SAJTÓKÖZLEMÉNY

Sikeresen tesztelték a BME-n Magyarország első többcsomópontos kvantumalapú titkosító hálózatát

Budapest, 2025. április 22 - Az egyedi kutatói és ipari együttműködésben elvégzett demonstráció Magyarországon első volt a maga nemében, és fontos mérföldkő a kiberbiztonsági fejlesztésekben.

Egyre gyakrabban lehet hallani informatikai biztonsági sérülékenységekről, feltört és lehallgatott kommunikációról, adatlopásról, illetéktelen hozzáférésekről. Ezen biztonsági fenyegetésekre a kvantumalapú megoldások nyújthatnak védelmet (*ebbe az irányba látják a megoldást az EU tagországok törvényhozói is, lásd NIS2, „Magyarország kiberbiztonságáról szóló 2024. évi LXIX törvény”*), amihez kvantum alapú kulcsszétosztó (QKD) hálózatokat is kell majd építeni.

Ezt sikerült elsőként demonstrálni egy egyedi kutatói és ipari együttműködéssel. Az együttműködés keretében az AdvaNet Magyarország Kft., a Budapesti Műszaki és Gazdaságtudományi Egyetem, a Magyar Telekom Nyrt. és a Netvisor Zrt. szakemberei megépítették Magyarország első több csomópontos, kulcsmenedzsmenttel rendelkező kvantumkulcs-szétosztó teszthálózatát.

A kvantumszámítógépek rohamos fejlődése alapjaiban kérdőjelezi meg a jelenlegi titkosítási rendszerek hosszú távú biztonságát, ezért rendkívül fontos, hogy időben felkészüljünk. A QKD jelenleg az egyik legígéretesebb válasz erre a kihívásra, hiszen fizikailag garantált biztonságot nyújt a titkosításhoz használt kulcs átvitele során.

Az első hazai, több csomópontos QKD hálózat megépítése nemcsak technológiai mérföldkő, hanem komoly előrelépés is a jövőbiztos kiberbiztonsági rendszerek irányába. Az együttműködés során iparági szereplőkkel, akadémiai és technológiai partnerekkel több különböző világ találkozott, közös tudásalapot építettek, és megmutatták, hogy bár a jövő titkosítási hálózatának a kiépítéséhez még sok kutatás, fejlesztés és tesztelés szükséges, a magyarországi szakmai szereplők élen járnak ezen a területen.

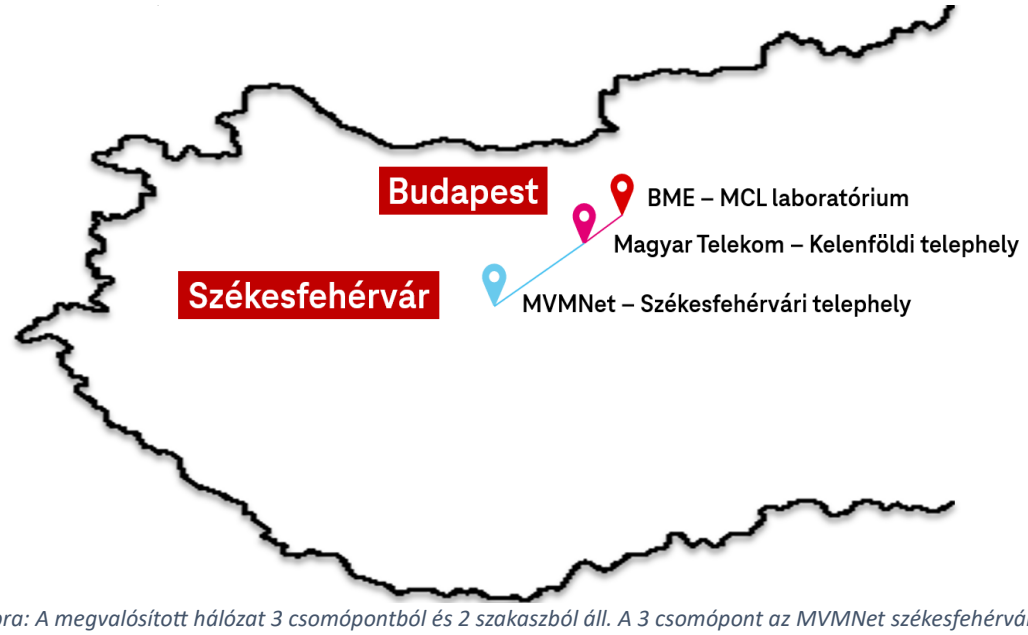
Április 22-én a BME Villamosmérnöki és Informatikai Karán mutatták be a résztvevő szervezetek az első hazai sikeres demonstráció hátterét. Mint Dr. Imre Sándor, a BME Villamosmérnöki és Informatikai Karának dékánja elmondta: *„Az elmúlt évek során számos hazai eredmény született a kvantumkommunikáció területén, egyre több kvantumkommunikációs kísérlet zajlik. Nagy előrelépést jelent, hogy most kereskedelmi forgalomban kapható eszközök segítségével sikerült megvalósítani Magyarországon az első többcsomópontos kvantum alapú titkosító hálózatot. 2025 a kvantumkutatás és a kvantumtechnológia nemzetközi éve, így külön öröm, hogy idén sikerült ezt a kísérletet elvégezni.”*

