

http://hvg.hu/hetilap/2017.26/201726_mi_azakvantumosszefonodas_kinai_attores_akettetort_merleg_es_akules_einstein_is_meglepodne

2017. június. 28. 00:00 2017. június. 28. 15:07 HVG Hetilap

Einstein is meglepődne

szerző: Szepesi András

Egymástól elválasztott részecskék, amelyek mégis kapcsolatban maradnak: a rejtélyes kvantummechanikai jelenség révén immár a Föld és egy műhold között is sikerült kapcsolatot teremteni.

A **kvantum-összefonódás** annyira felfoghatatlan jelenség, hogy még maga Einstein is ijesztőnek nevezte. Ezért is keltett feltűnést kínai kutatóknak az a múlt héten ismertett kísérlete, amellyel bizonyították, hogy az „összefonódott” elemi részecskék nem kevesebb, mint 1200 kilométeres távolságon is megőrzik a kapcsolatukat. Ehhez fotonpárokat (parányi fényrészecskéket) hoztak létre, amelyek – egyszerűen szólva – egymástól távolra kerülve is „tudták”, mi történik a párjukkal.

A jelenség megértéséhez közelebb visz az egyik forradalminak jóslat felhasználása: képes lesz feltörhetetlen titkosítást létrehozni. Minden titkosításnál szükség van egy kulcsra, amellyel megfejthető a kódolt üzenet. A számítógépes üzenetküldésben a titkos kulcsok készítése most egy nagy számokkal dolgozó matematikai műveleten (a faktoráláson) alapszik. Ez a módszer feltörhető ugyan, biztonságát mégis az adja, hogy a leggyorsabb szuperszámítógépeknek is évekbe telik a megfejtése. A jövőben megépülő kvantumszámítógépek (lásd Szuperpozícióban című írásunkat) viszont percek alatt feltörhetik majd a mai kódokat. A titokgazdák szerencséjére a kódfeltörő kvantumszámítógépek még távolabb vannak, mint a kvantummechanikán alapuló titkosítás, amely ellen maguk a kvantumszámítógépek is tehetetlenek.

Ahhoz, hogy feltörhető legyen egy üzenet, a kémnek szüksége van a kulcsra. Mi lenne, ha sohasem szerezhetné meg? Ezt a megoldást kínálja a kvantum-összefonódás. Ez a jelenség azon alapszik, hogy két részecske bizonyos tulajdonságai úgy összekapcsolódhatnak, hogy ami az egyikkel történik, az a másikkra is hatással van. Valahogy úgy, mint egy mérleg két karja: amíg az egyik fent van, a másik csak lent lehet. A kvantummechanikai csavart ebben az esetben az adja, hogy a két

részecske összefonódása akkor is fennmarad, ha eltávolítjuk őket egymástól. Mintha a mérleg két karja akkor is zavartalanul működne, ha szétszerelnék őket. **Sőt mindez elvben a távolság nagyságától teljesen független.**

Tegyük fel, hogy egy efféle csodamérlegnek egyvalaki az egyik, másvalaki a másik karját egy-egy sötét dobozba zárja, és elindul velük ellenkező irányban. Amikor valamelyikük úgy dönt, hogy megnézi a saját mérlegkarját, akkor kinyitja a dobozt. Ha ekkor például azt látja, hogy a kar éppen lent van, akkor biztosan tudhatja, hogy a mérleg másik fele – valahol a távolban – fent kell hogy legyen. A mérés, azaz az egyik doboz kinyitásának pillanata viszont meg is törí az összefonódást: a két mérlegkar közötti különös kapcsolat megszűnik. **Mégpedig azonnal, sőt – újabb felfoghatatlan eset – a fény sebességénél is gyorsabban.**

