C_{\mathcal{P}(A \rightarrow B)} = \sum_{\langle jk \rangle \in \mathcal{P}(A \rightarrow B)} C_{jk}$ célfüggvény mellett, maximalizálható a $\beta_j = \frac{\pi}{8}$ és $\gamma_{jk} = \frac{1}{2} \cos^{-1} \left(\frac{\Gamma_j - 1}{\Gamma_j + 1} \right)$ kapuparaméterekkel az L csomópontban, ahol Γ_j a j qubit nem-lokális kapcsolatainak száma.

3.2. Lemma. Az $F_{\langle jk \rangle}$ függvény maximalizálásának $f_C(F_{\langle jk \rangle})$ költsége a lokális műveletek időparamétere alapján meghatározható. A költségfüggvény a Γ_j paraméterrel skálázható.

1. Bevezetés

A kvantuminformatika alapvetően új lehetőségeket nyit a nagy teljesítményű számítógép-architektúrák és kommunikációs hálózatok megvalósítására. A kereskedelmi kvantumszámítógépek megjelenését követően olyan, alapvetően más informatikai protokollokra és eljárásokra, ún. *kvantuminformaticai protokollok*ra lesz szükség, amelyek biztosítják a kvantumszámítások hatékonyságát, hatékonyan alkalmazhatóak kvantumhálózati környezetekben, valamint garantálják a felhasználók adatainak biztonságát.

A QKD (quantum key distribution) kvantumkulcs-elosztási protokollok segítségével, a felhasználók abszolút biztonsággal oszthatnak meg titkos kulcsokat [1,2]. A hagyományos kriptográfiai módszerekkel ellentétben, amelyek matematikai függvények számítási komplexitására épülnek, a QKD biztonsága fizikai törvényeken alapul. A titkos kulcsot a kommunikációs felek (Alice és Bob) egy kvantumcsatornán keresztül hozzák létre [3], amely implementálható optikai szál vagy szabadtéri optikai csatorna segítségével. CVQKD (continuous-variable QKD) környezetben az információt *folytonos változóban* (continuous-variables), azaz fotoncsomagokban kódoljuk, általánosan Gaussi-modulációval, amely a koherens kvantumállapotok [2] pozíció- vagy impulzus kvadratúráit módosítja. A DVQKD-vel (discrete-variable QKD) összehasonlítva, ahol *diszkrét változókat* (fotonok) használunk, a folytonos változók modulációja és dekódolása nem igényel speciális telekommunikációs eszközöket és hálózatokat, így a CVQKD protokollok hatékonyan megvalósíthatóak a jelenlegi implementációs bázissal is. Ebből következően, a CVQKD rendszerek kiemelt jelentőségűek a kvantuminternet [4–8] kifejlesztése szempontjából, a különböző kvantumeszközök és kvantumszámítógépek közötti kommunikáció titkosításának biztosítására [9–14].

A kvantumszámítógépek fejlesztése napjainkban is zajlik [10–38]. A kvantumszámítógépek segíthetnek a nehéz számítási problémák megoldásában [39–41], ugyanakkor, a jelenlegi eredmények szerint, a kvantumszámítógépek nem képesek exponenciális sebességnövekedést nyújtani az NP-teljes és nehezebb problémák megoldása során. Azonban, a kvantumszámítógépek ún. *kvantum-sebességnövekedésén* [42] keresztül jelentős előnyök érhetőek el.

A kvantumszámítógépek kifejlesztésének első lépéseként, Shor [43] faktorizációs algoritmusát 2001-ben egy kisméretű NMR (nukleáris mágneses rezonancia) eszközzel valósították meg [44]. 2010-ben, a D-Wave [45] bejelentette az ún. annealing számítógépeket, korlátozott alkalmazási lehetőségekkel. A Google kvantuminformaticai kutatásai 2013-ban kezdődtek meg [46]. 2016-ban kifejlesztettek egy speciális algoritmust [47], valamint szimulálták a hidrogénmolekula energiaszintjeit is [48]. 2019-ben a Google bejelentette

az 53 qubites kapumodell-alapú (gate-model) szupravezető kvantumszámítógépet [11], amely elméletileg mindössze 3 perc alatt képes megoldani olyan optimalizálási problémákat, amelyek egy klasszikus szuperszámítógépnek 10 000 évig tartanának. Később, a Google 53 qubites kvantumszámítógépének elméleti kereteit is meghatározták [49]. Az IBM-nél a kvantuminformatikai kutatásokat 2016-ban kezdték el [50], az IBM Quantum Experience programon keresztül. Az IBM emellett lehetővé tette a felhasználók számára, hogy az IBM Quantum Cloud Services szolgáltatása segítségével algoritmusokat futtassanak az IBM kvantumprocesszorán. 2016 és 2019 között, az IBM 5 és 27 qubites kvantumprocesszorokat fejlesztett ki, 2020-ban bejelentették a 65 kvantumbites IBM Quantum Hummingbird processzort, 2021-ben a 127 qubites processzort, 2022-ben pedig egy 433 qubites processzort [51]. Az 1121 qubites processzor 2023-ban jelent meg [51]. Az Amazon 2020-ban indította el az Amazon Braket Cloud Quantum Computing Service [52] szolgáltatását.

A kvantumszámítógépek teljesítményére adekvát válaszként elindult a *quantuminternet* kifejlesztése [5, 8, 53–61]. A kvantuminternet elsődleges célja, hogy abszolút biztonságot, valamint fejlett hálózati szolgáltatásokat nyújtson a felhasználók számára [4–6, 53–55, 57, 62–78]. 2019-ben az USA létrehozta a National Quantum Initiative Act (NQIA) [79] keretrendszert, az uniós országok pedig az EuroQCI (European Quantum Communications Infrastructure) [80] kezdeményezést, amely a Quantum Technologies Flagship 2018 [81] projektet követi az European Quantum Manifesto [82] szerint. Az EuroQCI elsősorban egy teljes Európát érintő kvantumkulcs-elosztó hálózat kialakítására összpontosít, amely később a kvantuminternetre is kiterjeszthető. Az EuroQCI hálózat két fő szegmensből áll. A földi szegmens az optikai szálakon alapuló rendszereket köti össze [83, 84], az űrszegmens pedig a távoli földi állomások között biztosít kommunikációt LEO/MEO (low earth orbit/medium earth orbit) vagy GEO (geostationary earth orbit) műholdakon keresztül [85]. 2017-ben Kína is megkezdte a kutatásokat egy globális méretű kvantumkulcs-elosztó hálózat megvalósítására [86].

1.1. Motiváció

Mivel a hagyományos, egyvívós (single-carrier) CVQKD nem teszi lehetővé több alapvető erőforrás kihasználását az átviteli fázisban, a disszertációban definiálom a többvívós (multicarrier) CVQKD protokollt. Az egyvívós CVQKD-vel összehasonlítva, a többvívós átvitel ún. alvívó (subcarrier) állapotokat használ az információ továbbítására. A többvívós moduláció lehetővé teszi az átvitel azon további szabadságfokainak kihasználását, amelyek az egyvívós környezetben nem állnak rendelkezésre.

A kvantumszámítógépek a kvantummechanika jelenségeit használják fel a számítások hatékony végrehajtására. A kapumodell-alapú (gate-model) kvantumszámítógépek kiemelt jelentőségűek a kvantumszámítógépek és kvantumeszközök gyakorlati implementálhatósága szempontjából. Mivel a kapumodell kvantumszámítógépek kvantumáramköreinek implementációs költségei magasak (nagy mennyiségű kapu szükséges), így ezen költségek csökkentése alapvető fontosságú. A disszertációban definiálok egy protokollt a kapumodell kvantumszámítógépek áramköreinek optimalizálására. A protokoll célja az áramkörök komplexitásának (mélységének) csökkentése.

A kvantumszámítások skálázhatósága egy elosztott kvantumrendszerben bonyolult feladat a problémátér komplexitása miatt. Az elosztott kvantumszámítási modellnek tetszőleges kvantumrendszereket kell integrálnia, a kisebb kvantumeszközöktől a nagyméretű kvantumszámítógépekig, egészen a kvantuminternetig. Ebből következően, a skálázható, elosztott kvantumszámítási modell meghatározása és paraméterezése nehéz probléma. Jelenleg nem áll rendelkezésre általános megoldás. A disszertációban egy skálázható, elosztott kvantumszámítási protokollt is definiálok.

2. Doktori értekezés

2.1. Eredmények

A disszertáció újszerű kvantuminformatikai protokollokat definiál (Protokoll 1-3.).

A doktori értekezés eredményei:

- **Protokoll 1.** *Többvivős (multicarrier) CVQKD kvantumkulcs-elosztási protokoll* [87]. A standard (egyvivős) CVQKD környezetben a kvantumcsatorna zaját additív fehér Gauss-zajként modellezzük, a fizikai csatorna így egy Gaussi-kvantumcsatornának felel meg. Egy tetszőleges Gaussi-kvantumcsatornán azonban nem csak additív zajok jelenhetnek meg, a fizikai környezetek diverzitása miatt. Ebből következően, a standard CVQKD protokollok nem optimálisak tetszőleges Gaussi-kvantumcsatornákra. A 3. fejezetben definiálok a többvivős CVQKD protokollt. Bizonyítom, hogy a protokoll optimális tetszőleges Gaussi-kvantumcsatornákra. Az alvivő állapotok alcsatornákat képeznek a fizikai csatornából, ami jobb átviteli hatékonyságot és nagyobb tolerálható veszteséget eredményez a standard CVQKD protokollokhoz képest. Emellett, bizonyítom a többvivős CVQKD protokoll abszolút biztonságát.

- **Protokoll 2.** *Kvantumáramkör-optimalizációs protokoll* [88]. A kapumodell kvantumszámítógépek elengedhetetlenek a kvantumszámítások közeljövőben történő gyakorlati implementálhatóságához. A kapumodell kvantumszámítógépek unitér operátorok (kvantumkapuk) és kvantumállapotok segítségével valósulnak meg. Gyakorlati környezetekben a kvantumáramkörök komplexitása magas, amelyből következően az implementációs költségek (szükséges hardverkomponensek költségei) is magasak. Ezen költségek csökkentése alapvető fontosságú. A disszertáció 4. fejezetében definiálok egy protokollt a kapumodell kvantumszámítógépek áramköri komplexitásának csökkentésére. Definiálok a protokoll komponenseit, bizonyítom az kvantumáramköri mélységben realizálható csökkenés mértékét, valamint a protokoll komplexitását. A protokoll megoldást nyújt a kvantumszámítógépek fizikai rétegbeli költségeinek csökkentésére. A keretrendszer rugalmas, így tetszőleges áramköri mélységekre alkalmazható.
- **Protokoll 3.** *Elosztott kvantumszámítási protokoll* [89]. Az elosztott kvantumszámítások megvalósítása egy bonyolult probléma, a lehetséges kvantumrendszerek diverzitása, valamint a problémátér komplexitása miatt. A disszertáció 5. fejezete egy elosztott, kapumodell-alapú kvantumszámítási protokollt definiál. Bizonyítom, hogy a protokoll segítségével egy tetszőleges optimalizálási probléma célfüggvénye elosztott és skálázható módon maximalizálható. Meghatározom a protokoll hálózati tulajdonságait, skálázási jellemzőit, valamint paramétereit.

2.2. Tartalom és felépítés

A disszertáció felépítése a következő. A 2. fejezet összefoglalja a szükséges ismereteket. A 3. fejezet tárgyalja a többvivős CVQKD protokollt. A 4. fejezet a kvantumáramkör-optimalizációs protokollt definiálja. Az 5. fejezet az elosztott kvantumszámítási protokollt tárgyalja. A 6. fejezet zárja a disszertációt. Kiegészítő információkat a függelék tartalmaz.

3. Téziscsoportok

3.1. Téziscsoport 1. Többvivős CVQKD kvantumkulcs-elosztási protokoll

Az 1. téziscsoportban a többvivős CVQKD kvantumkulcs-elosztási protokollt definiálok. A CVQKD protokollban az információt koherens kvan-

tumállapotok hordozzák. A küldő, a folytonos kvantumváltozókat egy zajos kvantumcsatornán keresztül juttatja el a vevőhöz. Egy standard CVQKD környezetben, a zajt egy lehallgató által okozott additív fehér Gauss-zajként modellezzük (Gaussi-kvantum link). Egy tetszőleges Gaussi-kvantumcsatorna esetében azonban mind additív, mind multiplikatív zavarok jelen vannak az átvitelben. A multiplikatív zavar a különböző fizikai környezetek (pl. vezetéknélküli optikai átvitel) inherens tulajdonsága. Az additív és multiplikatív zavarokkal rendelkező fizikai csatornák számos gyakorlati környezetben általánosabb megközelítést jelentenek, mint a tisztán additív zajos csatornák. Ebből következően a standard CVQKD protokollok nem optimálisak, ha a fizikai összeköttetésben multiplikatív zavarok is jelen vannak. A disszertációban definiálom az *adaptív többvivős kvadrátúraosztásos modulációs protokollt* (adaptive multicarrier quadrature division, AMQD). A kifejlesztett protokoll optimális tetszőleges additív és multiplikatív zavarokkal rendelkező Gaussi-kvantumcsatornákra. A protokoll a kódolási fázisában, a küldő oldal alvivőket generál, amelyeket az átvitelt követően egy folytonos unitér transzformációval dekódol a vevő. Az alvivők ún. alcsatornákat képeznek a fizikai csatornából, ami jobb átviteli hatékonyságot, valamint nagyobb tolerálható veszteséget eredményez. Emellett bizonyítom a protokoll abszolút biztonságát is.

3.1.1. Motiváció

A CVQKD kvantumkulcs-elosztó rendszerek [1] lehetővé teszik az abszolút biztonságos kvantumkommunikáció megvalósítását a jelenlegi távközlési hálózatokon keresztül [3, 5, 58, 90–106]. A CVQKD rendszerek számos előnnyel rendelkeznek a DV protokollokkal szemben, mivel nem igényelnek speciális eszközöket [7, 54, 55, 57, 107–129] vagy különleges követelményeket gyakorlati implementációkban [94–99, 102–107]. A CVQKD rendszerek folytonos változókon alapulnak, mint például a pozíció- és impulzuskvadrátúrák [2, 94–99, 102–107]. Az általános CVQKD modellben, a Gauss-modulált koherens állapotokat egy zajos kvantumcsatornán továbbítjuk, ahol a lehallgató jelenléte Gaussi-zajt ad az átvitelhez [111, 112, 130–132].

A többvivős CVQKD keretrendszer a tetszőleges, véletlenszerű multiplikatív zajjal is rendelkező Gaussi-kvantumcsatornákra összpontosít, amely egy általánosabb megközelítést jelent gyakorlati rendszerekben. A csatornaátviteli együttható egy tetszőleges eloszlású paraméter [108–110, 115–118], amelyet a kvantumcsatorna fizikai jellemzői határoznak meg. A multiplikatív zajra példa a vezetéknélküli kvantumkommunikációs környezetek [92, 93, 133–135], ahol az additív zaj mellé multiplikatív zaj is társul az át-

vitel során. A kifejlesztett protokoll [87], így hatékonyan alkalmazható a CVQKD megvalósítására és optimalizálására a vezeték nélküli környezetekben, valamint a szabadterbeli optikai (free-space optical, FSO) [133–136] kvantumcsatornákon.

A CVQKD rendszerekben a Gaussi-moduláció egy robusztus és könnyen alkalmazható megoldás, így gyakorlati rendszerekben ezen moduláció jelenti az általános modulációs technikát. A CVQKD rendszerek azonban továbbra is érzékenyek a fizikai átvitel, valamint a gyakorlati eszközök pontatlanságaira [94–99, 102–107, 137–143]. A protokoll teljesítményét meghatározza a fizikai kvantumcsatorna zaja, valamint a csatorna átviteli (transzmissziós) paramétere [54, 55, 94–99, 144]. A kvantumcsatorna Gaussi zaja modellezi egy esetleges lehallgató optimális támadását [90, 91, 94–99], a fizikai csatornát így Gaussi-kvantumcsatornának nevezzük. Mivel a CVQKD implementálása szempontjából a tolerálható veszteség mértéke is központi paraméter, kívánatos lenne a kódolási és dekódolási folyamatban néhány optimalizálási lépést tenni a jelenlegi korlátok felülírása, valamint a kvantumszintű átvitel javítása érdekében.

Cél, hogy megoldást adjunk ezen problémákra az AMQD protokoll bevezetésével, amely mind az egyirányú, mind a kétirányú CVQKD rendszerekben alkalmazható az átvitel optimalizálása, valamint a tolerálható veszteség növelése érdekében. A hagyományos távközlésben az OFDM (orthogonal frequency-division multiplexing, ortogonális frekvenciaosztásos multiplexelés) egy jól ismert és széles körben alkalmazott technika a sávszélesség hatékonyságának javítására [130–132, 145–147]. Az OFDM rendszerekben az információ több vivőfrekvencián kerül kódolásra, fő előnye pedig az egyvivős átvittel szemben az, hogy az alvivőkön alapuló átvitel képes csillapítani a kedvezőtlen csatornakörülményekből adódó problémákat. A CVQKD esetében azonban nem létezik hasonló módszer. Ha a CV kvantumállapotokra is rendelkezésre állna hasonló megoldás, akkor CVQKD kvantumkommunikációs rendszerekben is hasonló előnyöket lehetne realizálni. Ezt szem előtt tartva, az AMQD segítségével definiálom a CV kvantumállapotokra épülő, többvivős CVQKD kvantumkulcs-elosztó protokollt, amelynek segítségével hasonló előnyök érhetőek el a kvantumszintű információátvitel során.

