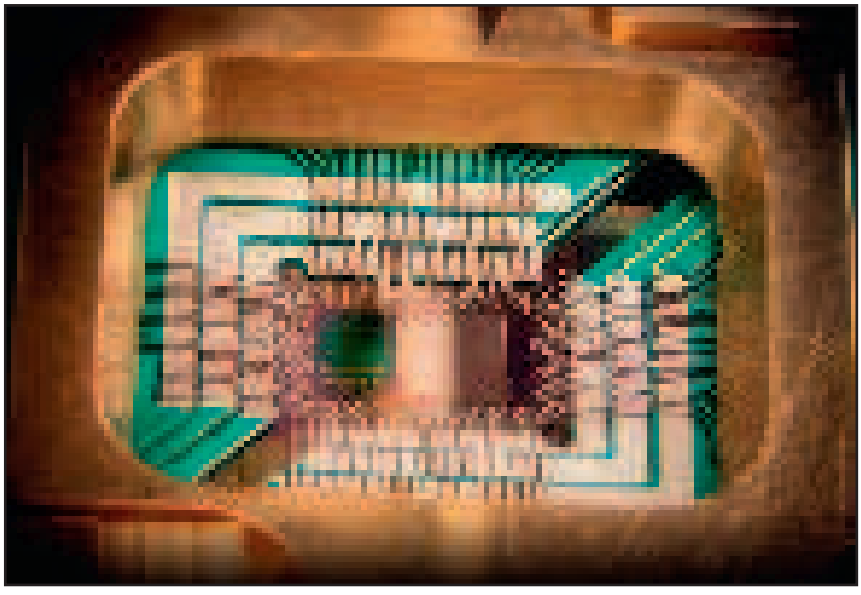
BACSÁRDI LÁSZLÓ – IMRE SÁNDOR

Kommunikáció mélyben és magasban

Faktorizáció, keresés adatbázisokban, véletlenszámok generálása, műveletek párhuzamosítása, kulcsszétosztás. Mindezek olyan informatikai fogalmak, amelyek megvalósítása hatalmas számítási kapacitást vagy különböző trükköket igényel napjaink számítógépeivel. De ha segítségül hívjuk a kvantummechanikát, akkor meglepően gyorsan és hatékonyan megbirkózhatunk a kapcsolódó feladatokkal.

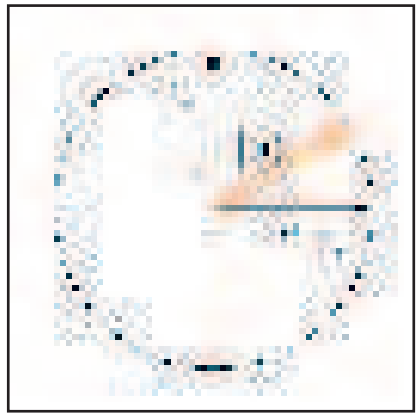
A kvantummechanika nem csak a matematika és a fizika számára érdekes, az informatikában is megjelent. Azokat a jelenségeket, amelyek még Einsteint is megdöbbentették, fel tudjuk használni ahhoz, hogy olyan kvantum alapú algoritmusokat alkossunk, amelyek a hagyományos társaikhoz képest hatékonyabban (gyorsabban, kevesebb művelettel) oldanak meg számításelméleti feladatokat, és biztonságosabbá teszik a kommunikációt. 1985-ben a brit-izraeli *Deutsch* publikálta először a kvantumszámítógép elméleti leírását. Jelenleg a kanadai D-Wave System cég terméke, a D-Wave One a legfejlettebb kereskedelmi forgalomban is kapható kvantumgép. A 2011 májusában elkészült gép egy 128 kvantumbites processzort használ (lásd **1. ábra**), amely tárolásához egy tíz négyzetméteres, meglehetősen hidegre hűtött (-150 Celsius-fok alatti) szobát használnak, bizonyos kvantumműveletek elvégzéséhez pedig abszolút nulla közeli hőmérséklet szükséges. Informatikai biztonsági területen pedig három másik cég (az 1999-ben alapított amerikai MagiQ Technologies, a 2001-ben egyetemi spin-off cégként alakult svájci id Quantique és az ausztrál QuintessenceLabs) kínál kereskedelmi forgalomban kapható termékeket. De nézzük meg, milyen előnyei vannak a kvantuminformatikának.

