Magyar Tudomány 184(2023)2, 202–211
DOI: 10.1556/2065.184.2023.2.8

Tanulmányok

A KVANTUM-ÖSSZEFONÓDÁS ÉS A 2022-ES FIZIKAI NOBEL-DÍJ

QUANTUM ENTANGLEMENT AND THE 2022 NOBEL PRIZE IN PHYSICS

Bacsárdi László[1], Kis Zsolt[2]

[1]PhD, Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar Hálózati Rendszerek és Szolgáltatások Tanszék, Budapest
bacsardi@hit.bme.hu
[2]PhD, Wigner Fizikai Kutatóközpont, Budapest
kis.zsolt@wigner.hu

ÖSSZEFOGLALÁS

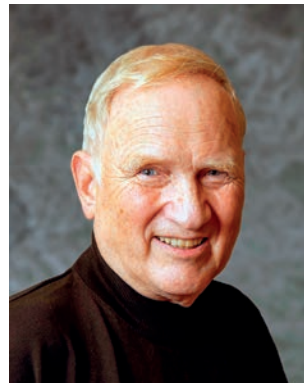
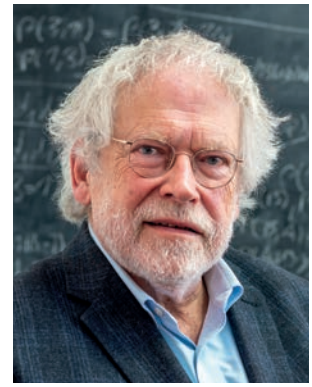
A 2022-es fizikai Nobel-díjat a francia Alain Aspect, az amerikai John F. Clauser és az osztrák Anton Zeilinger kapta az összefonódott fotonokkal végzett kísérleteikért, a Bell-egyenlőtlenségek megsértésének megállapításáért és a kvantuminformatika területén végzett úttörő munkásságukért. Ebben a cikkben megismertetjük az olvasót a kvantumfizika egyik legérdekesebb jelenségével, az összefonódással, amely számos kvantuminformatikai és kvantumkommunikációs alkalmazás alapegysége. Bemutatjuk a három Nobel-díjas fizikus kapcsolódó munkásságát, és kitérünk néhány olyan kvantuminformatikai területre és alkalmazásra, ahol az összefonódás fontos szerepet tölt be.

ABSTRACT

The 2022 Nobel Prize in Physics was awarded to the French Alain Aspect, the American John Clauser and the Austrian Anton Zeilinger for their experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science. In this article, we introduce one of the most interesting phenomenon of quantum physics, the quantum entanglement which serves as a basic building block of many quantum computing and quantum communication applications. We present the related works of the three Nobel Prize-winning physicists, and cover some quantum computing areas and applications where entanglement plays an important role.

Kulcsszavak: összefonódás, fizikai Nobel-díj 2022, kvantumfizika, kvantumkommunikáció

Keywords: entanglement, Nobel Prize in Physics 2022, quantum physics, quantum communication

A 2022. évi fizikai Nobel-díj három kitüntetettje.
Balról jobbra: Alain Aspect, John F. Clauser, Anton Zeilinger

(Ecole polytechnique Université Paris-Saclay – Mooc optique quantique, Wikimedia Commons, CC BY-SA 2.0 licenc; John Clauser, Wikimedia Commons, CC BY-SA 4.0 licenc; Jaqueline Godany, Wikimedia Commons, CC BY 4.0 licenc)

