KVANTUMINFORMÁCIÓ

A kvantummechanika megszületése nemcsak óriási ablakot nyitott a világra, de életünket megváltoztató eszközök sokaságát is adta a kezünkbe. Az anyag kis részecskéi, köztük az elektronok mozgásának hullámtermészete volt a kulcs a kristályos anyagok sávszűrő hatásának, a megengedett és tilos sávoknak felismeréséhez. Ezek nélkül nem lennének félvezető eszközeink, és nem is álmodhatnánk arról, hogy mobiltelefonon tartsunk minden eddiginél szorosabb kapcsolatot a hozzánk közelállókhoz. Alig vitatható, hogy ezektől az eszközöktől lett az átlagosan polgárosodott emberek közkincse olyan szintű kényelem és szabadság, amely százötven éve még csak a leggazdagabbaknak jutott osztályrészül. Hogy a víz egy kézmozdulatunkra jön a falból, már évtizedek óta természetesnek mondható, de az már igazán csak a mai életünknek lett alig nélkülözhető része, hogy még az oly sokat szidalmazott hírek is olyan bőségben jutnak el hozzánk, amelyben régen csak egy rendőrfőnöknek lehetett része, vagy annak sem. Az utóbbi egy-két évtizedben a kvantummechanika egy új területen kezdi ígérni életünk megváltoztatását: ez az információkezelés eszköztárának váratlan, új eszközökkel való kibővítése.

A kvantumjelenségek közös kulcsa az anyag legkisebb részeinek hullámszerű mozgása. Az elektronok nem körülrohangálják, hanem körülhullámozzák az atommagokat. A hullámok szétterjedhetnek és összetalálkozhatnak, ilyenkor erősíthetik vagy kioltathatják egymást: *interferálnak.* Mindez végtelenül sokszor változatosabb, mint egy golyócska rohangálása: nem csoda, hogy a hullámok mintázatára az élő és élettelen világ hallatlan sokfélesége épül. A kicsiny anyagrészek hullámmozgását és annak legfontosabb jelét, az interferenciát számtalan kísérlet bizonyítja, elektronoktól a náluk kétezerszer nehezebb neutronokon keresztül a többszázezerszer nehezebb óriásmolekulákig.

A kvantummechanikai információkezelés is mindenekelőtt a hullámmozgás kiaknázására épül: ha az egy bit információt alkotó *igen*t és a *nem*et két hullámformára bízzuk, például egy foton (fénykvantum) kétféle polarizációjára, vagy egy elektron kétféle *spin*jére (az is csak egy trükkösebb fajta polarizáció), akkor ezt a két komponenst különböző arányban és fázisokkal összetéve az interferencia számtalan kombinációt hoz létre. Az „igen” és „nem” ilyen, interferenciában született kombinációi alkotják együtt a *kvantumbit*et, röviden *qubit*et. Ez a kvantuminformáció alapfogalma, amelynek nevéről érdemes megjegyezni, hogy ugyanúgy mondják, mint a *cubit*et, ami a legelterjedtebb ókori mértékegységnek, a rőfnek a latin neve (angolul is így mondják); romantikusabb lelkű fizikusoknak erről az jut eszébe, hogy a qubit a minden dolgok igaz mértéke, Noé bárkájától a bankkártya kódjáig.

A qubitből önmagában még nem származna akkora nagy nyereség az információkezelésre. Az igazi szenzációt egy mélyebb kvantummechanikai tulajdonság hozza: az *összefonódás*. Ez azt jelenti, hogy az egymással kölcsönhatásba kerülő elektronok, atomok, molekulák közösen végzik hullámmozgásukat, és ezek a sok qubitnyi információt hordozó, sokrészecskés hullámok tudnak egymással interferálni. Erre aztán hallatlanul nagy teljesítőképességű algoritmusokat lehet építeni, amelyek eddig reménytelennek ítélt feladatok megoldásához foghatnak hozzá, csak legyen *kvantumszámítógép,* amelyen futnak ezek az algoritmusok.

Sajnos, itt van a dolog buktatója is. Az összefonódásba alig kivédhető kéretlen partnerként belelép az egész külvilág, és ez, mint egy óriási zajforrás, elrontja a hullámmozgás *koherenciáját*, vagyis elrontja interferenciaképességét, emiatt a nyolc-tíz qubitesnél nagyobb kvantumszámítógépek egyszerűen nem működnek.