1. ábra. A kanadai D-Wave cég egy kvantumprocesszora *(Forrás: Wikipedia)*



Kvantummechanikai alapokon

Sok ember számára a kvantummechanika szó régi, homályos emlékeket jelent, bonyolult egyenletekkel és matematikai

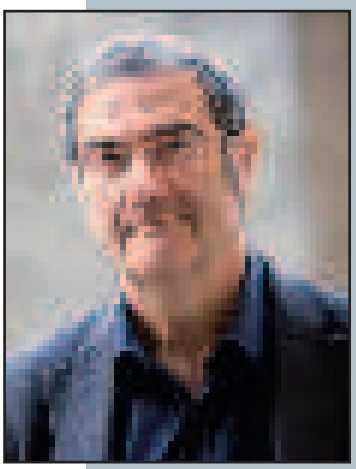


2. ábra. Kvantumbit szemléltetése a Descartes-féle koordinátarendszer segítségével. A vízszintes tengelyen a „ket nulla”, a függőlegesen a „ket egyes” bázisállapot található. A narancssárgával jelölt vektor az ismeretlen állapotú kvantumbit, amelyet az *a* és *b* komplex valószínűségi amplitúdóval jellemezhetünk

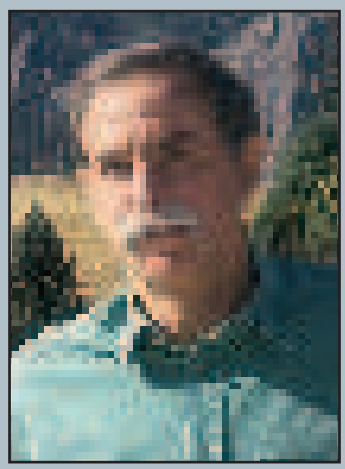
műveletekkel. Mi mérnökként az alkalmazás és alkalmazhatóság oldaláról közelítjük meg ezt a területet, és a *Schrödinger-egyenletek* által leírt világot négy kvantummechanikai posztulátumra helyezzük [1]. (Innentől kezdve a mindennapi világra klasszikus világként és klasszikus informatikaként fogunk hivatkozni.) Ezek olyan alapfeltevések, amelyeket nem bizonyítunk (nemcsak itt a cikkben, hanem egyébként sem), de később minden kapcsolódó levezetésben felhasználunk. Az első a rendszer állapotát írja le, a második az időbeli fejlődésre vonatkozik, és abban segít, hogy a teljes rendszer viselkedését zárt transzformációkkal tudjuk leírni. A harmadik a mérésre vonatkozik, és definiálja a kapcsolatot a kvantumvilág és a

Nobel-díj a kvantumszámítógép felé vezető úton

A fizikai Nobel-díjat megosztva kapta 2012-ben a francia *Serge Haroche* és az amerikai *David J. Wineland* az önálló kvantumrendszerek mérésével és manipulálásával kapcsolatos módszerek kidolgozásáért.



Serge Haroche



David Wineland

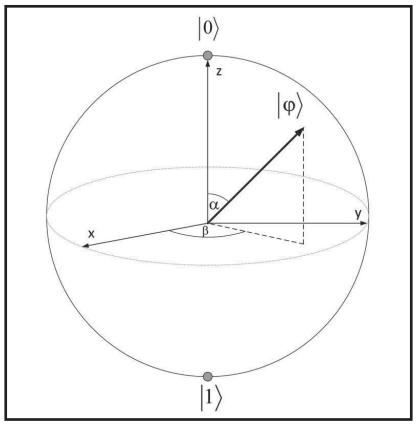
A két kitüntetettben közös, hogy mindketten 1944-ben születtek és elismert kvantumfizikusok. Serge Haroche, a College de France professzora, a Párizsban található intézmény jelenlegi vezetője. A Francia, az Európai és az Amerikai Fizikai Társaság tagja, a Nobel-díj előtt több kutatói díjjal kitüntették, többek között a legrangosabb francia tudományos elismeréssel, a CNRS (French National Centre for Scientific Research) aranymedáljával. Az amerikai David J. Wineland tanulmányait a Kaliforniai Egyetemen végezte Berkeley-ben, doktori disszertációját a Harvardon írta. A National Institute of Standards and Technology (NIST) kutatója.

A kvantumszámítógépek hátterében álló kvantuminformatikával kapcsolatban az elmúlt harminc évben sok publikáció látott napvilágot. Nagyon sok elméleti algoritmust ismerünk a területen, több algoritmus működését laboratóriumi körülmények között és azon túl is igazolták, és vannak már kereskedelmi forgalomban kapható kvantumeszközök is. A működő kvantumszámítógép megépítéséhez azonban még hosszú út vár a fizikusokra és a mérnökökre. Ahhoz, hogy előbb-utóbb kvantumszámítógépeket készíthessünk, kvantumbitekre és ezekből felépített zárt kvantumrendszerekre van szükségünk, amelyeket a környezet hatásaitól elszigetelhetünk, de mégis megfigyelhetünk és módosíthatunk. Nehéz ennek a két, egymásnak ellentmondó feltételnek (környezettől elszigetelt, de adatbevitelkor és adatkiolvasáskor mégis a környezettel kapcsolatba lépő) megfelelő rendszert létrehozni. A 2012. évi fizikai Nobel-díjasok jelentős előrelépést értek el ezen a területen.