EINSTEIN LOKÁLIS REALIZMUSA

Albert Einstein volt az egyik első kutató, aki lerakta a kvantummechanika alapjait még a 20. század elején. Az 1910–1920-as években számos, mára ikonikussá vált kutató járult hozzá a kvantummechanika fejlődéséhez, és a szigorú matematikai formalizmusok segítségével nyert eredmények interpretálásához, például Niels Bohr, Erwin Schrödinger, Werner Heisenberg, Wolfgang Pauli, hogy csak néhány híres, közismert nevet említsünk. Azonban az interpretációk nem voltak egybehangzóak. Niels Bohr és Werner Heisenberg nevéhez fűződik az ún. koppenhágai értelmezés, amely a mai napig a legszélesebb körben elfogadott. Ez többek között kimondja, hogy a kvantummechanikai hullámfüggvény abszolút értékének négyzete egy valószínűségi eloszlás, és ha bármilyen mérést végzünk egy elemi részecskén, ez az eloszlásfüggvény határozza meg, hogy az egyes lehetséges mérési eredményeknek mekkora a valószínűségük (a függvény független változója felel meg a lehetséges mért értékeknek). Ehhez még az is hozzájárul, hogy csak a mérés pillanatában dől el, hogy mi lesz a mérés kimenetele. Ezzel szemben Einstein szerint létezik az ember által végrehajtott méréstől független valóság, ahogy azt elhíresült mondásában megfogalmazta: „Isten nem kockázik.”

Einstein, Boris Podolsky és Nathan Rosen 1935-ben publikált egy cikket (Einstein et al., 1935, a továbbiakban EPR-cikként utalunk rá), amelyben egy paradox jelenségen keresztül akarták kimutatni, hogy a kvantummechanikai leírás nem

lehet teljes, mert ellentmond a cikkben megfogalmazott lokális realizmus elvének. A lokális realizmus kifejezés két elvből tevődik össze: A realizmus, azaz fizikai valóság értelmezése a következő: „Ha egy rendszer bármilyen módon történő megzavarása nélkül teljes bizonyossággal meg tudjuk jósolni egy fizikai mennyiség értékét, akkor létezik ennek a mennyiségnek megfelelő valóságelem." Emellett definiálták még a lokalitás elvét is, amely Einstein speciális relativitáselmélettel kapcsolatos korábbi munkáin alapul: eszerint egy adott helyen végrehajtott mérés nem befolyásolhatja egy tőle távoli rendszeren, közel egyidejűleg végrehajtott mérés eredményét, mivel a fizikai hatás nem terjedhet a fénynél nagyobb sebességgel. A cikkben egy gondolatkísérletet (németül *Gedankenexperiment*) dolgoztak ki egy közös forrásból eredő, szétrepülő részecskepárra, melyeken méréseket hajtanak végre, amikor egymástól már nagy távolságra kerülnek. A kvantummechanikai leírásban a részecskék ún. összefonódott kvantumállapotban (angolul *entangled state*) vannak. A mérések várható kimenetelét a kvantummechanika szabályai alapján számolva arra a következtetésre jutottak, hogy az ellentmond a lokális realizmus elvének. Ez számukra nem volt elfogadható, ezért a cikk végső konklúziója az, hogy inkább azt kell feltételezni, hogy a kvantummechanikai leírás nem teljes.

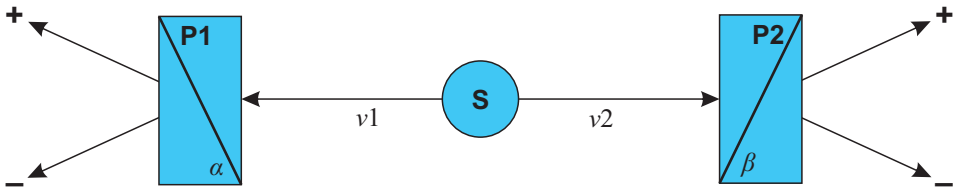
Az EPR-cikkben bemutatott paradoxon feloldására tett erőfeszítések – alternatív elméleti értelmezések kidolgozása, perdöntő kísérletek tervezése és kivitelezése – évtizedeken át foglalkoztatta a fizikusokat. A 2022-ben fizikai Nobel-díjjal elismert kutatók munkássága mérföldköveket jelentett ebben a folyamatban. Niels Bohr röviddel az EPR-cikk megjelenése után publikálta kritikáját (Bohr, 1935), amelyben kimutatta, hogy az EPR gondolatmenete hibás, mert nem fér össze a komplementaritás elvével. Az EPR-gondolatkísérletet a gyakorlatban megvalósítani igen körülményes lett volna, ezért David Bohm és Jakir (Yakir) Aharonov 1957-ben (Bohm–Aharonov, 1957) átfogalmazta egy feles spinű részecskékből álló párra, amelynek összspinje zérus vagy, alternatívaként, összefonódott, ortogonális polarizációjú fotonpárokra. Felismerték, hogy korrelációs mérésekkel lehetne eldönteni, hogy vajon az EPR-cikkben megfogalmazott paradoxon tényleg fennáll-e, és emiatt előfordulhat-e, hogy a kvantummechanikai leírás nem teljes. Ugyanakkor a gyakorlatban könnyen ellenőrizhető kritériumot nem adtak meg.