A hagyományos CVQKD kódolás esetén Alice, a küldő, modulálja majd külön-külön továbbítja az egyes koherens CV állapotokat. Ezt a szabványos modulációs sémát *egyvivős* (single-carrier) modulációnak nevezzük. Az AMQD moduláció működése a következő. Alice sorsol egy nulla átlagú, kör-szimmetrikus, komplex Gaussi véletlen vektort, amelyet az inverz Fourier-művelettel transzformál. Egy adott modulációs variancia mellett, Alice előállítja a Gaussi-alvivő CV kvantumállapotokat, amelyeket aztán továbbít

a kvantumcsatornán. Bob, a vevő, alkalmazza Alice inverz műveletét egy unitér transzformáció segítségével, ami lehetővé teszi számára, hogy visszatérje Alice koherens CV állapotainak zajos változatát. Ezt a fajta kommunikációt *többvivős* (multicarrier) CVQKD átvitelnek nevezzük [87, 93, 136, 148–154]. A többvivős átvitel során, a Gaussi-kvantumcsatorna több párhuzamos alcsatornának tekinthető, amelyeket *Gaussi-alkvantumcsatornáknak* nevezünk. Az alcsatornák mindegyike egy-egy adott alvivő kvantumállapot átvitelére szolgál.

Bizonyítom, hogy a fizikai csatornán keresztül küldött CV Gaussi-alvivők segítségével nagyobb tolerálható veszteség érhető el adott modulációs variancia mellett. Igazolom, hogy az alcsatornák információátviteli képessége összefüggésben áll az alvivő CV-k varianciájával, ami lehetővé teszi intelligens adaptív modulációs technikák kifejlesztését a többvivős CVQKD protokollon belül. Ennek lényege többek között, hogy az átvitelre csak alacsony zajszintű Gaussi-alcsatornákat használjuk, a zajos alcsatornákon pedig ne küldjünk értékes információt. Az adaptív kiosztás eredménye a protokoll jobb teljesítménye alacsony SNR (signal-to-noise ratio, jel-zaj viszony) értékek mellett, valamint nagyobb tolerálható veszteség. Ezen paraméterek kiemelt jelentőségűek zajos, alacsony SNR értékekkel rendelkező gyakorlati rendszerek (*általános implementációs környezet*) esetén.

Az AMQD moduláció számos fontos előnyt és tulajdonságot kínál a hagyományos CVQKD rendszerekhez képest. Kiemelendő a kvantumszintű átvitel optimalizálása, mivel az alvivő CV kvantumállapotok hatékonyabb kommunikációt tesznek lehetővé ugyanazon zajos fizikai kvantumcsatornán, adott modulációs variancia mellett.

3.1.2. Téziscsoport eredményei

A doktori értekezés 1. téziscsoportjának eredményei:

- *Definiálom a többvivős CVQKD protokollt.*
- *Vizsgálom a protokoll paramétereit és teljesítményét.*
- *Definiálok egy modulációs-variancia adaptációs technikát, amely optimális kommunikációt biztosít a fizikai kvantumcsatornán.*
- *Bizonyítom a többvivős CVQKD protokoll biztonságát.*

Az AMQD protokoll több extra szabadságfokot ad a CVQKD környezetéhez, így lehetőség nyílik olyan fejlett jelenségek bevezetésére, amelyek az egyvivős CVQKD környezetben nem állnak rendelkezésre. Ilyen például a

többsfelhasználós, többvivős CVQKD kommunikáció [93], az SVD-vel (singular value decomposition) kiegészített többvivős CVQKD [152], többdimenziós módszerek [149], valamint fejlett kvadratúra-detektálási technikák [150]. AMQD keretrendszer további biztonsági paraméterei, valamint a további kulcsrátá értékek bizonyítása [148]-ben található.

3.1.3. Vizsgálati modell

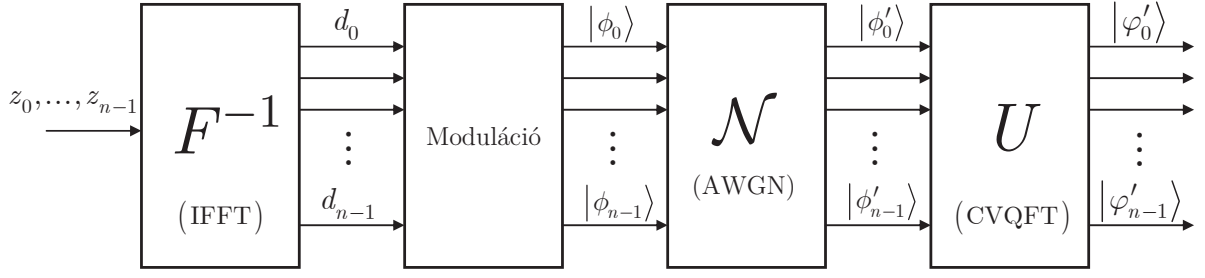
A többvivős CVQKD protokoll működésének összefoglalása a következő. Alice sorsol egy n -dimenziós, nulla átlagú, körszimmetrikus, komplex Gaussi vektort, $\mathbf{z} = \mathbf{x} + i\mathbf{p} = (z_0, \dots, z_{n-1})^T \in \mathcal{CN}(0, \mathbf{K}_{\mathbf{z}})$, $z_i = x_i + ip_i$, ahol $x_i \in \mathcal{N}(0, \sigma_{\omega_0}^2)$, és $p_i \in \mathcal{N}(0, \sigma_{\omega_0}^2)$ *i.i.d.* Gaussi véletlen változók, amelyek az x pozíció és p impulzus kvadratúrákat azonosítják az $\mathcal{S}$ fázistérben, míg $\sigma_{\omega_0}^2$ a modulációs variancia egyvivős átvitel esetén. A következő lépésben, Alice a $\mathbf{z}$ vektorra alkalmazza az inverz FFT (fast Fourier transform - gyors Fourier transzformáció) műveletet, aminek az eredménye a $\mathbf{d} = \mathbf{x} + i\mathbf{p} = (d_0, \dots, d_{n-1})^T \in \mathcal{CN}(0, \mathbf{K}_{\mathbf{d}})$, n -dimenziós, nulla átlagú, körszimmetrikus, komplex Gaussi véletlen vektor. Alice, a $\mathbf{d}$ vektor szerint előállítja a $|\phi_{0\dots n-1}\rangle$ Gaussi-alvivő CV kvantumállapotokat a $\sigma_{\omega}^2 \neq \sigma_{\omega_0}^2$ modulációs varianciát alkalmazva, ahol $|\phi_i\rangle$ az i -ik alvivő CV kvantumállapot. Az n alvivő állapot, a fizikai Gaussi-kvantumcsatornát n Gaussi-alkvantumcsatornára osztja az átvitel során, amelyek mindegyike $\sigma_{\mathcal{N}_i}^2$ független zajvarianciával rendelkezik. A dekódolási szakaszban, Bob alkalmazza az U -val jelölt CVQFT (continuous-variable quantum Fourier transform - folytonos változójú gyors Fourier transzformáció) unitér műveletet a vett zajos alvivő CV kvantumállapotokra, amelynek eredménye Alice zajos Gaussi változóit azonosítja CV kvantumállapotok formájában, $|\varphi'_{0\dots n-1}\rangle = |z'_{0\dots n-1}\rangle = |\mathbf{z}'\rangle$. Az átvitel során, a $|F(T_i(\mathcal{N}_i))|^2$ alcsatorna transzmissziós paraméterek diverzek, amelyet a protokoll adaptív modulációs eljárással kezel.

A többvivős CVQKD protokoll működését a 3.1. ábra foglalja össze.

3.1.4. Eredmények

1.1. Propozíció. *A protokoll az $\mathcal{N}$ fizikai Gaussi-kvantumcsatornát n Gaussi-alkvantum-csatornára osztja, $\mathcal{N}_i, i = \{0, \dots, n-1\}$, $\sigma_{\mathcal{N}_i}^2$ független zajvarianciákkal, ahol $\frac{1}{n} \sum_{i=0}^{n-1} \sigma_{\mathcal{N}_i}^2 = \sigma_{\mathcal{N}}^2$.*

Bizonyítás. A bizonyítás a disszertáció 3.2.5 alfejezetében található. ■



3.1. ábra. A többvivős CVQKD protokoll. Alice sorsol egy n -dimenziós, nulla átlagú, körszimmetrikus, komplex Gaussi véletlen vektort, $\mathbf{z}$, majd alkalmazza a F^{-1} inverz Fourier-transzformációt. A kapott $\mathbf{d}$ vektort alapján Gaussi-modulációval előállítja az alvivő CV kvantumállapotokat. A dekódolás során, Bob a U unitér CVQFT műveletet alkalmazza az n zajos alvivő CV állapotról, hogy Alice zajos változóit CV állapotok formájában visszanyerje. A $\mathcal{N}$ kvantumcsatorna additív Gaussi-zajjal jellemezhető (AWGN, additive white Gaussian noise - additív fehér Gaussi zaj), véletlenszerű transzmissziós együtthatókkal (multiplikatív zaj).

1.1. Tézis. Az $\nu_i = \sigma_{\mathcal{N}}^2 / |F(T_i(\mathcal{N}_i))|^2$ paraméter szerint, ahol $|F(T_i(\mathcal{N}_i))|^2 = \left| \sum_{k=0}^{n-1} T_k e^{\frac{-i2\pi i k}{n}} \right|^2$, $i = 0 \dots n-1$, meghatározható az $\sigma_{\omega}^2 = \nu_{Eve} - \min(\nu_i)$ optimális modulációs variancia az alkvantumcsatornák részére, ahol ν_{Eve} az optimális lehallgatáshoz tartozó biztonsági korlát paraméter.

Bizonyítás. A bizonyítás a disszertáció 3.3 alfejezetében található. ■

1.2. Tézis. A protokoll abszolút biztonságos tetszőleges véges méretű koherens támadások esetén.

Bizonyítás. A bizonyítás a disszertáció 3.4.1 alfejezetében található. ■

1.3. Tézis. A protokoll abszolút biztonságos tetszőleges optimális kollektív támadások esetén.

Bizonyítás. A bizonyítás a disszertáció 3.4.2 alfejezetében található. ■

1.1. Lemma. Adott $|T(\mathcal{N})|^2$ transzmissziós együttható mellett, $N_{tol,AMQD} \geq N_{tol,single}$, ahol $N_{tol,single}$ az egyvivős, $N_{tol,AMQD}$ pedig a többvivős CVQKD protokoll tolerálható zajmennyisége.

Bizonyítás. A bizonyítás a disszertáció 3.5 alfejezetében található. ■

3.1.5. Összefoglalás

Az 1. téziscsoportban definiáltam a többvivős CVQKD protokollt. Meghatároztam egy adaptív modulációs variancia allokációs mechanizmust a protokollon belül, valamint bizonyítottam a protokoll biztonságát. A protokoll keretet biztosít a CVQKD gyakorlati kvantumcsatornákon történő hatékony megvalósítására különböző implementációs környezetekben.

3.2. Téziscsoport 2. Kvantumáramkör-optimalizációs protokoll

A 2. téziscsoport egy kvantumáramkör-optimalizációs protokollt definiál kapumodell-alapú kvantumszámítógépekhez. A protokoll célja a kvantumáramkörök komplexitásának (kapuszám mennyiségének) csökkentése. Definiálom a protokoll egységeit, valamint a protokoll komplexitását. A protokoll segítségével, a kvantumszámítógépek fizikai költségei csökkenthetők. A protokoll keretrendszere rugalmas, így tetszőleges áramköri komplexitás esetén alkalmazható kapumodell-alapú kvantumszámítógépek optimalizálására.

3.2.1. Motiváció

A kapumodell kvantumszámítógépek jelentik a kvantumszámítások közeljövőben történő gyakorlati implementálhatóságának egyik alapját. Egy kapumodell kvantumszámítógép-környezetben a kvantumkapu struktúra mélysége (komplexitása) a kvantumműveletekhez szükséges kapuk (operátorok) számát jelenti [7, 13, 14, 22, 120, 155–166]. A kvantumszámítógépek hardverének kialakítása szempontjából alapvető fontosságú probléma a kvantumkapustruktúra méretének csökkentése. A probléma megoldása során, egy adott referencia kvantumáramkör (nem-redukált komplexitású áramkör) kimeneti kvantumállapotát szeretnénk előállítani egy redukált komplexitású kapustruktúrával. A kapumodell kvantumszámítógépeket kiemelten érinti a nagy áramköri komplexitás problémája. Ezen probléma releváns következménye a gyakorlati kvantumszámítások gyakorlati megvalósításához szükséges fizikai eszközök magas költsége. Célunk a bonyolultságcsökkentés problémájának megoldása egy univerzális (tetszőleges áramkörök esetén alkalmazható, platformfüggetlen), hatékonyan implementálható optimalizációs megoldással.

A kvantumszámítógép kvantumáramköre egy tetszőleges mélységű kvantumáramkörként modellezhető, amelyet L unitér operátor alkot. Minden egyes unitér operátor egy adott Pauli-operátorral, valamint egy kapu paraméterrel definiálható. A kvantumszámítógép bemeneti számítási problé-

mája egy P számítási problémával, valamint az ahhoz rendelt C célfüggvénnyel modellezhető. A C célfüggvény a kvantumszámítógépen keresztül, azaz a kvantumszámítógép áramköri struktúrájának unitér operátorain keresztül maximalizálható. A célfüggvény tartozhat kombinatorikus optimalizálási problémákhoz [13, 18, 19], komplex programozási problémákhoz [19], mint például a gráfszínezési probléma, a molekuláris konformációs probléma, ütemezési problémákhoz, útvonaltervezési problémákhoz [19], ill. egyéb bemeneti problémákhoz [11, 12, 12, 13, 13, 14, 17–19, 23, 49, 161, 167, 168].

A disszertációban egy optimalizációs protokollt definiálok kvantumszámítógépek kvantumáramköri komplexitásának csökkentésére. A protokoll célja egy tetszőleges referencia-quantumáramkör komplexitásának csökkentése, valamint a kvantumszámítógép bemeneti számítási problémájához rendelt célfüggvény maximalizálása. A protokoll meghatározza a referencia kvantumáramkör redukált komplexitású ekvivalensét, valamint a csökkentett komplexitású kvantumáramkör segítségével előállítja a referencia kimeneti kvantumállapotot. A protokoll része egy előfeldolgozási fázis a redukált struktúra meghatározására, valamint egy kvantumalgoritmus a referencia kimeneti kvantumállapot előállítására.

Az előfeldolgozási fázis egy gépi tanulási [169–172] egységet integrál a paraméterek optimalizálásához, valamint a redukált struktúra paramétereinek meghatározásához. A protokoll, az előfeldolgozási fázist követően, egy kvantumalgoritmust alkalmaz a redukált kvantumkapu-struktúra kimeneti kvantumállapotára, a referenciastruktúra kimeneti kvantumállapotának visszaállítására. A protokoll minden egysége univerzális, mivel nem támasztanak követelményeket a redukálandó referencia kvantumáramkör struktúrájával, a referenciastruktúrában lévő kapuk számával, valamint a referencia kvantumáramkör bemeneti kvantumállapotával szemben sem.

A protokollon belül alkalmazott kvantumalgoritmust egy fix méretű és paraméterezettségű kiegészítő hardverkomponensként definiáljuk, amely tetszőleges kapumodell kvantumszámítógép-környezethez illeszthető. Bizonyítom, hogy megfelelő paraméterek mellett, a protokoll kvantumalgoritmusának költsége nagyságrendekkel kisebb, mint az elérhető komplexitás-csökkenés nagysága. A protokoll lehetővé teszi továbbá a fizikai réteg megvalósítási költségeinek jelentős csökkentését, mivel a szükséges fizikai elemek és a nagy költségű hardverkomponensek száma csökkenthető.

3.2.2. Téziscsoport eredményei

A doktori értekezés 2. téziscsoportjának eredményei:

- *Definiálok egy kvantumáramkör-optimalizációs protokollt a kapumodell*

kvantumszámítógépek kvantumáramkörü komplexitásának csökkentésére.