A lézerfizikából született kvantumoptika a fény és az anyag kölcsönhatását vizsgálja, Magyarországon ilyen jellegű kutatómunkával az MTA Wigner Fizikai Kutatóközpont Szilárdtestfizikai és Optikai Intézetében foglalkoznak. Kvantumoptikai kutatást végzett a két 2012-es kitüntetett is. Serge Haroche egy úgynevezett fotoncsapdát hozott létre. Kísérleti berendezésében szupravezető anyagból készült, az abszolút nulla fok közeli hőmérsékletre lehűtött tükrök között mikrohullámú fotonok oda-vissza pattogva több ezer kilométert tettek meg, és a másodperc tizedrészéig megőrizték a hullámmozgásban tárolt információt. Ez az emberi mértékben rövid időpillanat kvantumfizikai szemmel nézve nagyon hosszú időnek tekinthető. Ez alatt az időtartam alatt megfelelően előkészített atomokat küldött át a francia kutató a fotoncsapdán, az atomok állapotváltozásainak a méréséből pedig következtetni tudtak a fotonok állapotváltozására, vagyis ki tudta olvasni azok értékét.

David Wineland egy másik módszert alkalmazva ioncsapdával dolgozott: ionokat tartott fogva elektromágneses mezőben. Az ioncsapdában tartott ionokra nem hat a külső környezet hőmérséklete és sugárzása, a csapdában tartott ionok energiaállapotát pedig lézer segítségével változtatják meg, ezáltal kódolva információt akár az ionok rezgő mozgásába, akár a színképükbe. Winelandnek az ioncsapdával való kutatásai során sikerült kétfelé terelni egy rezgő ion anyaghullámát, majd kutatócsoportjával több bites kvantumműveleteket is el tudtak végezni. Mindkét kitüntetett kutató munkája sokat ígérő lépéseket jelent a működő kvantumszámítógép felé vezető úton. Wineland kutatási eredményeit – egyfajta mellékterméként – a jelenleginél pontosabb atomórák készítéséhez is fel lehet használni.

BACSÁRDI LÁSZLÓ



3. ábra. A kvantumbit szemléltetése a Bloch-gömbön. A vastagon jelölt vektor az ismeretlen állapotú kvantumbit

4. ábra. A kvantumbit szemléltetése fraktál alapú megközelítés segítségével. A fekete sávrész a 0 értékhez, a fehér az 1-hez tartozik. A sávrészek szélessége a mérési valószínűséget, a rajtuk elhelyezett vízszintes vonal magassága a fázist jelöli

klasszikus világ között, a negyedik pedig az összetett rendszerekre vonatkozik [1].

Az első posztulátum lehetővé teszi, hogy bevezessük a kvantumbit fogalmát (angolul quantum bit vagy qubit), amely a kvantuminformatika alapvető információs egysége. Míg a klasszikus bit esetében két jól meghatározott értékről beszélünk (0 és 1), addig a kvantumbit az előző két alapállapot tetszőleges kombinációjában (ún. szuperpozíciójában) létezhet, azaz végtelen sok állapotban lehet. Amikor azonban végrehajtjuk a mérést, akkor egy klasszikus 0 vagy 1 értéket kapunk vissza. A kvantumbitet a bázisállapotaival és komplex valószínűségi amplitúdóival adjuk meg, az alábbi módon:

$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

ahol az a és b olyan komplex számok, amelyek abszolútérték-négyzete egyet ad. Az a és b valószínűségi amplitúdó abszolútértékének négyzete azt mutatja meg, mekkora valószínűséggel mérünk 0-t illetve 1-et (innen származik a valószínűségi amplitúdó elnevezés). A fenti zárójelezést a *Dirac-jelölést* követve használjuk, és a fenti kvantumbitet „ket fi”-nek ejtjük (és