AZ ÖSSZEFONÓDÁS KUTATÓI

Ahogy fentebb írtuk, Einstein nem fogadta el, hogy a valóságban csak a mérés pillanatában dől el, hogy mi egy kvantumrendszer állapota. Úgy vélte, hogy a végállapotban (mérésben) tapasztalható véletlenszerűség abból származik, hogy nem ismerjük a rendszert leíró valamennyi paramétert, és ezek véletlenszerű

ingadozása okozza a kísérletben megfigyelt véletlen eloszlást. Ennek a gondolatnak matematikai megfogalmazása az ún. rejtett paraméter elméletek, amelyek kidolgozásához Bohm is hozzájárult (Bohm, 1952). John S. Bell 1964-ben publikált művében (Bell, 1964) kidolgozott egy rejtett paraméter elméletet feles spinű részecskék spinjének mérésére, és ezt felhasználva meghatározta két távoli feles spinű részecske közötti spinkorrelációs mérés várható eredményét. Kimutatta, hogy három különböző spinkorrelációs mérés eredményét adott módon kombinálva egy olyan felső korlátot lehet kapni, amelyet a rejtett paraméter elmélet keretein belül nem lehet túllépni. Ugyanakkor, a korrelációs függvényeket a kvantummechanika szabályai alapján kiértékelve ez az egyenlőtlenség sérül. Az egyenlőtlenség ellenőrzésére javasolt korrelációs mérések már alkalmasak voltak arra, hogy kísérletileg is elvégezzék azokat.

Bell cikkének megjelenése után öt évvel publikálta *John F. Clauser* szerzőtársaival a Bell-egyenlőtlenség módosított változatát (CHSH-egyenlőtlenség) polarizációban összefonódott fotonpárokra. Ők is kimutatták, hogy a rejtett paraméter elméletek nem férnek össze a kvantummechanika bizonyos jóslataival. Az egyenlőtlenség kiértékeléséhez szükséges korrelációs méréseket elvileg könnyen el lehet végezni: a két távoli mérőhelyen egy-egy polarizátorra és egyfoton-érzékenységű detektorokra van szükség. A polarizátorok meghatározott irányú beállításai mellett meg kell mérni azon események előfordulási arányát, amikor mindkét detektor egyszerre jelez (ez az ún. koincidenciamérés). A javasolt kísérletet 1972-ben Stuart J. Freedman és Clauser végezte el elsőként (Freedman–Clauser, 1972). Az összefonódott fotonpárokat gerjesztett elektronhéjú kalciumatomok segítségével állították elő: az atomok $J = 0 \rightarrow J = 1 \rightarrow J = 0$ impulzusmomentum állapotokon keresztül jutottak alapállapotba (bomlási kaszkád), ennek során polarizációsan összefonódott fotonpárokat bocsátottak ki. A polarizátorok egymással bezárt szögének függvényében megmérték a koincidenciák számát, ebből pedig meghatározták a korrelációs függvény szögfüggését. A kapott görbe egybevágott a kvantummechanikai jóslattal. A mérés hatékonysága igen alacsony volt, 200 órába telt egyetlen korrelációs függvény kimérése.



