Budapesti Műszaki és
Gazdaságtudományi Egyetem

Hálózati Rendszerek és Szolgáltatások Tanszék

Optikai megoldások kvantum-kulcsszétosztó rendszerek adóegységeihez

Tézisfüzet

Szerző:
Schranz Ágoston

Témavezető:
Gerhátné Dr. Udvary Eszter Ph. D.
egyetemi docens

Budapest, 2021

Tézisek és a tézisekhez kapcsolódó publikációk összefoglalása

I. tézis – Polarizációmodulált felületsugárzó lézerek BB84-adóegységekben

Bevezetés

A kvantumalapú kulcsszétosztás (quantum key distribution, QKD) a kvantumkriptográfia egy fejlett területe, mely olyan protokollokkal foglalkozik, amelyek lehetővé teszik a lehallgatás észlelését két fél kommunikációján, akik egy titkosítási kulcsot kívánnak megosztani egymással. Az első ilyen protokoll, a BB84 1984-ből származik; az egyik fizikai megvalósítása egyetlen foton lineáris polarizációjába kódolja a küldeni kívánt információt. A protokoll négy különböző polarizációs állapotot használ, melyek közül nem mind merőleges egymásra.
Javaslatot tettem egy egyéni megoldásra, amely két felületsugárzó lézert (vertical cavity surface-emitting laser, VCSEL) használ a BB84 adóegységében, melyek egyenként két-két állapot kibocsátásáért felelősek. Egy ilyen struktúra költség- és méretbeli csökkenést eredményezhet az adóegységet tekintve. Megvizsgáltam továbbá az így előállított kvantumállapotok további szabadsági fokait is, melyek lehetőséget nyújthatnak a lehallgatónak az észrevétlen működésre. Olyan realisztikus megfontolásokon alapuló intézkedéseket javasoltam, amelyek védelmet nyújtanak ezen kiskapuk ellen, figyelembe véve a megvalósítás fizikai megkötéseit is.

I.a altézis – Javaslat egy új, polarizációban modulált VCSEL-eket használó BB84-adóstruktúrára

Bemutattam egy új adóegység-struktúrát a BB84 néven ismert QKD-protokollhoz, ami a triviális struktúra négy fényforrásához képest csak két darab VCSEL-t használ. Annak érdekében, hogy a BB84-ben használt négy különböző kvantumállapota

mind előállítható legyen, a VCSEL-ek polarizációváltási mechanizmusát használom ki. Ezek a váltások merőleges polarizációs sajátállapotok között következnek be; a szándékos váltások előidézését polarizációmodulációnak nevezik. A VCSEL-ek további előnyeként bemutattam, mely tulajdonságaik miatt alkalmasabbak alacsony teljesítményű alkalmazási területeken, mint az élsugárzó lézerek.

I.b altézis – Áramvezérelt polarizációmodulációs megoldások és impulzusformálás

Javasoltam két különböző áramvezérléssel elért polarizációmodulációs megoldást. Az első a VCSEL munkaponti áramát a küszöbáram közelében állítja be, majd különböző amplitúdójú áramimpulzusokat használ a két merőleges polarizációs állapot eléréséhez. A második megoldás munkaponti árama a polarizációváltás pontjához közeli, és e pont körüli kisjelű modulációval alakíthatóak ki a különbözőképpen polarizált fényimpulzusok. Megmutattam, hogy ha az adóegységet kiegészítjük egy elektroabszorpciós modulátorral, két nehézség is megoldható egyszerre. Első ezek közül, hogy a csillapítás gyorsan változtatható, így kiküszöbölhető a különböző polarizációs állapotú fényimpulzusok eredendően eltérő teljesítményszintjének problémája. A modulátor emellett impulzusformálásra is használható, aminek segítségével egyrészt elnyomhatóak az impulzusok esetlegesen helytelenül polarizált részei, valamint tetszőlegesen pontos időtartománybeli átfedés érhető el a merőlegesen polarizált jelek között.