ehhez hasonlóan, „ket nulláról” és „ket egyről” beszélünk). A $|\varphi\rangle = 0{,}6|0\rangle - 0{,}8|1\rangle$ kvantumbitről például tudjuk, hogy 0,36 valószínűséggel 0-át kapunk a mérés végén, 0,64 valószínűséggel pedig 1-et. Mivel egységnyi hosszú vektorokról beszélünk, a legegyszerűbb egy Descartes-féle koordinátarendszerben körként elképzelni a kvantumbitet, a körvonal tetszőleges pontja lehet a bitünk értéke. (Ez a kétdimenziós kvantumbit, de tudjuk definiálni magasabb dimenziókra is.) A két tengely pedig a két bázisállapot, a „ket nulla” és a „ket egy”. Természetesen a körvonal csak egy geometriai megfeleltetés, ha szeretnénk, akkor *Felix Bloch* nyomán akár a *Bloch-gömbön* is ábrázolhatjuk a kvantumbitet (ekkor a gömb felületén vehet fel tetszőleges értéket). Egy fiatal magyar fizikushallgató, *Galambos Máté* pedig nemrég fraktál alapú reprezentációt készített, munkájával első helyezést ért el a BME Villamosmérnöki és Informatikai Kar Tudományos Diákköri Konferenciáján [2]. Az **2., 3.** és **4. ábrán** különböző reprezentációkat tüntettük fel.

Fizikailag kvantumbit lehet bármilyen két jól megkülönböztethető állapottal rendelkező kvantumrendszer (pl. elektron spinállapotai, atomi hiperfinom állapotok stb.), a kommunikáció területén a foton különböző polarizációs állapotait (vízszintes, függőleges) feleltethetjük meg a bázisállapotoknak.

A mérési posztulátum egyrészt rámutat arra, hogy a mérőműszerünk csak valamekkora valószínűséggel mutatja a mérés végeredményét. Ha a valós világban ráállunk egy mérlegre, biztosak lehetünk abban, hogy újra és újra megismételve, ráállva a mérlegre ugyanazt az értéket mérjük (kivéve, ha közben elfogyasztottunk egy bőséges vacsorát), és valóban a testsúlyunkat mutatja. A kvantummérlegre ráállva nem lehetünk biztosak abban, hogy a megjelenő hatalmas szám valóban a sok elfogyasztott süteményt tükrözi, vagy éppen nem a helyes értéket látjuk. De ez a posztulátum még egy érdekességet tartogat: a mérés hat a teljes rendszerre, és megváltoztatja annak állapotát. Vagyis azáltal, hogy ráállunk a mérlegre, megváltozunk mi magunk és a mérleg is. Mindezek alapján leszögezhetjük, hogy egy-egy mérési elrendezés megtervezése különösen fontos a kvantuminformatikában. Ha roszszul választjuk ki a mérési operátorokat (vagyis rosszul állítjuk be a mérőműszert), akkor könnyen előfordulhat, hogy nem értelmezhető eredményt kapunk. Szerencsére jól bevált receptek állnak rendelkezésünkre, mint például a projektív mérés (más néven *Neumann-mérés*) vagy a pozitív operátor értékű mérés (az angol positive-operator valued measure elnevezés rövidítéséből POVM).

A kvantumbitek állapotait egyetlen rendszerré egyesítve több bites kvantumregisztereket tudunk készíteni. Ahhoz, hogy kvantumáramkörökről beszéljünk, a mérést elvégző mérőműszerek mellett még kvantumkapukra van szükségünk. Ezek a kvantumkapuk a kvantumrendszert egyik állapotából egy kiválasztott másikba viszik át. Ennek megfelelően az állapot időfejlődését szabályozó második posztulátum segítségével írhatóak le. Ezek a speciális időfejlesztési lépések valamilyen geometriai transzformációt hajtanak végre a bemeneti kvantumbit állapotát jellemző vektoron. Tudjuk a kvantumbitet forgatni, tükrözni, negálni és még nagyon sok más műveletet is elvégezhetünk [3].

Összefonódás

A negyedik posztulátum az összetett rendszerek részrendszereinek állapotára vonatkozó leírást adja, amelynek következményei közül az összefonódás sokáig a fizikusok előtt is rejtélyes volt. Ha szeretnénk egy ismerősünk előtt rávilágítani erre, vázoljuk fel neki az alábbi gondolatkísérletet. (Szigorúan csak elméletben, ezért ne gyűjtsük össze a kóbor állatokat!) Vegyünk egy nagy dobozt, amelyet tökéletesen elszigetelünk a külvilágtól, egy zárt rendszert alkotva. Tegyünk bele egy élő macskát, egy radioaktív készítményt, egy Geiger–Müller-számlálót, egy kalapácsot, és egy méregfiolát. A radioaktív izotóp vagy kibocsát egy alfa-részecskét, vagy nem. Ha igen, akkor a számláló jelez és leengedi a kalapácsot, amely összetöri a méregfiolát, a macska pedig meghal. Kérdezzük meg ismerősünktől, hogy szerinte a macska élő vagy holt állapotban van a teljesen zárt dobozban. Mivel a macska élő / nem élő állapota összefonódott a bomló atom elbomlott / nem bomlott el állapotával, ezért bizony egyszerre van élő és holt állapotban szegény állat a Nobel-díjas osztrák fizikus, *Schrödinger* által 1935-ben felvázolt gondolatkísérletben (**5. ábra**). Ha kinyitom a dobozt (végrehajtok egy mérést), akkor azonban egyértelműen látni fogom, hogy a macska él-e még vagy halott - de egészen odáig élőhalott állapotban létezik. A doboz kinyitásával a macska gyilkosává válunk? Vagy csak választunk egyet a párhuzamos világegyetemek közül? Vagy értelmetlen ebben a formában feszegetni ezt a kérdést? A kvantummechanika különböző iskolái más-más választ kínálnak [4].