1. ábra. Alain Aspect kísérletének sémája
S: összefonódott fotonpárforrás; P1 és P2: polarizációs kockák, amelyek szétválasztják az egy adott irányban és rá merőleges irányban polarizált fotonokat (wikipedia.com)

A Bell-egyenlőtlenség első sikeres ellenőrzése *Alain Aspect* és munkatársai nevéhez fűződik (Aspect et al., 1982). Hasonló fotonpárforrást használtak, mint Clauser, azonban a szétrepülő fotonok polarizációs analízisét már nem egyszerű polarizátorral, hanem polarizációs kockával végezték, amely mindkét kimenetén volt fotonszámláló *(1. ábra).* Ez jelentősen lerövidítette a mérés idejét, és kiküszöbölte a kiskapuk egy részét, amelyek teret adtak volna egy rejtett paraméter elméleten alapuló értelmezésnek. Egy-egy korrelációs függvényt mindössze 100 másodperc alatt mértek ki, a teljes mérési idő (a polarizációs kockák beállítása nélkül) pedig ennek mindössze négyszerese. A CHSH-egyenlőtlenségben a korrelációs mérésekből kapható felső határ 2, amennyiben a rejtett paraméterek határozzák meg a szétrepülő fotonpárok korrelációját. Ha a kvantummechanika helyes, akkor a CHSH-egyenlőtlenség felső korlátja $2\sqrt{2}$. A mért korrelációs értékeket behelyettesítve az egyenlőtlenségbe 2,7 értéket kaptak, amely 95%-a a kvantummechanikai jóslatnak. A mérés hibája mindössze 1-2% volt, tehát ki lehet jelenteni, hogy nem rejtett paraméterek határozzák meg az összefonódott fotonpárok polarizációs állapotának korrelációját.

Mindezek az eredmények tehát nem Einsteint és a lokális realizmus elvét igazolják, hanem a koppenhágai valószínűségi értelmezést támasztják alá. Továbbá kiemelik, hogy a kvantummechanikai mérés hatása egy rendszerre nem lokális.

A Bell-tesztet 1982 óta számos kísérleti laboratóriumban elvégezték, és nemcsak összefonódott fotonpárokra, hanem például feles spinű elektronokra is. Minden esetben az egyenlőtlenség sérülését tapasztalták. Egyúttal megjelentek a különféle alkalmazások is, amelyek az összefonódott kvantumállapotú fotonpárok különleges korrelációs tulajdonságán alapultak. Ennek a kutatási iránynak egyik úttörője *Anton Zeilinger* volt. Számos igen magas hivatkozású cikkben publikálta eredményeit, amelyek szerteágazó témakörökben születtek. A teljesség igénye nélkül néhány kiemelkedő munkája: nagy fényességű, polarizációban összefonódott fotonpárforrás fejlesztése (Kwiat et al., 1995), kvantumállapot teleportáció kísérleti demonstrációja (Bouwmeester et al., 1997), nagy sűrűségű kvantumkódolás kísérleti demonstrációja (ez a kvantumkommunikáció témakörben jelentős) (Mattle et al., 1996) és még számos további kiemelkedő kísérleti és elméleti eredmény.

KVANTUMSZÁMÍTÓGÉP SZÜLETIK

Napjainkban egyre inkább a hétköznapok részévé válik, hogy a kvantumfizika törvényeit az informatikában is alkalmazni tudjuk, akár kvantumszámítógépekről, akár kvantumkommunikációról van szó. Több mint negyven évvel ezelőtt ez még nem így volt. 1981 májusában az IBM (International Business Machines Corporation) és az MIT (Massachusetts Institute of Technology) *Physics of Computation Conference* címmel szervezett egy háromnapos konferenciát, amelyen közel hat-

van fizikus és számításelmélettel foglalkozó szakember találkozott. Az itt elhangzott előadások 1982-ben jelentek meg egy folyóiratban, így a *kvantumszámítógép* kifejezés megjelenése az 1981-es és 1982-es évszámhoz is köthető (Feynman, 1982). A kvantum-elektrodinamika területén végzett munkásságért 1965-ben Nobel-díjban részesült Richard Feynman ugyanis ezen a konferencián előadásában azt a kérdést feszegette, hogy lehetséges-e a fizikai rendszereket számítógépen szimulálni. Feynman kérdése lavinát indított el, és egyre többen kezdtek el kvantummechanikán alapuló informatikával, azaz kvantuminformatikával foglalkozni.