- *Bizonyítom a protokoll komplexitását, valamint az elérhető komplexitás-csökkentés mértékét.*
- *Az algoritmus egy implementálható megoldást nyújt az áramkörü komplexitás, valamint a kvantumszámítógépek implementációs költségeinek csökkentésére.*
- *Az eredmények alkalmazhatóak kapumodell kvantumszámításokhoz és a kapumodell-alapú kvantum eszközökhöz.*

3.2.3. Vizsgálati modell

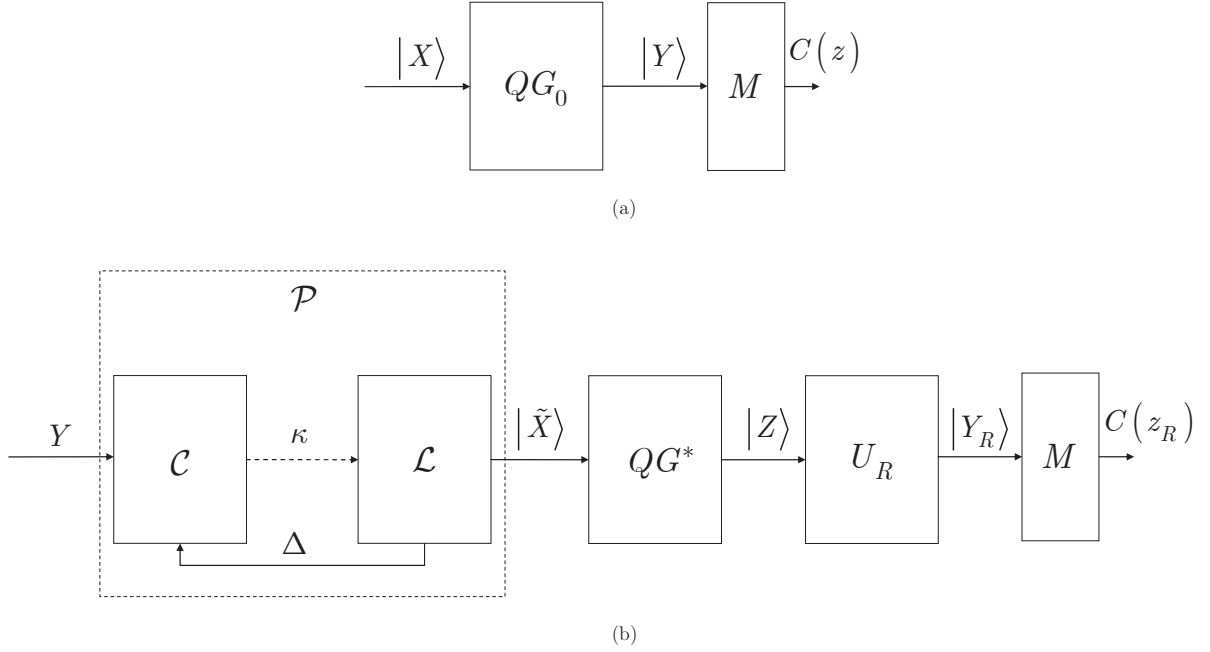
A $\mathcal{P}$ előfeldolgozási fázis meghatározza a QG^* redukált komplexitású kvantumáramkörhöz tartozó $|\tilde{X}\rangle$ bemeneti kvantumállapotot, valamint a QG^* struktúra paramétereit.

Az U_R operátor egy kvantumalgoritmust implementál $\mathcal{R}$ kvantumregiszter halmazzal a QG_0 referencia kvantumáramkör $|Y\rangle$ kimeneti kvantumállapotának meghatározására, a redukált komplexitású QG^* kvantumáramkör $|Z\rangle$ kimeneti kvantumállapotából. Az U_R operátor univerzális, azaz független az QG_0 struktúrában található L kapumennyiségtől, így az U_R operátor komplexitása állandó, tetszőleges kvantumáramkör esetén.

A QG_0 referencia kvantumáramkör (tetszőleges, nem-redukált komplexitású kvantumáramkör) valamint annak $|X\rangle$ bemeneti kvantumállapota a 3.2.(a) ábrán látható. A 3.2.(b) ábrán a protokoll rendszermodellje látható. A protokollt a $\mathcal{P}$ előfeldolgozási fázis, valamint a U_R operátor implementálja. Az U_R operátor a fizikai rétegben valósul meg, míg $\mathcal{P}$ egy logikai rétegbeli folyamat. A redukált struktúrához a $|\tilde{X}\rangle$ bemeneti kvantumállapot, valamint a QG^* redukált kvantumkapu-struktúra tartozik. A QG_0 referencia-áramkör $|Y\rangle$ referencia kimeneti kvantumállapotát a redukált struktúra segítségével kapjuk meg, amelynek jelölése $|Y_R\rangle$. A kimeneti állapotokat egy M méréssel mérjük, hogy a célfüggvény kiértékeléséhez szükséges klasszikus bitsorozatot kinyerjük. A következő iterációs lépésben az áramkörök kapuparamétereit kalibráljuk, amíg az optimális célfüggvény értéket el nem érjük.

3.2.4. Eredmények

2.1. Tézis. *A $\mathcal{P}$ előfeldolgozással meghatározhatóak a redukált komplexitású QG^* kapustruktúra $U(\vec{\theta}_i)$ kapuparamétere, $i = 1, \dots, n$, valamint a $|\tilde{X}\rangle$ re-*



3.2. ábra. (a). A nem-redukált QG_0 kvantumáramkör (referencia kvantumáramkör) adott $|X\rangle$ bemeneti kvantumállapottal, valamint $|Y\rangle$ kimeneti kvantumállapottal. A $|Y\rangle$ kimeneti állapot az M mérési operátorral bemérésre kerül, amelynek eredménye a z klasszikus bitsorozat, amely alapján a $C(z)$ célfüggvény értéke meghatározásra kerül. (b). A kvantumáramkör-optimalizációs protokoll sematikus modellje. Előfeldolgozási fázis: a QG_0 struktúra $|Y\rangle$ kimenetének Y klasszikus reprezentációja előfeldolgozásra kerül a $\mathcal{P}$ blokk segítségével. A $\mathcal{P}$ blokk $\mathcal{C}$ számítási alblokkja előállítja a κ vektort, amely ezt követően az $\mathcal{L}$ gépi tanulási alblokkhoz kerül, amely meghatározza a Δ hibaparamétert. A $\mathcal{P}$ előfeldolgozási fázis kimenete $\tilde{X}$, valamint a redukált struktúra kapuparaméterei, amelyek meghatározzák a QG^* redukált struktúrát. Kvantumalgoritmus: a $\tilde{X}$ kimenet, valamint a kapuparaméterek alapján a $|\tilde{X}\rangle$ bemeneti kvantumállapot, valamint QG^* redukált-struktúra meghatározásra kerül. A QG^* redukált struktúra kimenete a $|Z\rangle$ kvantumállapot, amely az U_R kvantumalgoritmushoz kerül tovább. A U_R operátor előállítja a $|Y_R\rangle$ kimeneti kvantumállapotot, amely ekvivalens a QG_0 referencia kvantumáramkör $|Y\rangle$ kimenetével. A $|Y_R\rangle$ állapot ezt követően az M mérési operátorral kerül bemérésre, amelynek eredménye a z_R bitsorozat, amely alapján kiértékelésre kerül a $C(z_R)$ célfüggvény értéke.

dukált bemeneti kvantumállapot, tetszőleges nem-redukált QG_0 kapustruktúra és $|X\rangle$ bemeneti állapot esetén.

Bizonyítás. A bizonyítás a disszertáció 4.4.1 alfejezetében található. ■

2.2. Tézis. *Az U_R operátorral a nem-redukált QG_0 struktúra $|Y\rangle$ kimeneti kvantumállapota előállítható a QG^* redukált struktúra $|Z\rangle$ kimeneti kvantumállapotából.*

Bizonyítás. A bizonyítás a disszertáció 4.4.2 alfejezetében található. ■

2.3. Tézis. *A U_R operátor $\mathcal{O}(\sqrt{n})$ komplexitással implementálható tetszőleges L kapuszámú, nem-redukált QG_0 struktúra esetén.*

Bizonyítás. A bizonyítás a disszertáció 4.4.4 alfejezetében található. ■

2.1. Lemma. *Adott $\partial \geq 1$ redukciós arány mellett, a $G \in [0, 1]$ redukciós nyereség $G = 1 - \frac{1}{\partial}$.*

Bizonyítás. A bizonyítás a disszertáció 4.4.5 alfejezetében található. ■

3.2.5. Összefoglalás

A kapumodell kvantumszámítógépek jelentik a kvantumszámítások közeljövőben történő gyakorlati implementálhatóságának egyik alapját. A kapumodell kvantumszámítógépek kvantumkapuk és kvantumállapotok segítségével valósulnak meg. A gyakorlati rendszerekben a kvantumáramkörök kapuszáma (áramköri komplexitás), így az implementációs költségek is magasak. Ezen költségek csökkentése alapvető fontosságú. A 2. téziscsoportban definiáltam egy optimalizációs protokollt a kapumodell kvantumszámítógépek áramköri komplexitásának csökkentésére.

3.3. Téziscsoport 3. Elosztott kvantumszámítási protokoll

Az 3. téziscsoportban definiálok egy elosztott, kapumodell-alapú kvantumszámítási protokollt. Az elosztott, skálázható kvantumszámítások megvalósítása nehéz probléma, a lehetséges kvantumrendszerek sokfélesége, valamint

a problémátér komplexitása miatt. Bizonyítom, hogy a protokoll képes egy optimalizálási probléma célfüggvényét elosztott, skálázható módon maximalizálni. Meghatározom a protokoll jellemzőit, valamint releváns paramétereit optimalizálási problémák megoldására.

3.3.1. Motiváció

A kvantumszámítógép-architektúrák és a kvantuminternet [5, 6, 144, 173–181, 181–189] elosztott kvantumrendszereknek tekinthetők [190–204]. A kvantumszámítások elvégzése egy elosztott kvantumrendszerben egy maximalizálási problémaként is megközelíthető. A bemeneti számítási probléma egy célfüggvényt definiál, amely elosztott módon kerül maximalizálásra távoli kvantumszámítógépek együttműködésével. Az elosztott problémamegoldás optimalizálása egyenértékű az elosztott kvantumrendszer adott bemeneti problémához tartozó célfüggvényének maximalizálásával. A célfüggvény elosztott módon történő maximalizálására kvantumszámítógépek [10–13, 49, 167, 205–207], kvantumcsatornák, kvantumterminálok, [8, 58, 63, 78, 194, 195, 197, 200, 202] alkalmazásával egy általános kvantuminternetes hálózati környezetben kerül sor.

A skálázható kvantumszámítások problémája egy elosztott kvantumrendszerben kihívást jelent a lehetséges problémátér komplexitása miatt. Az elosztott kvantumszámítási modellnek tetszőlegesen skálázott kvantumrendszereket kell tartalmaznia, a kisebb kvantumeszközöktől a nagyméretű kvantumszámítógépekig, egészen a kvantuminternetig. Ebből következően, az elosztott kapumodell kvantumszámítási modell skálázható modelljének definiálása és paraméterezése nehéz probléma, és jelenleg nem áll rendelkezésre általános megoldás.

A téziscsoportban a skálázható kvantumfeldolgozás problémáját vizsgálom elosztott kapumodell kvantumszámítógép környezetben. Definiálom a kapumodell kvantumszámítások skálázható elosztott modelljét, valamint az elosztott kvantuminformáció-feldolgozás skálázási jellemzőit.

Egy tetszőlegesen skálázott kvantumrendszer kis, közepes vagy nagy skálázottságú elosztott kvantumrendszereket integrál. A rendszermodell tetszőleges számú kvantumcsomópontból áll, amelyeket különböző szintű összefonódott kapcsolatok kötnek össze (az összefonódás szintje a forrás- és célcsoomópont közötti áthidalt csomópontok számára utal). A kvantumrendszer vonatkozhat egy kvantumkészülékre, kvantumszámítógépre vagy egy tetszőleges kvantuminternetes környezetre, amelyben több kvantumszámítógép (kvantumcsomópont) osztozik az összefonódáson, hogy elosztott kvantumszámításokat végezzen. A kvantumcsomópontoknak a célfüggvény maximalizálását

elosztott módon kell elérni, úgy, hogy minden egyes csomópont lokális egységeket alkalmaz, és tetszőleges szintű összefonódással kapcsolódik egymáshoz. Egy kis méretű rendszerben a kvantumcsomópontok egyszintű összefonódással kapcsolódnak egymáshoz, míg egy közepes vagy nagy méretű rendszer esetében a kvantumcsomópontok közötti összefonódás szintje tetszőlegesen nagy lehet. A csomópontok lokális egységeit úgy határozzuk meg, hogy az elosztott kvantumrendszer lehetővé tegye a kapumodell kvantumszámítások elosztott módon történő megvalósítását.

Definiálok egy skálázható elosztott kvantumrendszer rendszermodelljét, elosztott kapumodell kvantumszámítások skálázható végrehajtására. Vizsgálom a rendszermodell tulajdonságait, a kvantumcsomópontok lokális kapuparamétereit a célfüggvény maximalizálásához többszintű összefonódással kapcsolódó kvantumszámítógépek mellett, valamint definiálok a rendszer költségfüggvényét. Vizsgálom a dekoherencia hatását az elosztott célfüggvény kiértékelésében és maximalizálásában. Az eredmények alkalmazhatók kvantumszámítógépekben, kvantumeszközökben, kvantumhálózatokban és a kvantuminternetes környezetekben végzett elosztott skálázható kvantumszámításokhoz. A levezetések a közeljövőben is implementálható qubit-alapú rendszerekre fókuszálnak (qubit-alapú kvantumszámítógép-architektúrák, valamint többrészes qubit-összefonódással összekapcsolt hálózati struktúrák), az eredmények azonban tetszőleges dimenziós kvantumrendszerekre kiterjeszthetők.

3.3.2. Téziscsoport eredményei

A doktori értekezés 3. téziscsoportjának eredményei:

- *Definiálok egy elosztott skálázható, kapumodell-alapú kvantumszámítási protokollt.*
- *Meghatározom a protokoll paramétereit, valamint bizonyítom, hogy a protokollal tetszőleges optimalizálási probléma célfüggvénye maximalizálható elosztott, skálázható módon.*
- *Vizsgálom a dekoherencia hatásait az elosztott célfüggvény kiértékelésre, valamint definiálok a skálázható elosztott kvantumszámításhoz tartozó költségfüggvényt.*

3.3.3. Vizsgálati modell

Az N skálázható elosztott fizikai rendszer rendszermodellje a következő. A $N = (V, S)$ -ban a $|V|$ kvantumcsomópont $|S|$, l szintű összefonódott kap-

csolatokon keresztül kommunikálnak, ahol V a kvantumcsomópontok halmaza, S pedig az összefonódott kapcsolatok halmaza. Két csomópont, x és y között az összefonódott kapcsolat kétrészes kvantum összefonódást jelöl. Qubit rendszerek esetén, a $d = 2$ dimenziós, kétrészes maximálisan összefonódott állapotok az ún. Bell-állapotok; itt feltételezhetjük a $|\beta_{00}\rangle$ állapotot, $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ a rendszermodellben.

Egy l szintű összefonódott kapcsolat esetén a $d(x, y)_{L_l}$ hop-távolság (közbenső csomópontok száma x és y csomópontok között) N -ben $d(x, y)_{L_l} = 2^{l-1}$, $d(x, y)_{L_l} - 1$ köztes csomóponttal az x és y csomópontok között. Így az $l = 1$ érték, az x és y kvantumcsomópont közötti közvetlen kapcsolatra utal, közbenső kvantumcsomópontok nélkül az N elosztott rendszerben. Az összefonódott kapcsolat l szintje azt feltételezi, hogy minden egyes összefonódási szint megduplázza a x és y közötti hop-távolságot, ami egy általános modell a kvantumhálózatokban. Ezt használják az ún. duplázó összefonódás-elosztó architektúrában is, amelyben az összefonódási szinteket az összefonódás-csere végrehajtásával növelik [58, 59]. Az l paraméter általánosságban tetszőleges hop-távolságot modellezhet a csomópontok között.

Az N skálázható elosztott rendszer általános modellje a 3.3. ábrán látható.