A világban óriási versenyfutás folyik azért, hogy mégis legyenek hatékonyabb kvantumszámítógépek. A történet az egyes ionokat vagy atomokat csapdában tartó, a hőmozgás zaja ellen mély hőmérsékletekre lehűtő és a külvilágtól hatékonyan elszigetelő, szobanagyságú vákuumtechnikai eszközökkel kezdődött. Ezeket mára sikerült apró chipekre ültetni, amelyekből talán hamarosan elég sokat össze lehet kapcsolni és számítógéppé szervezni úgy, hogy egy-egy számítási feladat időtartamára megőrizhető legyen a rendszerben futó kvantummechanikai hullámmozgások koherenciája.

A chipre ültetett ion- vagy atomcsapda nem az egyetlen lehetőség: kicsiny, a mikroszkopikus és makroszkopikus határmezsgyéjén álló, divatos szóval élve *mezoszkopikus* félvezető eszközöknek többféle változata is versenyben áll azon az úton, amely az összefonódott elektronok közös hullámmozgását vezérelni képes kvantumos

Ioncsapda céljaira készült chip: a közepén látható cikk-cakk vonalban folyó áram mágneses tere tartja fogva azokat az ionokat, amelyeknek célszerűen kiválasztott energiaszintjei qubiteket alkotnak.

áramkörök megteremtése felé halad; a félvezetők ipari tömeggyártása nemsokára eléri a megkívánt kis méreteket. Egyes szupravezető eszközök, bár gyártásuk és kezelésük sok tekintetben nehezebb, a koherencia megőrzésére különösen alkalmasnak látszanak.

A feladat azonban óriási. Gondoljuk meg: a jól szervezhető kis eszközök félvezető vagy szupravezető kristályokból készülhetnek. Ezek rugalmasak, a hő hatására rezegnek: a kelvin törtrészére kell őket hűteni. Kristályhibáik is vannak: javítani kell a kristálynövesztést. Szennyező atomok is vannak bennük: ezektől meg kell őket tisztítani, minden eddiginél nagyobb mértékben. És akkor még mindig ott vannak, az elektronok kihagyhatatlan partnereiként, az atommagok a maguk billegő spinjeivel, amelyeket csak még sokkal erősebb hűtéssel vagy óriási mágnesekkel lehet leállítani. A fizikusok nem hagynak magukkal kibabrálni: egyes változatokban éppen ezeket a zajforrásként roppant kellemetlen magspineket használják fel információfeldolgozásra, megfelelő molekulába vagy félvezető eszközbe építve be őket. A fejlesztés rendíthetetlenül folyik, a nagyritkán a napilapok hasábjain is megjelenő kis előrelépések mögött óriási munka húzódik meg.

Van azonban a kvantuminformációnak egy sokkal lazább, és közvetlen alkalmazásokat kínáló ága, amelyhez a könnyen megvalósítható, néhány qubites – alapesetben akár csak egyetlen qubites – kvantumszámítógép is elegendő: ez a *kvantumtitkosírás,* és néhány hasonló titkosítási feladat, amelyek már eladható termékké értek, és a belőlük befolyó pénz eltartja az egész nagy tudományterületet.

A kvantumos alapú titkosítás alapja a kvantummechanikának – az interferencia és az összefonódás mellett – harmadik alapvető sajátsága: ez a hírhedt *kvantummérés,* amit leírni sokkal könnyebb, mint igazán megérteni. A kvantummérés: véletlen választás többféle lehetőség közül; a választás eredményét a hullám állapota csak statisztikailag határozza meg, de az eredmény megszületése közben a hullám ugrásszerűen éppen olyanná változik, mint amilyennek mértük.

Miért is jó ez titkosításra? Azért, mert a finom kvantumrendszerekbe kódolt titkot kikémlelni csak kvantummérésekkel lehet, és a méréssel járó ugrásszerű változás leleplezi a kémkedőt.

Az alapszituációt 1984-ben *Bennett* és *Brassard,* az IBM kutatói találták ki. Alice titkos üzenetet akar küldeni Bobnak (hívhatnánk őket A-nak és B-nek is, csak úgy sokkal unalmasabb lenne). Az üzenetet nyilvánosan küldik, de egy kulcsnak használt titkos bitsorozat által elkódolva, így aztán csak a kulcs ismerője tudja elolvasni. A kvantummechanikát éppen a kulcs továbbítására használják: a kulcsot üvegkábelen, egyes fotonok polarizációjába kódolva küldik el egymásnak. A foton mindennél finomabb kvantumrendszer, ha valamin, akkor rajta észre lehet venni, ha valaki – mondjuk, egy ipari kém – útközben le akarta olvasni a polarizációját, hogy hozzájusson a titkos kódhoz. Ha a rendszer ilyet észlel, utasítja a küldőt, hogy indítson útnak újabb bitsorozatot.

