QUANTUM CRYPTOGRAPHY: QUANTUM KEY DISTRIBUTION, A NON-TECHNICAL APPROACH

KVANTUMKRIPTOGRÁFIA: KVANTUMKULCS-ELOSZTÁS, EGY NEM-TECHNIKAI MEGKÖZELÍTÉS[1]

FRIGYIK András[2]

Abstract

With the rapid development of quantum computers the currently secure cryptographic protocols may not stay that way. Quantum mechanics provides means to create an inherently secure communication channel that is protected by the laws of physics and not by the computational hardness of certain mathematical problems. This paper is a non-technical overview of quantum key distribution, one of the most well-known application of quantum cryptography, a type of cryptography poised to exploit the laws of quantum mechanics.

Keywords

secure communication, quantum cryptography, quantum key distribution, BB84, entanglement

Absztrakt

A kvantumszámítógépek gyors fejlődésének köszönhetően a jelenleg biztonságos kriptográfiai rendszerek nem feltétlenül maradnak azok. A kvantummechanika lehetőséget ad arra, hogy egy olyan kommunikációs csatornát hozzunk létre, amely biztonságát a fizika törvényei garantálják, és nem azon alapul, hogy bizonyos matematikai számításokat klasszikusan nagyon nehéz kiszámolni. A cikk egy nem-technikai áttekintése a kvantumkulcs-elosztásnak, amely talán a legismertebb alkalmazása a kvantumkriptográfiának, egy olyan fajta kriptográfiának, amelyik közvetlenül a kvantummechanika törvényeire építkezik.

Kulcsszavak

biztonságos kommunikáció, kvantumkriptográfia, kvantumkulcs-elosztás, BB84, összefonódottság

[1] A tanulmány angol nyelvű változata a Proceedings of the Engineering Symposium at Bánki, ESB21, 2021 jelent meg.

[2] frigyik.andras@uni-obuda.hu | ORCID: 0000-0002-4220-4680 | associate professor, Óbuda University | egyetemi docens, Óbudai Egyetem

BEVEZETÉS

Közeleg a Q-Nap! A közelmúltban megjelent egy *Feature* cikk [1] a *Nature* című lapban, amelyben a szerző igyekszik felmérni milyen veszélyt jelentenek a kvantumszámítógépek a jelenleg használatban lévő kriptográfiai rendszerekre. A fent említett Q-Nap arra a napra utal, amikor a kvantumszámítógépek (*Quantum computers*) képessé válnak a jelenleg alkalmazott biztonsági védelmek feltörésére.

A kommunikációs rendszereink biztonsága ma azon az elven alapul, hogy bizonyos matematikai problémák nehezek: Még ha hozzá is férnénk egy szuperszámítógéphez akkor sem tudnánk kiszámolni az eredményt ésszerű időn belül. Számok prímekre bontása vagy a diszkrét logaritmus problémája (számelméleti változata a jól ismert logaritmus keresési kérdésnek) nehéz mert nem ismerünk olyan algoritmust amelyik minden esetben hatékonyan meg tudná oldani a problémát. Viszont, ha valaki azt állítja, hogy tudja a megoldását egy ilyen jellegű matematikai problémának, akkor azt könnyű leellenőrizni.

Ha azoknak van igazuk akik a kvantumszámítógépek eljövetelét hirdetik akkor a helyzet egyik napról a másikra megváltozhat. Ezek a számítógépek elviekben képesek lesznek arra, hogy a jelenleg gyakorlatilag megoldhatatlan problémákat nagyon hatékonyan megoldják. Annak érdekében, hogy a titkos adatainkat megvédjük több dolgot is tehetünk. Az egyik ilyen lehetőség a postkvantum vagy kvantum utáni kriptográfia. Egy másik lehetőség az, hogy a titkosításhoz használt kulcsot extrém biztonsággal juttassuk el a felhasználóhoz: A kvantummechanika segítséget nyújt ahhoz, hogy lehallgatásbiztos kommunikációs csatornát hozzunk létre. Ha a lehallgató személynek nincs mit feltörnie akkor teljesen mindegy milyen számítógéphez van hozzáférése. Ez a cikk igyekszik egy nem-technikai bevezetőt adni egy most is fejlesztés alatt álló módszerhez, amit kvantumkulcs-elosztásnak hívnak. Világossá szeretném tenni milyen szerepet játszik a kvantummechanika ebben a folyamatban.