I.c altézis – Védekezés spektrális támadások ellen a frekvenciák, bitértékek és polarizációs bázisok közti bijekciók megszüntetésével

Megmutattam, hogy az új adóegység-struktúra érzékeny egy úgynevezett spektrális támadásra, melynek során a támadó a fotonok frekvenciáját megmérve próbálja megkülönböztetni az eltérő polarizációs állapotokat. A triviális struktúrában ez a támadás egyszerűen kivédhető, amennyiben négy olyan fényforrást használunk, melyeknek spektruma páronként nagy átfedésben áll egymással; a VCSEL-ek polarizációs sajátállapotai között viszont mindig van egy nagyobb mértékű frekvenciakülönbség. Javasoltam egy védekezési módszert a spektrális támadás ellen, ami akkor is megbízható, ha a lehallgató a fotonok megsemmisítése nélkül is képes megmérni azok frekvenciáját. Ehhez először két olyan VCSEL-t kell választani az adóegységhez, melyek alacsonyabb és magasabb frekvenciájú sajátállapotainak

spektrumai páronként nagymértékű átfedéssel rendelkeznek. Ezt követően az egyes frekvenciaértékekhez komplementer, ellentétes módon kell hozzárendelni a hordozott bitek értékeit a két lézer esetében. Ez a módszer biztosítja, hogy ne legyen korreláció a bitek értékei és a frekvencia, valamint a használt polarizációs bázis és a frekvencia között. A támadó így nem képes információt nyerni a polarizációról a spektrális szabadsági fok felhasználásával – nem többet, mint a triviális struktúra használata esetén tudna.

Kapcsolódó saját publikációk: **C6**, **C7**, **B1**

II. tézis – Fotonok beérkezési idejei közti különbségen alapuló kvantum-véletlenszámgenerátor matematikai modellezése

Bevezetés

A kvantum-véletlenszámgenerálás (quantum random number generation, QRNG) lehetőségeit az elmúlt évtizedtől kezdve széleskörűen kutatják, mivel ezek az eszközök lehetőséget biztosítanak eredendően véletlenszerű, jó minőségű véletlen bitek előállítására a kvantumfizikai mérésekben rejlő véletlenség kihasználásával. Egyenletes eloszlású bitsorozatokra több alkalmazási területen is nagy igény mutatkozik, melyek közül talán a legjelentősebb a szimmetrikus kulcsú titkosítás. Az álvéletlenszám-generátorokkal ellentétben a QRNG-módszerek nem determinisztikusak, azonban problémát jelent, hogy a véletlenséget nem lehetséges bizonyítani a kimeneten megjelenő bitek elemzésével. Éppen ezért rendkívül fontos, hogy minden generátor-architektúra működési elvét alaposan ismerjük és behatóan tanulmányozzuk, mielőtt felhasználnánk az általuk generált biteket.
Levezettem egy kvantum-véletlenszámgenerátor matematikai modelljét, mely két egymást követő, fotondetekciók közti időintervallum hosszát hasonlítja össze, és a különbségük előjele alapján állít elő biteket, elvetve az egyenlőnek mért eseteket. Két fő metrikára, a bitgenerálási hatásfokra és bitgenerálási rátára fókuszálva alkottam meg a modellt, megmutatva, hogyan változnak ezek a releváns bemeneti paraméterek függvényében. Szimulációk segítségével megvizsgáltam azt is, hogy a fizikai elrendezés valós eszközeinek eltérései a modellhez képest mekkora változást okoznak, majd gyakorlatban is megvalósítottam a generátort, és kiértékeltem a modell hitelességét. Az elméleti és kísérleti úton kapott eredmények nagymértékű egyezést mutatnak.

II.a altézis – Bitgenerálási hatásfok és sebessége levezetése a modell bemeneti paramétereinek függvényében

Meghatároztam a lényeges paramétereket, melyek segítségével a módszer valósághűen modellezhető, és kihagytam azokat, melyek a saját fizikai implementációmban elhanyagolhatóak az eszközparamétereknek köszönhetően. Valószínűségelméleti módszerekkel levezettem a bitgenerációs hatásfok és sebesség kifejezéseit a három paraméter – a bemeneti fotonráta, λ; a mérőórajel periódusideje, τ; illetve a vevőrendszer holtideje, τ_d – függvényében. Megmutattam, hogy amennyiben utóbbi két paraméter fixnek tekinthető, λ, tehát az optikai teljesítmény változtatásával nem lehetséges a két metrikát egyidejűleg maximalizálni, és a legnagyobb elérhető bitgenerálási sebességhez az ideálisnál alacsonyabb hatásfok tartozik.