David Deutsch 1985-ben megalkotta az univerzális – számítási sebességét és kapacitását tekintve a hagyományos (kvantumos nézőpontból klasszikusnak nevezett) számítógépekhez képest jóval gyorsabb – kvantumszámítógép elvét (Deutsch, 1985). A következő évtizedben pedig az univerzális kvantumszámítógépen futtatható több algoritmus is született. Deutsch és Richard Jozsa 1992-ben bemutatott egy olyan problémát, amelynek megoldása klasszikus algoritmusok számára nehéz, az általuk javasolt kvantumalgoritmus azonban gyorsan megoldja (Deutsch–Jozsa, 1992). Ethan Bernstein és Umesh Vazirani 1997-ben javasolt egy olyan algoritmust, amely a Deutsch–Jozsa-algoritmus kiterjesztésének tekinthető (Bernstein–Vazirani, 1997). Lov Kumar Grover pedig egy évvel korábban mutatta meg, hogy kvantumalgoritmus segítségével hatékonyan tudunk keresni rendezetlen adatbázisban (Grover, 1996). De az 1990-es évek legjelentősebb hatást gyakorló kvantumalgoritmusa talán Peter Shor nevéhez köthető, aki 1994-ben a faktorizációs problémát rendkeresésre visszavezetve megalkotott egy olyan algoritmust, amelynek segítségével nagyon gyorsan el tudjuk készíteni egy szám prímtényezős felbontását (Shor, 1997). Napjaink biztonsági megoldásainak egy része azonban pont azon alapul, hogy ha két nagyon nagy prímszámot összeszorzunk, akkor a kapott szám klasszikus számítógépek segítségével csak nagyon lassan bontható prímtényezőire. Shor algoritmusa a mai napig fenyegetést jelent az úgynevezett aszimmetrikus kulcsú titkosítást használó protokollokra, lévén a titkosításul használt kulcs hosszának logaritmusával arányos lépésben lehet azokat feltörni. De természetesen a kvantumszámítógépeket még számtalan más területen használhatjuk, kutatva olyan tudományos és ipari problémák megoldását, amelyek még a szuperszámítógépek számára is nehézséget jelentenek. Felhasználhatóak például új gyógyszerek felfedezésére, vállalati kockázatelemzésre, tengeri logisztika optimalizálására és még számos helyen.

Kutatóintézetek mellett a világon már több cég is készített kvantumszámítógépet, különböző architektúrákra (például szupravezető kvantumbitekre, fotonalapú kvantumbitekre) alapozva. Az IBM ráadásul 2017-től az interneten mindenki számára ingyenesen elérhetővé tette a saját kvantumszámítógépét. A jelenleg IBM Quantumnak nevezett környezetben akár grafikus, akár parancssoros felület segítségével lehet különböző programokat fejleszteni, és azokat egy működő kvantumszámítógépen futtatni.

A KVANTUMKOMMUNIKÁCIÓ KEZDETEI

A már említett, 1981-es konferenciának több neves résztvevője is volt, többek között Charles Bennett, a kvantumkommunikáció atyja. 1984-ben szerzőtársával, Gilles Brassarddal együtt publikáltak egy olyan kvantumkriptográfiai megoldást, amely biztonságos kommunikációt tesz lehetővé távoli felek között (Bennett–Brassard, 1984). Az ötletük a kvantumfizika számos elemét felhasználta, többek között azt is, hogy a nincs másolás tétel (No Cloning Theorem) miatt ismeretlen kvantumállapotról nem tudunk másolatot készíteni. Utóbbi miatt egy támadó nem tudja észrevétlenül lehallgatni a kvantumkulcscserét, ugyanis a támadó megjelenése zajt visz a rendszerbe, így a kommunikáló felek a zajszint megemelkedéséből értesülnek a támadó jelenlétéről.