A cikk további része a következő módon alakul: A 2. fejezet az első olyan rendszerről szól amelyik közvetlenül használta a kvantummechanikát titkosításra. A rendszer kizárólag a Heisenberg-féle határozatlansági elven alapul. A 3. fejezetben egy olyan rendszert írunk le amelyik a kvantummechanika egy másik sajátos jelenségén, az összefonódottságon alapul és ennek segítségével teszi a csatornát biztonságossá. Nem könnyű egy kvantum rendszert létrehozni és vezérelni. Általánosságban, egy komplex rendszer jobban ki van szolgáltatva minden fajta támadásnak, mint egy egyszerű. Az eszközfüggetlen megvalósítása a titkosító rendszereknek éppen ezt a hátrányt próbálja kiküszöbölni: A protokoll bármilyen eszközzel megvalósítható mindaddig amíg az az eszköz az előírásoknak megfelelően működik. Vannak olyan megoldások is, amelyek még akkor is lehallgatás biztosak ha az eszközt egy ellenséges fél hozta létre. A 4. fejezet ezt a témát járja körbe.

A cikk a kriptográfia kvantumos oldalára kíván koncentrálni. A klasszikus kriptográfia fogalmait megtalálhatja az olvasó bármelyik ezzel foglalkozó tankönyvben, például lásd [4] vagy [24]. Nagyon sok cikk foglalkozik a kvantumkulcs elosztás technikai leírásával, pl. lásd [5] és [6], csak hogy egy párat említsünk.

Ennek a cikknek az ötlete akkor született meg amikor kezembe akadt Mordechai Rorvig cikke [22] a *Quanta magazine*-ben valamint Nyári Norberté [23] a *Biztonságtudományi Szemle* folyóiratban.

ALAPÖTLET: BB84

A kriptográfiában a kulcs-elosztás célja az, hogy nagyon-nagy biztonsággal (kerül amibe kerül) megosszunk egy kis mennyiségű információt, ami később egyszer használatos kulcsként szolgál más üzenetek biztonságos kódolására és dekódolására. Feltételezzük, hogy a kommunikáló felek korábban nem osztottak meg titkos információt egymással: Csak az éppen megosztott kulcsot használhatják titkos kommunikációra.

Kvantumkulcs-elosztás esetén a kommunikáló felek a kvantummechanika segítségével teszik biztonságossá a elosztás folyamatát. A kvantumkulcs-elosztásról szóló első cikket [2, 3] 1984-ben publikálta Charles H. Bennett és Gilles Brassard, innen jön a protokoll neve: BB84. A szokásokhoz híven a kommunikáló feleket Aliznak és Bobnak fogjuk hívni és a lehallgató személy neve Éva lesz, az angol Eve-ből, ami a lehallgatásra (*eavesdropping*) utal. Aliz csak és kizárólag Bobbal szeretné megosztani egy titkos kulcsot, hogy aztán titokban tudjon kommunikálni vele. Ennek érdekében egy kvantum és egy klasszikus csatornát nyit Bob felé, de ezt csak akkor használja amikor a protokoll ezt megengedi. A protokollon kívül a két fél nem kommunikál. A kvantum csatorna kvantum biteket használ, olyan biteket, amelyek megfigyelhetően a kvantummechanika szabályai szerint viselkednek. A klasszikus csatorna szokásos klasszikus biteket használ. A kétfajta bit nagyon másképpen viselkedik ha kérdéseket teszünk fel nekik.

Egyik módja, hogy elképzeljünk egy bitet a következő: Képzeljünk el egy kör alapú kijelzőt (egy tárcsát) rajta egy mutatóval. Ha ábrázolni szeretnénk az 1-es és a 0-s értéket azt nagyon sokféleképpen megtehetjük. Például a mutató irányulhat északra (fel) vagy délre (le) és ekkor azt mondhatjuk, hogy a bit, amit ábrázol 1-es értékű. Vagy mutathat keletre, illetve nyugatra, ami a 0-s értéknek felelhet meg. Egy másik lehetőség az, hogy az 1-es értéket a mutató északkeleti vagy délnyugati állásához rendeljük és északnyugati vagy délkeleti pozíció a 0-s értéknek felel meg.