5. ábra. Gondolatkísérlet Schrödinger különleges macskájával. *(Forrás: Wikipedia)*

1935-ben Einstein annak a meggyőződésének adott hangot, hogy a kvantummechanika elmélete nem teljes, további rejtett változók léteznek. Elég sok időnek el kellett telnie, amíg sikerült kísérletileg is megmutatni, hogy az összefonódásból származó, alább bemutatandó korrelált viselkedés valóban létezik, és a kvantumrendszerek másképp viselkednek, mint az Einstein követői által kidolgozott rejtett paraméteres elméletek. Az összefonódott állapotokat *Einstein*, *Podolsky* és *Rosen* által 1935-ben írt cikk nyomán EPR-pároknak, a kétbites összefonódottakat pedig Bell-pároknak nevezünk az ír fizikus által 1964-ben publikált egyenlőtlenségek előtt tisztelegve. De mi is az az összefonódás (angol szakszóval entanglement)?

Összefonódásról akkor beszélünk, amikor különböző részecskék (fotonok, elektronok, de akár apró gyémántok is) kapcsolatba lépnek egymással, és miután szétválnak, a közöttük lévő kapcsolat eredményeként állapotuk egyetlen korrelált kvantummechanikai állapottal írható le. A legegyszerűbb összefont állapotban a pár kétállapotú tagjai minden időpillanatban ugyanabban (vagy éppen az „ellentétes” kiegészítő) állapotban vannak, függetlenül a közöttük lévő távolságtól. Ha

a Marsra augusztusban leszállt Curiosity elvitte volna magával a Földről egy bizonyos összefonódott qubit-pár egy tagját, míg a pár másik fele a NASA Sugárhajtás Laboratóriumában (JPL) maradt volna, akkor azt követően, hogy a Curiosity megméri a Marson a pár nála lévő felét, a bármikor később elvégzett mérés során a JPL-nél ugyanazt a mérési értéket kapják a kutatók. Ha a Marson nullát mutat a mérőműszer, akkor függetlenül a két bolygó távolságától és a fénysebességgel kapcsolatos megkötésektől, itt a Földön minden statisztikus szórás nélkül ugyanazt az értéket mutatja a mérőműszer. Természetesen vihetett volna magával olyan összefonódott qubit-párt, amelynél az egyik oldalon nullát mérve a másik oldalon biztosan egyet kapunk, de a lényeg az összefonódáson van. Fénysebességnél gyorsabb kommunikációra azonban nem használhatjuk, mert bármelyik qubit-tagon elvégzett mérés eredménye önmagában teljesen véletlenszerű. Vagyis nem tud a földi pár viselkedését egyértelműen irányító információt küldeni a marsi rover, mert nem tudja befolyásolni, hogy nullát vagy egyest mérjen a mérőműszere – de ettől még nagyon sok mindenre fel tudjuk használni ezt a jelenséget. Például használhatjuk véletlenszám-generátorként, amelyre bizony nagyon sok informatikai eljárásnál szükség van. 2004-ben a világ első olyan banki tranzakcióját valósították meg Bécsben, ahol az összefonódás segítségével állították elő a titkosításhoz szükséges véletlenszámokat. Továbbá nemcsak összefonódott párokról beszélhetünk, hanem további tagokat is hozzáfonódtatva a rendszerhez létre tudunk hozni összefonódott hármasokat, négyeseket és így tovább.

