A kvantumkriptográfia infokommunikációs alkalmazásai

GYÖNGYÖSI LÁSZLÓ, IMRE SÁNDOR

Budapesti Műszaki és Gazdaságtudományi Egyetem, Híradástechnikai Tanszék
{gyongyosi, imre}@hit.bme.hu

Kulcsszavak: kvantumkriptográfia, kvantumkommunikáció, kvantuminformatika

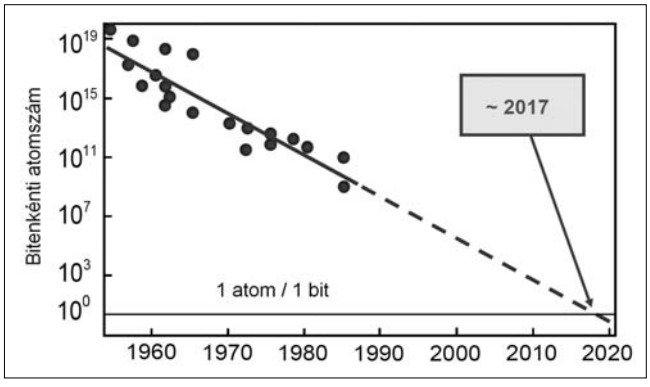
A Moore-törvény alapján, 2017-re várhatóan egy bit információt egy atom tárol majd, így már néhány éven belül elérkezhet a kvantuminformatika világa. A kvantumszámítógépek megjelenésével a jelenlegi titkosítási módszerek nagy része veszélybe kerül. A kvantumszámítógép működése a kvantumelméletre épül, és alkalmas arra, hogy minden mai modern, feltörhetetlennek vélt kódot másodpercek alatt feltörjön. A rejtjelezők ezért már ma olyan módszeren dolgoznak, amely a kvantumszámítógéppel szemben is képes megőrizni a titkokat. Az új, abszolút feltörhetetlen kód: a kvantumkriptográfia. A kvantumkriptográfia alapú titkosítást már a gyakorlatban is megvalósították, laboratóriumi és szabadtéri körülmények között is. A protokoll működőképes, és valóban egy olyan titkosítási módszert nyújt, amely elméletileg sem törhető fel.

1. Bevezető

A Moore-törvényt figyelembe véve – amely szerint a számítógépek bonyolultsága exponenciálisan nő az időben – 2017-re várhatóan egy bit információt egyetlen atomban fogunk kódolni. Ahogyan azt tehát a számítástechnika mai helyzetéből jósolni lehet, a hagyományos technológiák hamarosan elérik a végső fizikai határokat, az elemi műveleteket egyetlen elektron hajtja majd végre. A kvantumeffektusok így már néhány éven belül olyan nagymértékű hatást gyakorolhatnak a számításokra, amely alapvetően befolyásolja, meghatározza a későbbi fejlesztések irányvonalát.

A *kvantumszámítógépek* megjelenésével a jelenlegi titkosítási módszerek nagy része veszélybe kerül. A napjainkban alkalmazott nyílvános kulcsú titkosító algoritmusok biztonsága ugyanis nehéznek vélt matematikai problémákra, például a faktorizáció nehézségére épül, melyek megoldásához szükséges lépésszám *exponenciálisan* növekszik az input méretének növekedésével. A kvantumszámítógép azonban ezeket a nehéz problémákat polinomiális lépésszámmal oldaná meg, és így hatékonyan feltörhetővé tenné a mai rejtjelező algoritmusokat.

1. ábra A számítástechnika fejlődési üteme



A Peter Shor által 1994-ben közzétett *kvantumalgoritmus* például *polinomiális* idő alatt képes megoldani a faktorizáció problémáját. Az algoritmus egyrészt azon alapul, hogy a faktorizációval szemben, a legnagyobb közös osztó megtalálására ismert gyors klasszikus algoritmus is, másrészt pedig a faktorizációs probléma visszavezethető a periódus keresési feladatra. A kvantumalgoritmus *kvantum-regisztereken* végzi el a prímtényezőkre bontást, a faktorizálandó szám maradékosztályainak periodicitási tulajdonságát kihasználva. A kvantumalgoritmussal, egyetlen kvantumszámítógép segítségével *másodpercnyi* időtartam alatt feltörhető azon kód, mely napjaink klasszikus számítógép-hálózatainak együttesen is több hónapig tartana [6].

A jövőben így olyan titkosítási módszereket kell találnunk, amely megvédenek bennünket a kvantumszámítógépek támadásától. A *kvantumkriptográfia* lehet az a titkosítási eljárás, amely ellenáll a kvantumszámítógépek hatalmas számítási teljesítményének is. A kvantumkriptográfia az *egyszeri kulcsos módszert* (OTP, One Time Pad) használja az adatok titkosítására, mely, mint ismeretes, *elméletileg sem törhető fel,* szemben a napjainkban alkalmazott titkosítási eljárások *gyakorlati feltörhetetlenségével.*

2. A kvantumkriptográfia megszületése

Amíg a rejtjelfejtők a kvantumszámítógépre várnak, addig a rejtjelezők olyan módszeren dolgoznak, amely a kvantumszámítógéppel szemben is képes megőrizni a titkokat, azaz *még kvantumszámítógéppel sem törhető fel.* A módszer a kvantumelméletre épül, ugyanúgy, mint a kvantumszámítógép. Az abszolút feltörhetetlen kód a kvantumkriptográfia.

A kvantumkriptográfia története a hatvanas évek végén kezdődött. Stephen Wiesner ekkor vetette fel a kvantumpénz fogalmát. A kvantumpénz elméleti alap-

ja a fotonok fizikája volt. Wiesner ötletét nem valósították meg, azonban egy régi barátja, Charles Bennett figyelmét felkeltette. Wiesner odaadta a kvantumpénzzel kapcsolatos jegyzeteit Bennettnek. Bennettnek azonnal megtetszett az ötlet. Sokat gondolkozott azon, hogyan lehetne a gyakorlatban is megvalósítani. A kvantumpénz ötletét megosztotta Gilles Brassarddal, a Montreali Egyetem számítógéptudósával. Többször megvitatták a dolgot, s arra a következtetésre jutottak, hogy Wiesner ötletét a kriptográfiában lehetne hasznosítani. Wiesner kvantumpénze azért biztonságos, mert a bankjegyekbe zárt fotonok polarizációját lehetetlen megállapítani.

Bennett és Bassard a kódolt üzenetek polarizált fotonok formájába öntésén, s azok ílymódon történő továbbításán kezdett el gondolkodni [1,2]. Az így küldött kódüzeneteket elméletileg a támadó, Eve nem tudná elolvasni, s ezáltal megfejteni sem [3].

2.1. Kvantumrendszerek jellemzése

A fizikai rendszerek időfejlődését a klasszikus fizikában a Hamilton-féle kanonikus egyenletek írják le, míg a kvantumrendszerek időfejlődésének leírására a Schrödinger-egyenlet szolgál. A Schrödinger-egyenletben egy kvantumrendszer kezdeti $|\psi(0)\rangle$ állapotából történő reverzibilis időfejlődését a $|\psi(t)\rangle = U_t\,|\psi(0)\rangle$ transzformáció szabja meg, ahol U_t az időfejlődést leíró evolúció-operátor. Az U_t operátor mindig *unitér*, így minden kvantumtranszformáció unitér leképzést realizál a kvantumrendszeren belül, a végrehajtott transzformáció pedig logikailag reverzibilis. Egy kvantumrendszer állapotterét hullámfüggvények Hilbert-tereként ábrázoljuk. A Hilbert-tér egy $|\psi(t)\rangle$ egységvektora reprezentálja a kvantumrendszer egy adott időpontbeli állapotát.

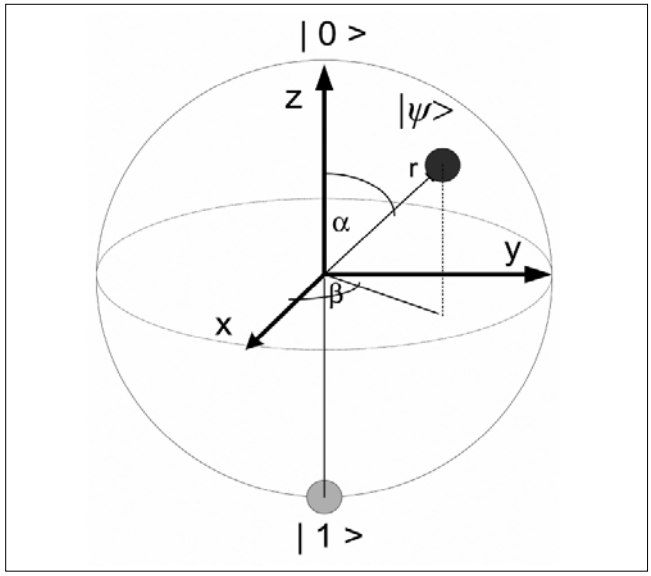
A kvantumállapotokat, valamint a rájuk ható transzformációkat leírhatjuk vektorokkal vagy mátrixokkal, de célszerűbb a Dirac-féle *„bra/ket”* szimbólumok használata. A $|x\rangle$ jelölés egy *„ket”*, ami egy *oszlopvektornak* felel meg, míg a $\langle x|$ jelölés egy *„bra”*-t, azaz egy *sorvektort* jelent, amely éppen a $|x\rangle$ *„ket”* adjungáltja. A *„bra/ket”*-ek leírhatók vektorokkal is:

$$|0\rangle = \begin{pmatrix}1 & 0\end{pmatrix}^T \text{ és } |1\rangle = \begin{pmatrix}0 & 1\end{pmatrix}^T.$$

A mikrorészecskék tulajdonságainak magyarázásakor a részecske állapotváltozásait *komplex számokkal,* valószínűségi amplitúdókkal írjuk le [3].