A hálózat 3 pontja a BME I épületben lévő kvantumkommunikációs laborjában, Budapest-Kelenföld távközlési helyiségben, illetve Székesfehérváron található. A kísérlet lényege, hogy kvantumkommunikáció segítségével osszunk meg kulcsot több csomóponton keresztül, ahol ezt a kulcsot a hagyományos távközlés titkosítására használjuk. A hálózat 3 rétegből áll. Az alsó rétegen Toshiba kvantumkulcsszétosztó eszközök osztanak meg 1-1 kulcsot a BME-Kelenföld illetve a Kelenföld-Székesfehérvár szakaszokon. A középső rétegen lévő szerverek végzik a kulcsmenedzsmentet, ezek segítségével lehet a két szélső csomópont között is titkosítást végezni. A

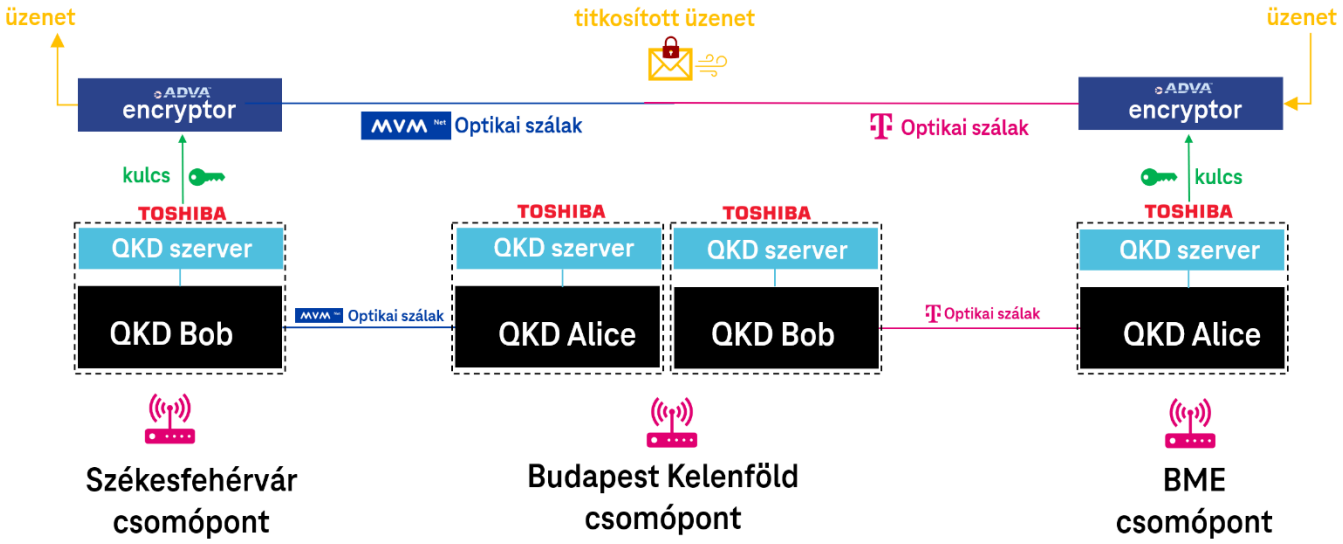
felső rétegen pedig Székesfehérváron és a BME laborjában 1-1 klasszikus WDM (hullámhossz-osztásos optikai átvitel) távközlési eszköz található, amik az ott lévő QKD szerverektől kapott kulcsokkal tudnak bármilyen egymás közötti kommunikációt titkosítani.