Lehetséges kvantuminformatikai alkalmazások

A kommunikáció során két fél továbbít egymásnak üzeneteket egy kommunikációs csatornán, és mindezt úgy, hogy mindez minél hatékonyabban és biztonságosabban történjen. Miután a felek megosztoztak az összefonódott párokon, a *Bennett* és *Wiesner* által 1992-ben leírt szupersűrűségű algoritmussal, egy kvantumbit segítségével két klasszikus bitnyi információt tudnak átküldeni a kommunikációs csatornán. (Az algoritmusnak klasszikus esetben két bitet kellene átküldenie, kvantumosan csak egy kvantumbit kerül átküldésre, innen a szupersűrű elnevezés.) A kvantumteleportáció során előre megosztott összefonódott pár használatával egy kvantumbitet teleportálunk úgy, hogy a csatornán csak két klasszikus bitet küldünk át. Meghökkentő? Bizony, a teleportáció során mindössze két klasszikus 0 vagy 1 értéket küldünk át a kommunikáló felek között, és a fogadó fél képes előállítani a küldőnél lévő, tetszőleges állapotú kvantumbitet. A *Bennett* által 1993-ban leírt ötlet működését 1997-ben kísérletileg is igazolták, 2010-ben pedig már szabad légkörben 16 kilométeres távolságot hidaltak át vele kínai kutatók. Kvantumbitek másolására nem lehet azonban felhasználni, mert az eredeti kvantumbit megsemmisül az algoritmus során. (A teleportáció szó ellenére nincs szó fénynél gyorsabb kommunikációról, hiszen a két klasszikus bitet át kell küldenünk valahogyan, ezt pedig maximum fénysebességgel tehetjük meg.)

Nem csak a kommunikáció területén használhatunk kvantum alapú megoldásokat. Nincs szükség összefonódott párokra a *Grover* által készített algoritmusban, amely rendezetlen adatbázisban keres, a klasszikus keresőalgoritmusoknál eredményesebben. (Amíg a klasszikus megoldások a rendezetlen adatbázis elemszámával arányos lépésben találnak rá a keresett elemre, addig a Grover-algoritmus lépésszáma az elemszám gyökével arányos). Az 1996-ban publikált algoritmust 1998-ban már implementálták is. A kvantuminformatika a prímfaktorizációban is áttörést jelent. A faktorizáció során egy adott szám törzstényezős felbontását keressük, és az amerikai *Shor* megoldása kiválóan alkalmas arra, hogy nagyon nagy számok esetében is nagyon gyorsan meghatározza, melyik két prímszám szorzatából állítható el. Az informatikai biztonság területén pedig a nyilvános kulcsú titkosítás elve pont azon alapszik, hogy a faktorizáció egy lassan elvégezhető folyamat. 2009-ben egy 232 számjegyű számot klasszikus számítógépekkel próbáltak meg feltörni, a kísérletre fordított összesített gépidő 2000 év volt. Ezzel szemben a Shor-algoritmus segítségével másodpercek alatt törhetővé válik ez a szám. Azonban a gyakorlati implementációval még számos probléma van, 2009-ben még csak a 15-ös számot feltörő rendszert készítettek [5].

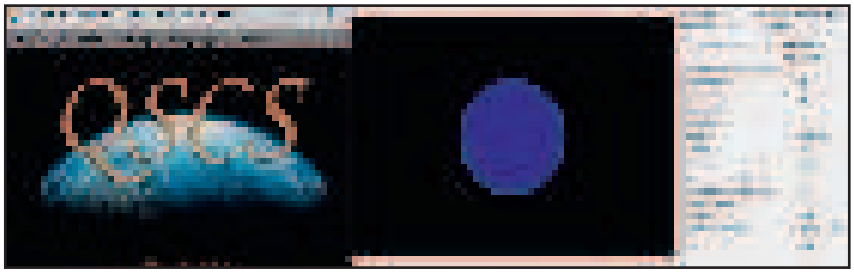
Nehézségek

A kvantummérnökök élete több okból is nehéz. A „No Cloning Theorem” értelmében egy tetszőleges állapotú kvantumbitről nem lehet tökéletes másolatot készíteni. Vagyis a bázisállapotokat (pl. a hagyományos nullának és egynek megfeleltethető kvantumbitet) tudjuk másolni, de a cikkben már többször említett tetszőleges értékű kvantumbitet már nem. Másrészt az önálló kvantumbit határozott kvantumállapotára nagyon hamar hatást gyakorol a környezete (ez a dekoherencia), így a kvantumbitek fizikai megvalósítását két, egymásnak látszólag ellenmondó szempont is nehezíti. Egyrészt szeretnénk, ha a kvantumbitek nem lépnének kapcsolatba a környezettel, másrészt azonban két kvantumbitnek egymással mégis csak interakcióba kellene lépnie. Továbbá jó lenne, ha a kvantumbitek hosszú ideig megőriznék állapotukat. Az is gond, hogy a qubitek leggyakoribb kvantumoptikai megvalósításában használt fotonpárokat nehéz egymás közelségében tartani.