2.1.1. A kvantumbit

Egy klasszikus rendszeren belüli, „klasszikus értelmezésű” bit, a két logikai állapot között nem vehet fel értékeket. Ezzel ellentétben, a *kvantumbitek* lehetnek a 0 és 1 állapot között is, amelyet az $\alpha|0\rangle + \beta|1\rangle$ állapotvektorral írhatunk le, ahol α, β a $|0\rangle$ és $|1\rangle$ bázisállapotokhoz tartozó *valószínűségi amplitúdók*. A kvantumállapot mérése során, az α, β valószínűségi amplitúdóknak megfelelő valószínűséggel kerül a rendszer a $|0\rangle$ vagy $|1\rangle$ kimeneti állapotok valamelyikébe. A valószínűségi amplitúdókra fennáll $|\alpha|^2 + |\beta|^2 = 1$ normáltsági feltétel, az egyes kimeneti állapotokhoz tartozó mérési valószínűségek pedig ezen valószínűségi amplitúdók négyzetével jellemezhetőek. Így, az $\alpha|0\rangle + \beta|1\rangle$ állapotú kvantumbiten végrehajtott mérés eredménye $|\alpha|^2$ valószínűséggel $|0\rangle$, illetve $|\beta|^2$ valószínűséggel $|1\rangle$ lesz. A kvantumbitek állapotának szemléltetésére a Bloch-gömböt használjuk. A Bloch-gömb egy-egy feléhez a kvantumbit egy-egy bázisállapota tartozik. Általánosan, a gömb északi fele a $|0\rangle$ állapotnak felel meg, a déli fele pedig $|1\rangle$-nek, a többi pont pedig ezen két bázisállapot *szuperpozíciója*.



2. ábra A kvantumbit szemléltetése Bloch-gömbön

A Bloch-gömbi reprezentáció során két fontos szöget különböztetünk meg. Az α szög a $|0\rangle$ és $|1\rangle$ vektor arányát jelenti az összegben, – azaz az adott állapothoz tartozó valószínűségi amplitúdókat – míg a β szög a *relatív kvantum fázist* jelöli. Az állapotvektor a Bloch-gömbön bárhol elhelyezkedhet, így a kvantumbit a felvehető *végtelen sok* állapot közül bármelyikben lehet. Az α szög az $\vec{r}$ vektor és a *z* tengely által bezárt szög, a β szög pedig a vektor irányát határozza meg.

2.2. Foton, mint kvantumbit

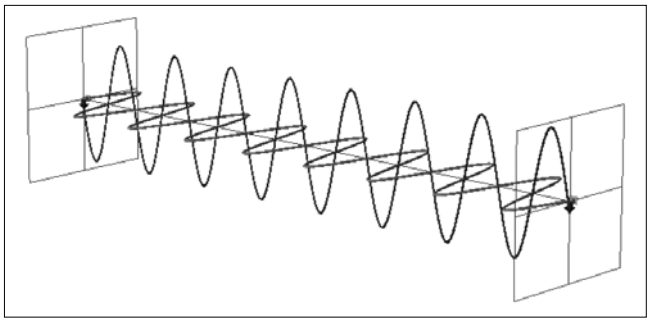
A kvantumbitek megvalósíthatóak fotonokkal is, hiszen a fotonok polarizációs szögei megfeleltethetőek a kvantumbitek $|0\rangle$ és $|1\rangle$ bázisállapotainak. A fotonok horizontális $|h\rangle$ és vertikális $|v\rangle$ polarizációs állapotait így a következőkben a $|0\rangle$ és $|1\rangle$ bázisértékekkel azonosítjuk. A kvantumbitként alkalmazott foton $|\psi\rangle$ állapotát, azaz polarizációját is leírhatjuk a $|\psi\rangle = a\cdot|\rightarrow\rangle + b\cdot|\uparrow\rangle$ állapotvektorral, ahol a $|\rightarrow\rangle, |\uparrow\rangle$ jelölés alatt a *vízszintes,* illetve *függőleges* polarizációt értjük. A klasszikus bitekhez hasonlóan, amelyek a 0 vagy 1 állapotban lehetnek, a fotonok is felvehetik a $|0\rangle$ vagy $|1\rangle$ állapotot, vagy akár e két állapot lineáris kombinációjának megfelelő $|\psi\rangle = a\cdot|\rightarrow\rangle + b\cdot|\uparrow\rangle$ *szuperpozíciós* állapotot. A foton polarizációját a $|\psi\rangle$ irányvektor jelképezi a függőleges és vízszintes polarizációk bázisában.

A kvantummechanika mérési posztulátuma szerint egy méréshez mindig tartozik egy *ortonormált* bázis,

amely mérés a mérendő $|\psi\rangle$ kvantumállapotot az ortonormált bázis egyik bázisvektorába transzformálja át. Így, az $|\psi\rangle = a \cdot |\rightarrow\rangle + b \cdot |\uparrow\rangle$ polarizációjú foton, rektilineáris $\{|\rightarrow\rangle, |\uparrow\rangle\}$ bázisú mérési eredménye $|a|^2$ valószínűséggel $|\rightarrow\rangle$, valamint $|b|^2$ valószínűséggel $|\uparrow\rangle$ lesz.

A fotonok esetében kétféle bázisban kódoljuk, illetve dekódoljuk a kvantumállapotokat, a vízszintes-függőleges bázisállapotokat tartalmazó $\{|\rightarrow\rangle, |\uparrow\rangle\}$ *rektilineáris*, illetve az átlósan polarizált kvantumállapotokat tartalmazó *diagonális* $\{|\nearrow\rangle, |\nwarrow\rangle\}$ bázisban. A természetes fény rengeteg atom, illetve molekula által kibocsátott sugárzásból áll, azonban a síkban poláros fényben az elektromos térerősség vektor egyetlen síkban halad.

A *3. ábrán* láthatjuk, hogy az elektromos térerősség vektor a *z* terjedési iránnyal merőlegesen, az *xy* síkban halad.



3. ábra A fény polarizációja

3. A kvantumkriptográfia működési elve

A kvantumkriptográfia általános modelljében a két kommunikációs fél, Alice és Bob egy kétirányú *klasszikus*, valamint egy egyirányú, Alice-tól Bob felé irányuló *kvantum-csatornán* keresztül állnak kapcsolatban egymással [1]. A kvantumcsatorna felhasználásával a részecskék kvantumállapotukat megőrizve küldhetők át. A csatornák nem megbízhatóak, hiszen a klasszikus csatorna lehallgatható, a kvantumcsatornán pedig a támadó, Eve elfoghat és újraküldhet részecskéket [2].

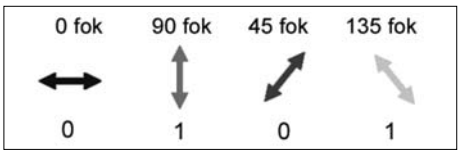
A kvantumkriptográfia segítségével azonban Alice és Bob képesek megegyezni egy olyan kulcsban, amit rajtuk kívül senki más nem ismer. A közös kulcs kialakítását már sikeresen megvalósították, 1997-ben Highes és társai 24 km-es távolságon mutatták be a protokoll működését, egy szabványos üvegszálas optikai kábelen keresztül. 2002-ben pedig 10 km-es távolságon, a légkörben is sikerült megvalósítaniuk a kísérletet.

3.1. A titkos kulcs kialakítása

A kulcskialakítás első szakaszában Alice $\langle\updownarrow,\leftrightarrow\rangle$ rektilineáris (vízszintes-függőleges) és $\langle\nearrow,\nwarrow\rangle$ diagonális (átlós) polarizációs séma véletlenszerű váltogatásával küld egy, egyesekből és nullákból álló véletlenszerű fotonfüzért.

A protokoll általános modelljét a *4. ábrán* láthatjuk.

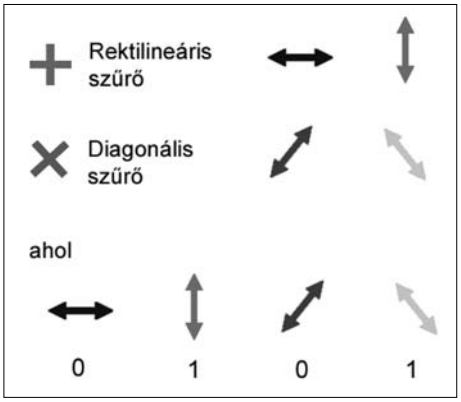
Az 1-eseket és 0-kat bizonyos *polarizáltságú* fotonok helyettesítik. A fotonok polarizációs szögeihez rendelt logikai értékeket az *5. ábra* mutatja.