II.b altézis – A matematikai vizsgálat leegyszerűsítése a hatásfoknak az adott diszkrét valószínűségi eloszlás eltolására való invarianciájának kihasználásával

Megmutattam, hogy a hatásfok a τ_d/τ-aránynak csak a törtrészétől függ, és nem változik, ha az arány alsó egészrészét növeljük vagy csökkentjük. Ez nagyban leegyszerűsíti a vizsgálatot, és lehetővé teszi, hogy minden létező paraméterkombinációhoz analitikus megoldást rendeljünk. A bitgenerációs sebesség azonban függ a holtidő teljes hosszától – így a τ_d/τ egészrészétől is –, viszont közvetlenül számítható azáltal, hogy a hatásfokra meghatározott formulát megszorozzuk a fotondetektor kimeneti számlálási rátájával.

II.c altézis – Újraindítható vagy folytonos mérőórajelek használatából adódó különbségek elhanyagolhatósága a nagy pontosságú tartományban

Bevezettem a nagy pontosságú tartomány fogalmát, ahol $\lambda\tau \ll 1$, és megfogalmaztam a sejtést, hogy ezen tartományban a folytonos mérőórajel negatív hatásai majdnem teljesen elhanyagolhatóak az újraindítható órajel használatához képest. Ezt az állítást szimulációkkal is alátámasztottam, megmutatva, hogy a bitek közti korrelációk a nagy pontosságú tartományban kellően alacsonyak, míg a bitgenerációs hatásfok és sebesség gyakorlatilag megegyezik a modellben meghatározott értékekkel.

II.d altézis – A matematikai modell gyakorlati validálása a felhasznált eszközök fizikai korlátai ellenére

Kísérleti úton igazoltam a matematikai modellem helyességét. Megmutattam, hogy a mért bitgenerációs hatásfok és sebesség változó bemeneti fotonráta és fix értékű τ valamint τ_{d} mellett nagy mértékű egyezést mutat az elméleti levezetések által jósoltakkal. A valós eszközök okozta limitációk – folytonos mérőórajel, nem-konstans holtidő – hatásai elég kicsik ahhoz, hogy a vizsgált metrikák ne térjenek el a modellezett értékektől. Teszteltem a generált bitsorozatok véletlenségének minőségét, és megmutattam, hogy a nagy pontosságú tartományban a folytonos mérőórajel használata nem teszi tönkre az előállított bitek egyenletes eloszlását.

Kapcsolódó saját publikációk: **J1**

III. tézis – A beérkezési idők különbségén alapuló véletlenszámgenerálási módszer hatásfokának növelése

Bevezetés

A technológiai követelmények fejlődésével egyre fontosabb lesz, hogy a véletlen biteknek ne csak a minősége legyen magas, hanem kellő sebességgel és hatásfokkal legyenek előállítva. A tökéletes matematikai biztonság csak akkor garantálható szimmetrikus kulcsú titkosítási rendszerekben, ha a titkos kulcs generálási sebessége nagyobb, mint az üzenet bitsebessége, ezért a folyton növekvő kommunikációs sebességekhez kell hangolni a véletlenszám-generátorok sebességét is. Hasonló javulást elérhetünk jobb paraméterekkel rendelkező fizikai eszközök felhasználásával, teljesen új architektúrák kifejlesztésével, de akár pusztán matematikai módszerekkel is, amelyek a valószínűségi változókra hatnak még a bitek hozzárendelése előtt
Megalkottam a II. tézisből ismert véletlenszám-generálási módszer finomított változatát, mely képes mind a bitgenerálási hatásfok, mind a bitgenerálási ráta növelésére azáltal, hogy csoportokat képez m darab egymást követő különbségképzés előjeléből, majd minden egyes csoporthoz több bitet rendel. A finomított és az eredeti módszert kvantitatív módon összehasonlítottam, és levezettem a bitgenerálási ráta nyereségének matematikai kifejezését. Figyelembe vettem, hogy a kis fényteljesítmény-ingadozásokból fakadóan az új valószínűségi változók eloszlása nem teljesen egyenletes, és vizsgáltam, hogyan hat ez a bitek véletlenségének minőségére.

Végül kísérletileg igazoltam, hogy az új módszer tényleg képes olyan véletlen bitsorozatok előállítására, melyek sikeresen teljesítik a NIST tesztcsomagjának minden egyes véletlenségi tesztjét további utófeldolgozás nélkül.