A BB84-nek nevezett protokoll a világ első kvantumalapú kulcscsere (angolul *quantum key distribution,* innen a QKD rövidítés) protokollja lett, amelyet azóta továbbiak követtek. 1991-ben Artur Ekert egy összefonódáson alapuló QKD-protokollt ismertetett, amelyet aztán E91-protokollnak neveztek el. Bár Zeilinger neve sokak számára a kvantumteleportáció első sikeres kísérletével fonódott összsze, az ő csoportja volt az első, amely a gyakorlatban valósította meg az összefonódáson alapuló kulcsszétosztást – 1998-ban elvégezve egy sikeres kísérletet, amelyet aztán 2000-ben publikáltak folyóiratban. (Még egy zárójeles megjegyzés: Bennett 1993-ban az egyik szerzője volt annak a kvantumteleportációs protokollnak, amelyet 1997-ben Zeilinger sikeresen demonstrált.)

A QKD segítségével biztonságos módon tudunk megosztani egy klasszikus bitsorozatot két távoli fél között. Ezt a bitsorozatot aztán a felek fel tudják használni arra, hogy olyan titkosítási algoritmusokat használjanak, amelyek a kvantumszámítógépek számára is feltörhetetlenek. Az egyik ilyen például a One-Time-Pad, amelynek során a titkosítandó üzenet minden egyes bitjéhez hozzáadjuk a titkosítási kulcs egy-egy bitjét. Matematikailag bizonyított, hogy ha kulcs elegendően hosszú, és egy kulcsbitet csak egyszer használunk fel, akkor a titkosítás feltörhetetlen. Nem véletlen, hogy mind a BB84-es, mind az E91-es protokoll továbbfejlesztéséből olyan megoldások születtek, amelyeket különböző gyártók kereskedelmi gyakorlatba ültettek át, így napjainkra pár százezer eurós összegért már kereskedelmi forgalomban kapható QKD-berendezések érhetőek el.

A KVANTUMINTERNET FELÉ VEZETŐ ÚTON

A világ különböző pontjain működő kvantumszámítógépeket előbb-utóbb érdemes lehet összekapcsolni egymással, és ebben is kulcsszerepet fog játszani az összefonódás. A korábban már említett No Cloning Theorem miatt sajnos egy kvantumhálózat kialakítása azért nem egyszerű feladat, mert a kvantumbiteket

hordozó fotonokon nem tudunk erősítést végrehajtani, így azok – annak az optikai szálnak a tulajdonságaitól függően, amin haladnak – 30–50–80 kilométer után már akkora csillapítást szenvednek, hogy nem tudjuk detektálni. Ahhoz, hogy a jövőben kvantuminternetet hozhassunk létre, szükségünk lesz kvantummemóriákra (összefonódást használnak a működésükhöz), illetve többek között egy összefonódás-megosztás (angolul *entanglement swapping*) nevű protokollra. Kvantum-információelméleti mélységet mellőző összefoglalója ennek a következő: Létrehozunk A és B pont között egy összefonódott fotonpárt, majd létrehozunk egy másik összefonódott fotonpárt B és C pont között. Az összefonódás megosztása segítségével azt tudjuk elérni, hogy A és C pontok között legyen egy összefonódott fotonpárunk. Miért hasznos ez? Mert ha a pontpárok közötti távolság mondjuk 50-50 kilométer, akkor a végén A és C közötti 100 kilométeres távolságban lesz egy megosztott összefonódott fotonpárunk. Ha újabb pontok bevonásával folytatjuk ezt az elvet, akkor egyre nagyobb távolságokat tudunk áthidalni – ezért ez a protokoll a kvantuminternet rendkívül fontos építőeleme. S itt ismét visszajutunk Zeilingerhez, ugyanis az összefonódás-megosztás első sikeres kísérlete is az ő nevéhez fűződik.