5. ábra A fotonokhoz tartozó bináris értékek

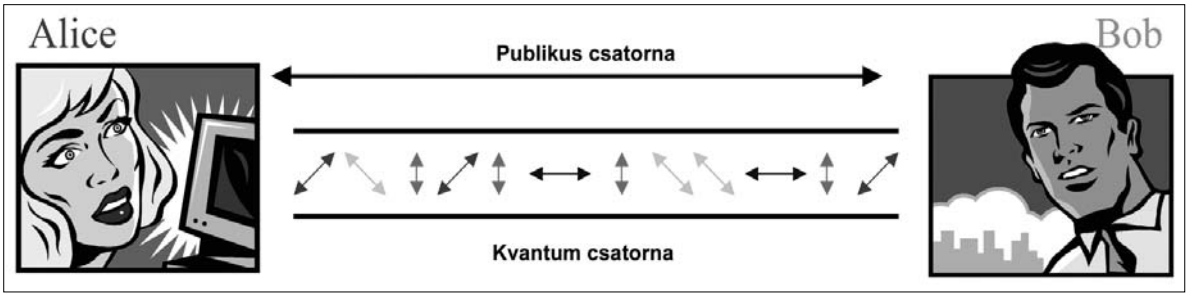
A vízszintesen polarizált foton $\leftrightarrow$ logikai 0-át, míg a függőlegesen polarizált $\updownarrow$ foton a logikai 1-et jelenti. Hasonlóképpen, az átlósan polarizált fotonok közül a 45 fokos szögben polarizált $\nearrow$ foton jelenti a 0-át, míg a 135 fokos $\nwarrow$ a logikai 1-et.

Arra, hogy Alice fotonokkal helyettesítse az egyeseket és nullákat, két módszert alkalmazhat, a $\langle\updownarrow,\leftrightarrow\rangle$ elemű rektilineáris, illetve a $\langle\nearrow,\nwarrow\rangle$ elemű diagonális módszert. A $\langle\updownarrow,\leftrightarrow\rangle$ rektilineáris módszer esetén a logikai 0 értéket a $\leftrightarrow$, a logikai 1-et pedig a $\updownarrow$ polarizációs állapot reprezentálja. A $\langle\nearrow,\nwarrow\rangle$ diagonális, azaz átlós módszer esetében a logikai nullát a $\nearrow$, az 1-et pedig a $\nwarrow$ kvantumállapot jelenti. Az egyes bázisokhoz tartozó polarizációs állapotokat a *6. ábrán* láthatjuk.



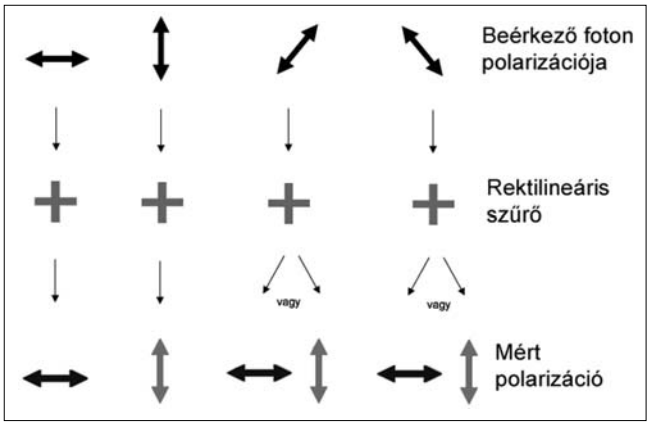
6. ábra A rektilineáris és diagonális szűrővel előállítható fotonok és azok értékei

Bobnak, a dekódoló oldalon minden egyes foton polarizációját meg kell állapítania, tehát minden egyes alkalommal el kell döntenie, hogy hogyan állítsa be polárszűrőjét. Bob azonban nem tudhatja, hogy melyik fotont milyen módszerrel küldte Alice, ezért az *esetek fe-*



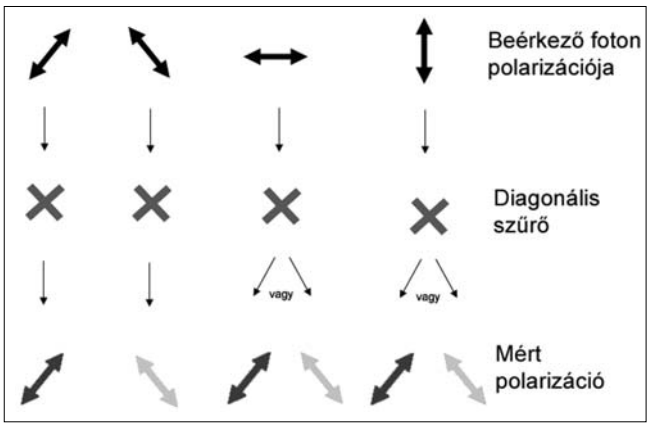
4. ábra A kvantumkriptográfia általános modellje

lében csak tévesen tudja megállapítani a polarizációt. Bob a ⟨↕,↔⟩ bázisban tökéletesen felismeri a függőlegesen és vízszintesen polarizált fotonokat, az átlósakat azonban nem. A ⟨↗,↖⟩ bázisban kódolt kvantumbiteket így *véletlenszerűen* függőlegesnek vagy vízszintesnek azonosítja. A rektilineáris bázisban végrehajtott mérések lehetséges kimeneteleit a *7. ábrán* foglaltuk össze.



7. ábra
Lehetséges mérési eredmények rektilineáris szűrő esetében

Hasonlóképpen, ha ⟨↗,↖⟩ szűrőt alkalmaz, akkor az átlósan polarizált fotonokat tökéletesen felismeri, de a vízszintes és függőleges fotonokat helytelenül átlós polarizáltságúaknak azonosítja, *véletlenszerű logikai értékekkel*. A diagonális bázisú mérések lehetséges kimeneteleit a *8. ábrán* láthatjuk.



8. ábra
Lehetséges mérési eredmények diagonális szűrő esetében

Egy bináris üzenet elküldésekor Alice a ⟨↕,↔⟩ rektilineáris és ⟨↗,↖⟩ diagonális módszert véletlenszerűen váltogatja.

Legyen példánkban az átküldendő üzenet a következő, 12 bites bináris sztring: *„011010111010”*. Az Alice által elküldött kvantumállapotok vételekor Bobnak meg kell állapítania a fotonok polarizációját. Mivel nem tudja, hogy Alice melyik fotonnál milyen polarizációs sémát alkalmazott, így Bob véletlenszerűen váltogatja a rektilineáris és diagonális detektorát. Törvényszerűen időnként eltalálja melyik a helyes, másszor nem, ekkor azonban rosszul értelmezheti Alice fotonját.

Abban az esetben, ha a csatornát nem hallgatta le Eve, akkor Bob a *9. ábrán* látható kulcshoz juthat.

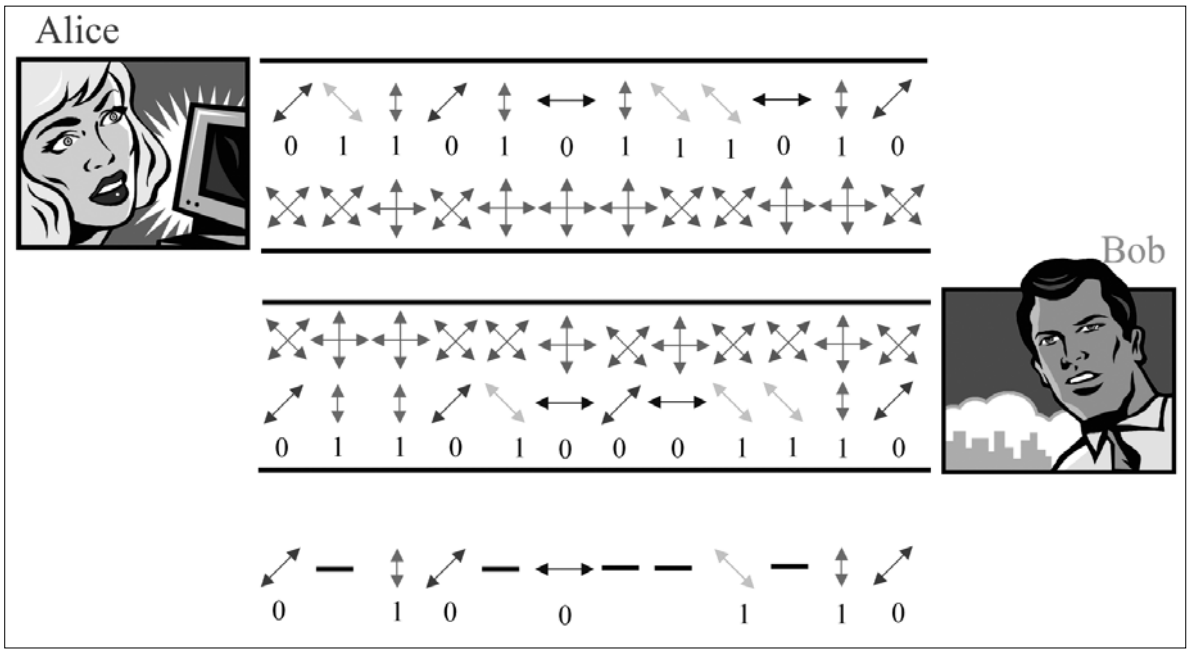
Amennyiben Bob eszerint az ábra szerint választotta meg detektorait, akkor Alice *„011010111010”* üzenetét *„011010001110”*-nak dekódolhatta. Azaz, ha Bob diagonális szűrőt használ az első foton vizsgálatához, akkor helyes eredményt kap, azaz ↗-t. Viszont, ha Bob rektilineáris szűrőt használ az első foton vizsgálatához, akkor a ↗ polarizációjú fotont tévesen ↕ vagy ↔ polarizáltságúnak fogja értelmezni. Ha ↔ polarizáltságúnak értelmezi, akkor az nem okoz problémát Bobnak, hiszen szintén logikai nullát reprezentál. Abban az esetben, ha Eve *nem próbálta meg lehallgatni a csatornát,* akkor biztosak lehetünk abban, hogy ahol Bob azonos polarizációjú szűrőt választott, ott ugyanazon az értéket kapja, mint amit Alice elküldött.

