A kvantum-infokommunikáció jövőképe

BACSÁRDI LÁSZLÓ

BME, Hálózati Rendszerek és Szolgáltatások Tanszék

Jelenünk: a második kvantumtechnológiai forradalom kora

A kvantummechanika születését követően az első kvantumtechnológiai forradalom számos eszközt adott számunkra, és ma már elképzelhetetlen lenne az életünk napelemek, nukleáris energia, félvezetők vagy éppen lézerek nélkül. Napjainkban a második kvantumtechnológiai forradalom korát éljük, amelyet az jellemez, hogy képesek vagyunk egyedi részecskéket (atomokat, spineket, fotonokat) is manipulálni, oly módon, amely korábban elképzelhetetlennek tűnt. Ez a forradalom négy nagy területen jelenik meg: kvantumszámítógép, kvantumkommunikáció, kvantumszimuláció és kvantumérzékelés. 2023-ban közel negyven milliárd dollárra becsülték a kvantumtechnológiával kapcsolatos kutatások és fejlesztések értékét. A négy terület közül a kvantumkommunikációnak, amelyet inkább már kvantum-infokommunikációnak nevezhetnénk, kiemelt jelentősége van, már most több kereskedelmi célú termék érhető el a piacon, s folyamatosan jelennek meg újabb cégek innovatív termékeikkel.

A kvantum-infokommunikáció számos érdekes megoldást kínál számunkra, mint a kvantum alapú kulcsszétosztás, kvantum alapú véletlenszámok, illetve a kvantuminternet. A **kvantum alapú kulcscsere** (angolul quantum key distribution, QKD) során kvantumcsatornán keresztül osztunk meg egy titkos kulcsot, amelyet utána klasszikus szimmetrikus kulcsú titkosításra használunk fel. Ennek révén növelni tudjuk a rendszereink biztonsági szintjét, ugyanis a kvantum alapú kulcsszétosztás biztonságát a kvantumfizika törvényei garantálják, biztosítva, hogy passzív támadást (lehallgatást) nem tudunk végrehajtani, aktív támadásról (beavatkozásról) pedig értesülnek a kommunikáló felek. A **kvantum alapú véletlenszám-generátorok** (angolul quantum random number generator, QRNG) segítségével kvantumfizikai folyamatokra alapozva tudunk véletlen számokat előállítani. Mind QKD-eszközökből, mind QRNG-eszközökből számos érhető el a piacon, s van olyan mobilgyártó, aki a készülékébe is integrált QRNG chipet. A jelenleg inkább kísérleti körülmények között létező **kvantuminternet** olyan jellegű megoldásokat takar, amelyek lehetővé teszik majd, hogy nagy távolságba juttassunk el kvantuminformációt, kihasználva olyan meglepő kvantumfizikai jelenségeket, mint az összefonódás.

Jelenünk: Magyarország a világtérképen

Magyarországon többen is foglalkoznak különböző kvantumtechnológiai fejlesztésekkel. A Kvantuminformatika Nemzeti Laboratórium (KNL) segíti a kvantumtechnológia térnyerését a hazai oktatásban és kutatás-fejlesztési projektekben, inkubátorként és szakmai referenciaként működik a hazai vállalkozások és a magyar kormány szervei számára, valamint megjeleníti és képviseli a hazai kvantumtechnológiai ökoszisztémát európai uniós és egyéb szervezetekben. A KNL öt tagja a HUN-REN Wigner Fizikai Kutatóközpont, a Budapesti Műszaki és Gazdaságtudományi Egyetem Természettudományi Kara (BME TTK) és Villamosmérnöki és Informatikai Kara (BME VIK), az Eötvös Loránd Tudományegyetem (ELTE) Informatikai Kara és Természettudományi Kara. A BME Villamosmérnöki és Informatikai Karán már több mint 20 éve foglalkoznak kvantuminformatikával és kvantumkommunikációval, az elméleti kutatások mellett az egyetem szakemberei különböző kvantumkommunikációs rendszerek építésébe is belevágtak. A Műegyetem szakmai eredményeire alapozva a Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) vezetésével a BME, ELTE és HUN-REN Wigner FK részvételével 2023 januárjában indult el a QCIHungary projekt, amely az európai kvantumkommunikációs infrastruktúra részeként egy nemzeti kvantumkommunikációs infrastruktúra kezdeti kialakítását célozta meg.