HAZAI KUTATÁSOK

A kvantuminformatika hazai kutatói is több irányból jutottak el erre a tudományterületre. Matematikai oldalról Petz Dénes (Budapesti Műszaki és Gazdaságtudományi Egyetem, BME) munkássága nemzetközi viszonylatban is meghatározó, a kvantumentrópiáról szóló legjelentősebb monográfia szerzője. Elméleti fizikai oldalról Diósi Lajos eredményei kiemelkedőek, nevéhez fűződik például a Diósi–Penrose-modell, a kvantummechanikai mérés problémájának egy lehetséges megoldása. Az utóbbi években több kiemelkedő elméleti eredmény született, amelyek többek közt Vértesi Tamás (ATOMKI), Zimborás Zoltán (Wigner Részecske- és Magfizikai Intézet, RMI), Tóth Géza (Wigner Szilárdtestfizikai és Optikai Intézet, SZFI), Kiss Tamás (Wigner SZFI) kutatócsoportjaihoz kötődnek. A kísérleti áttörést azonban, mint a Nobel-díj odaítélése is mutatja, a fény használata, vagyis a kvantumoptika hozta. Ezen a területen fontos, hogy Magyarországon a kristályfizikának az 1930-as évekre visszanyúló hagyományai vannak. A nemlináris optikai kristályok alkalmasak nemklasszikus állapotú fény, így például összefonódott fotonpárok előállítására. Az 1975-ben alapított Gyulai–Tarján-féle kristályfizikai iskola, a Kristályfizikai Kutatólaboratórium (később a Wigner Fizikai Kutatóközpont része) tevékenysége pedig biztosította ezek előállítását – többek között Zeilinger is használt itt előállított BBO-kristályokat. Innen nőtt ki később a Janszky József vezette, nemzetközileg is elismertté vált kvantumoptikai csoport. Az elméleti kvantumoptika terén Benedict Mihály szegedi tudományos iskolája

szintén kiemelkedő, illetve a korábbi KFKI-ban (Központi Fizikai Kutatóintézet, jelenleg Wigner Fizikai Kutatóközpont, FK) dolgozó Varró Sándor munkássága említendő.

A Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Karán Imre Sándor vezetésével közel húsz éve foglalkoznak kvantuminformatikai és kvantumkommunikációs kutatásokkal, vezetékes és szabadtéri kvantumkommunikációs rendszerek fejlesztésével. A hazai kvantumtechnológiai fejlesztéseknek nagy lökést adott a magyar állam támogatásával 2017 novemberében elindult, négyéves nemzeti kvantumtechnológiai program. A HunQuTech konzorciumot a Wigner FK vezetésével a Budapesti Műszaki és Gazdaságtudományi Egyetem, az Eötvös Loránd Tudományegyetem (ELTE), a Bonn Hungary Electronics, Ericsson Magyarország, a Femtonics és a Nokia Bell Labs alkotta, és a kutatók négy év során kvantumbitek létrehozásával, kvantumszámítógépen futtatható algoritmusok megalkotásával és kvantumkommunikációs rendszerek megépítésével foglalkoztak.

A program folytatásaként 2020 októberében létrejött a Kvantuminformatika Nemzeti Laboratórium a BME, az ELTE és a Wigner partnerségével, amely Domokos Péter (Wigner SZFI) vezetésével a 2020–2025 közötti időszakra három stratégiai célt tűzött ki maga elé: „Regionális kvantumkommunikációs hálózat létrehozása", „Fotonokon, atomokon és mesterséges atomokon alapuló hardverkomponensek fejlesztése", „Kvantumszámításban élvonalbeli tudással rendelkező hazai szakértelem felépítése". 2021-re a BME Természettudományi Karának kutatói többek között összefonódott fotonforrást építettek, 2022 áprilisában pedig a BME Villamosmérnöki és Informatikai Kar kutatói az országban elsőként demonstrálták saját fejlesztésű hardverrel és szoftverrel a kvantumalapú kulcsszétosztást a Magyar Telekom élő hálózatán. 2022. május végén a BME kutatói egy több mint 20 kilométeres távolságú, hazai QKD-rekordot is felállítottak – a sikeres demonstrációban jelen cikk szerzői is aktívan részt vettek.

KÖSZÖNETNYILVÁNÍTÁS

Kis Zsolt köszönetét fejezi ki kollégájának, Corradi Gábornak a kézirat átolvasásáért és kritikai megjegyzéseiért.