A következő szakaszban, a helyzet tisztázása érdekében Alice a publikus csatornát használva felhívja Bobot, s közli vele, hogy milyen polarizációs sémát használt az egyes fotonokon. A fotonok pontos állapotait azonban nem árulja el. Alice így például elmondhatja Bobnak, hogy az első fotont a ⟨↗,↖⟩ séma szerint kódolta, azonban azt már *nem közli,* hogy amit küldött az ↗ vagy ↖ állapotú foton volt-e. Ezt követően, Bob közli Alice-szel a helyesen dekódolt kvantumbitek *sorszámait*. Ezen pozíciókban Bob helyesen vizsgálta be a fotonokat, így helyesen állapította meg azok logikai értékeit is. Alice és Bob így figyelmen kívül hagyhatja azon fotonokat, amelyeknél Bob rosszul választott bázist, s a továbbiakban csak a helyesen értelmezett fotonokkal foglalkoznak. Az előbbi példában a polárszűrők sorrendje *„X++XX+X+XX+X”* volt, így a megtartott bitfüzérünk *„0100110”* lett.

A kulcsmegosztáshoz, s ezáltal a kvantumkriptográfia megvalósításához három *előkészítő* szakasz szükséges. A három szakasz tehát lehetővé teszi Alice-nek és Bobnak, hogy megállapodjanak egy normál számsorozatban. A kialakított üzenet egyik meghatározó tulajdonsága azonban, hogy az teljesen véletlenszerű, az üzenet ugyanis Alice teljesen véletlenszerű logikai érték illetve detektorválasztásából generálódott. Maga a számsorozat pedig nem hordoz tényleges üzenetet, mindössze egy *véletlenszerű kulcs,* amely teljesen véletlenszerűen kialakított füzért használjuk az *egyszer használatos kód* (OTP) szimmetrikus kulcsaként.

3.2. Eve megjelenése

Az előbbi példánál nem feltételeztük azt, hogy Eve hallgatózna, így nem kaphatott Bob téves eredményt *megfelelő bázisválasztás* esetében sem. Tekintsük most azt az esetet, amikor Eve hallgatózik a kommunikációban. Eve a kvantumcsatornán keresztül próbál hozzájutni a titkos kulcsunkhoz, azonban Eve sem tudhatja azt, hogy Alice milyen polarizáltságú szűrőt alkalmazott fotonjai elküldéséhez. Így például, ha az előző példában küldött üzenet esetén Eve ⟨↗,↖⟩ szűrőt használ az első foton vizsgálatához, akkor helyes eredményt kap, azaz ↗-t. Viszont, ha rektilineáris szűrővel próbálja meg megállapítani a kvantumbit állapotát, akkor a ↗ polari-

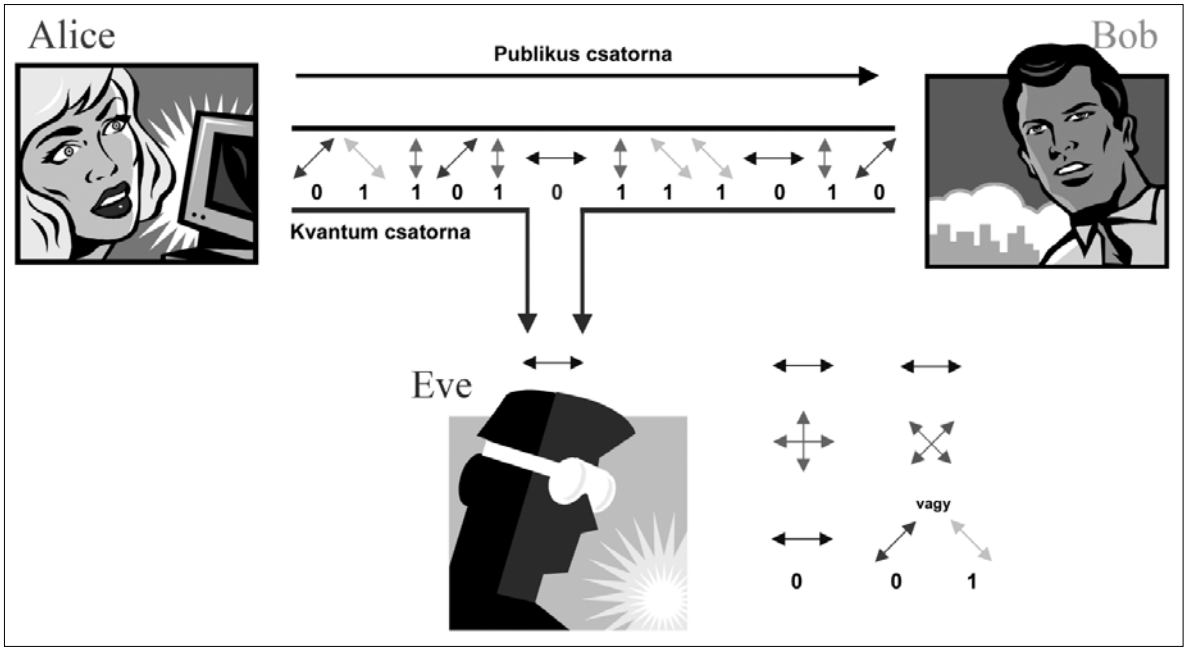


9. ábra Alice és Bob detektor-egyeztetést követően kialakított kulcsa

zációjú fotont tévesen ↕ vagy ↔ polarizáltságúnak fogja értelmezni. Amennyiben ↔ polarizáltságúnak értelmezi, valamint Bob a ⟨↗,↘⟩ bázisú szűrő helyett a téves ⟨↕,↔⟩ bázist választja a kvantumállapot detektálásához, akkor azzal ténylegesen nem okozna problémát, hiszen ezen polarizációs állapot is logikai nullát reprezentál. Azonban, ha ↕-nek értelmezi – *annak eredeti értékét megváltoztatva* – már logikai egyet továbbít a kvantumcsatornán keresztül. A téves detektorválasztásokat azonban a felek kiszűrik, így ezen bit mindenféleképpen kikerül a végleges kulcsból.

Eve helyzetét nagymértékben megnehezíti az, hogy minden egyes fotont csak *egyetlen egyszer* vizsgálhat. A fotont nem oszthatja két fotonra, és nem vizsgálhatja mindkét bázisban egyszerre. Eve így nem lehet biztos abban, hogy az elfogott kódszöveg pontos-e, ennek következtében nincs reménye a megfejtésére sem. Eve megpróbálhatja bemérni az Alice által elküldött fotont, de nem tudja, hogy rektilineáris vagy diagonális bázist használjon-e. Így az esetek *felében* rosszul dönt. Ekkor azonban még mindig pontosan olyan helyzetben van, mint Bob, aki szintén csak az esetek felében találja el a helyes bázist. Ezt követően azonban Alice közli Bobbal, hogy melyik fotonnál melyik lett volna a helyes detektor, így csak azok a fotonok kerülnek a kulcsfüzérbe, amelyeket Bob jól mért be. Eve-en azonban ez nem segít, mivel ezeknek a fotonoknak a felénél nem megfelelő detektort használt, ezért a kulcsot alkotó fotonok felének polarizációját is rosszul méri be.

A kvantumkriptográfia így lehetővé teszi, hogy Alice és Bob megállapodjon egy kulcsban, amely titkos kulcsot Eve csak hibásan lehet képes beazonosítani. Eve jelenléte a kvantum-kommunikációban pedig egyértelműen detektálható, a kvantumcsatornán okozott *irrever-*



10. ábra Eve hallgatózik a kvantum-csatornán

zibilis zavarok következtében. A mérési próbálkozásokkal Eve megváltoztatja a foton polarizációját, s ezen polarizációváltozások nyilvánvalóak Alice és Bob számára [7].

Abban az esetben például, ha Alice ↔-t küld, Eve pedig a nem megfelelő ⟨↗,↖⟩bázisú detektorral vizsgálja, akkor a detektor arra kényszeríti a beérkező ↔ állapotú fotont, hogy ↗ vagy pedig ↖ állapotban lépjen tovább. Ha Bob a maga ⟨↕,↔⟩ bázisú detektorával megvizsgálja az átalakított fotont, akkor lehetséges, hogy az Alice által küldött ↔-t kapja, de az is lehetséges, hogy ↕-ként fogja értelmezni, ami helytelen. Alice tehát egy vízszintesen polarizált fotont küldött, amihez Bob a megfelelő detektort használta, mégis rosszul mérte be az elküldött fotont. Ha tehát Eve rossz detektort választ, akkor *„csavar"* bizonyos fotonokon, amivel a vevőt esetenként hibára késztetheti, még akkor is, ha megfelelő detektort használ. Azonban ha Alice és Bob végez egy rövid ellenőrzést, akkor ezek a hibák kiküszöbölhetőek.

Alice-nek és Bobnak meg kell győződniük arról, hogy a kialakított füzér azonos-e. A füzér azonosságáról megbizonyosodni a legegyszerűbben úgy lehetne, ha Alice felhívná Bobot és közölné vele a sorrendet. Ekkor azonban ha Eve elfogja a hívást, hozzájuthatna a teljes kulcshoz. A teljes füzér egyeztetése azonban felesleges, ugyanis elég, ha Alice véletlenszerűen kiválaszt bizonyos mennyiségű elemet a bitfüzérből. Ha Bob ezeket helyesnek nyilvánítja, akkor elenyészően alacsony a valószínűsége annak, hogy Eve lehallgatta az eredeti adást.