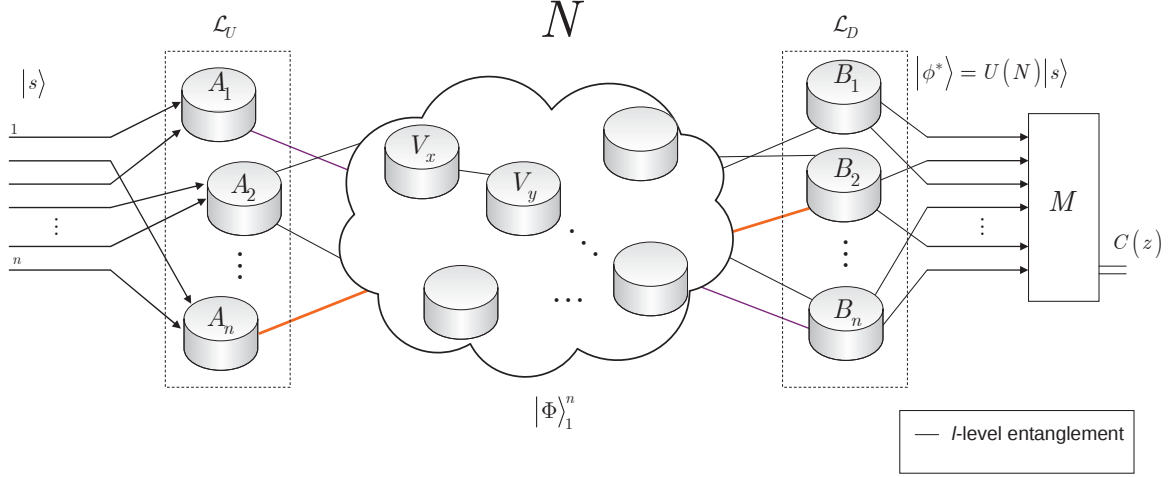
3.3.4. Eredmények

3.1. Tézis. *Egy tetszőleges N kvantumrendszer skálázható az összefonódott kapcsolatok összefonódási szintje, a kvantumcsomópontok lokális műveleteinek kapuparaméterei, valamint a csomópontokban végzett lokális mérések segítségével. Az N elosztott rendszer kapumodell kvantumszámításokat valósít meg skálázható, elosztott módon.*

Bizonyítás. A bizonyítás a disszertáció 5.3.1 alfejezetében található. ■

3.1. Propozíció. *Egy adott V_x csomópontban, a j lokális qubit összefonódott kapcsolatban áll a lokális k qubittel, $\langle jk \rangle$, valamint Γ_j nem-lokális qubittel, $n_1, \dots, n_{\Gamma_j}$. A nem-lokális qubitek nem szomszédosak k qubittel (Γ_j és k között nincs kapcsolat). Azon qubitek száma, amelyek kapcsolatban állnak j qubittel, de k -val nem, összesen $\Gamma_j + 1$.*

Bizonyítás. A bizonyítás a disszertáció 5.3.1 alfejezetében található. ■



3.3. ábra. Az N struktúra modellje skálázható elosztott kvantumszámítá-
sok végrehajtására. A $|s\rangle = |+\rangle_1 \dots |+\rangle_n$ bemeneti állapot n forráscso-
móponthoz kerül, $A_1, \dots, A_n$, majd köztes csomópontok láncolatán és l
szintű összefonódott kapcsolatokon keresztül eljut az n vevőcsomópontok-
hoz, $B_1, \dots, B_n$, ahol $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|s\rangle = \frac{1}{\sqrt{2^n}} \sum_z |z\rangle$, míg $|z\rangle$ egy
 n -qubit hosszúságú alapállapot. Az N elosztott rendszer célja egy beme-
neti probléma C célfüggvényének elosztott módon történő maximalizálása.
A rendszer elosztott módon megvalósítja az $U(N)$ műveletet, és előállítja a
 $|\phi^*\rangle = U(N)|s\rangle$ kimeneti állapotot. Az M elosztott mérésekre az n vevő-
csomópontban kerül sor, amelynek eredménye a z bitsorozat. A z bitsorozat
lehetővé teszi a csomópontok számára, hogy kiértékeljék a $C(z)$ célfüggvény
értéket. Az $|s\rangle$ bemeneti állapot az $\mathcal{L}_U(|s\rangle) = \mathcal{L}_U(|+\rangle_1 \dots |+\rangle_n)$ elosz-
tott feltöltési operátorral kerül feltöltésre a $|\Phi\rangle_1^n = U(N) \frac{1}{\sqrt{2}}((|00\rangle_1^{n2(L-1)} +$
 $(|11\rangle_1^{n2(L-1)}) = U(N) \frac{1}{\sqrt{2}}(|0\rangle_1^n (|0\rangle_{n+1}^{n2(L-1)} + |1\rangle_1^n (|1\rangle_{n+1}^{n2(L-1)})$ elosztott há-
lózati állapotba, ahol $|\Phi\rangle_i = U(\vec{\theta}_i) \frac{1}{\sqrt{2}}(|0\rangle_1 (|0\rangle_2^{2(L-1)} + |1\rangle_1 (|1\rangle_2^{2(L-1)})$,
ahol 1 a $\mathcal{P}(A_i \rightarrow B_i)$ számítási útvonal első állapotát azonosítja. Az
 $|\Phi\rangle_1^n$ hálózati állapot n számítási útvonalat tartalmaz, ahol az i -ik
útvonal $\mathcal{P}(A_i \rightarrow B_i)$, $i = 1, \dots, n$, az $U(\vec{\theta}_i) = U_{i,L} U_{i,L-1} \dots U_{i,1}$
műveletet valósítja meg, ahol $U_{i,1} = U(\beta_{i,1}, X_{i,1}) U(\gamma_{i,1}, Z_{i,1})$. Az
 $\mathcal{L}_U(|s\rangle) = \mathcal{L}_U(|+\rangle_1) \dots \mathcal{L}_U(|+\rangle_n)$ feltöltési művelet elosztottan kerül meg-
valósításra az n csomópont között, ahol $\mathcal{L}_U(|+\rangle_i)$ az A_i forráscsomó-
pont művelete, $\mathcal{L}_U(\alpha_i|0\rangle + \beta_i|1\rangle) = U(\vec{\theta}_i)(\alpha_i(|0\rangle_2^{2(L-1)} + \beta_i(|1\rangle_2^{2(L-1)}) =$
 $U(\vec{\theta}_i) \frac{1}{\sqrt{2}}((|0\rangle_2^{2(L-1)} + (|1\rangle_2^{2(L-1)})$. Az $\mathcal{L}_D$ letöltési folyamat eredménye a B_i
vevőcsomópontban $\mathcal{L}_D(U(\vec{\theta}_i) \frac{1}{\sqrt{2}}((|0\rangle_2^{2(L-1)} + (|1\rangle_2^{2(L-1)})) = U(\vec{\theta}_i)|+\rangle_i$. Az
 $\mathcal{L}_U$ és $\mathcal{L}_D$ műveletek a csomópontokban így az $\mathcal{L}_D(\mathcal{L}_U(|+\rangle_1 \dots |+\rangle_n)) =$
 $U(N)|s\rangle$ unitér műveletet valósítja meg elosztott módon.

3.2. Propozíció. Az A_i forráscsomópontban a $\mathcal{L}_U(|+\rangle_i)$ feltöltési folyamat megvalósítható az $\mathcal{M}_B$ Bell-méréssel, amely a $|+\rangle_i$ bemeneti állapotban, valamint $|\Phi\rangle_i$ első állapotán kerül végrehajtásra, ahol $|\Phi\rangle_i$ a $\mathcal{P}(A_i \rightarrow B_i)$ számítási útvonalhoz rendelt hálózati rendszerállapot.

Bizonyítás. A bizonyítás a disszertáció 5.3.1 alfejezetében található. ■

3.2. Tézis. Tetszőleges optimalizálási probléma C célfüggvénye maximalizálható N segítségével, skálázható elosztott módon, az $F = \sum_{\langle jk \rangle \in N} F_{\langle jk \rangle} = \max_{\forall \theta} \langle \phi^* | C | \phi^* \rangle$ függvény segítségével, ahol $\langle jk \rangle$ l -szintű, $l \geq 1$, összefonódottságot azonosít j és k qubitek között.

Bizonyítás. A bizonyítás a disszertáció 5.3.3 alfejezetében található. ■

3.1. Lemma. Az N hálózat $\mathcal{D}(N)$ elosztott számítási tere egy kiterjesztett korrelációs tér, n összefonódott $\mathcal{P}(A_i \rightarrow B_i)$, $i = 1, \dots, n$ számítási útvonallal.

Bizonyítás. A bizonyítás a disszertáció 5.3.4 alfejezetében található. ■

3.3. Tézis. A $\mathcal{P}(A \rightarrow B)$ számítási útvonalhoz tartozó $F_{\mathcal{P}(A \rightarrow B)}$ függvény, adott $C_{\mathcal{P}(A \rightarrow B)} = \sum_{\langle jk \rangle \in \mathcal{P}(A \rightarrow B)} C_{jk}$ célfüggvény mellett, maximalizálható a $\beta_j = \frac{\pi}{8}$ és $\gamma_{jk} = \frac{1}{2} \cos^{-1} \left(\frac{\Gamma_j - 1}{\Gamma_j + 1} \right)$ kapuparaméterekkel az L csomópontban, ahol Γ_j a j qubit nem-lokális kapcsolatainak száma.

Bizonyítás. A bizonyítás a disszertáció 5.3.5 alfejezetében található. ■

3.2. Lemma. Az $F_{\langle jk \rangle}$ függvény maximalizálásának $f_C(F_{\langle jk \rangle})$ költsége a lokális műveletek időparamétere alapján meghatározható. A költségfüggvény a Γ_j paraméterrel skálázható.

Bizonyítás. A bizonyítás a disszertáció 5.4 alfejezetében található. ■

3.3.5. Összefoglalás

A 3. téziscsoportban egy elosztott, skálázható kvantumszámítási protokollt definiáltam. Vizsgáltam a protokoll tulajdonságait, az elosztott problémamegoldás és skálázás jellemzőit, valamint a protokoll költségfüggvényét.

4. Összefoglalás

A disszertációban új kvantuminformatikai protokollokat definiáltam. A kvantumszámítások segítségével, a hagyományos számítógépeknél hatékonyabban oldhatóak meg számítási problémák, míg a kvantumkommunikáció megfelelő választ jelent azon számítási teljesítményre, amely a kvantumszámítógépek megjelenésével elérhetővé válik. A kvantumkommunikáció lehetővé teszi az abszolút biztonságos kommunikáció megvalósítását a jövő hálózataiban, valamint a kvantuminterneten belül. Amint a kvantumszámítógépek kereskedelmi használatra is elérhetővé válnak, a globális kvantumkommunikációs hálózat struktúrájának is készen kell állnia.

A kereskedelmi kvantumszámítógépek, valamint a kvantuminternet jelenleg még csupán fejlesztési fázisban állnak, a hatékony kvantuminformatikai protokollok tervezése azonban már napjainkban kiemelt jelentőségű feladat. A disszertáció ezt a célt szolgálja, újszerű és hatékony kvantuminformatikai protokollok definiálásán keresztül.

A jövőbeli kutatások feladatai közé tartozik a további, hatékony szolgáltatások és protokollok definiálása a kvantumszámítások, valamint a kvantumkommunikációs hálózatok részére. A kvantumszámításokat, valamint a kapumodell kvantumszámítógépeket illetően, kiemelt jelentőségű a hatékony kvantumalgoritmusok fejlesztése olyan kutatási területek számára, mint az orvostudomány, biológia, fizika, matematika, biokémia, gazdaságtudomány, mérnöki tudományok vagy kognitív tudományok. Kiemelten fontos kutatási terület a molekuláris kvantumszámítások és a kvantumbiológia, amelyek a kvantummechanikát biológiai rendszerekre alkalmazzák molekuláris szinten. Ami a kvantumkommunikációs hálózatokat illeti, fontos kutatási téma a kvantuminternet szabványainak megtervezése és kidolgozása. A hagyományos hálózatokhoz hasonlóan, a kvantuminternet protokolljainak szabványosítása segít egy egységes platform definiálásában, amely a globális kvantumkommunikációs hálózati struktúra létrehozásához szükséges. Ezen problémák megoldásának első ígéretes megközelítéseként, nemzetközi támogatással, valamint kutatói együttműködéssel megalakult a kvantuminternet-kutatócsoport (QIRG) [6] is.

5. Publikációs lista

Publikációk a PhD fokozat megszerzését követően (2013 szeptember).

5.1. Folyóiratcikk

- [1] Laszlo Gyongyosi: Adaptive Problem Solving Dynamics in Gate-Model Quantum Computers, *Entropy*, DOI: 10.3390/e24091196, 2022.
- [2] Laszlo Gyongyosi, Sandor Imre: Subchannel Estimation and Subcarrier Detection for Multiuser Multicarrier Continuous-Variable Quantum Key Distribution, *Quantum Eng*, 2022.
- [3] Laszlo Gyongyosi: Approximation Method for Optimization Problems in Gate-Model Quantum Computers, *Chaos, Solitons Fractals*, DOI: 10.1016/j.csfx.2021.100066, 2021.
- [4] Laszlo Gyongyosi, Sandor Imre: Advances in the Quantum Internet, *Communications of the ACM*, DOI: 10.1145/3524455, 2022.
- [5] Laszlo Gyongyosi: Post-Processing Optimization for Continuous-Variable Quantum Key Distribution, *Theor. Comput. Sci.*, DOI: 10.1016/j.tcs.2021.08.023, 2021.
- [6] Laszlo Gyongyosi, Sandor Imre: Scalable Distributed Gate-Model Quantum Computers, *Scientific Reports*, Nature, DOI: 10.1038/s41598-020-76728-5, 2021.
- [7] Laszlo Gyongyosi, Sandor Imre: Resource Prioritization and Balancing for the Quantum Internet, *Scientific Reports*, Nature, DOI: 10.1038/s41598-020-78960-5, 2020.
- [8] Laszlo Gyongyosi: Energy Transfer and Thermodynamics of Quantum Gravity Computation, *Chaos, Solitons and Fractals*, DOI: 10.1016/j.csfx.2020.100050, 2020.
- [9] Laszlo Gyongyosi: Dynamics of Entangled Networks of the Quantum Internet, *Scientific Reports*, Nature, DOI: 10.1038/s41598-020-68498-x, 2020.
- [10] Laszlo Gyongyosi: Decoherence Dynamics Estimation for Superconducting Gate-Model Quantum Computers, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-020-02863-7, 2020.
- [11] Laszlo Gyongyosi, Sandor Imre: Routing Space Exploration for Scalable Routing in the Quantum Internet, *Scientific Reports*, Nature, DOI: 10.1038/s41598-020-68354-y, 2020.
- [12] Laszlo Gyongyosi: Objective Function Estimation for Solving Optimization Problems in Gate-Model Quantum Computers, *Scientific Reports*, Nature, DOI: 10.1038/s41598-020-71007-9, 2020.
- [13] Laszlo Gyongyosi, Sandor Imre: Entanglement Concentration Service for the Quantum Internet, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-020-02716-3, 2020.

- [14] Laszlo Gyongyosi: Unsupervised Quantum Gate Control for Gate-Model Quantum Computers, *Scientific Reports*, Nature, DOI: 10.1038/s41598-020-67018-1, 2020.
- [15] Laszlo Gyongyosi, Sandor Imre: Circuit Depth Reduction for Gate-Model Quantum Computers, *Scientific Reports*, Nature, DOI: 10.1038/s41598-020-67014-5, 2020.
- [16] Laszlo Gyongyosi: Quantum State Optimization and Computational Pathway Evaluation for Gate-Model Quantum Computers, *Scientific Reports*, Nature, DOI: 10.1038/s41598-020-61316-4, 2020.
- [17] Laszlo Gyongyosi, Sandor Imre: Entanglement Accessibility Measures for the Quantum Internet, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-020-2605-y, 2020.
- [18] Laszlo Gyongyosi, Sandor Imre: Theory of Noise-Scaled Stability Bounds and Entanglement Rate Maximization in the Quantum Internet, *Scientific Reports*, Nature, DOI: 10.1038/s41598-020-58200-6, 2020.
- [19] Laszlo Gyongyosi: Correlation Measure Equivalence in Dynamic Causal Structures of Quantum Gravity, *Quantum Eng.*, Wiley, DOI: 10.1002/QUE2.30, 2019.
- [20] Laszlo Gyongyosi: Order Statistics and Random Matrix Theory of Multicarrier Continuous-Variable Quantum Key Distribution, *Int. J. Commun. Syst.*, Wiley, DOI:10.1002/dac.4314, 2019.
- [21] Laszlo Gyongyosi, Sandor Imre: Optimizing High-Efficiency Quantum Memory with Quantum Machine Learning for Near-Term Quantum Devices, *Scientific Reports*, Nature, DOI: 10.1038/s41598-019-56689-0, 2019.
- [22] Laszlo Gyongyosi: Multicarrier Continuous-Variable Quantum Key Distribution, *Theoretical Computer Science*, Elsevier, DOI: 10.1016/j.tcs.2019.11.026, 2019.
- [23] Laszlo Gyongyosi, Sandor Imre: Theory of Quantum Gravity Information Processing, *Quantum Eng.*, Wiley, DOI: 10.1002/que2.23, 2019.
- [24] Laszlo Gyongyosi, Sandor Imre: Subcarrier Domain of Multicarrier Continuous-Variable Quantum Key Distribution, *J. Stat. Phys.*, Springer Nature, DOI: 10.1007/s10955-019-02404-2, 2019.
- [25] Laszlo Gyongyosi, Sandor Imre: High-Retrieval Efficiency Quantum Memory for the Quantum Internet, *SPIE Photonics West OPTO 2020 Proceedings*, 2020.
- [26] Laszlo Gyongyosi, Sandor Imre: Training Optimization for Gate-Model Quantum Neural Networks, *Scientific Reports*, Nature, DOI: 10.1038/s41598-019-48892-w, 2019.