Tegyük fel Aliz előkészít egy klasszikus bitet a tárcsa és mutató segítségével és elküldi azt Bobnak. Bob rendelkezésére két különböző maszk áll. Az egyiket egyenes vonalúnak (*rectilinear*, R) nevezzük és a bevágások a maszkon észak-déli, illetve kelet-nyugati irányúak. A másikat diagonálisnak (*diagonal*, D) és ennek a maszknak a bevágásai északkelet-délnyugati, illetve északnyugat-délkeleti irányúak. Ha Aliz egy olyan tárcsát küldött Bobnak, ahol a mutató északra néz és Bob az R maszkot használja akkor ki tudja olvasni a bit értékét, ami 1 lesz. Ha Bob a D maszkot használja, akkor semmit nem kap eredményül, de mégis hozzájut bizonyos információhoz, mégpedig ahhoz, hogy nem a megfelelő maszkot használta.

Ezek után tegyük fel, hogy Aliz egy kvantum bitet készít elő egy kvantum tárcsát és mutatót használva, de ugyanazt az ábrázolást használva, mint korábban. Az előkészített bitet, ismét, elküldi Bobnak. Bob ugyanazokkal a maszkokkal rendelkezik, mint eddig. Ha az Aliz által küldött tárcsán a mutató északra néz és Bob az R maszkot használja akkor a helyes értéket, az 1-est, kapja. Azaz, ha Aliz állandóan olyan tárcsákat küld, amelyen a mutató északra néz és Bob állandóan az R maszkot használja akkor folyton a jó eredményt fogja kapni. De ha Bob úgy dönt, hogy a D maszkot használja inkább, akkor azt fogja tapasztalni, hogy minden esetben kap valamilyen értéket, de az esetek felében 1-est kap, míg a többi esetben 0-s értéket fog megfigyelni. Ebben a viselkedésben nyilvánul meg a kvantumos jellege a bitnek. Ha Aliz csak egyetlen bitet küld Bobnak és Bob szabadon választhat

a maszkok közül, akkor nincs módja arra, hogy eldöntse, helyesen döntött és a jó maszkot használta vagy rosszul döntött és értelmetlen eredményt kapott.

Hogyan használhatjuk fel ezt a jelenséget arra, biztonsággal kommunikáljunk? Egy lehetséges válasz a BB84 protokoll.

A folyamat azzal kezdődik, hogy Aliz létrehoz *n* darab véletlen bitet. A sorozat egy része fogja majd a folyamat végén alkotni a titkos kulcsot. Ezen kívül Aliz létrehoz egy másik véletlen bit sorozatot, amelynek a hossza szintén *n*. Ez a második sorozat fogja megmondani Aliznak, bitről-bitre, hogyan ábrázolja az első sorozat bitjeit. Például, a második sorozat minden egyes 1 értékű bitje jelentheti azt, hogy Aliz ezekben az esetekben R jellegű ábrázolást (azaz olyan ábrázolás, amit Bob R maszkkal helyesen fog tudni kiolvasni) fog használni a megfelelő első sorozatbeli bitek esetén. Hasonlóan, ha a második sorozatban egy bit 0, akkor az annak megfelelő első sorozatbeli bitnél Aliz D jellegű ábrázolást fog választani, amit Bob D maszk használata esetén helyesen fog tudni kiolvasni.

Aliz random bitjei	1	0	1	0	0	1	0	0	0	1	1	1
Random bitek	1	1	0	1	1	0	0	0	1	1	0	0
Ábrázolás jellege	R	R	D	R	R	D	D	D	R	R	D	D
Tényleges ábr.	↕	↔	⤢	↔	↔	⤢	⤡	⤡	↔	↕	⤢	⤢

1. Táblázat: A BB84 protokoll első néhány lépése (saját szerkesztés)

Tegyük fel, hogy Aliz létrehozott egy tizenkét bit hosszú sorozatot első körben és még tizenkettőt a második körben. Az 1. Táblázatban látható a folyamat első néhány lépése. Aliz úgy döntött, hogy észak-déli irányú mutató fogja jelenteni az 1-es értéket az R jellegű ábrázolás esetén és az északkelet-délnyugati irányú mutató fogja jelenteni ugyanezt az értéket a D jellegű ábrázolás esetén.