Miután Alice és Bob nyíltan egyeztette a számokat, ezeket elvetik és kettejük közös, bináris számjegyekből álló egyszeri kulcsa az egyeztetésnél felhasznált bitek számával csökken. Amennyiben Alice és Bob eltérésre bukkan a vizsgált bitek között, akkor tudni fogják azt, hogy Eve hallgatózik. Ekkor az egész kulcsot kénytelenek eldobni.

3.2.1. Téves bázisú lehallgatás következményei

A következőkben tekintsük azt az esetet, amikor Eve téves polarizációjú szűrővel próbálja meg bemérni az Alice által küldött ↔ vízszintes polarizáltságú fotont. Eve ⟨↕,↔⟩ bázis helyett ⟨↗,↖⟩ bázist használ, miáltal módosítja a Bob felé továbblépő foton polarizációját. Példánkban legyen a *módosított foton* polarizációja↖. Ebben az esetben, ha Bob megfelelő bázisú detektort választ – tehát azt, amit Alice eredetileg is használt – akkor véletlenszerűen ↔-t vagy ↕-t kap. A *11. ábrán* azon esetet modelleztük, amikor a vevő a módosított polarizációjú fotont ↔-nak méri.

Ez esetben Bob nullát kapott, ami a detektoregyeztetésnél sem derül ki, ugyanis mindketten azonos polarizációjú szűrőt választottak és a kapott logikai érték is megegyezik a küldöttel. A kulcs tehát *0100110* lesz. Most nézzük azt, ha Bob tévesen 1-et kap, azaz a↖ polarizációjú fotont a rektilineáris szűrővel ↕-nek méri. A mérések kimenetele ekkor a *12. ábrán* látható módon alakul.

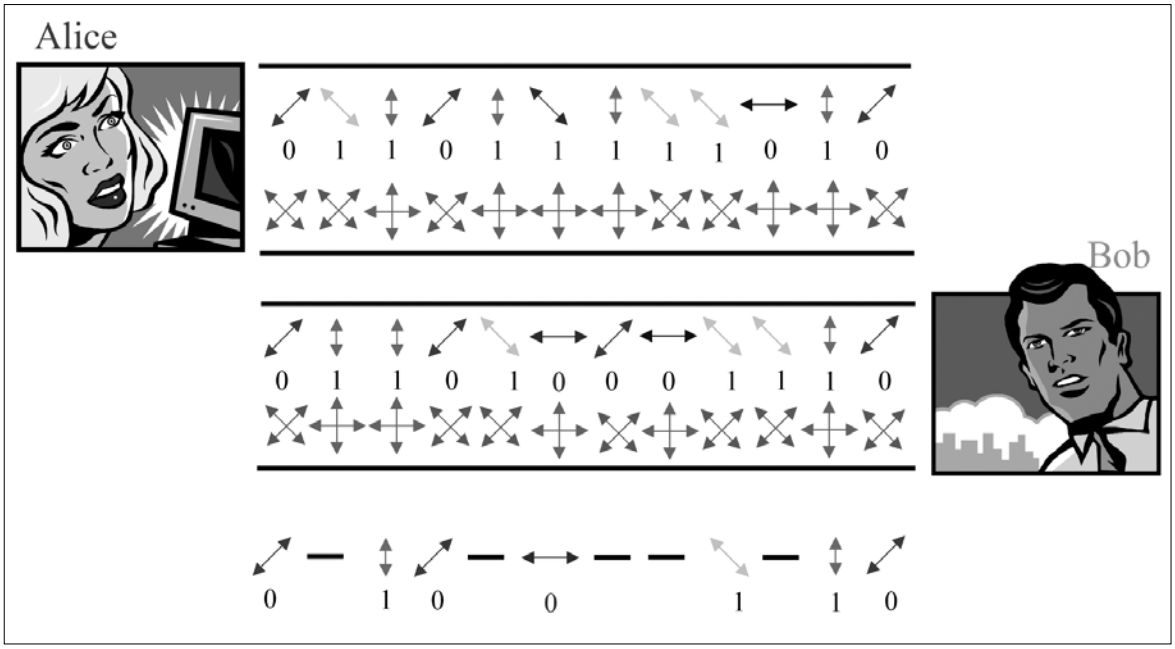
Ebben az esetben az ellenőrző szakaszban egyértelműen fény derül arra, hogy azonos bázisú detektorhasználat esetén eltér a küldött és mért érték.

3.3. A protokoll lépéseinek összefoglalása

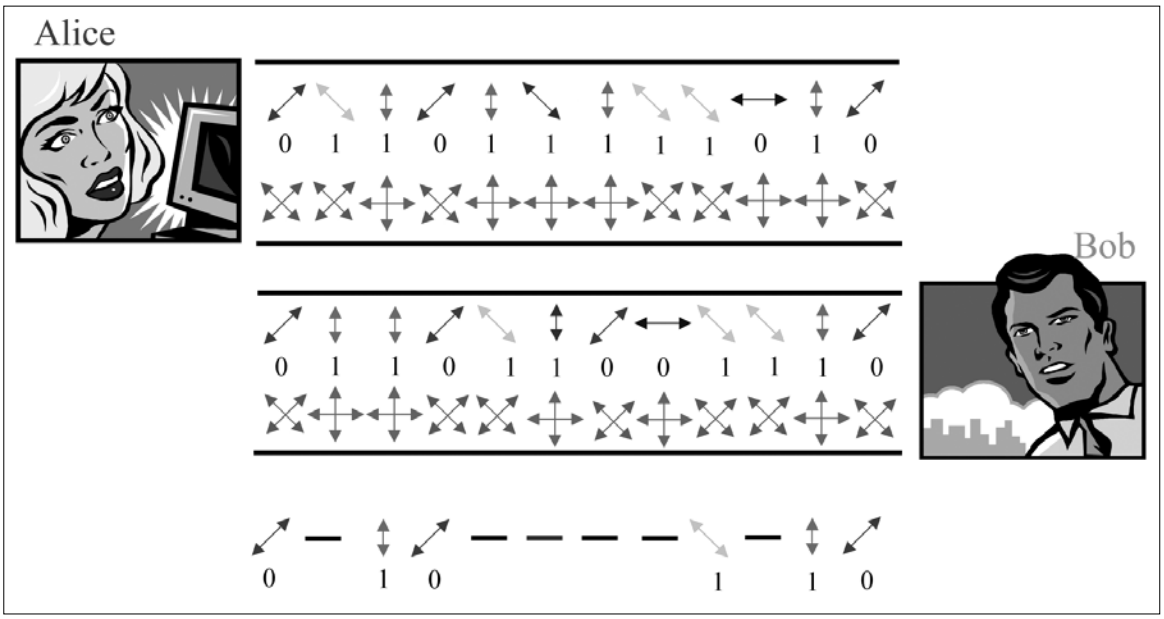
A kvantumkriptográfia tehát egy olyan titkosítási módszer, amely *fizikailag* teszi lehetetlenné az Alice és Bob közötti kommunikáció pontos lehallgatását. A kvantumkriptográfia segítségével Alice és Bob teljesen titokban megállapodhat egy egyszeri kulcsban, s a továbbiakban ezen kulccsal kódolják üzeneteiket [1].

Összegzésként a módszer öt fő lépése:

1. *Alice fotonfüzért küld Bobnak, aki ezt bevizsgálja.*
2. *Alice közli Bobbal, hogy az érkező fotonoknál melyik esetben választotta a megfelelő detektort. A helyes mérés eredményét nem árulja el, ezért azt a beszélgetést Eve hiába hallgatja le.*



11. ábra Bob azonos polarizációjú detektor estén helyes eredményt kapott



12. ábra Bob ebben az esetben rossz értéket kapott

3. *Alice és Bob elveti a nem megfelelő méréseket, csak a többivel foglalkoznak.*
4. *Alice és Bob néhány számjegy egyeztetésével ellenőrzi a kulcs érintetlenségét.*
5. *Ha az ellenőrzés eredménye megfelelő, akkor az egyszeri kulccsal kódolhatják üzeneteiket. Ha nem, akkor viszont tudják, hogy Eve hallgatózott, így kénytelenek újrakezdeni a műveletet.*

3.4. A kvantumkommunikáció sikeres lehallgatásának valószínűsége

A protokollon belüli kvantumkommunikációban Eve csak bizonyos valószínűséggel lehet képes helyesen meghatározni a kvantumcsatornára küldött kvantumállapot bázisát, illetve a helyes polarizációs állapotot. A protokoll által alkalmazott kvantumkommunikáció tulajdonságaiból következően leírhatjuk a sikeres kvantumállapot azonosításához tartozó explicit valószínűségeket is.

Abban az esetben, ha Eve megpróbálja bemérni az Alice által küldött kvantumállapotot, az esetek 50%-ban rossz bázist fog választani, miáltal az adott fotont kicseréli egy másikra. Eve így 50%-os valószínűséggel kap azonos állapotot. Ugyanakkor 50%-os valószínűséggel rossz bázist használ, azaz a fotonokat csak újabb 50%-os valószínűséggel tudja helyesen beazonosítani. Vagyis, ha *rossz bázist* választ, akkor összesen $1/2 \cdot 1/2 = 1/4$, tehát 25% valószínűséggel *helyes bitet* mér, illetve 25% valószínűséggel rosszat. Ugyanakkor, ha Eve jó detektort választ, – aminek a valószínűsége 50% – akkor biztosan jó állapotot mér. Eve-nek így *összesen 75% esélye van* arra, hogy jó állapotot mérjen és 25% annak a valószínűsége, hogy rosszat. Így Eve közbeavatkozása, minden fotonnál 25% valószínűséggel hibát okoz a kommunikációban.