- [27] Laszlo Gyongyosi, Sandor Imre: Secret Key Rate Adaption for Multicarrier Continuous-Variable Quantum Key Distribution, *SN Comput. Sci.*, Springer Nature, DOI: 10.1007/s42979-019-0027-7, 2019.
- [28] Laszlo Gyongyosi, Sandor Imre: State Stabilization for Gate-Model Quantum Computers, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-019-2397-0, 2019.
- [29] Laszlo Gyongyosi, Sandor Imre: A Poisson Model for Entanglement Optimization in the Quantum Internet, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-019-2335-1, 2019.
- [30] Laszlo Gyongyosi, Sandor Imre: Statistical Quadrature Evolution by Inference for Multicarrier Continuous-Variable Quantum Key Distribution, *Quantum Studies: Mathematics and Foundations*, Springer Nature, DOI: 10.1007/s40509-019-00202-9, 2019.
- [31] Laszlo Gyongyosi: Singular Value Decomposition Assisted Multicarrier Continuous-Variable Quantum Key Distribution, *Theoretical Computer Science*, Elsevier, DOI: 10.1016/j.tcs.2019.07.029, 2019.
- [32] Laszlo Gyongyosi, Sandor Imre: Secret Key Rates of Free-Space Optical Continuous-Variable Quantum Key Distribution, *Int. J. Commun. Syst.* (Wiley), DOI: 10.1002/dac.4152, 2019.
- [33] Laszlo Gyongyosi, Laszlo Bacsardi, Sandor Imre: A Survey on Quantum Key Distribution, *Infocom. J.*, HTE, IEEE Communications Society, DOI: 10.36244/ICJ.2019.2.2, 2019.
- [34] Laszlo Gyongyosi, Sandor Imre: Quantum Circuit Design for Objective Function Maximization in Gate-Model Quantum Computers, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-019-2326-2, 2019.
- [35] Laszlo Gyongyosi, Sandor Imre: Dense Quantum Measurement Theory, *Scientific Reports*, Nature, DOI: 10.1038/s41598-019-43250-2, 2019.
- [36] Laszlo Gyongyosi, Sandor Imre: Diversity Space of Multicarrier Continuous-Variable Quantum Key Distribution, *Int. J. Commun. Syst.* (Wiley), DOI: 10.1002/dac.4003, 2019.
- [37] Laszlo Gyongyosi, Sandor Imre: Entanglement Access Control for the Quantum Internet, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-019-2226-5, 2019.
- [38] Laszlo Gyongyosi, Sandor Imre: Gaussian Quadrature Inference for Multicarrier Continuous-Variable Quantum Key Distribution, *Quantum Studies: Mathematics and Foundations*, Springer Nature, DOI: 10.1007/s40509-019-00183-9, 2019.

- [39] Laszlo Gyongyosi, Sandor Imre: Opportunistic Entanglement Distribution for the Quantum Internet, *Scientific Reports*, Nature, DOI: 10.1038/s41598-019-38495-w, 2019.
- [40] Laszlo Gyongyosi, Sandor Imre: Adaptive Routing for Quantum Memory Failures in the Quantum Internet, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-018-2153-x, 2018.
- [41] Laszlo Gyongyosi, Sandor Imre: Time Complexity Reduction for Gate-Model Quantum Computers, *SPIE Quantum Information Science, Sensing, and Computation Proceedings*, 2019.
- [42] Laszlo Gyongyosi, Sandor Imre: A Survey on Quantum Computing Technology, *Computer Science Review*, Elsevier, DOI: 10.1016/j.cosrev.2018.11.002, ISSN: 1574-0137, 2018.
- [43] Laszlo Gyongyosi, Sandor Imre: Secret Key Rate Proof of Multicarrier Continuous-Variable Quantum Key Distribution, *Int. J. Commun. Syst.* (Wiley), DOI: 10.1002/dac.3865, ISSN: 1099-1131, 2018.
- [44] Laszlo Gyongyosi, Sandor Imre: Reconciliation Optimization for Continuous-Variable Quantum Key Distribution, *SPIE Photonics West OPTO 2019 Proceedings*.
- [45] Laszlo Gyongyosi, Sandor Imre: Topology Adaption for the Quantum Internet, *Quantum Information Processing*, Springer Nature, DOI: 10.1038/s41598-018-30957-x, ISSN: 1570-0755, 1573-1332, 2018.
- [46] Laszlo Gyongyosi, Sandor Imre: Multilayer Optimization for the Quantum Internet, *Scientific Reports*, Nature, DOI:10.1038/s41598-018-30957-x, 2018.
- [47] Laszlo Gyongyosi, Sandor Imre: Decentralized Base-Graph Routing for the Quantum Internet, *Physical Review A*, American Physical Society, DOI: 10.1103/PhysRevA.98.022310, 2018.
- [48] Laszlo Gyongyosi, Sandor Imre: Entanglement Availability Differentiation Service for the Quantum Internet, *Scientific Reports*, Nature, DOI:10.1038/s41598-018-28801-3, 2018.
- [49] Laszlo Gyongyosi, Sandor Imre: Multiple Access Multicarrier Continuous-Variable Quantum Key Distribution, *Chaos, Solitons and Fractals*, Elsevier, DOI: 10.1016/j.chaos.2018.07.006, ISSN: 0960-0779, 2018.
- [50] Laszlo Gyongyosi, Sandor Imre, Hung Viet Nguyen: A Survey on Quantum Channel Capacities, *IEEE Communications Surveys and Tutorials*, IEEE, DOI: 10.1109/COMST.2017.2786748, 2018.

- [51] Laszlo Gyongyosi, Sandor Imre: Low-Dimensional Reconciliation for Continuous-Variable Quantum Key Distribution, *Appl. Sci.*, DOI: 10.3390/app8010087, ISSN 2076-3417, 2018.
- [52] Laszlo Gyongyosi, Sandor Imre: A Poisson Model for Entanglement Optimization in the Quantum Internet, *2018 SPIE Quantum Information Science, Sensing, and Computation Proceedings*, 2018.
- [53] Laszlo Gyongyosi, Sandor Imre: Dynamic Topology Resilience for Quantum Networks, *2018 SPIE Photonics West OPTO Proceedings*, 2018.
- [54] Laszlo Gyongyosi, Sandor Imre: Entanglement-Gradient Routing for Quantum Networks, *Scientific Reports*, Nature, DOI:10.1038/s41598-017-14394-w, 2017.
- [55] Laszlo Gyongyosi: Quantum Imaging of High-Dimensional Hilbert Spaces with Radon Transform, *International Journal of Circuit Theory and Applications (IJCTA), Special Issue on Quantum Circuits* (Wiley), 2017.
- [56] Laszlo Gyongyosi, with S. Imre, A. Mraz, Zs. Kis, L. Bacsardi: Quantum Circuit-based Modeling of Continuous-Variable Quantum Key Distribution System, *International Journal of Circuit Theory and Applications (IJCTA), Special Issue on Quantum Circuits* (Wiley), 2017.
- [57] Laszlo Gyongyosi, Sandor Imre: Statistical Quadrature Evolution by Inference for Continuous-Variable Quantum Key Distribution, *SPIE Photonics West OPTO 2017 Proceedings*, „Advances in Photonics of Quantum Computing, Memory, and Communication X”, 2016.
- [58] Laszlo Gyongyosi, Sandor Imre: Gaussian Quadrature Inference for Continuous-Variable Quantum Key Distribution, *Proceedings of SPIE Quantum Information and Computation IX*, 2016.
- [59] Laszlo Gyongyosi, Sandor Imre: Adaptive Gaussian Quadrature Detection for Continuous-Variable Quantum Key Distribution, *SPIE Photonics West OPTO 2016 Proceedings*, „Advances in Photonics of Quantum Computing, Memory, and Communication IX”, 2015.
- [60] Laszlo Gyongyosi, Sandor Imre: Multidimensional Manifold Extraction for Multi-carrier Continuous-Variable Quantum Key Distribution, *Proceedings of SPIE Quantum Information and Computation XIII*, 2015.
- [61] Laszlo Gyongyosi: A Statistical Model of Information Evaporation of Perfectly Reflecting Black Holes, *International Journal of Quantum Information (IJQI)*, DOI: 10.1142/S0219749915600254, 2014.

- [62] Laszlo Gyongyosi: The Private Classical Capacity of a Partially Degradable Quantum Channel, *Physica Scripta - Special Issue on Quantum Information*, Institute of Physics (IOP), Online ISSN: 1402-4896 Print ISSN: 0031-8949, 2014.
- [63] Laszlo Gyongyosi, Sandor Imre: Eigenchannel Decomposition for Continuous-Variable Quantum Key Distribution, *SPIE Photonics West OPTO 2015 Proceedings*, „Advances in Photonics of Quantum Computing, Memory, and Communication VIII”, 2015.
- [64] Laszlo Gyongyosi: The Structure and Quantum Capacity of a Partially Degradable Quantum Channel, *IEEE Access*, ISSN: 2169-3536, 2014.
- [65] Laszlo Gyongyosi, Sandor Imre: Geometrical Analysis of Physically Allowed Quantum Cloning Transformations for Quantum Cryptography, *Information Sciences*, ELSEVIER, ISSN: 0020-0255; (2014).
- [66] Laszlo Gyongyosi: Quantum Information Transmission over a Partially Degradable Channel, *IEEE Access*, ISSN: 2169-3536 (2014).
- [67] Laszlo Gyongyosi: The Correlation Conversion Property of Quantum Channels, *Quantum Information Processing*, ISSN: 1570-0755 (print version), ISSN: 1573-1332 (electronic version). 2013.
- [68] Laszlo Gyongyosi, Sandor Imre: Adaptive Multicarrier Quadrature Division Modulation for Continuous-Variable Quantum Key Distribution, *Proceedings of SPIE Quantum Information and Computation XII*, 2014.
- [69] Laszlo Gyongyosi, Sandor Imre: Long-distance Continuous-Variable Quantum Key Distribution with Advanced Reconciliation of a Gaussian Modulation, *Proceedings of SPIE Photonics West OPTO 2013*, „Advances in Photonics of Quantum Computing, Memory, and Communication VII”, 2014.

5.2. Konferenciák

- [1] Laszlo Gyongyosi, Sandor Imre: Opportunistic Entanglement Distribution for the Quantum Internet, *Proceedings of Quantum Computing, Communication, and Simulation III*, SPIE OPTO 2023, 28 Jan - 2 Feb 2023, San Francisco, California, USA.
- [2] Laszlo Gyongyosi, Sandor Imre: Scalable Distributed Gate-Model Quantum Computers, *Bulletin of the American Physical Society*, APS March Meeting 2022, Session on Scalable Quantum Computing Architectures, March 14–18, 2022, Chicago, USA.
- [3] Laszlo Gyongyosi, Sandor Imre: Problem Solving Dynamics for Gate-Model Quantum Computers, *Proceedings of SPIE Quantum Information Science, Sensing, and Computation XIV*, 3 - 7 April 2022, Orlando, Florida, USA.

- [4] Laszlo Gyongyosi, Sandor Imre: Resource Optimization for the Quantum Internet, *Proceedings of Quantum Computing, Communication, and Simulation II*, SPIE OPTO 2022, 22 - 27 Jan 2022, San Francisco, California, USA.
- [5] Laszlo Gyongyosi, Sandor Imre: Distributed Quantum Computation for Near-Term Quantum Environments, *Proceedings of SPIE Quantum Information Science, Sensing, and Computation XIII*, 11 - 15 April 2021, Orlando, Florida, USA.
- [6] Laszlo Gyongyosi, Sandor Imre: Entangled Network Dynamics of the Quantum Internet, *Proceedings of Advanced Optical Techniques for Quantum Information, Sensing, and Metrology*, SPIE OPTO 2021, 6 - 11 March 2021, San Francisco, California, USA.
- [7] Laszlo Gyongyosi, Sandor Imre: Scalable Distributed Gate-Model Quantum Computers, *Proceedings of the Frontiers in Optics 2020 (FiO 2020)*, Optical Society of America (OSA), 14-17 Sept. 2020, Washington, D.C., USA.
- [8] Laszlo Gyongyosi, Sandor Imre: Quantifying the Dynamics of Entangled Networks of the Quantum Internet, *Proceedings of the Frontiers in Optics 2020 (FiO 2020)*, Optical Society of America (OSA), 14-17 Sept. 2020, Washington, D.C., USA.
- [9] Laszlo Gyongyosi, Sandor Imre: Quantum Memory Optimization with Quantum Machine Learning for Quantum Secure Direct Communication, *Proceedings of the 10th International Conference on Quantum Cryptography (QCrypt 2020)*, 10-14 Aug 2020, Amsterdam, Netherlands.
- [10] Laszlo Gyongyosi, Sandor Imre: Training Optimization for Gate-Model Quantum Neural Networks, *Bulletin of the American Physical Society*, APS DAMOP 2020, 51st Annual Meeting of the APS Division of Atomic, Molecular and Optical Physics, Session on Quantum Computation: Gates, Algorithms, and Architectures, June 1–5, 2020; Portland, Oregon, USA.
- [11] Laszlo Gyongyosi, Sandor Imre: Objective Function Maximization by Machine Learning for Gate-Model Quantum Computers, *Proceedings of Quantum Information Science, Sensing, and Computation XII*, SPIE Defense, 26 - 30 April 2020, Anaheim, California, USA.
- [12] Laszlo Gyongyosi, Sandor Imre: Time Complexity Reduction for Gate-Model Quantum Computers, *Bulletin of the American Physical Society*, APS March Meeting 2020, Session on General Quantum Algorithms, March 2 - 6, 2020, Denver, Colorado, USA.
- [13] Laszlo Gyongyosi, Sandor Imre: High-Retrieval Efficiency Quantum Memory for the Quantum Internet, *Proceedings of Advanced Optical Techniques for Quantum Information, Sensing, and Metrology*, SPIE OPTO 2020, 1 - 6 February 2020, San Francisco, California, USA.

- [14] Laszlo Gyongyosi, Sandor Imre: Training Optimization for Gate-Model Quantum Neural Networks, *Proceedings of Quantum Information Processing 2020 (QIP 2020)*, January 06-10, 2020, Shenzhen, China.
- [15] Laszlo Gyongyosi, Sandor Imre: Dense Quantum Measurement Theory, *Proceedings of Quantum Information Processing 2020 (QIP 2020)*, January 06-10, 2020, Shenzhen, China.
- [16] Laszlo Gyongyosi, Sandor Imre: Resource Prioritization and Resource Balancing for the Quantum Internet, *Proceedings of the Frontiers in Optics 2019 (FiO 2019)*, Optical Society of America (OSA), 15-19 Sept. 2019, Washington, D.C., USA.
- [17] Laszlo Gyongyosi, Sandor Imre: Measurement Optimization for Gate-Model Quantum Computers, *Proceedings of the Frontiers in Optics 2019 (FiO 2019)*, Optical Society of America (OSA), 15-19 Sept. 2019, Washington, D.C., USA.
- [18] Laszlo Gyongyosi, Sandor Imre: Secret Key Reconciliation for Long-Distance Quantum Key Distribution with Discrete and Continuous Variables, *Proceedings of the 9th International Conference on Quantum Cryptography (QCrypt 2019)*, 26-30 Aug. 2019, Montreal, Canada.
- [19] Laszlo Gyongyosi, Sandor Imre: Optimization of Objective Function Estimation for Gate-Model Quantum Computers, *Bulletin of the American Physical Society*, APS DAMOP 2019, 50th Annual Meeting of the APS Division of Atomic, Molecular and Optical Physics, Session on Quantum simulation and algorithms, May 27–31, 2019; Milwaukee, Wisconsin, USA.
- [20] Laszlo Gyongyosi, Sandor Imre: Dense Measurements for Gate-Model Quantum Computers, *Bulletin of the American Physical Society*, APS March Meeting 2019, Session on General Quantum Information and Quantum Computation, March 4–8, 2019; Boston, Massachusetts, USA.
- [21] Laszlo Gyongyosi, Sandor Imre: Time Complexity Reduction for Gate-Model Quantum Computers, *Proceedings of SPIE Quantum Information Science, Sensing, and Computation XI*, 14 - 18 April 2019, Baltimore, Maryland, USA.
- [22] Laszlo Gyongyosi, Sandor Imre: Dense Measurements for Quantum Computations, *Proceedings of Quantum Information and Measurement (QIM) V: Quantum Technologies*, OSA (The Optical Society of America), 04 April 2019 – 06 April 2019, University of Rome La Sapienza, Rome, Italy.
- [23] Laszlo Gyongyosi, Sandor Imre: A Universal Quantum Algorithm for Time Complexity Reduction of Quantum Computers, *Proceedings of Quantum Information Processing 2019 (QIP 2019)*, January 14-18, 2019, University of Colorado Boulder, USA.