Kulcsszétosztás

A szépszámú laboratóriumi kísérleti eredmények ellenére a kvantuminformatika elmélete nagyon sok területen jóval előrébb tart, mint a tényleges implementációk, ugyanakkor a biztonsági oldalon már kulcsrakész kereskedelmi termékek kaphatóak. Ahhoz, hogy a kommunikációnk biztonságos legyen, az üzeneteket titkosítani kell. A klasszikus titkosításra igaz a következő: ha mind a két fél ugyanazt a kulcsot használja a kódoláshoz és dekódoláshoz, és a kulcs hossza megegyezik az üzenet hosszával, továbbá egy kulcsot csak egyszer használnak fel, akkor a titkosítás feltörhetetlen. Ezt szimmetrikus kulcsú titkosításnak nevezzük (utalva arra, hogy a titkosításhoz és visszafejtéshez használt kulcs azonos). A kritikus kérdés csupán az, hogyan jutnak hozzá ehhez a kulcshoz a felek. Egy lehetőség, hogy személyesen találkoznak és egyeztetik, de az informatika világában ennél automatizáltabb (és költségkímélőbb) megoldásokra van szükség. Ezek a kulcsszétosztó protokollok, amelyekből nagyon sok létezik a klasszikus világban. Természetesen vigyázni kell, hogy egy támadó ne változtathassa meg a kulcsot miközben egyeztetjük, másrészt ne hallgatózhasson észrevétlenül. Hiszen, ha lehallgatja egy illetéktelen fél a kulcscserét, akkor tudni fogja az üzeneteink titkosításához használt kulcsot, és nem lesznek titkaink előtte. Ebben nyújt hatalmas segítséget a kvantum alapú kulcscsere (angol szakszóval quantum key distribution – QKD). Korábban említettük, hogy tetszőleges kvantumbit tökéletes másolása nem lehetséges, és ezt a tulajdonságot alaposan kihasználják a kvantum alapú eljárások. Egy támadó csak úgy tudja lehallgatni a kulcscsere során a kulcsot, ha a két fél közé ékelődve egyesével elkapja a kvantumbiteket, majd továbbküldi. Mivel lemásolni nem tudja magának, meg kell mérnie – a mérés azonban (amennyiben nem ismeri a bázisokat, amelyekben mérnie kell) valószínűségi alapon működik csak, így pontatlan eredményt kap, nem fogja megismerni a kulcsot. Ráadásul a támadó jelenlétéről azonnal érte-

sülnek a kommunikáló felek. Ez a *Bennett* és *Brassard* által 1984-ben publikált BB84 algoritmus alapgondolata, amelyet azóta további kulcscserélő protokollok követtek, mint például a szintén *Bennett* által 1992-ben közölt B92, az összefonódást is felhasználó E91 (*Ekert*, 1991) vagy S09 (*Serna*, 2009). BB84 esetén az eddig elért legnagyobb sebesség 1 Mbps volt 2008-ban. 2007-ben egy svájci népszámlálás adatait védték kvantum eszközökkel, míg 2008-ban egy bécsi konferencián hat pont között hoztak létre egy QKD-val védett számítógéphálózatot. A terület túlmutat az alkalmazott kutatáson is, a cikk elején említett három biztonsági cég QKD-n alapuló eszközöket kínál a kereskedelmi forgalomban.



6. ábra. A BME Híradástechnikai Tanszék és az NymE Informatikai és Gazdasági Intézet kutatóinak együttműködésében készülő műholdas kvantumkommunikáció-szimulátor kezdőképernyője (balra) és egy Föld-űr csatornára vonatkozó szimulációs eredménye (jobbra)

Műholdra fel

A jelenlegi céges kulcsszétosztó termékeknek azonban van egy nagy hátrányuk: a kvantumbiteket a foton polarizációs állapotaiba kódolják, és a kommunikációhoz optikai szálat használnak. Ez azt jelenti, hogy ha megvesszük a szükséges eszközöket, be kell szerezni pár tíz kilométernyi optikai szálat is, amellyel összekötjük a két gépet. Jelismétlőt és jelerősítőt ráadásul nem lehet elhelyezni, hiszen ismeretlen kvantumbiteket nem tudunk másolni (ezáltal erősíteni). A kutatók érdeklődése így már elég korán a szabadlégköri csatornák felé fordult. Az első szabadtéri kvantum alapú kulcsszétosztást 1991-ben hajtották végre *Bennett* vezetésével, 30 centiméteres távon. 1998-ban egy amerikai kutatócsoport elérte az 1 km-es távolságot, 2002-ben pedig a 10 kilométert. 2006-ban egy nemzetközi kutatócsoport a Kanári-szigeteken 144 kilométeres távon demonstrálta a szabadtéri kulcscsere létjogosultságát. Ezek a növekvő távolságok azt mutatják, lehetőségünk lesz kilépni a technikával a világűrbe, és akár műhold-műhold, akár Föld-űr kommunikációban alkalmazni. 2008-ban az Európai Űrügynökség a következő évek egyik legfontosabb áttörésének jelölte meg a kvantum alapú űrkommunikáció sikeres megvalósítását. Úr-űr kommunikáció esetében fontos figyelembe venni a napjainkra rendelkezésre álló ún. egyfoton források tulajdonságait és teljesítőképességét, a detektorok véges méreteit, a diffrakció miatti fókuszálási hibákat, míg Föld-műhold (illetve műhold-Föld) kommunikáció esetén az előzőekben felsoroltakon túl a légkör gázai által okozott veszteségeket, illetve a pára és a por járulékos hatásait is. A légkör alsó rétegeiben mindezek mellett jelentős veszteségeket okoznak az optikai turbulenciák. Mindenesetre a jelenlegi kutatási eredmények biztatóak, és néhány éven belül talán a gyakorlatban is sikerül megvalósítani kvantum alapú kulcsszétosztást műhold-műhold vagy műhold-Föld irányban. (A **6. ábra** egy magyar kutatók által készített szimulációs szoftvert mutat, amellyel a kvantum alapú űrkommunikációt vizsgálják.)