Nagy hangsúlyt kell fektetni a következő generáció képzésébe is, a Műegyetemen ezért indult el 2023 tavaszán az országban elsőként a kvantuminformatika mellékspecializáció mérnökinformatikus mesterszakos hallgatók számára. De a Műegyetemen futó egyéb, kvantuminformatikával és kvantumkommunikációval foglalkozó tárgyaknak köszönhetően már több ezren hallottak a magyar mérnökök közül arról, milyen fontos is ez a terület.

A kvantum-infokommunikációra a HTE is kiemelt figyelmet fordít. 2021 novemberében a HTE Infokom konferencián a „Kvantumkommunikáció 2030" elnevezésű kerekasztal-beszélgetés során szakértőkkel egy tízéves jövőképre tekintettünk ki (a felvétel elérhető a HTE YouTube-csatornáján), és a 2024-es HTE Infokom konferencián is elő fog kerülni a témakör. A HTE Távközlési Szakosztály által szervezett Távközlési klubon is rendszeresen visszatérnek a kvantumos világ különböző kérdései, 2024-ben is lesz kvantumkommunikációval foglalkozó HTE Távközlési Klub. A HTE által kiadott Infocommunications Journalban pedig a területen elért izgalmas kutatási eredményekről lehet olvasni hazai és nemzetközi szerzőktől.

Jövőbe nézve: a terület 2040-ben

Azt, hogy 2021-ben mit gondoltunk arról, milyen lesz a kvantum-infokommunikációs világ 9 évvel később, meg lehet nézni a HTE Youtube csatornáján a Kvantumkommunikáció 2030 panelbeszélgetés felvételén. De vajon milyen lesz a terület 2040-ben? Többféle forgatókönyv is lehetséges, de a 75 éves HTE előtt tisztelegve egy optimista jövőkép jelenik meg most a jósgömbben.

Képesek leszünk arra, hogy kifejlesszünk hatékony hibajavító megoldásokat, amelyek stabilabbá fogják tenni a kvantumkapuk működését. Ennek a technológiai fejlődésnek köszönhetően el fogunk jutni a nagy kvantumbitszámmal megbízhatóan operáló kvantumszámítógépek korába. Ezeken olyan kvantumalgoritmusokat tudunk futtatni, amelyek segítségével hatékonyabbá tehetjük a gyógyszerkutatást, a pénzügyi kockázatbecslést, a nagyméretű adatbázisokban való keresést. A kvantumszámítógépek – méretükből adódóan – továbbra is az ezzel foglalkozó szakemberek számára lesznek elérhetőek, azaz a mindennapi életünkben továbbra is a megszokott klasszikus eszközeinket fogjuk használni, de egyre többször fogjuk igénybe venni a kvantumszámítást mint szolgáltatást (Quantum-as-a-Service (QaaS). Azon szervezetek, akik számára kritikus, hogy megbízható hardver- és szoftverelemekből építkező eszközeik legyenek (és ne kelljen megbízni egy másik országban működő szolgáltatóban), saját kvantumszámítógéppel fognak rendelkezni.

Azokon a helyeken, ahol számít a biztonság (kommunikáció, adatok titkosítása, digitális aláírások stb.) olyan megoldásokat fogunk használni, amelyek matematikailag és/vagy fizikailag bizonyítottan védettek a kvantumszámítógép támadásaival szemben. A matematikailag bizonyított eljárások közé tartoznak az úgynevezett posztkvantum algoritmusok, amelyek használata széles körben elterjedt lesz. Ugyanakkor még mindig nem fogjuk pontosan látni, hogy a kvantumszámítógép információelméleti szempontból milyen problémaosztályokban képes feladatokat megoldani, ezért a klasszikus kriptográfiával foglalkozó szakemberek továbbra is dolgozni fognak azon, hogy a kvantumszámítógép által jelentett biztonsági fenyegetésre válaszul újabb és újabb posztkvantum-algoritmusokat alkossanak.