- [24] Laszlo Gyongyosi, Sandor Imre: Improved Reconciliation for Continuous-Variable Quantum Key Distribution, *Proceedings of Advances in Photonics of Quantum Computing, Memory, and Communication XII*, SPIE OPTO 2019, 2 - 7 February 2019, San Francisco, California, USA.
- [25] Laszlo Gyongyosi, Sandor Imre: Problem Solving Optimization by Machine Learning for Gate-Model Quantum Computers, *Proceedings of Quantum Techniques in Machine Learning (QTML2018)*, 12-16 Nov. 2018, Durban, South Africa.
- [26] Laszlo Gyongyosi, Sandor Imre: Unsupervised Machine Learning Control of Quantum Gates in Gate-Model Quantum Computers, *Proceedings of the Frontiers in Optics 2018 (FiO 2018)*, Optical Society of America (OSA), 16-20 Sept. 2018, Washington, D.C., USA.
- [27] Laszlo Gyongyosi, Sandor Imre: Entanglement Concentration Service for the Quantum Internet, *Proceedings of the Frontiers in Optics 2018 (FiO 2018)*, Optical Society of America (OSA), 16-20 Sept. 2018, Washington, D.C., USA.
- [28] Laszlo Gyongyosi, Sandor Imre: Post-Processing Optimization for Continuous-Variable Quantum Key Distribution, *Proceedings of QCrypt 2018, 8th International Conference on Quantum Cryptography*, 27–31 August 2018, Shanghai, China.
- [29] Laszlo Gyongyosi, Sandor Imre: Layout Generation with Decoherence Estimation for Gate-Model Quantum Computer Architectures, *Bulletin of the American Physical Society*, APS DAMOP, 49th Annual Meeting of the APS Division of Atomic, Molecular and Optical Physics APS Meeting, Session on Quantum Information Science, May 28–June 1 2018; Ft. Lauderdale, Florida, USA.
- [30] Laszlo Gyongyosi: Quantum Circuit Design Automation for Quantum Computers, *Proceedings of the 2018 International Conference on Quantum Communication, Measurement and Computing (QCMC 2018)*, March 12-16, 2018, Louisiana State University, Baton Rouge, USA.
- [31] Laszlo Gyongyosi, Sandor Imre: A Poisson Model for Entanglement Optimization in the Quantum Internet, *Proceedings of SPIE Quantum Information Science, Sensing, and Computation X*, 15 - 19 April 2018, Orlando, Florida, USA.
- [32] Laszlo Gyongyosi, Sandor Imre: Quantum Circuit Designs for Gate Model Quantum Computers, *Bulletin of the American Physical Society*, APS March Meeting 2018, APS Division of Quantum Information (DQI) Session, March 5–9, 2018; Los Angeles, California, USA.
- [33] Laszlo Gyongyosi, Sandor Imre: Dynamic Topology Resilience for Quantum Networks, *Advances in Photonics of Quantum Computing, Memory, and Communication XI*, SPIE OPTO 2018, 27 January - 1 February 2018, San Francisco, California, USA.

- [34] Laszlo Gyongyosi: Entanglement Distribution and Routing in Quantum Communication Networks, *Quantum Summit 2017*, 11-17 Oct 2017, Chengdu, China.
- [35] Laszlo Gyongyosi: Efficient Decentralized Routing in Quantum Networks, *QCrypt 2017, 7th International Conference on Quantum Cryptography*, 18-22 Sept 2017, University of Cambridge, Cambridge, United Kingdom.
- [36] Laszlo Gyongyosi: Multicarrier Continuous-Variable Quantum Key Distribution, *QCrypt 2017, 7th International Conference on Quantum Cryptography*, 18-22 Sept 2017, University of Cambridge, Cambridge, United Kingdom.
- [37] Laszlo Gyongyosi, Sandor Imre: Hamiltonian Dynamics for Entanglement Distribution in Quantum Networks, *SPIE Quantum Communications and Quantum Imaging XV*, 6 - 10 August 2017, San Diego, California, USA.
- [38] Laszlo Gyongyosi, Sandor Imre: Decentralized Routing and Diameter Bounds in Entangled Quantum Networks, *APS DAMOP 2017*, 48th Annual Meeting of the APS Division of Atomic, Molecular and Optical Physics, Session on Quantum Networks and Photon Sources, Bulletin of the American Physical Society, The American Physical Society, June 5–9, 2017; Sacramento, California, USA.
- [39] Laszlo Gyongyosi, Sandor Imre: Fast Entanglement Establishment via Local Dynamics for Quantum Repeater Networks, *APS March Meeting 2017*, Session on Entanglement in Open Quantum Systems, Bulletin of the American Physical Society, The American Physical Society, March 13–17, 2017; New Orleans, Louisiana, USA.
- [40] Laszlo Gyongyosi, Sandor Imre: Statistical Quadrature Evolution by Inference for Continuous-Variable Quantum Key Distribution, *SPIE Photonics West OPTO 2017*, „Advances in Photonics of Quantum Computing, Memory, and Communication X”, 28 Jan - 2 Feb 2017, San Francisco, California, USA.
- [41] Laszlo Gyongyosi, Sandor Imre: Statistical Quadrature Evolution for Continuous-Variable Quantum Key Distribution, *APS DAMOP 2016, 47th Annual Meeting of the APS Division of Atomic, Molecular, and Optical Physics*, Section on Quantum Information Theory, Bulletin of the American Physical Society, The American Physical Society, Volume 61, Number 7, May 23–27, 2016; Providence, Rhode Island, USA.
- [42] Laszlo Gyongyosi: Diversity Extraction for Multicarrier Continuous-Variable Quantum Key Distribution, *IEEE Signal Processing Conference Proceedings*, 2016 24th European Signal Processing Conference (EUSIPCO 2016), Section on Quantum Communications, Budapest, 29 Aug - 2 Sept, 2016.
- [43] Laszlo Gyongyosi, with Albert Mraz, Sandor Imre: Performance Evaluation of Scalar Reconciliation for Continuous-Variable Quantum Key Distribution, *IEEE Signal*

Processing Conference Proceedings, 2016 24th European Signal Processing Conference (EUSIPCO 2016), Section on Quantum Communications, Budapest, 29 Aug - 2 Sept, 2016.

- [44] Laszlo Gyongyosi, Sandor Imre: Gaussian Quadrature Inference for Continuous-Variable Quantum Key Distribution, *SPIE Quantum Information and Computation IX*, 17 - 21 Apr 2016, Baltimore, Maryland, USA, 2016.
- [45] Laszlo Gyongyosi, Sandor Imre: Adaptive Gaussian Quadrature Detection for Continuous-Variable Quantum Key Distribution, *SPIE Photonics West OPTO 2016*, „*Advances in Photonics of Quantum Computing, Memory, and Communication IX*”, 13-18 Feb 2016, San Francisco, California, USA.
- [46] Laszlo Gyongyosi: Entropy Transfer of Quantum Gravity Information Processing, *APS DAMOP 2015*, *46th Annual Meeting of the APS Division of Atomic, Molecular, and Optical Physics*, Bulletin of the American Physical Society, The American Physical Society, Volume 60, Number 7, June 8–12, 2015; Columbus, Ohio, USA.
- [47] Laszlo Gyongyosi, Sandor Imre: Multidimensional Manifold Extraction for Multicarrier Continuous-Variable Quantum Key Distribution, *SPIE Quantum Information and Computation XIII*, 20 - 24 Apr 2015, Baltimore, Maryland, USA, 2015.
- [48] Laszlo Gyongyosi, Sandor Imre: Adaptive Quadrature Detection for Multicarrier Continuous-Variable Quantum Key Distribution, *APS March Meeting 2015*, Session on Quantum Foundations and Technologies, Bulletin of the American Physical Society, March 2–6, 2015; San Antonio, Texas, USA.
- [49] Laszlo Gyongyosi, Sandor Imre: Eigenchannel Decomposition for Continuous-Variable Quantum Key Distribution, *SPIE Photonics West OPTO 2015*, „*Advances in Photonics of Quantum Computing, Memory, and Communication VIII*”, 7-12 Feb 2015, San Francisco, California, USA.
- [50] Laszlo Gyongyosi, Singular Layer Transmission for Continuous-Variable Quantum Key Distribution, *2014 IEEE Photonics Conference*, 12 - 16 October 2014, San Diego, California USA.
- [51] Laszlo Gyongyosi, Sandor Imre: Quantum Imaging of High-Dimensional Hilbert Spaces with Radon Transform, *2014 Frontiers in Optics/Laser Science XXX (FiO/LS)*, 19-23 October 2014, Tucson, Arizona, USA.
- [52] Laszlo Gyongyosi, Sandor Imre: Information Processing with Quantum Gravity, *Photon14 Conference*, Quantum Electronics and Photonics 2014, Section on Quantum Information, Institute of Physics (IOP), Imperial College London, London, UK.

- [53] Laszlo Gyongyosi: Information Processing Structure of Quantum Gravity, *Gordon Research Conference on Quantum Science: Simulation, Verification, and Control of Complex Quantum Many-Body Systems*, July 27 - August 1, Stonehill College, Easton, MA, USA, 2014.
- [54] Laszlo Gyongyosi: Multiuser Quadrature Allocation for Continuous-Variable Quantum Key Distribution, *Quantum Theory from Problems to Advances (QTPA)*, International Centre for Mathematical Modeling in physics, engineering and cognitive sciences (ICMM), June 9-12, 2014, Linnaeus University, Växjö, Sweden.
- [55] Laszlo Gyongyosi: Quantum Imaging of High-Dimensional Hilbert Spaces with Radon Transform, *Quantum Theory from Problems to Advances (QTPA)*, International Centre for Mathematical Modeling in physics, engineering and cognitive sciences (ICMM), June 9-12, 2014, Linnaeus University, Växjö, Sweden.
- [56] Laszlo Gyongyosi, Sandor Imre: Information Processing with Quantum Gravity Environment, *Quantum Theory from Problems to Advances (QTPA)*, International Centre for Mathematical Modeling in physics, engineering and cognitive sciences (ICMM), June 9-12, 2014, Linnaeus University, Växjö, Sweden.
- [57] Laszlo Gyongyosi, Sandor Imre: Information Processing Structure of Quantum Gravity, *APS DAMOP 2014*, 45th Annual Meeting of the APS Division of Atomic, Molecular and Optical Physics, *Session on Quantum Information Theory*, The American Physical Society, Volume 59, Number 8, June 2–6, 2014; Madison, Wisconsin, USA.
- [58] Laszlo Gyongyosi, Sandor Imre: Adaptive Multicarrier Quadrature Division Modulation for Continuous-Variable Quantum Key Distribution, *SPIE Quantum Information and Computation XII*, 8 - 9 May 2014, Baltimore, Maryland, USA, 2014.
- [59] Laszlo Gyongyosi, Sandor Imre: Long-Distance Continuous-Variable Quantum Key Distribution with Scalar Reconciliation and Gaussian Adaptive Multicarrier Quadrature Division, *APS March Meeting 2014*, Session on Quantum Communication, Decoherence, and Cryptography, Bulletin of the American Physical Society, Volume 59, Number 1, March 3–7, 2014; Denver, Colorado, USA.
- [60] Laszlo Gyongyosi, Sandor Imre: Long-distance two-way continuous variable quantum key distribution over optical fiber with Gaussian modulation, *SPIE Photonics West OPTO 2014*, „*Advances in Photonics of Quantum Computing, Memory, and Communication VII*”, Session: Quantum Communication and Quantum Computing with Photons II, 1-6 Feb 2014, San Francisco, California, USA.
- [61] Laszlo Gyongyosi: Long-Distance Two-way Continuous-Variable Quantum Key Distribution with a Gaussian Modulation, *Single Photon Workshop 2013 (SPW 2013)*, Oak Ridge National Laboratory, Quantum Information Science Group, Oct. 15-18, 2013, Oak Ridge, USA.

- [62] Laszlo Gyongyosi: Improved Long-Distance Two-way Continuous Variable Quantum Key Distribution over Optical Fiber, Session on Quantum Communications, *2013 Frontiers in Optics/Laser Science XXIX (FiO/LS)*, 6-10 October 2013, Orlando, Florida, USA. OSA JEAN BENNETT MEMORIAL AWARD 2013, THE OPTICAL SOCIETY OF AMERICA, ORLANDO, FLORIDA, USA, 2013.
- [63] Laszlo Gyongyosi, Sandor Imre: Entanglement Sharing without Entanglement Transmission, Session on Quantum Communications, *2013 Frontiers in Optics/Laser Science XXIX (FiO/LS)*, 6-10 October 2013, Orlando, Florida, USA.
- [64] Laszlo Gyongyosi, Sandor Imre: Quantum Communication over Partially Degradable Quantum Channels, Session on Optics and Photonics of Disordered Systems, *2013 Frontiers in Optics/Laser Science XXIX (FiO/LS)*, 6-10 October 2013, Orlando, Florida, USA.
- [65] Laszlo Gyongyosi, Sandor Imre: Long-Distance Two-way Continuous Variable Quantum Key Distribution over Optical Fiber with Gaussian Modulation, *IONS-NA 7, 7th North American IONS conference*, 2-4 Oct 2013, Center for Optoelectronics and Optical Communications, The University of North Carolina at Charlotte (UNCC), USA.

Irodalomjegyzék

- [1] Pirandola, S. et al. Advances in Quantum Cryptography, *Advances in Optics and Photonics* DOI: 10.1364/AOP.361502 (2020).
- [2] Gyongyosi, L., Bacsardi, L. and Imre, S. A Survey on Quantum Key Distribution, *Infocom. J* XI, 2, pp. 14-21, DOI: 10.36244/ICJ.2019.2.2 (2019).
- [3] Gyongyosi, L., Imre, S. and Nguyen, H. V. A Survey on Quantum Channel Capacities, *IEEE Commun. Surv. Tutor.*, vol. 20, no. 2, pp. 1149—1205, DOI: 10.1109/COMST.2017.2786748 (2018).
- [4] Gyongyosi, L. and Imre, S. Advances in the Quantum Internet, *Communications of the ACM*, DOI: 10.1145/3524455 (2022).
- [5] Pirandola, S. and Braunstein, S. L. Unite to build a quantum internet. *Nature* 532, 169–171 (2016).
- [6] Quantum Internet Research Group (QIRG), web: <https://datatracker.ietf.org/rg/qirg/about/> (2018).
- [7] Lloyd, S., Shapiro, J. H., Wong, F. N. C., Kumar, P., Shahriar, S. M. and Yuen, H. P. Infrastructure for the quantum Internet. *ACM SIGCOMM Computer Communication Review*, 34, 9–20 (2004).
- [8] Kimble, H. J. The quantum internet. *Nature*, 453:1023–1030 (2008).

- [9] Gyongyosi, L. and Imre, S. A Survey on Quantum Computing Technology, *Comput Sci Rev*, DOI: 10.1016/j.cosrev.2018.11.002 (2019).
- [10] Preskill, J. Quantum Computing in the NISQ era and beyond, *Quantum* 2, 79 (2018).
- [11] Arute, F. et al. Quantum supremacy using a programmable superconducting processor, *Nature*, Vol 574, DOI:10.1038/s41586-019-1666-5 (2019).
- [12] Harrow, A. W. and Montanaro, A. Quantum Computational Supremacy, *Nature*, vol 549, pages 203-209 (2017).
- [13] Farhi, E., Goldstone, J., Gutmann, S. and Neven, H. Quantum Algorithms for Fixed Qubit Architectures. *arXiv:1703.06199v1* (2017).
- [14] Farhi, E. and Neven, H. Classification with Quantum Neural Networks on Near Term Processors, *arXiv:1802.06002v1* (2018).
- [15] Alexeev, Y. et al. Quantum Computer Systems for Scientific Discovery, *arXiv:1912.07577* (2019).
- [16] Loncar, M. et al. Development of Quantum InterConnects for Next-Generation Information Technologies, *arXiv:1912.06642* (2019).
- [17] Foxen, B. et al. Demonstrating a Continuous Set of Two-qubit Gates for Near-term Quantum Algorithms, *Phys. Rev. Lett.* 125, 120504 (2020).
- [18] Ajagekar, A., Humble, T. and You, F. Quantum Computing based Hybrid Solution Strategies for Large-scale Discrete-Continuous Optimization Problems. *Computers and Chemical Engineering* Vol 132, 106630 (2020).
- [19] Ajagekar, A. and You, F. Quantum computing for energy systems optimization: Challenges and opportunities, *Energy*, Volume 179, Pages 76-89 (2019).
- [20] Harrigan, M. et al. Quantum Approximate Optimization of Non-Planar Graph Problems on a Planar Superconducting Processor, *arXiv:2004.04197v1* (2020).
- [21] Rubin, N. et al. Hartree-Fock on a superconducting qubit quantum computer, *Science* 369 (6507), 1084-1089 (2020).
- [22] Farhi, E., Goldstone and J., Gutmann, S. A Quantum Approximate Optimization Algorithm, *arXiv:1411.4028v1* (2014).
- [23] Farhi, E., Goldstone, J., Gutmann, S. and Zhou, L. The Quantum Approximate Optimization Algorithm and the Sherrington-Kirkpatrick Model at Infinite Size, *arXiv:1910.08187* (2019).
- [24] Sax, I. et al. Approximate Approximation on a Quantum Annealer, *Proceedings of the 17th ACM International Conference on Computing Frontiers (CF 2020)* (2020).