Ebben a törésben rejlik a szuperbiztonságos titkosítás kulcsa. Ha kvantumösszefonódott részecskékkel küldjük a titkos kulcsokat az adó és a vevő között, akkor a kulcs ellopása lehetetlenné válik: amikor a kém, a hacker megpróbálja kinyitni az ellopott kulcsdobozt, a mérlegkarok azonnal beállnak. Ez a „kulcslopás” egy mérésnek felel meg. A kvantummechanikában pedig minden egyes mérés megváltoztatja a rendszer állapotát. A kém a lopás után megpróbálhatja továbbküldeni a kulcsot a címzettnek, hogy ne vegyék észre a kémkedést, de mivel a lopással már megváltoztatta a rendszer állapotát (elrontotta a kulcsot), a címzett rossz kulcsot kap. Nemcsak a kommunikáció sikertelen, hanem az is nyilvánvalóvá válik, hogy lehallgatási kísérlet történt. Az üzenetküldés csak akkor lehet sikeres, ha a mérés, azaz a kulcs felhasználása kizárólag egyszer, a végpontban történik.

Ami a fénysebességnél is gyorsabb „kulcstörést” illeti, ez csak látszólag mond ellent annak a fizikai törvénynek, amely szerint az információ nem terjedhet gyorsabban a fénynél. A kvantummechanika határozatlanságai miatt ez a jelenség nem jár információcserével. Merthogy a fizika mai állása szerint ez a kulcstörés nem számít valódi üzenetnek – bármennyire csábító lenne is, hogy a kvantumösszefonódás segítségével szinte azonnal lehetne üzeneteket fogadni akár fényévnnyi távolságból is. A kulcsküldésnél az összefonódott, majd szétválasztott fényrészecskék is „csak” fénysebességgel mozognak, **miközben – újabb nehezen felfogható jelenségként – a kulcstörés azonnali.**

Magát a módszert **kvantumkulcselosztásnak** hívják, kifejlesztése az 1980-as évekig vezethető vissza. 2004-ben Ausztriában már banki átutalás titkosítására is használták, bár csak kísérleti jelleggel. Az elvet a gyakorlatban már többször bizonyították,

hasznosításához azonban le kell küzdeni a távolságokat. Ennek a csúcspontját jelenti a **Pan Csian-vej által vezetett kutatócsoport legfrissebb eredménye: pontosan 1203 kilométeres távolságon sikerült tesztelni a kvantum-összefonódást.** A Hofej városában működő műegyetem csoportjának a Micius nevű kis műhold közvetítésével sikerült fotonokat szétosztani két kínai város, Tölingha és Licsiang között úgy, hogy azok a célba érve is megtartották összefonódásukat. A feladat legkritikusabb része az, hogy a fotonok sértetlenül utazzanak, ami nem egyszerű, mert még a levegő részecskéi is megzavarhatják az állapotukat.

A kínai világcsúcs jelentős lépés a titkosításban, mert bizonyítja, hogy a **kvantum-összefonódás** a gyakorlatban is működik nagyobb távolságokon át. Kutatók világszerte dolgoznak azon, hogy földi állomások és műholdak rendszere alkosson kvantumhálózatot, sőt akár **kvantuminternetet**. A kvantumverseny kimenetele még nem dőlt el: a németországi Fényfizikai Intézet kutatóinak sikerült kvantumállapotokat küldeniük egy 38 ezer kilométer magasan keringő műholdról a Földre. Ezek nem összefonódott részecskék voltak, de később ezek is alkalmasak lehetnek kvantumkulcsok elosztására. A kutatócsoport egyik vezetője, Christoph Marquardt szerint az Egyesült Államok akár még előrébb is járhat a kvantumversenyben. Szerinte „hangos a csend”, ő gyanúsna tartja, hogy a tengerentúlon működő csoportok a közelmúltban leálltak a kvantumkulcs-elosztással kapcsolatos tudományos cikkek publikálásával. „Ennek két oka lehet: a kísérleteik vagy nem működtek, vagy túlságosan is jól működtek.”