Miután Eve bemérte Alice elküldött kvantumállapotát, azt visszahelyezi a kvantumcsatornára, majd továbbítja Bob felé. A Bobhoz kerülő, bemért kvantumállapot logikai értéke így az esetek 25%-ban eltér az Eve által visszahelyezett bit értékétől, hiszen Bob szintén 25% valószínűséggel mást fog mérni, mint amit Eve küldött. Tehát a 75%-os helyes érték 25%-ban rossz eredményt fog szolgáltatni, amely így $3/4 \cdot 1/4 = 3/16 = 0.1875$, tehát 18,75%-nyi hibát jelent. Továbbá, a 25% hibásan továbbküldött fotont pedig 75% valószínűséggel rossznak fogja mérni Bob, amely ismét $3/16 = 0.1875$, azaz 18,75%-nyi hibát jelent a kvantum-kommunikációban.

Összefoglalva, Bob *18,75% + 18,75% = 37,5%*-ban nem azt fogja fogadni, amit Alice eredetileg küldött, függetlenül attól, hogy éppen azonos bázist használtak-e, hiszen Eve mindkettőjüktől függetlenül tudja csak megválasztania a bázisát. Egy ilyen jelentős hibát Alice és Bob könnyen észrevehet, ha néhány azonos bázissal átküldött bitet egyeztetnek a klasszikus csatornán, amit elvetnek a kulcsból. A kvantumbitek hitelesítése során, a felek kiszűrik a téves bázisú kiolvasásokat, majd a megmaradt, helyes bázisban dekódolt kvantumbitek helyességét ellenőrzik, azok bitértékeinek összehasonlításával. A téves bázisú dekódolások eltávolítása után kialakult bitsorozatban lévő különbségek pedig egyértelműen felfedik Eve közbeavatkozását.

3.5. A kvantumkód megszerzésének valószínűsége

A protokollon belüli kvantumkommunikáció lehallgatásával Eve, az esetek (3/4) részében juthat helyes eredményre, így egy N kvantumbites kvantumkód észrevétlen lehallgatásának valószínűsége $(3/4)^N$, ami elhanyagolható, ha N értéke megfelelően megválasztott.

Így, már egy igen alacsony értéket – mindösszesen 50 kvantumbitet – tartalmazó kulcs esetén, Eve mindösszesen $(3/4)^{50} = 0.0000005663216564269$ valószínűséggel lehet képes helyesen beazonosítani a küldött bitsorozatot. A protokollon belüli kvantumkommunikáció észrevétlen támadása így $(3/4)^N$ valószínűséggel maradhat csak felderítetlenül, ami elhanyagolhatónak tekinthető a gyakorlatban alkalmazott N értékek mellett. Eve támadása így nagyon nagy valószínűséggel kiszűrhető, hiszen a kvantumcsatorna támadása nem marad-

hat észrevétlen, mivel elkerülhetetlen hibákat okoz a kvantumkommunikációban. Amennyiben a felek nem találnak eltérést a helyes bázisban dekódolt kvantumbiteket tartalmazó bitfüzérben, akkor Alice és Bob biztos lehet abban, hogy az elküldött biteket nem szerezte meg senki.

A gyakorlatban a kvantumbitet kibocsátó forrás, az átviteli csatorna és esetlegesen maga az adattároló egység is szolgálhat zajforrásként a kvantumkommunikációban, miáltal romolhat a letisztázott bitsorozat tökéletes állapota. A hibával számolnunk kell, elkerülhetetlen, mindaddig, amíg az egy tolerálható érték alatt marad. Eve esetleg próbálkozhatna azzal is, hogy visszafogja magát és hallgatózását bizonyos küszöb alatt tartja, így abban reménykedve, hogy a terminálnak nem tűnik fel tevékenysége. Azonban a gyakorlatban ezen próbálkozása csak elhanyagolhatóan kis valószínűséggel segítené a kvantumbitek sikeres megszerzésében.

3.6. A kvantumkriptográfia működésének formális modellezése

A kvantumkriptográfia esetében a véletlenszerűség kitüntetett szerepet kap, hiszen az adó által elküldött foton bázisától és polarizációjától kezdve, a lehallgató szintén véletlenszerű mérési eredményein keresztül, egészen a vevő szintén véletlenszerűen bemért fotonjáig, a fő szerepet a véletlenszerű működés játssza. A protokoll során a $k \in \{0,1\}^N$, $N>0$ közös kulcs kialakítása egy dedikált kvantumcsatornán keresztül történik, bármiféle előzetes információcsere nélkül [5]. Miután a közös kulcs kialakult, Alice és Bob szimmetrikus kulcsú titkosítást alkalmazva kódolják üzeneteiket.

3.6.1. A protokoll lépéseinek formális leírása

Kommunikáció a kvantumcsatornán keresztül:

1) Alice generál egy *n* bitből álló, véletlenszerű bitsorozatot. A bitsorozat az átküldeni kívánt értékeket szimbolizálja. $A = \{a_i \mid 0 \le i \le n-1\} = [a_0, a_1, \ldots a_{n-1}]$.

2) Alice, az *A* halmazban lévő véletlenszerű bitekhez, szintén véletlenszerűen választ bázist. A bázis lehet rektilineáris, ekkor a $\beta = \langle \updownarrow, \leftrightarrow \rangle$ jelölést használjuk, illetve lehet diagonális, ekkor a $\beta = \langle \nearrow, \searrow \rangle$ jelölést alkalmazzuk. A bitekhez tartozó detektorsorrendet így a következőképpen jelölhetjük:

$$B = \{\beta_i \mid 0 \le i \le n-1\} = [\beta_0, \beta_1, \ldots \beta_{n-1}].$$

3) Alice, az *A* halmaz bitjeit a *B* halmazban lévő, indexnek megfelelő bázissal kódolja, majd a létrehozott kvantumbitet átküldi a kvantumcsatornán.

4) Bob minden egyes fotont egyenként detektál.

5) A fotonok detektálásához véletlenszerűen választ bázist, majd dekódolja a kvantumbitet. Bob minden egyes fotont β' bázisban dekódol, azaz vagy $\langle \updownarrow, \leftrightarrow \rangle$ bázist választ, vagy $\langle \nearrow, \searrow \rangle$ bázist.

A kapott dekódolt bitsorozat Bob oldalán tehát a következő:

$$A' = \{a'_i \mid 0 \le i \le n-1\} = [a'_0, a'_1, \ldots a'_{n-1}].$$

Kommunikáció a publikus csatornán keresztül:

1) *Bázisegyeztetési szakasz*

Ebben a szakaszban Bob közli Alice-el, hogy az *A'* dekódolt bitsorozatban, az adott a'_i bit detektálásához milyen β_i bázist választott.

2) *Hibás detektorválasztások kiszűrése*

Miután Bob közölte Alice-szel a választott detektorokat, Alice elárulja az adott a'_i bithez tartozó bázist. Alice ezek után az *A* sorozatból eldobja azokat a biteket, ahol különböző detektorokat választottak. Ugyanígy tesz Bob is a másik oldalon, így a kulcsban csak azon a_i, a'_i bitek maradnak, amelyekre teljesül a $\beta_i = \beta'_i$ összefüggés.

A kialakított kulcs az *elsődleges* kulcs. Az Alice és Bob oldalán kialakult kulcs jelölése legyen $k_{ELSŐDLEGES_A}$ és $k_{ELSŐDLEGES_B}$.

3) *Hibaellenőrzési szakasz*

Alice és Bob a kialakult elsődleges kulcsból, egy esetleges lehallgatás detektálása érdekében feláldoznak egy bizonyos nagyságú részt. Ezen kulcsrész jelölése legyen $k_{Ellenőrzés}$. Helyes bázisú mérés során kapott hibás bit esetén egyértelmű a lehallgatás ténye, így a kulcsot azonnal elvetik a felek. A sikeres ellenőrzés után kialakul az *egyeztetett* kulcs mindkét oldalon:

$$k_{EGYEZTETETT_A} = k_{ELSŐDLEGES_A} - k_{Ellenőrzés_A}.$$
$$k_{EGYEZTETETT_B} = k_{ELSŐDLEGES_B} - k_{Ellenőrzés_B}.$$

4) *Megerősítési szakasz*

A megerősítési szakasz célja a támadó által esetlegesen megszerzett információ további redukálása. Miután a feláldozott kulcsrészletben nem találtunk hibát, a kialakult egyeztetett kulcson még további, biztonsági ellenőrzéseket hajtunk végre. A kulcsból nem egy adott részt választunk ki, hanem véletlenszerűen egy-egy bitet.

Ebben a szakaszban Alice meghatározza a kommunikáció bithiba-arányát kifejező λ értéket, illetve a γ-vel jelölt biztonsági paramétert [1].