- [25] Brown, K. A. and Roser, T. Towards storage rings as quantum computers, *Phys. Rev. Accel. Beams* 23, 054701 (2020).
- [26] Gyongyosi, L. Quantum State Optimization and Computational Pathway Evaluation for Gate-Model Quantum Computers, *Scientific Reports*, DOI: 10.1038/s41598-020-61316-4 (2020).
- [27] Gyongyosi, L. Unsupervised Quantum Gate Control for Gate-Model Quantum Computers, *Scientific Reports*, DOI: 10.1038/s41598-020-67018-1 (2020).
- [28] Gyongyosi, L. and Imre, S. Circuit Depth Reduction for Gate-Model Quantum Computers, *Scientific Reports*, DOI: 10.1038/s41598-020-67014-5 (2020).
- [29] Gyongyosi, L. Objective Function Estimation for Solving Optimization Problems in Gate-Model Quantum Computers, *Scientific Reports*, DOI: 10.1038/s41598-020-71007-9 (2020).
- [30] Gyongyosi, L. Decoherence Dynamics Estimation for Superconducting Gate-Model Quantum Computers, *Quantum Inf Process* 19, 369, DOI: 10.1007/s11128-020-02863-7 (2020).
- [31] Teplukhin, A., Kendrick, B. and Babikov, D. Solving complex eigenvalue problems on a quantum annealer with applications to quantum scattering resonances, *Phys. Chem. Chem. Phys.*, DOI: 10.1039/D0CP04272B (2020).
- [32] Gill, S. S. et al. Quantum Computing: A Taxonomy, Systematic Review and Future Directions, *ACM Comput Surv*, submitted (2020).
- [33] Xin, T. Improved Quantum State Tomography for Superconducting Quantum Computing Systems, *arXiv:2006.15872v1* (2020).
- [34] Farhi, E., Kimmel, S. and Temme, K. A Quantum Version of Schoning's Algorithm Applied to Quantum 2-tsat, *arXiv:1603.06985* (2016).
- [35] Farhi, E., Gamarnik, D. and Gutmann, S. The Quantum Approximate Optimization Algorithm Needs to See the Whole Graph: A Typical Case, *arXiv:2004.09002v1* (2020).
- [36] Arute, F. et al. Observation of separated dynamics of charge and spin in the Fermi-Hubbard model, *arXiv:2010.07965* (2020).
- [37] Farhi, E., Gamarnik, D. and Gutmann, S. The Quantum Approximate Optimization Algorithm Needs to See the Whole Graph: Worst Case Examples, *arXiv:arXiv:2005.08747* (2020).
- [38] Lloyd, S. Quantum approximate optimization is computationally universal, *arXiv:1812.11075* (2018).

- [39] Reiher, M., Wiebe, N., Svore, K. M., Wecker, D., Troyer, M. Elucidating reaction mechanisms on quantum computers. *Proc Natl Acad Sci* 114:7555-7560, DOI: 10.1073/pnas.1619152114 (2017).
- [40] Mandra, S., Katzgraber, H. G. A deceptive step towards quantum speedup detection. *Quantum Sci Technol*, 3:04LT (2018).
- [41] Moret-Bonillo, V. Can artificial intelligence benefit from quantum computing? *Prog Artif Intell*, 3:89-105, DOI: 10.1007/s13748-014-0059-0 (2015).
- [42] Ronnow, T. F, Wang, Z., Job, J., Boixo, S., Isakov, S. V., Wecker, D., Martins, J. M., Lidar, D. A. and Troyer, M. Defining and detecting quantum speedup. *Science*, 345:420-424, DOI: 10.1126/science.1252319 (2014).
- [43] Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science* 124-134 (1994).
- [44] Vandersypen, L. M. K. et al. Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance, *Nature* 414, 883-887 (2001).
- [45] D-Wave, URL: <https://www.dwavesys.com/> (2010).
- [46] Quantum Computing Google Research, URL: <https://research.google/research-areas/quantum-computing/> (2013).
- [47] Denchev, V. S., Boixo, S., Isakov, S. V., Ding, N., Babbush, R., Smelyanskiy, V., Martinis, J. and Neven, H. What is the computational value of finite-range tunneling? *Phys Rev X* 6, 1-17, DOI: 10.1103/PhysRevX.6.031015 (2016).
- [48] O’Malley, P. J. J. et al. Scalable Quantum Simulation of Molecular Energies, *Phys Rev X*, 6, 031007 (2016).
- [49] Aaronson, S. and Chen, L. Complexity-theoretic foundations of quantum supremacy experiments. *Proceedings of the 32nd Computational Complexity Conference, CCC ’17*, pages 22:1-22:67 (2017).
- [50] IBM. A new way of thinking: The IBM quantum experience. URL: <http://www.research.ibm.com/quantum>. (2016).
- [51] Gambetta, J. IBM Quantum Roadmap. URL :<https://research.ibm.com/blog/ibm-quantum-roadmap> (2020).
- [52] Gonzalez, C. Cloud based QC with Amazon Braket, *Digitale Welt*, vol. 5, no. 2, pp. 14–17 (2021).
- [53] Wehner, S., Elkouss, D., and R. Hanson. Quantum internet: A vision for the road ahead, *Science* 362, 6412 (2018).

- [54] Pirandola, S., Laurenza, R., Ottaviani, C. and Banchi, L. Fundamental limits of repeaterless quantum communications, *Nature Communications*, 15043, doi:10.1038/ncomms15043 (2017).
- [55] Pirandola, S., Braunstein, S. L., Laurenza, R., Ottaviani, C., Cope, T.P. W., Spedalieri, G. and Banchi, L. Theory of channel simulation and bounds for private communication, *Quantum Sci. Technol.* 3, 035009 (2018).
- [56] Pirandola, S. Bounds for multi-end communication over quantum networks, *Quantum Sci. Technol.* 4, 045006 (2019).
- [57] Laurenza, R. and Pirandola, S. General bounds for sender-receiver capacities in multipoint quantum communications, *Phys. Rev. A* 96, 032318 (2017).
- [58] Van Meter, R. *Quantum Networking*, John Wiley and Sons Ltd, ISBN 1118648927, 9781118648926 (2014).
- [59] Gyongyosi, L. and Imre, S. Decentralized Base-Graph Routing for the Quantum Internet, *Physical Review A*, DOI: 10.1103/PhysRevA.98.022310, <https://link.aps.org/doi/10.1103/PhysRevA.98.022310> (2018).
- [60] Gyongyosi, L. and Imre, S. Optimizing High-Efficiency Quantum Memory with Quantum Machine Learning for Near-Term Quantum Devices, *Scientific Reports*, Nature, DOI: 10.1038/s41598-019-56689-0 (2019).
- [61] Gyongyosi, L. and Imre, S. Theory of Noise-Scaled Stability Bounds and Entanglement Rate Maximization in the Quantum Internet, *Scientific Reports*, Nature, DOI: 10.1038/s41598-020-58200-6 (2020).
- [62] Van Meter, R., Ladd, T. D., Munro, W. J. and Nemoto, K. System Design for a Long-Line Quantum Repeater, *IEEE/ACM Transactions on Networking* 17(3), 1002-1013 (2009).
- [63] Van Meter, R., Satoh, T., Ladd, T. D., Munro, W. J. and Nemoto, K. Path selection for quantum repeater networks, *Networking Science*, Volume 3, Issue 1–4, pp 82–95 (2013).
- [64] Van Meter, R. and Devitt, S. J. Local and Distributed Quantum Computation, *IEEE Computer* 49(9), 31-42 (2016).
- [65] Gyongyosi, L. and Imre, S. Dynamic topology resilience for quantum networks, *Proc. SPIE 10547*, Advances in Photonics of Quantum Computing, Memory, and Communication XI, 105470Z; doi: 10.1117/12.2288707 (2018).
- [66] Gyongyosi, L. and Imre, S. Topology Adaption for the Quantum Internet, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-018-2064-x (2018).

- [67] Gyongyosi, L. and Imre, S. Entanglement Access Control for the Quantum Internet, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-019-2226-5 (2019).
- [68] Gyongyosi, L. and Imre, S. Opportunistic Entanglement Distribution for the Quantum Internet, *Scientific Reports*, Nature, DOI:10.1038/s41598-019-38495-w (2019).
- [69] Gyongyosi, L. and Imre, S. Adaptive Routing for Quantum Memory Failures in the Quantum Internet, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-018-2153-x (2018).
- [70] Gyongyosi, L. and Imre, S. Entanglement-Gradient Routing for Quantum Networks, *Scientific Reports*, DOI:10.1038/s41598-017-14394-w, <https://www.nature.com/articles/s41598-017-14394-w> (2017).
- [71] Rozpedek, F., Schiet, T., Thinh, L., Elkouss, D., Doherty, A., and S. Wehner, Optimizing practical entanglement distillation, *Phys. Rev. A* 97, 062333 (2018).
- [72] Humphreys, P. et al., Deterministic delivery of remote entanglement on a quantum network, *Nature* 558 (2018).
- [73] Liao, SK. et al. Satellite-to-ground quantum key distribution, *Nature* 549, pages 43-47 (2017).
- [74] Ren, J.-G. et al. Ground-to-satellite quantum teleportation, *Nature* 549, pages 70–73 (2017).
- [75] Hensen, B. et al., Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, *Nature* 526 (2015).
- [76] Hucul, D. et al., Modular entanglement of atomic qubits using photons and phonons, *Nature Physics* 11(1) (2015).
- [77] Noelleke, C. et al, Efficient Teleportation Between Remote Single-Atom Quantum Memories, *Physical Review Letters* 110, 140403 (2013).
- [78] Sangouard, N. et al., Quantum repeaters based on atomic ensembles and linear optics, *Reviews of Modern Physics* 83, 33 (2011).
- [79] Monroe, C. et al. The U.S. National Quantum Initiative: From Act to Action. *Science*, vol. 364, no. 6439, pp. 440–442 (2019).
- [80] European Commission. *The future is quantum: EU countries plan ultra-secure communication network*. URL: <https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network> (2020).

- [81] European Commission. *Quantum Technologies Flagship kicks off with first 20 projects*. URL: <https://ec.europa.eu/commission/presscorner/detail/en/IP186205> (2020).
- [82] Quantum Flagship. *Quantum Manifesto: A New Era of Technology*. URL: <https://qt.eu/app/uploads/2018/04/93056Quantum-ManifestoWEB.pdf> (2018).
- [83] OPENQKD. *Truly secure quantum communication is here*. URL: <https://openqkd.eu/> (2020).
- [84] QUAPITAL. *Building the first reliable Quantum Internet on top of Europe's glass fiber network*. URL: <https://quapital.eu/> (2020).
- [85] QTSPACE. *Quantum Technologies in Space*. URL: <http://www.qtspace.eu/> (2020).
- [86] Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* 356, 1140 (2017).
- [87] Gyongyosi, L. Multicarrier Continuous-Variable Quantum Key Distribution, *Theoretical Computer Science*, DOI: 10.1016/j.tcs.2019.11.026 (2019), see also *arXiv:1310.1608* (2013).
- [88] Gyongyosi, L. and Imre, S. Circuit Depth Reduction for Gate-Model Quantum Computers, *Sci. Rep*, DOI: 10.1038/s41598-020-67014-5 (2020).
- [89] Gyongyosi, L. and Imre, S. Scalable Distributed Gate-Model Quantum Computers, *Sci Rep*, DOI: 10.1038/s41598-020-76728-5 (2021).
- [90] Grosshans, F. and Grangier, P. Reverse reconciliation protocols for quantum cryptography with continuous variables, *arXiv:quant-ph/0204127v1* (2002).
- [91] Pirandola, S., Mancini, S., Lloyd, S. and Braunstein, S. L. Continuous-variable quantum cryptography using two-way quantum communication, *Nature Phys.* 4 726 (2008).
- [92] Adcock, M. R. A., Hoyer, P. and Sanders, B. C. Limitations on continuous variable quantum algorithms with Fourier transforms, *New Journal of Physics* 11 103035 (2009).
- [93] Gyongyosi, L. and Imre, S. Multiple Access Multicarrier Continuous-Variable Quantum Key Distribution, *Chaos, Solitons and Fractals*, Elsevier, DOI: 10.1016/j.chaos.2018.07.006, ISSN: 0960-0779 (2018).
- [94] Pirandola, S., Garcia-Patron, R., Braunstein, S. L. and Lloyd, S. Direct and Reverse Secret-Key Capacities of a Quantum Channel, *Phys. Rev. Lett.* 102 050503 (2009).
- [95] Pirandola, S., Serafini, A. and S. Lloyd, Correlation matrices of two-mode bosonic systems, *Phys. Rev. A* 79 052327 (2009).

- [96] Pirandola, S., Braunstein, S. L. and Lloyd, S. Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography, *Phys. Rev. Lett.* 101 200504 (2008).
- [97] Weedbrook, C., Pirandola, S., Lloyd, S. and Ralph, T. Quantum Cryptography Approaching the Classical Limit, *Phys. Rev. Lett.* 105 110501 (2010).
- [98] Weedbrook, C., Pirandola, S., Garcia-Patron, R., Cerf, N. J., Ralph, T., Shapiro, J. and Lloyd, S. Gaussian quantum information, *Rev. Mod. Phys.* 84, 621 (2012).
- [99] Jouget, P. et al. Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nature Photonics* volume 7, pages 378–381 (2013).
- [100] Imre, S. and Balazs, F. *Quantum Computing and Communications – An Engineering Approach*, John Wiley and Sons Ltd, ISBN 0-470-86902-X, 283 pages (2005).
- [101] Petz, D. *Quantum Information Theory and Quantum Statistics*, Springer-Verlag, Heidelberg, Hiv: 6. (2008).
- [102] Leverrier, A., García-Patrón, R., Renner, R. and Cerf, N. J. Security of Continuous-Variable Quantum Key Distribution Against General Attacks, *Physical Review Letters* 110, 030502 (2013).
- [103] Renner, R. and Cirac, J. I. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography, *Physical Review Letters* 102, 110504 (2009).
- [104] Furrer, F., Franz, T., Berta, M., Leverrier, A., Scholz, V. B., Tomamichel, M. and Werner, R. F. Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks, *Physical Review Letters* 109, 100502 (2012).
- [105] Leverrier, A. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States, *Physical Review Letters* 114, 070501 (2015).
- [106] Leverrier, A. and Grangier, P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation, *Physical Review A* 83, 042312 (2011).
- [107] Leverrier, A. and Grangier, P. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation, *Physical Review Letters* 102, 180504 (2009).
- [108] Zwillinger, D. and Kokoska, S. *Standard Probability and Statistics Tables and Formulae*, CRC Press. ISBN 978-1-58488-059-2 (2010).
- [109] Gentle, J. E. *Computational Statistics*, Springer. ISBN 978-0-387-98145-1 2009).
- [110] Billingsley, P. *Probability and Measure* (Third ed.), John Wiley & sons, ISBN 0-471-00710-2 (1995).

- [111] Pinsker, M. S., Prelov, V. V. and van der Meulen, E. C. Information transmission over channels with additive-multiplicative noise, *Information Theory, 1998. Proceedings.* 1998 IEEE International Symposium on (1998).
- [112] Mitra, A. M. S. P. Capacity of Multivariate Channels with Multiplicative Noise: Random Matrix Techniques and Large-N Expansions, *Journal of Statistical Physics*, Volume 125, Issue 5–6, pp 1223–1242 (2006).
- [113] Lodewyck, J., Bloch, M., Garcia-Patron, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N. J., Tualle-Brouiri, R., McLaughlin, S. W. and Grangier, P. *Phys. Rev. A* 76, 042305 (2007).
- [114] Qi, B. and Lim, C. C. W. Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator, *arXiv:1708.08742v1* (2017).
- [115] Gyongyosi, L. and Imre, S. Low-Dimensional Reconciliation for Continuous-Variable Quantum Key Distribution, *Appl. Sci.*, DOI: 10.3390/app8010087, ISSN 2076-3417 (2018).
- [116] Gyongyosi, L. and Imre, S. Singular layer transmission for continuous-variable quantum key distribution, *IEEE Photonics Conference (IPC) 2014*, IEEE, DOI: 10.1109/IPCon.2014.6995246 (2014).
- [117] Gyongyosi, L. and Imre, S. *Proc. SPIE 9377, Advances in Photonics of Quantum Computing, Memory, and Communication VIII*, 937711, DOI:10.1117/12.2076532 (2015).
- [118] Gyongyosi, L. Diversity Extraction for Multicarrier Continuous-Variable Quantum Key Distribution, *Proceedings of the 2016 24th European Signal Processing Conference (EUSIPCO 2016)* (2016).
- [119] Lloyd, S. Capacity of the noisy quantum channel. *Phys. Rev. A*, 55:1613–1622 (1997).
- [120] Lloyd, S., Mohseni, M. and Rebentrost, P. Quantum algorithms for supervised and unsupervised machine learning. *arXiv:1307.0411* (2013).
- [121] Lloyd, S., Mohseni, M. and Rebentrost, P. Quantum principal component analysis. *Nature Physics*, 10, 631 (2014).
- [122] Bacsardi, L. On the Way to Quantum-Based Satellite Communication, *IEEE Comm. Mag.* 51:(08) pp. 50-55. (2013).
- [123] Muralidharan, S., Kim, J., Lutkenhaus, N., Lukin, M. D. and Jiang, L. Ultrafast and Fault-Tolerant Quantum Communication across Long Distances, *Phys. Rev. Lett.* 112, 250501 (2014).