III.a altézis – Vektorváltozók kialakítása az eseményenként elérhető min-entrópia növelése érdekében

Javaslatot tettem az előzőekben megismert bitgenerálási módszer megváltoztatására úgy, hogy az időkülönbségek előjelei egyenletes eloszlást kövessenek. Levezettem, hogy ez csupán a bemeneti fotonráta (λ), a mérési órajel periódusideje (τ) és a holtidő (τ_d) bizonyos kombinációi mellett lehetséges. Megmutattam, hogy ez önmagában nem elégséges ahhoz, hogy összehasonlításonként egynél több bitet generáljunk, mert a min-entrópia alsó egészrésze továbbra is egy. A $\lfloor H_\infty \rfloor < H_\infty$ korlátozás mindig jelen van, ha az eseménytér számossága nem kettő egész kitevős hatványa. Megmutattam azonban, hogy lehetséges m-hosszú csoportokat képezni egymást követő összehasonlítások eredményeiből úgy, hogy az új vektorváltozók min-entrópiája és annak alsó egészrésze között kisebb legyen a különbség; ezáltal magasabb bitgenerálási hatásfokok érhetőek el. Bemutattam azt is, hogy a konkrét esetben az $m = 2$ illetve $m = 7$ választások ténylegesen magasabb hatásfokot eredményeznek, míg a vektorváltozók eredményterének a nagysága kezelhetően kicsi marad.

III.b altézis – Az új módszer bitgenerálási sebességnyeresége az eredetihez képest

Több módon számszerűsítettem a régi módszerhez képest elért javulások mennyiségét: összehasonlítva a két metódus bitgenerálási sebességeit az új módszer munkapontjában, valamint bevezetve a bitgenerálási sebességnyereséget $G_{\mathrm{R}m}$, mint az új és régi módszerek maximális sebességeinek arányát fix τ és τ_d mellett. Annak függvényében, hogy a holtidő milyen hosszú az órajel periódisidejéhez képest, a nyereség értéke jelentősen változik 1 és 2 között, megmutatva, hogy az új módszer minden paraméterkombináció mellett gyorsabb átlagsebességgel képes biteket előállítani.

III.c altézis – Hibamodell, a min-entrópia korlátai és rendszerszintű kiegyenlítetlenség-mentességet biztosító kódolás

Megalkottam a metódushoz egy hibamodellt, amelyben a különbségek előjelei nem egyenletes, de szimmetrikus eloszlást követnek. Meghatároztam a maximálisan tolerálható hibaértéket, amin belül az eloszlás min-entrópiája még meghaladja az egyes m-hosszú csoportokhoz rendelt bitek számát. Megmutattam, hogy a kiegyenlítetlenséget a nullás és egyes bitek között rendszerszintűen ki lehet küszöbölni bármekkora hibaérték mellett a szimmetriákat kihasználva. Ehhez gondosan meg kell válogatni, mely események lesznek végső soron elvetve, valamint garantálni kell, hogy a maximális Hamming-távolságú bitcsoportokat azonos valószínűségű eseményekhez rendeljük. Megalkottam egy algoritmust, amely m tetszőleges értéke mellett képes megvalósítani egy ehhez hasonló kiegyenlítetlenség-mentes kódolási függvényt.

III.d altézis – Az új véletlenszám-generálási módszer működésének kísérleti igazolása

Kísérleteket végeztem, és megerősítettem, hogy a javasolt módszer valóban képes jó minőségű véletlenszámok előállítására, még gyakorlati korlátok mellett is, mint a fotonráta enyhe fluktuációja és a folytonos mérőórajel használata. Megoldottam a lassú teljesítményingadozásokvól fakadó problémákat azáltal, hogy a mérési órajel periódusidejét szoftveresen hangoltam a változásokat lekövetve. Megmutattam, hogy a hibamodell jó leírást ad az egyenletes eloszlástól való eltérésekről, és hogy a hiba mértéke az előzetesen meghatározott korlátok között tartható. Bemutattam, hogy még az ideálistól eltérő körülmények között is lehet olyan finoman hangolni a beállításokat, hogy a generált bitsorozatok nem szorulnak utófeldolgozásra ahhoz, hogy sikeresen teljesítsenek minden véletlenségi tesztet. Az adott fizikai architektúrán a bitgenerációs sebesség 47.25%-kal megnőtt az eredeti módszerhez képest.

Kapcsolódó saját publikációk: **J5**

Publikációk listája

Ez a lista az összes publikációmat tartalmazza, ami megjelent a tézisfüzet írásáig bezárólag; közülük nem mindegyik kapcsolódik a tézisekhez. Azok, melyk az egyes téziseket támasztják alá, külön jelölve vannak az adott tézis után.