Az eddig főként pont-pont megoldásként alkalmazott kvantumos kulcsszétosztást itthon először próbálták ki egy több csomópontos hálózatként, megtapasztalva egy valódi QKD hálózathoz elengedhetetlen kulcsmenedzsment funkcióit, tapasztalatot gyűjtve az eszközök üzemeltetéséről és a kvantumkommunikáció során megosztott kulcsok hagyományos titkosító eszközökkel történő felhasználásáról is. Mivel a bitenként közel 1 fotonnal történő kvantumos kommunikáció távolsági limitje viszonylag alacsony, hálózatba kötéssel és kulcsmenedzsmenttel ezt is ki lehet küszöbölni.

Az április 22-i rendezvényen Dr. Imre Sándor, a BME Villamosmérnöki és Informatikai Kar dékánja köszöntötte a megjelenteket, majd a hálózat megalkotásában részt vevő négy partner képviselői – Gerhátné Dr. Udvary Eszter *(BME Hálózati Rendszerek és Szolgáltatások Tanszék)*, Buzás Attila *(AdvaNet Magyarország Kft.)*, Babics Emil *(Magyar Telekom Nyrt.)*, Máthé János *(NETvisor Zrt.)* – engedtek betekintést a kísérlet hátterébe. Ezt követően Sóki András *(Magyar Telekom Nyrt.)*, Horváth Attila Róbert *(NETvisor Zrt.)*, Dr. Matolcsy Balázs *(BME Hálózati Rendszerek és Szolgáltatások Tanszék)* és Szőke Barnabás *(AdvaNet Magyarország Kft.)* ismertette a demonstráció technikai hátterét, végül a BME kvantumkommunikációs laborjában lehetett megtekinteni a működő hálózat egyetem oldali csomópontját. A rendezvényt Dr. Bacsárdi László, a BME Mobil Kommunikáció és Kvantumtechnológiák Laboratórium vezetőjének a gondolatai zárták a közel 80 kilométeres távolságú sikeres kísérlettel kapcsolatban, amely az egyetem és a három cég közreműködésében valósult meg.



1. ábra: A megvalósított hálózat 3 csomópontból és 2 szakaszból áll. A 3 csomópont az MVMNet székesfehérvári telephelyén, a Magyar Telekom Kelenföldi telephelyén, valamint Budapesti Műszaki és Gazdaságtudományi Egyetem Mobil Kommunikációs és Kvantumtechnológiák Laboratóriumában (BME I épület) található. A két szakasz hossza Székesfehérvár és Kelenföld között 76 km, Kelenföld és az egyetem között 2,5 km



1. ábra: A hálózat egyszerűsített architektúrája.

***QKD** (quantum key distribution – kvantum kulcsszétosztó eszköz: Olyan eszköz, amely kvantumkommunikációval (elméletben bitenként 1 fotonnal) oszt meg titkos kulcsot a két pár (Alice és Bob) között, ebben a kísérletben a BB84 protokoll alapján.*

***szerver**: Minden QKD eszközhöz tartozik egy Linux alapú szerver, amely kezeli a kapcsolatot, megjeleníti a mérési adatokat (pl. bithiba arány, kulcssebesség), és végzi a kulcsmenedzsmentet.*

***enkriptor:** Hagyományos titkosító eszköz, amely a QKD szerverektől kapott kulcsokkal titkosítja az adatforgalmat a két végpont között.*

***router**: A távoli eléréshez VPN-t hoztunk létre; a routerek mobilinterneten keresztül kommunikálnak egymással.*

A QKD eszközök és az enkriptorok között optikai, a szerverek és az enkriptorok között pedig réz alapú Ethernet kapcsolat van. A csomópontokon belül a routerek vezetékesen kapcsolódnak a helyi szerverhez és enkriptorhoz, egymással pedig mobilinternet segítségével kommunikálnak.

További információ: Budapesti Műszaki és Gazdaságtudományi Egyetem, Kommunikációs Igazgatóság
Tel.: +36-1-463-2250; +36-30-458-7240, E-mail: kommunikacio@bme.hu