Magyar kutatások

Magyarországon több helyen is foglalkoznak kvantuminformatikához kapcsolódó matematikai, fizikai és mérnöki kutatással, többek között az MTA Wigner Fizikai Kutatóközpontban, a Szegedi Tudományegyetemen, és a Műegyetemen. Utóbbin a Természettudományi Karon a kvantumszámítógép fizikai leírásával és információelmélettel, a Villamosmérnöki és Informatikai Karon pedig a Számítástudományi és Információelméleti Tanszéken kvantumalgoritmusokkal foglalkoznak. A kommunikáció terén a BME Híradástechnika Tanszékén működő Mobil Kommunikáció és Kvantumtechnológiák Laboratórium munkatársai folytatnak kutatásokat (többek között jelen cikk szerzői is) kvantumcsatorna szuperaktiválása, kvantum-ismétlők (repeaterek), pilot kvantumbit alapú csatornakódolás, kvantumhálózat tervezése, kvantum alapú műholdas kommunikáció modellezése és szimulációja területén. A tanszéki kutatócsoportot egy akadémiai doktor vezeti, egy doktorjelölt és egy pár hónapja a kvantumos űrkommunikáció területén Ph.D-fokozatot szerzett fiatal kutató mellett még hallgatók és doktoranduszok vesznek részt a munkában.

Moore nyugodt álma

Gordon Moore, az Intel társalapítója 1965-ben publikált cikkében az integrált áramkörökön lévő tranzisztorok száma és a chipek mérete közötti összefüggésre mutatott rá. Állítása szerint nagyjából 18 havonta a tranzisztorok száma megduplázódik, míg a chipek mérete a felére csökken. A róla elnevezett *Moore-törvény* azóta is működik, és előrejelzése alapján előbb-utóbb el fogjuk érni azt a méretartományt, amikor a tranzisztorok mérete az atomi tartomány szintjére csökken. A klasszikus számítástechnikai elemeket megvalósító félvezető eszközök tovább nem sűríthetők, így kérdésessé válhat a Moore-törvényben megfogalmazott tendencia továbbfolytatása. De mindazok, akik kvantuminformatikával foglalkoznak, tudják, hogy ettől még továbbra is képesek leszünk számítógépeket építeni. Ekkora mérettartományban nem lesznek érvényesek a klasszikus fizikában megszokott Ebers–Moll-egyenletek, helyettük a kvantummechanika törvényeit kell alkalmazni. A kvantumszámítógép egyelőre még a távoli jövő eszköze, de működő kvantuminformatikai megoldások – különösen a kvantumkommunikáció területén – már nemcsak bíztató irányokat mutatnak, hanem kereskedelmi forgalomban is kaphatóak. Moore-nak nem kell éjjelente nyugtalanul forgolódnia, a kvantuminformatika egyre felkészültebben várja az eljövendő időszakot.

A szerzők köszönetet mondanak Patkós Andrásnak a cikk elkészítésében nyújtott segítségért.

IRODALOM:
[1] M. A. Nielsen and I. L. Chuang, „Quantum Computation and Quantum Information,” Cambridge University Press, 2000
[2] M. Galambos, S. Imre, „New Method for Representation of Multi-qubit Systems Using Fractals”. ICQNM 2011
[3] S. Imre, F. Balázs, „Quantum Computing and Communications, An Engineering Approach”, Willey, 2005
[4] John Gribbin, Schrödinger macskája - Kvantumfizika és valóság, Akkord, 2001
[5] J.A. Politi et al, „Shor's quantum factoring on a photonic chip”, Science, Vol 325, p1221, September 2009