Az egyes fotonokból álló gyenge fényjelet polarizáló, majd analizáló kristálylemezkék a legegyszerűbb, egyetlen qubites kvantumszámítógépek, de önmagukban nem elég jók: az üvegkábelen kilométereket utazva a foton eltorzul, zajossá lesz, a titkos üzenet elvész. Itt jönnek be a játékba a már éppen létező, kicsit nagyobb, néhány qubites kvantumszámítógépek: ők éppen elegendők a kvantumos zajszűrés megoldására, és arra is, hogy kivédjék a ravaszabb kémek praktikáit, akik álcázni próbálják az általuk lehallgatáskor elvégzett kvantummméréseket. Mulatságos követni, hogy akárcsak az evolúció során, amikor a zergék és oroszlánok egyszerre váltak egyre gyorsabbakká, itt egyszerre születnek a lehallgatás és az ellene való védekezés egyre trükkösebb stratégiái. Viharosan fejlődnek a szükséges technika többi részei is: maguk az üvegkábelek, a fotonokat érzékelő detektorok, az adatfeldolgozás technikái. Műholdak és földi bázisok kommunikációja kedvéért kidolgozták az üvegkábel nélkül, levegőn át küldött jelek kvantumos titkosítását is. A kvantumtitkosírás már több helyen működik a világban; nem olcsó, de gazdagabb hadseregek vagy ipari titkaikat féltő nagyvállalatok jól megfizetik az erre szakosodott fizikuscsapatok munkáját. Az egyik legnevezetesebb csapat a Genfi tó partján küldözgeti titkos kódjait falurólfalura, felhasználva egy partnerként közreműködő telefontársaság optikai kábeleit, hogy tesztelje egyre megbízhatóbban működő eszközeit.

A titkosítás új lehetőségei nem merülnek ki a levelezésben. A tervek között szerepel hamisíthatatlan vízjelű kvantumpénz megalkotása, amely megint csak azért hamisíthatatlan, mert a hamisításhoz kvantummérést kell végezni, ami kitörölhetetlen nyomot hagy.

Egy romantikusabb alkalmazás a következő: Alice és Bob vonzódnak egymáshoz, de mindketten szégyenlősek és félnek a visszautasítástól. Hogy eldöntsék, találkozzanak-e, titkolt szándékukat – igent vagy nemet – egy kvantumszámítógépre bízzák, amely képes a titkot úgy kezelni, hogy ha mindketten IGEN-t küldenek, azt mindketten megtudják, de ha nem, akkor az, aki NEM-et mondott, sosem tudja meg, mit mondott a másik. Az igazsághoz azonban hozzátartozik, hogy ezt a műveletet klasszikus számítógép is meg tudja oldani.

A fizikus öröme többszörös ebben a fejlődésben. Ha csak a külső megrendelők kegyeit lesnénk, ha elfogadnánk az azonnali eladhatóságot, mint a tudományos kutatás egyedül érvényes mértékét, a kvantuminformatikusok közül szinte mindenki csak a titkosírással foglalkozna. De nem: a ki-tudja-mikor-megvalósuló nagy kvantumszámítógép megértése is rohamléptekkel halad előre, és közben apránként megismerjük a kvantummechanikai összefonódás fizikájának elbűvölő részleteit, amelyek sok mindent új fénybe helyeznek: a kémiai kötés természetét, a bonyolult mágneses anyagok viselkedését, a kvantumrendszerek irreverzibilis folyamatait, a termodinamikai entrópia és az információ kapcsolatát, a környezeti zaj szerepét az atomok kvantumos viselkedéséből a nagy tárgyak klasszikus fizikájába való átmenetben, és még sok olyan fontos és érdekes összefüggést, amelyek talán még évtizedekig rejtve maradtak volna, ha a fizikusok nem kapnak rá erre az egzotikus és regénybeillő tudományterületre.

Geszti Tamás
ELTE, Komplex Rendszerek Fizikája Tanszék