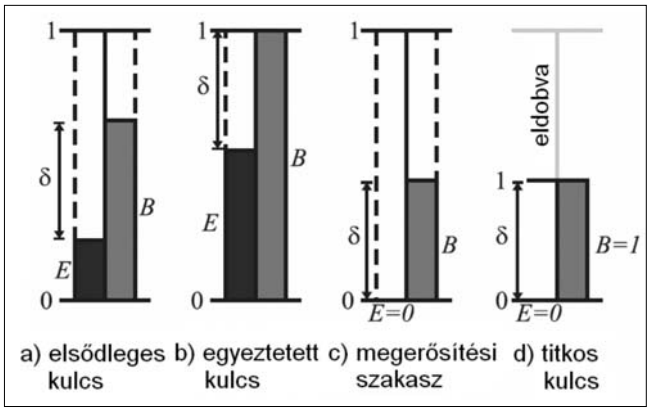
Miután ezen értékek kialakultak, Alice véletlenszerűen kiválaszt $r = n - \lambda - \gamma$ bitet az egyeztetett kulcsból. Azonban az ellenőrzés során ahelyett, hogy a konkrét bitértékeket átküldenék egymásnak, a *paritásokat* vizsgálják [2]. A folyamat során az *n* bites kulcsunkról készítünk egy $n - \lambda - \gamma$ bites lenyomatot, azaz egy véletlenszerű *f* hash függvényt alkalmazunk, a következő leképezést realizálva: $f : \{0,1\}^n \to \{0,1\}^{n-\lambda-\gamma}$, ahol $\gamma > 0$.

Ekkor, annak a valószínűsége, hogy az egyeztetés során egy esetleges lehallgató megszerzi a kulcsunkat, a következőképpen adható meg:

$$P \le \frac{2^{-\gamma}}{\ln 2}.$$

Az előző lépésben történt hibaellenőrzési eljárás nem biztosítja azt, hogy Eve nem juthatott hozzá a kulcsunk bizonyos részeihez. A megerősítési szakasz fő célja tehát ezen rejtett hibák kiszűrése.

A *13. ábrán* a kulcsok méreteinek változását láthatjuk az egyes ellenőrzési szakaszokban.



13. ábra
A kulcsméretek alakulása a kulcskialakítási szakaszokban

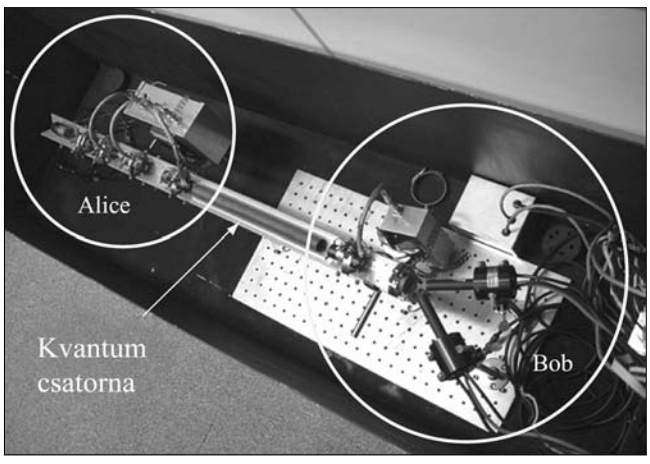
4. A kvantumkriptográfia gyakorlati megvalósítása

Wiesner tanulmánya tehát egy abszolút biztos kommunikációs rendszer létrejöttét segítette elő. A kriptográfusok lelkesen üdvözölték Bennett és Brassard kvantumkriptográfiáját, néhányan azonban úgy tartották, hogy a gyakorlatban megvalósíthatatlan. Bennett és Bassard azonban biztosak voltak a dolgukban. 1988-ban Bennett elkezdte összegyűjteni a kvantumkriptográfia megvalósításához szükséges eszközöket, segítségként maga mellé vette John Smolin kutatót.

Egy fénytől elzárt laboratóriumba vonultak és megpróbáltak polarizált fotonokat küldeni a helyiség egyik pontjáról a másikra. A fotonküldést egy Alice nevezetű számítógép irányította, a vételi oldalon pedig egy Bobnak keresztelt számítógép döntötte el, hogy melyik fotonhoz milyen detektort használ. Alice-nek és Bobnak sikerült fotonokat küldenie és fogadnia, elvetve a helytelenül bemért biteket, így megállapodva egy egyszeri kulcsban. Bennett kísérlete bebizonyította, hogy két számítógép képes abszolút titkosan kommunikálni egymással.

A gyakorlati megvalósítás azonban nem egyszerű feladat, mert a fotonok nehezen közlekednek. Ha Alice levegőn át küld egy bizonyos polarizációjú fotont, akkor az útjában álló levegő molekulái megváltoztatják polarizációjukat. Jobb megoldás a száloptika alkalmazása. A Genfi egyetemnek 1995-ben sikerült száloptika alkalmazásával megvalósítani egy Genf és Nyon közötti 23 km-es távolságon alkalmazni a kvantumkriptográfiát. A szabadtérben megvalósított eddigi legnagyobb távolság 23 km volt, ezt Münchenben hajtották végre. A szabadtéri kvantumkommunikáció azonban egyelőre sokkal lassabbnak bizonyul, mint az optikai szálas kivitelezés.

14. ábra
A kvantumkriptográfia első kísérleti megvalósítása



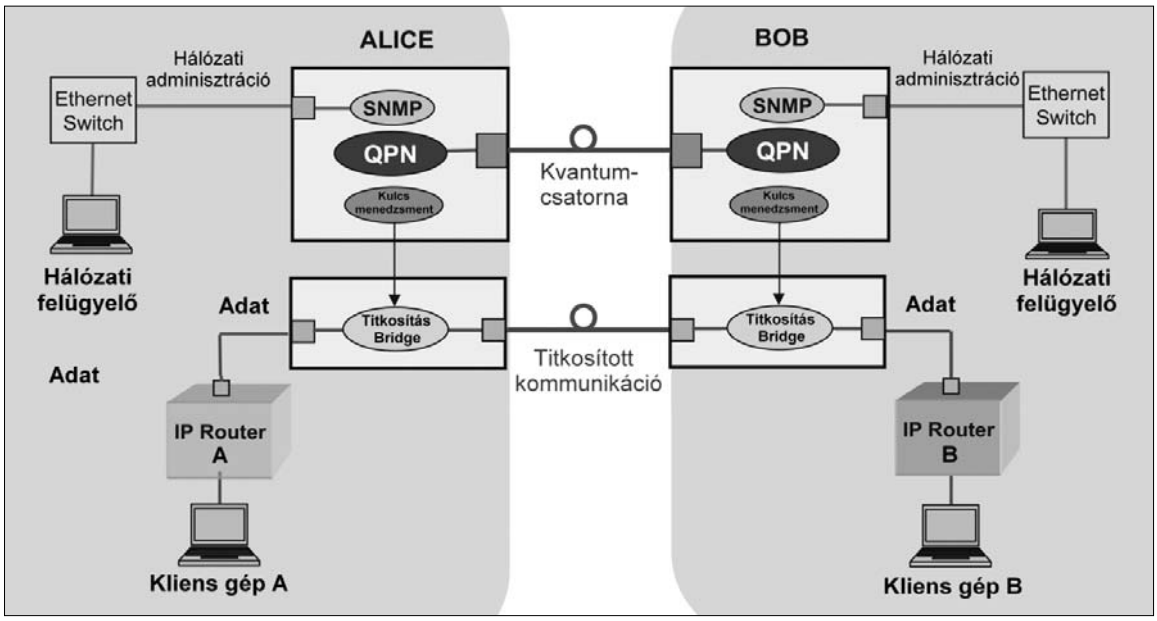
Az első kvantumkriptográfiára épülő banki tranzakciót Ausztriában, Bécsben hajtották végre. Anton Zeilinger laboratóriumából a fejlesztőcsapat egy 3000 eurós átutalást intézett a bank felé, kihasználva a kvantumcsatorna nyújtotta abszolút biztonságot. A kvantumkriptográfia megvalósításához szükséges eszközök már ma is elérhetőek a piacon. A technológia azonban jelenleg még drága, így a potenciális vásárlói kör is meglehetősen szűkre szabott. Az új eszközök elsősorban kutatóintézetek és kormányzati hivatalok, bankok számára jelenhetnek egy fejlettebb, biztonságosabb alternatívát.

A fotonok véletlenszerű viselkedése a kvantummechanikában egy olyan jelenség, amelyet a gyakorlatban több helyen is felhasználhatunk. Így, az előzőekben tárgyalt kvantumkriptográfián kívül alkalmazhatjuk például *valódi véletlenszám-generátorként* is. A foton alapú véletlenszám előállításhoz szükséges eszközök már kereskedelmi forgalomban is elérhetőek, PCI, USB-eszközként, illetve OEM-chipként, egy egyszerű perifériaként illeszthetőek egy klasszikus számítógéphez. Egy klasszikus, determinisztikus működésű számítógéppel csak *álvéletlen-számokat* állíthatunk elő, így az a *valódi véletlenszám-generátort* csak közelíteni képes. A kvantummechanika jelenségeire építve azonban lehetőségünk adódik a valódi véletlenszámok előállítására is, egy klasszikus számítógépes rendszeren belül is.

4.1. Kvantumkriptográfiai eszközök

A jelenleg forgalmazott kvantumtitkosító eszközökkel 80-110 km-es távolságon valósítható meg a tökéletesen biztonságos kommunikáció. Az optikai szál alapú implementációk esetén a detektorok pontatlansága, illetve a különböző zajforrások jelentik a szűk keresztmetszetet. Emellett, jelenleg még nem áll rendelkezésünkre az optikai erősítőhöz hasonlító „kvantumállapot-erősítő” eszköz, így a kvantumbiteket gyenge koherens lézernyalábbal küldjük át a kvantumcsatornán. A kvantumkriptográfia implementációjához szükséges eszközök az adatkapcsolati rétegben működnek, transzparens módon.