A fizikailag bizonyítottan védett kvantum alapú megoldásokat – amelyek a fizika törvényeire alapozva védettek a támadásoktól – sok helyen fogják használni. Ilyenek pl. az úgynevezett kvantum alapú kulcsszétosztó hálózatok, amelyek a mindennapi infrastruktúra részét fogják képezni a kormányzati, a pénzügyi és a kritikus infrastruktúrát üzemeltető szektorok esetén. Az Európai Unió területén üzemelni fog az Európai Kvantumkommunikációs Infrastruktúra (European Quantum Communication Infrastructure, EuroQCI) legújabb verziója, amely alapgondolatát 2019-ben júniusában fogalmazták meg az EuroQCI deklarációjában. Az EU-s tagországok közötti optikai szálas kapcsolatokon túl az európai kvantumkommunikációs műholdak is az összeköttetés szerves részét fogják jelenteni.

Már a 2020-as évek közepén is számos kvantumkommunikációs cég jelent meg a piacon, de az elérhető termékek köre még szélesebb lesz 2040-re. A földi környezetben (optikai szálon) használható megoldásokon túl számos cég fog kínálni általa üzemeltetett kvantumkommunikációs műholdakra alapozott szolgáltatást, amelyekről optikai kommunikációval (vagyis lézerjelek segítségével) lehet majd továbbítani a kulcsokat. A kriptográfiai szempontból kritikus hardvereszközök jelentős része fog tartalmazni integrált kvantum alapú véletlenszám-generátort.

A kvantuminformatikus és a kvantumkommunikációs mérnök kifejezésekkel leírt szakma már nemcsak egy fehér holló jellegű ritkaság lesz, hanem szélesebb körben is elismertté válik, hasonlóan ahhoz, ahogy a 2020-as években az űrmérnök kifejezés és az űrmérnök képzés is elterjedt hazánkban.

A kutatások jövője: kvantuminternet

A jósgömbben idáig látottak levezethetőek a jelenlegi technológiai trendekből. Amely terület jövőbeli technológiai érettségét homály fedi, az a kvantuminternet világa. Egy olyan hálózaté, amelyek segítségével több csomóponton áthaladva vagyunk képesek kvantuminformációt továbbítani. Egy olyan hálózaté, amely különleges hardvereszközöket és különleges szoftvereket tartalmaz. A kvantuminternet segítségével képesek leszünk jelentősen megnövelni az összefonódáson alapuló kvantumkommunikációs protokollok működési távolságát és összekapcsolni távoli helyeken működő kvantumszámítógépeket.

Ilyen hálózat – nagy távolságban – jelenleg a kvantumfizika törvényei szerint (különösen a Nincs másolás tétel miatt) nem megvalósítható, ugyanis nem tudunk olyan erősítőket építeni, mint amit a klasszikus világban megszokhattunk. Az összefonódás-megosztás (entanglement swapping) és a kvantummemóriák segítségével azonban lehetőségünk lenne a kvantumteleportáció protokollját használva távoli kvantumrendszerek összekapcsolására. Számos kutatás zajlik ezzel kapcsolatban szerte a világon, Európában és Magyarországon is. (A Műegyetem kutatói is kidolgoztak olyan protokollokat, amelyeket a kvantuminterneten lehet majd használni). Ráadásul nemcsak földi környezetben működhet: többek között az Európai Űrügynökség is vizsgálja, hogyan lehetne kvantummemóriákat a műholdakon elhelyezni. Az Internet Engineering Task Force (IETF) kvantuminternettel foglalkozó munkacsoportja már kidolgozta a kvantuminternet első szabványos protokolljait, vannak kísérleti rendszerek Európában is, de a tényleges, nagy távolságú kvantuminternethez szükség van megfelelő hardverekre. Csak bízni lehet abban, hogy a kapcsolódó kutatások sikeresek lesznek, és a különböző fizikai technológiákra alapozott kvantummemóriák koherenciaideje a milliszekundumról/percekről órákra/napokra fog nőni. Ha ez megtörténik, akkor 2040-re a kvantumkulcs-csere hálózatok mellett a kvantuminternet is a műszaki világ része lesz.