IRODALOM

Aspect, A – Grangier, P. – Roger, G. (1982): Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. *Physical Review Letters,* 49, 91–94. DOI: 10.1103/PhysRevLett.49.91, https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.49.91

Bell, J. S. (1964): On the Einstein Podolsky Rosen Paradox. *Physics,* 1, 195–200. https://cds.cern.ch/record/111654/files/vol1p195-200_001.pdf

Bennett, C. H. – Brassard, G. (1984): Quantum Cryptography: Public Key Distribution and Coin Tossing. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing,* Bangalore, India, 10–12 December 1984, 175–179. https://arxiv.org/abs/2003.06557

Bernstein, E. – Vazirani, U. (1997): Quantum Complexity Theory. *SIAM Journal on Computing,* 26, 5, 1411–1473. DOI: 10.1137/S0097539796300921

Bohm, D. (1952): A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I. *Physical Review,* 85, 166–179. https://quantum.country/assets4/Bohm1952.pdf

Bohm, D. – Aharonov, Y. (1957): Discussion and Experimental Proof for the Paradox of Einstein, Rosen, and Podolsky. *Physical Review,* 108, 1070–1076. http://www.physics.drexel.edu/~bob/Entanglement/Bohm_Aharonov_EPR.pdf

Bohr, N. (1935): Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review,* 48, 696–702. DOI: 10.1103/PhysRev.47.777, https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777

Bouwmeester, D. et al. (1997): Experimental Quantum Teleportation. *Nature,* 390, 575–579. DOI: 10.1038/37539, https://www.nature.com/articles/37539

Clauser, J. F. et al. (1969): Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters,* 23, 880–884. DOI: 10.1103/PhysRevLett.23.880, https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.23.880

Deutsch, D. (1985): Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London A,* 400, 1818, 97–117. DOI: 10.1098/rspa.1985.0070, https://www.cs.princeton.edu/courses/archive/fall04/cos576/papers/deutsch85.pdf

Deutsch, D. – Jozsa, R. (1992): Rapid Solutions of Problems by Quantum Computation. *Proceedings of the Royal Society of London A,* 439, 1907, 553–558. DOI: 10.1098/rspa.1992.0167, https://www.isical.ac.in/~rcbose/internship/lectures2016/rt08deutschjozsa.pdf

Einstein, A. – Podolsky, B. – Rosen, N. (1935): Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review,* 47, 777–780. DOI: 10.1103/PhysRev.47.777, https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777

Feynman, R. P. (1982): Simulating Physics with Computers. *International Journal of Theoretical Physics,* 21, 467–488. DOI: 10.1007/BF02650179, https://s2.smu.edu/~mitch/class/5395/papers/feynman-quantum-1981.pdf

Freedman, S. J. – Clauser, J. F. (1972): Experimental Test of Local Hidden-Variable Theories. *Physical Review Letters,* 28, 938–941. DOI: 10.1103/PhysRevLett.28.938, https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.28.938

Grover, L. K. (1996): A Fast Quantum Mechanical Algorithm for Database Search. In: *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, Philadelphia, Pennsylvania USA, May 22–24, 1996. New York: Association for Computing Machinery, 212–219. DOI: 10.1145/237814.237866, https://dl.acm.org/doi/10.1145/237814.237866

Kwiat, P. G. et al. (1995): New High-Intensity Source of Polarization-Entangled Photon Pairs. *Physical Review Letters,* 75, 4337–4340. DOI: 10.1103/PhysRevLett.75.4337, https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.75.4337

Mattle, K. et al. (1996): Dense Coding in Experimental Quantum Communication. *Physical Review Letters,* 76, 4656–4659. DOI: 10.1103/PhysRevLett.76.4656, https://www.kth.se/social/files/5cacafd256be5b729eed1c1b/Quantum%20Dense%20Coding.pdf

Shor, P. (1997): Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Scientific & Statistical Computing,* 26, 1484–1509. DOI: 10.1137/S0097539795293172, https://arxiv.org/pdf/quant-ph/9508027.pdf