15. ábra Kvantumtitkosító berendezés



16. ábra Kvantum-kriptográfia alkalmazása hálózati környezetben

A kvantumtitkosító eszközökkel megvalósított hálózati kommunikáció egy lehetséges implementációja látható a *16. ábrán*, ahol a hálózaton belüli adatkommunikáció titkosítását a kvantumcsatornán kialakított kulccsal hajtjuk végre [8]. A kvantumcsatorna egy szabványos optikai szál segítségével is megvalósítható, így a már kiépített optikai hálózatok tökéletesen alkalmazhatóak a kvantumkriptográfia gyakorlati implementációiban. A kvantumkriptográfia hálózati rendszereken belüli alkalmazása során azonban figyelembe kell vennünk, hogy az üvegszálon csak passzív optikai elemek lehetnek, a foton szintű kommunikáció következtében pedig a modell rendkívül érzékeny a detektor-zajokra [8].

A kvantumtitkosító eszközök LAN, MAN, SAN hálózatokon belül is alkalmazhatóak. A gyakorlati implementációk a fellépő zavarok következtében egyelőre csak limitált távolságon (<100km) képesek garantálni a tökéletes biztonságot. Azonban kaszkádosítással nagyméretű hálózati rendszerek védelme is megvalósítható, így a kvantum-titkosítás által nyújtott biztonság egy-egy hálózat egészére kiterjeszthető.

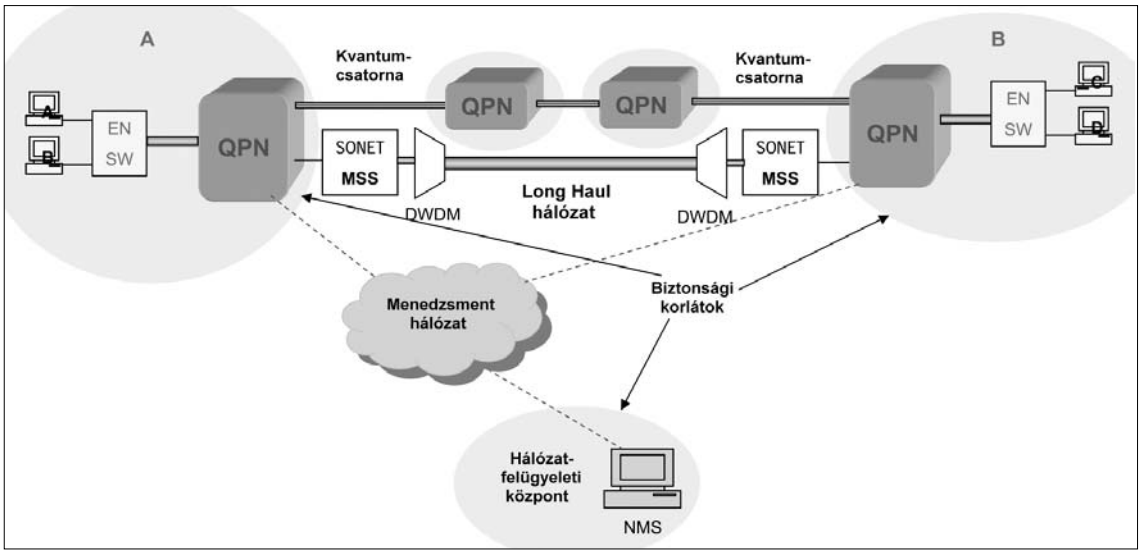
A *17. ábrán* egy „long-haul” hálózati implementáció gyakorlati megvalósításának vázlatát láthatjuk [8].

Az eszközök támogatják az összes fejlett, illetve napjainkban alkalmazott titkosító és hitelesítő algoritmust, így például a 128, 192, 256 bites AES-t valamint a HMAC-SHA1, HMAC-SHA-256 stb. módszereket. Az eszközök legtöbbje beépített véletlenszámgenerátorral rendelkezik, a protokoll lehallgathatatlanságát pedig a beépített intelligens lehallgatás-detektáló rendszer garantálja.

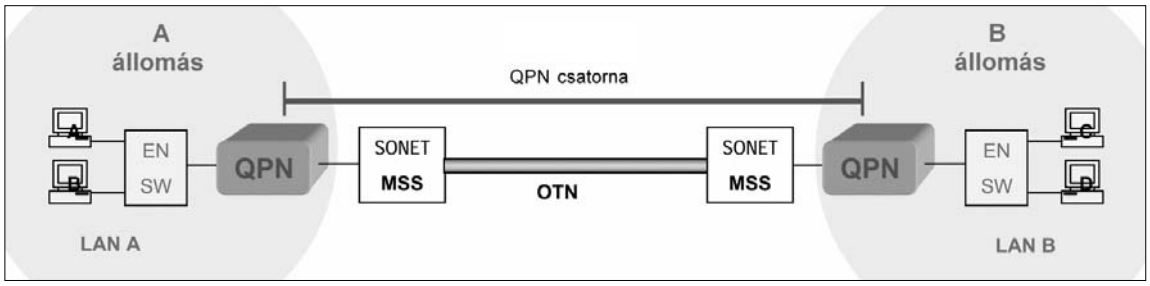
A kvantumkriptográfia által védett kommunikáció kiterjeszthető LAN-ok közötti kommunikációra is, ahogyan azt a *18. ábrán* láthatjuk [8].

Az eszközökkel megoldható Ethernet-hálózatok technikailag vagy logikailag elkülönülő részeinek összekapcsolása is, a hálózaton belüli adatforgalom kvantum-alapú titkosítása mellett. A kvantum-kommunikációhoz szükséges kvantumcsatornát Gigabit Ethernet hálózatok között is felépíthetjük [8].

Összefoglalva, az optikai szál alapú gyakorlati implementációk egyik legfontosabb tulajdonsága, hogy a protokoll a már kiépített optikai hálózatokon keresztül is megvalósítható. A kvantumcsatorna implementálásához mindösszesen egy dedikált optikai üvegszál szükséges a küldő és a vevő között.



17. ábra Long haul megvalósítás



18. ábra LAN-ok közti kvantum-kommunikáció

5. Összefoglalás

Mennyi idő múlva terjedhet el a gyakorlatban a kvantumkriptográfia? Jelenleg nem kínál előnyöket, mert napjaink titkosító algoritmusai révén rendelkezésünkre állnak a gyakorlatban feltörhetetlen kódok [4], azonban, ha a kvantumszámítógépek valósággá válnak, akkor az RSA és a többi modern kriptográfiai eljárás mind használhatatlan lesz, így szükségessé válik a kvantumkriptográfia használata. De vajon a kvantumkriptográfia időben a segítségünkre lesz?

A kvantumkriptográfia nemcsak gyakorlatilag feltörhetetlen kód, hanem abszolút értelemben is az. A kvantumelmélet lehetetlenné teszi, hogy Eve helyesen értelmezze az Alice és Bob közötti megállapodás értelmében kialakult kulcsot. Kijelenthető, hogy ha egy kvantumkriptográfiával titkosított üzenetet valaha is megfejtenének, akkor hibás a kvantumelmélet, ami az egész fizikát alapjaiban döntené össze. A módszer biztonságos kommunikációt garantál a kormánynak, katonaságnak, az üzleti életben, s a nagyközönség számára is.

A szerzőről

GYÖNGYÖSI LÁSZLÓ 2008-ban szerzett kitüntetéses diplomát a BME Villamosmérnöki és Informatikai Kar műszaki informatika szakán, infokommunikációs rendszerek biztonsága szakirányon. Jelenleg PhD hallgató a BME Villamosmérnöki és Informatikai Kar Híradástechnikai Tanszékén. Főbb kutatási területei a kvantuminformatika, a kvantum-kommunikációs protokollok, valamint a kvantumkriptográfia.

IMRE SÁNDOR Budapesten született 1969-ben. 1993-ban szerzett diplomát a BME Villamosmérnöki és Informatikai Karán. 1996-ban dr. univ., 1999-ben PhD, 2007-ben MTA Doktora fokozatott szerzett. Jelenleg a BME Híradástechnikai Tanszékén egyetemi tanár, vezeti a Mobil Távközlési és Informatikai Laboratóriumot, valamint a BME Mobil Innovációs Központjának tudományos kutatási igazgatója. Főbb kutatási területei a korszerű mobil infokommunikációs rendszerek rádiós és hálózati kérdései, valamint a kvantumalapú informatika.

Irodalom

[1] Bennett, Ch.H., Brassard, G., Crépeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Transactions on Information Theory 41(6), pp.1915–1923., November 1995.

[2] Brassard, G., Crépeau, C.: 25 years of quantum cryptography. SIGACT News 27(3), pp.13–24., 1996.

[3] Imre, S., Balázs, F.: Quantum Computing and Communications – An Engineering Approach. John Wiley and Sons Ltd, 2005.

[4] Diffie, W., M.E. Hellman: New directions in cryptography. IEEE Transactions on Information Theory IT-22(6), pp.644–654., 1976.

[5] Ekert, A.: Quantum cryptography based on Bell's theorem. Physical Review Letters 67(6), pp.661–663., 1991.

[6] Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proc. of 35th Annual Symposium on Foundations of Computer Science (1994)

[7] Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned Nature 299, p.802 (1982).

[8] Audrius Berzanskis: Applications of Quantum Cryptography in Government, MagiQ Technologies, SC05, November 12-18, 2005.

19. ábra Gigabit Ethernet hálózatok közti kvantumtitkosítás megvalósítása