- [124] Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I. and Fedorov, A. K.. Quantum-secured blockchain, *Quantum Sci. Technol.* 3, 035004 (2018).
- [125] Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52, R2493-R2496 (1995).
- [126] Biamonte, J. et al. Quantum Machine Learning. *Nature*, 549, 195-202 (2017).
- [127] Laudenbach, F. et al. Continuous-Variable Quantum Key Distribution with Gaussian Modulation - The Theory of Practical Implementations, *Adv. Quantum Technol.* vol 1, issue 1, pp 1-37, 1800011 (2018).
- [128] Gyongyosi, L. and Imre, S. Long-distance Continuous-Variable Quantum Key Distribution with Advanced Reconciliation of a Gaussian Modulation, *Proceedings of SPIE Photonics West OPTO 2013* (2013).
- [129] Gyongyosi, L. and Imre, S. Gaussian Quadrature Inference for Multicarrier Continuous-Variable Quantum Key Distribution, *SPIE Quantum Information and Computation XIV*, 17 - 21 Apr 2016, Baltimore, Maryland, USA (2016).
- [130] Tse, D. and Viswanath, P. *Fundamentals of Wireless Communication*, Cambridge University Press (2005).
- [131] Middleton, D. *An Introduction to Statistical Communication Theory: An IEEE Press Classic Reissue*, Hardcover, IEEE, ISBN-10: 0780311787, ISBN-13: 978-0780311787 (1960).
- [132] Kay, S. *Fundamentals of Statistical Signal Processing, Volumes I-III*, Prentice Hall (2013).
- [133] Kiasaleh, K. Channel Estimation for FSO Channels Subject to Gamma-Gamma Turbulence, *Proc. International Conference on Space Optical Systems and Applications (ICSOS)* 2012, 9-5, Corsica, France, October 9-12 (2012).
- [134] Benkhelifa, F., Rezki, Z. and Alouini, M. S. Low SNR Capacity of FSO Links over Gamma-Gamma Atmospheric Turbulence Channels, *IEEE Communications Letters* (Volume: 17, Issue: 6) (2013).
- [135] Garcia-Zambrana, A., Castillo-Vázquez, C. and Castillo-Vázquez, B. On the Capacity of FSO Links over Gamma-Gamma Atmospheric Turbulence Channels Using OOK Signaling, *EURASIP Journal on Wireless Communications and Networking* (2010).
- [136] Gyongyosi, L. and Imre, S. Secret Key Rates of Free-Space Optical Continuous-Variable Quantum Key Distribution, *Int. J. Commun. Syst.* (Wiley), DOI: 10.1002/dac.4152 (2019).

- [137] Gyongyosi, L. and Imre, S. Adaptive Gaussian quadrature detection for continuous-variable quantum key distribution, *Proceedings Volume 9762, Advances in Photonics of Quantum Computing, Memory, and Communication IX*; 97620E; DOI: 10.1117/12.2211743 (2016).
- [138] Gyongyosi, L. and Imre, S. Proceedings Volume 8997, *Advances in Photonics of Quantum Computing, Memory, and Communication VII*; 89970C; DOI: 10.1117/12.2038532 (2014).
- [139] Imre, S. and Gyongyosi, L. *Advanced Quantum Communications - An Engineering Approach*. Wiley-IEEE Press (New Jersey, USA) (2012).
- [140] Gyongyosi, L. and Imre, S. Multidimensional Manifold Extraction for Multicarrier Continuous-Variable Quantum Key Distribution, *SPIE Quantum Information and Computation XIII*, 20 - 24 Apr 2015, Baltimore, Maryland, USA (2015).
- [141] Gyongyosi, L. and Imre, S. Geometrical Analysis of Physically Allowed Quantum Cloning Transformations for Quantum Cryptography, *Information Sciences*, Elsevier, pp. 1-23, DOI: 10.1016/j.ins.2014.07.010 (2014).
- [142] Zhao, W., Liao, Q., Huang, D. et al. Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency division multiplexed modulation, *Quant. Inf. Proc.* 18:00 39. DOI:10.1007/s11128-018-2147-8 (2019).
- [143] Zhang, H., Mao, Y., Huang, D., Li, J., Zhang, L. and Guo, Y. Security analysis of orthogonal-frequency-division-multiplexing-based continuous-variable quantum key distribution with imperfect modulation, *Phys. Rev. A* 97 52328 (2018).
- [144] Pirandola, S. End-to-end capacities of a quantum communication network, *Commun. Phys.* 2 51 (2019).
- [145] Chow, P. S. *Bandwidth optimized digital transmission techniques for spectrally shaped channels with impulse noise*, Ph. D. thesis, Stanford University (1993).
- [146] Yu, W. and Cioffi, J. M. On Constant Power Water-filling, *IEEE International Conference on Communications*, doi: 10.1109/ICC.2001.937077 (2001).
- [147] Shieh, W. and Djordjevic, I. *OFDM for Optical Communications*. Elsevier (2010).
- [148] Gyongyosi, L. and Imre, S. Secret Key Rate Proof of Multicarrier Continuous-Variable Quantum Key Distribution, *Int. J. Commun. Syst.* (Wiley), DOI:10.1002/dac.3865 (2018).
- [149] Gyongyosi, L. and Imre, S. Diversity Space of Multicarrier Continuous-Variable Quantum Key Distribution, *Int. J. Commun. Syst.* (Wiley), DOI:10.1002/dac.4003 (2019).

- [150] Gyongyosi, L. and Imre, S. Gaussian Quadrature Inference for Multicarrier Continuous-Variable Quantum Key Distribution, *Quantum Studies: Mathematics and Foundations*, Springer Nature, DOI:10.1007/s40509-019-00183-9 (2019).
- [151] Gyongyosi, L. and Imre, S. Statistical Quadrature Evolution by Inference for Multicarrier Continuous-Variable Quantum Key Distribution, *Quantum Studies: Mathematics and Foundations*, Springer Nature, DOI: 10.1007/s40509-019-00202-9 (2019).
- [152] Gyongyosi, L. Singular Value Decomposition Assisted Multicarrier Continuous-Variable Quantum Key Distribution, *Theoretical Computer Science*, Elsevier, DOI: 10.1016/j.tcs.2019.07.029 (2019).
- [153] Gyongyosi, L. and Imre, S. Subcarrier Domain of Multicarrier Continuous-Variable Quantum Key Distribution, *J. Stat. Phys.* Springer Nature, DOI: 10.1007/s10955-019-02404-2 (2019).
- [154] Gyongyosi, L. and Imre, S. Secret Key Rate Adaption for Multicarrier Continuous-Variable Quantum Key Distribution, *SN Comput. Sci.*, Springer Nature, DOI: 10.1007/s42979-019-0027-7 (2019).
- [155] Debnath, S. et al. Demonstration of a small programmable quantum computer with atomic qubits. *Nature* 536, 63-66 (2016).
- [156] Barends, R. et al. Superconducting quantum circuits at the surface code threshold for fault tolerance. *Nature* 508, 500-503 (2014).
- [157] Ofek, N. et al. Extending the lifetime of a quantum bit with error correction in superconducting circuits. *Nature* 536, 441-445 (2016).
- [158] Kielpinski, D., Monroe, C. and Wineland, D. J. Architecture for a large-scale ion-trap quantum computer. *Nature* 417, 709-711 (2002).
- [159] Monz, T. et al. Realization of a scalable Shor algorithm. *Science* 351, 1068-1070 (2016).
- [160] Goodfellow, I., Bengio, Y. and Courville, A. *Deep Learning*. MIT Press. Cambridge, MA (2016).
- [161] Farhi, E., Goldstone, J. and Gutmann, S. A Quantum Approximate Optimization Algorithm Applied to a Bounded Occurrence Constraint Problem. *arXiv:1412.6062* (2014).
- [162] Rebentrost, P., Mohseni, M. and Lloyd, S. Quantum Support Vector Machine for Big Data Classification. *Phys. Rev. Lett.* 113. (2014).
- [163] Lloyd, S. The Universe as Quantum Computer, *A Computable Universe: Understanding and exploring Nature as computation*, H. Zenil ed., World Scientific, Singapore, 2012, *arXiv:1312.4455v1* (2013).

- [164] Lloyd, S., Garnerone, S. and Zanardi, P. Quantum algorithms for topological and geometric analysis of data. *Nat. Commun.*, 7, arXiv:1408.3106 (2016).
- [165] Lloyd, S., Mohseni, M. and Rebentrost, P. Quantum principal component analysis. *Nature Physics*, 10, 631 (2014).
- [166] Gyongyosi, L. A Universal Quantum Algorithm for Time Complexity Reduction of Quantum Computers, *Proceedings of Quantum Information Processing 2019* (QIP 2019), University of Colorado Boulder, USA (2019).
- [167] Gyongyosi, L. and Imre, S. Training Optimization for Gate-Model Quantum Neural Networks, *Scientific Reports*, Nature, DOI: 10.1038/s41598-019-48892-w (2019).
- [168] Guerreschi, G. G. and Smelyanskiy, M. Practical optimization for hybrid quantum-classical algorithms, *arXiv:1701.01450* (2017).
- [169] Hosen, M. A., Khosravi, A., Nahavandi, S. and Creighton, D. Improving the Quality of Prediction Intervals Through Optimal Aggregation, *IEEE Transactions on Industrial Electronics*, vol. 62, no. 7, pp. 4420-4429 (2015).
- [170] Precup, R-E., Angelov, P., Costa, B. S. J. and Sayed-Mouchaweh, M. An overview on fault diagnosis and nature-inspired optimal control of industrial process applications, *Computers in Industry*, vol. 74, pp. 75-94 (2015).
- [171] Saadat, J., Moallem, P. and Koofgar, H. Training echo state neural network using harmony search algorithm, *International Journal of Artificial Intelligence*, vol. 15, no. 1, pp. 163-179 (2017).
- [172] Vrkalovic, S., Lunca, E-C. and Borlea, I-D. Model-free sliding mode and fuzzy controllers for reverse osmosis desalination plants, *International Journal of Artificial Intelligence*, vol. 16, no. 2, pp. 208-222 (2018).
- [173] Caleffi, M. End-to-End Entanglement Rate: Toward a Quantum Route Metric, 2017 *IEEE Globecom*, DOI: 10.1109/GLOCOMW.2017.8269080 (2018).
- [174] Caleffi, M. Optimal Routing for Quantum Networks, *IEEE Access*, Vol 5, DOI: 10.1109/ACCESS.2017.2763325 (2017).
- [175] Caleffi, M., Cacciapuoti, A. S. and Bianchi, G. Quantum Internet: from Communication to Distributed Computing, *NANOCOM '18: Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication* (2018).
- [176] Castelvechi, D. The quantum Internet has arrived, *Nature*, News and Comment, <https://www.nature.com/articles/d41586-018-01835-3> (2018).
- [177] Cacciapuoti, A. S., Caleffi, M., Tafuri, F., Cataliotti, F. S., Gherardini, S. and Bianchi, G. Quantum Internet: Networking Challenges in Distributed Quantum Computing, *IEEE Network* DOI: 10.1109/MNET.001.1900092 (2018).

- [178] Cuomo, D., Caleffi, M. and Cacciapuoti, A. S. Towards a Distributed Quantum Computing Ecosystem, <https://digital-library.theiet.org/content/journals/10.1049/iet-qtc.2020.0002>, DOI: 10.1049/iet-qtc.2020.0002 (2020).
- [179] Chakraborty, K., Rozpedeky, F., Dahlbergz, A. and Wehner, S. Distributed Routing in a Quantum Internet, *arXiv:1907.11630v1* (2019).
- [180] Khatri, S., Matyas, C. T., Siddiqui, A. U. and Dowling, J. P. Practical figures of merit and thresholds for entanglement distribution in quantum networks, *Phys. Rev. Research* 1, 023032 (2019).
- [181] Kozłowski, W. and Wehner, S. Towards Large-Scale Quantum Networks, *Proc. of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication*, Dublin, Ireland (2019).
- [182] Pathumsoot, P., Matsuo, T., Satoh, T., Hajdusek, M., Suwanna, S. and Van Meter, R. Modeling of Measurement-based Quantum Network Coding on IBMQ Devices, *Phys. Rev. A* 101, 052301 (2020).
- [183] Pal, S., Batra, P., Paterek, T. and Mahesh, T. S. Experimental localisation of quantum entanglement through monitored classical mediator, *arXiv:1909.11030v1* (2019).
- [184] Miguel-Ramiro, J. and Dur, W. Delocalized information in quantum networks, *New J. Phys.*, DOI: 10.1088/1367-2630/ab784d (2020).
- [185] Pirker, A. and Dur, W. A quantum network stack and protocols for reliable entanglement-based networks, *New J. Phys.* 21 033003, DOI: 10.1088/1367-2630/ab05f7 (2019).
- [186] Khatri, S. Policies for elementary link generation in quantum networks, *arXiv:2007.03193* (2020).
- [187] Miguel-Ramiro, J., Pirker, A. and Dur, W. Genuine quantum networks: superposed tasks and addressing, *arXiv:2005.00020v1* (2020).
- [188] Gyongyosi, L. Dynamics of Entangled Networks of the Quantum Internet, *Scientific Reports*, DOI: 10.1038/s41598-020-68498-x (2020).
- [189] Gyongyosi, L. and Imre, S. Routing Space Exploration for Scalable Routing in the Quantum Internet, *Scientific Reports*, DOI: 10.1038/s41598-020-68354-y (2020).
- [190] Gisin, N. and Thew, R. Quantum Communication. *Nature Photon.* 1, 165-171 (2007).
- [191] Xiao, Y. F., Gong, Q. Optical microcavity: from fundamental physics to functional photonics devices. *Science Bulletin*, 61, 185-186 (2016).

- [192] Zhang, W. et al. Quantum Secure Direct Communication with Quantum Memory. *Phys. Rev. Lett.* 118, 220501 (2017).
- [193] Enk, S. J., Cirac, J. I. and Zoller, P. Photonic channels for quantum communication. *Science*, 279, 205-208 (1998).
- [194] Briegel, H. J., Dur, W., Cirac, J. I. and Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* 81, 5932-5935 (1998).
- [195] Dur, W., Briegel, H. J., Cirac, J. I. and Zoller, P. Quantum repeaters based on entanglement purification. *Phys. Rev. A*, 59, 169-181 (1999).
- [196] Duan, L. M., Lukin, M. D., Cirac, J. I. and Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414, 413-418 (2001).
- [197] Van Loock, P., Ladd, T. D., Sanaka, K., Yamaguchi, F., Nemoto, K., Munro, W. J. and Yamamoto, Y. Hybrid quantum repeater using bright coherent light. *Phys. Rev. Lett.*, 96, 240501 (2006).
- [198] Zhao, B., Chen, Z. B., Chen, Y. A., Schmiedmayer, J. and Pan, J. W. Robust creation of entanglement between remote memory qubits. *Phys. Rev. Lett.* 98, 240502 (2007).
- [199] Goebel, A. M., Wagenknecht, G., Zhang, Q., Chen, Y., Chen, K., Schmiedmayer, J. and Pan, J. W. Multistage Entanglement Swapping. *Phys. Rev. Lett.* 101, 080403 (2008).
- [200] Simon, C., de Riedmatten, H., Afzelius, M., Sangouard, N., Zbinden, H. and Gisin N. Quantum Repeaters with Photon Pair Sources and Multimode Memories. *Phys. Rev. Lett.* 98, 190503 (2007).
- [201] Tittel, W., Afzelius, M., Chaneliere, T., Cone, R. L., Kroll, S., Moiseev, S. A. and Sellars, M. Photon-echo quantum memory in solid state systems. *Laser Photon. Rev.* 4, 244-267 (2009).
- [202] Sangouard, N., Dubessy, R. and Simon, C. Quantum repeaters based on single trapped ions. *Phys. Rev. A*, 79, 042340 (2009).
- [203] Dur, W. and Briegel, H. J. Entanglement purification and quantum error correction. *Rep. Prog. Phys.* 70, 1381-1424 (2007).
- [204] Sheng, Y. B., Zhou, L. Distributed secure quantum machine learning. *Science Bulletin*, 62, 1025-1019 (2017).
- [205] Gyongyosi, L. and Imre, S. Dense Quantum Measurement Theory, *Scientific Reports*, Nature, DOI: 10.1038/s41598-019-43250-2 (2019).

- [206] Gyongyosi, L. and Imre, S. State Stabilization for Gate-Model Quantum Computers, *Quantum Information Processing*, Springer Nature, DOI: 10.1007/s11128-019-2397-0 (2019).
- [207] Gyongyosi, L. and Imre, S. Quantum Circuit Design for Objective Function Maximization in Gate-Model Quantum Computers, *Quantum Information Processing*, DOI: 10.1007/s11128-019-2326-2 (2019).