Folyóiratcikkek

J1 Ágoston Schranz és Eszter Udvary. "Mathematical analysis of a quantum random number generator based on the time difference between photon detections". *Optical Engineering* 59.4 (2020), 44104. old. DOI: 10.1117/1.OE.59.4.044104

J2 Ádám Marosits, Ágoston Schranz és Eszter Udvary. "Amplified spontaneous emission based quantum random number generator". *Infocommunications Journal* 12.2 (2020), 12–17. old. DOI: 10.36244/icj.2020.2.2

J3 Ágoston Schranz és Eszter Udvary. "Error probability in polarization sensitive communication systems in terms of moments of the channel's rotation angle". *Optical and Quantum Electronics* 53.1 (2021. jan.), 62. old. ISSN: 0306-8919. DOI: 10.1007/s11082-020-02690-1

J4 Balázs Matolcsy, Eszter Udvary és Ágoston Schranz. "Common-mode noise filtering with space-divided differential 2x2 VLC for V2V applications". *Optical and Quantum Electronics* 53.4 (2021), 182. old. DOI: 10.1007/s11082-021-02808-z

J5 Ágoston Schranz, Eszter Udvary és Balázs Matolcsy. "Efficiency Improvement of a Time-of-Arrival Quantum Random Number Generator". *Optical Engineering* 60.3 (2021), 34112. old. DOI: 10.1117/1.OE.60.3.034112

Konferenciacikkek

C1 Ágoston Schranz, Eszter Udvary és Zsolt Kis. "Photon statistics determination for single photon based quantum key distribution". *18th International Conference on Transparent Optical Networks (ICTON)*. IEEE. 2016, 1–4. old. DOI: 10.1109/ICTON.2016.7550483

C2 Eszter Udvary, Ágoston Schranz és Balázs Matolcsy. "Dispersion and off-set filtering in RSOA based networks". *18th International Conference on*

Transparent Optical Networks (ICTON). 2016, 1–4. old. DOI: 10.1109/ICTON.2016.7550690

C3 Ágoston Schranz. "Experimental Investigation of VCSEL for Quantum Communications". *Mesterpróba 2016*. 2016, 8–11. old.

C4 Ágoston Schranz. "Investigation of VCSEL Polarization for Quantum Key Distribution". *International Interdisciplinary PhD Workshop 2016*. 2016, 117–120. old.

C5 Gábor Szabó, Ágoston Schranz és Eszter Udvary. "Nonlinear Modulation Characteristics of LEDs in Radio on Visible Light Systems". *International Interdisciplinary PhD Workshop 2016*. 2016, 6–10. old.

C6 Ágoston Schranz és Eszter Udvary. "Transmitter Design Proposal for the BB84 Quantum Key Distribution Protocol using Polarization Modulated Vertical Cavity Surface-emitting Lasers". *Proceedings of the 6th International Conference on Photonics, Optics and Laser Technology*. INSTICC. SciTePress, 2018, 252–258. old. ISBN: 978-9-897-58286-8. DOI: 10.5220/0006638002520258

C7 Ágoston Schranz és Eszter Udvary. "Quantum Bit Error Rate Analysis of the Polarization based BB84 Protocol in the Presence of Channel Errors". *Proceedings of the 7th International Conference on Photonics, Optics and Laser Technology - Volume 1: PHOTOPTICS*. INSTICC. SciTePress, 2019, 181–189. old. ISBN: 978-9-897-58364-3. DOI: 10.5220/0007384101810189

C8 Ágoston Schranz, Ádám Marosits és Eszter Udvary. "Effects of Sampling Rate on Amplified Spontaneous Emission Based Single-Bit Quantum Random Number Generation". *21st International Conference on Transparent Optical Networks (ICTON)*. IEEE. 2019, 1–4. old. DOI: 10.1109/ICTON.2019.8840188

Könyvfejezetek

B1 Ágoston Schranz és Eszter Udvary. "Polarization Modulated Vertical-Cavity Surface-Emitting Lasers in Quantum Key Distribution". *Optics, Photonics and Laser Technology 2018*. 223. köt. Springer Series in Optical Sciences. Springer, Cham., 2019, 75–92. old. DOI: 10.1007/978-3-030-30113-2_4