Aliz random bitjei	1	0	1	0	0	1	0	0	0	1	1	1
Random bitek	1	1	0	1	1	0	0	0	1	1	0	0
Ábrázolás jellege	R	R	D	R	R	D	D	D	R	R	D	D
Tényleges ábr.	↕	↔	⤢	↔	↔	⤢	⤡	⤡	↔	↕	⤢	⤢
Bob random bitjei	1	1	0	1	1	1	0	0	1	0	0	0
Maszk	R	R	D	R	R	R	D	D	R	D	D	D

1. Táblázat: Bob mérései (saját szerkesztés)

A következő lépésben Aliz elküldi az első bitsorozatot Bobnak a megfelelő ábrázolásokat használva a kvantum csatornán keresztül: Például fotonokat küld optikai szálon át. Mivel Bob nem tudja Aliz milyen ábrázolás mellett döntött az egyes bitek esetén, ő is létrehoz tizenkét véletlen bitet (*n* bitet, általános esetben) és a kapott bitek alapján választja ki a maszkokat, amelyet az egyes bitek kiolvasásához használni fog. Például dönthet úgy, hogy minden egyes 1-es bit R maszkot jelent és minden egyes 0-s bit egy D maszkot. A mérésének eredményét a 2. Táblázatban láthatjuk.

Aliz random bitjei	1	0	1	0	0	1	0	0	0	1	1	1
Random bitek	1	1	0	1	1	0	0	0	1	1	0	0
Ábrázolás jellege	R	R	D	R	R	D	D	D	R	R	D	D
Tényleges ábr.	↕	↔	↗	↔	↔	↗	↘	↘	↔	↕	↗	↗
Bob random bitjei	1	1	0	1	1	1	0	0	1	0	0	0
Maszk	R	R	D	R	R	R	D	D	R	D	D	D
Fogadott bitek	1	0	1	0	0	0	0	0	0	0	1	1
Megtartott bitek	ok	ok	ok	ok	ok		ok	ok	ok		ok	ok

2. Táblázat: Megtartandó bitek (saját szerkesztés)

Minden olyan esetben, amikor a bit ábrázolása és a maszk megegyezik Bob a helyes eredményt fogja kiolvasni. Ha a bit ábrázolása és a maszk nem egyezik meg az eredmény véletlenszerű lesz. Az esetek közel felében Bob 1-es értéket fog látni és a másik felében 0-s értéket. Amint Bob elkészült a kapott bitek vizsgálatával, a kommunikáló felek kapcsolatba lépnek egymással a klasszikus csatornán keresztül. Ez a csatorna lehallgatható, de nem zavarható. Ezen a csatornán keresztül összevetik Aliz által választott ábrázolási jelleget Bob maszk választásaival. Csak azokat a biteket fogják megtartani, amelyeknél a választások megegyeztek. A 3. Táblázat mutatja Bob mérési eredményeit és hogy mely biteket fogják a felek megtartani.

Tegyük fel, hogy Éva, a lehallgató, figyeli a kvantum csatornát is és a klasszikusat is. Továbbá, tegyük fel, hogy a rendszer tervezői figyelembe vették Kerckhoff elveinek legalább egyikét, ami azt jelenti, hogy a protokoll is és a fizikai megvalósítás részletei is publikusak. Ebben az esetben Éva tudja, hogy a csak kétféle maszkra van szüksége és azt is tudja, hogy milyen jellegű maszkokra. Ennek ellenére, ha bármilyen kapcsolatot létesít a kvantum bitekkel, amelyeket Aliz küldött Bobnak, akkor fennáll a veszélye annak, hogy módosítja azokat: Ha a rossz maszkot használja akkor nem megsemmisíti a bitet, hanem módosítja azt. Éva számára, a kapott eredménye megkülönböztethetetlen egy valódi eredménytől. Ha Éva le tudná másolni a kvantum biteket, amit Aliz küldött és lehallgatva a klasszikus csatornát megszerezné a megfelelő maszk választásokat akkor el tudná dönteni mely biteket tartották meg a kommunikáló felek. De a kvantummechanika nem-klónozhatósági tétele meggátolja Évát ebben. A tétel, a jelenlegi helyzetre alkalmazva, azt mondja ki, hogy nem lehet pontos másolatot készíteni egy tetszőleges ismeretlen kvantum bitről. Mivel Éva számára az elfogott kvantum bit teljesen ismeretlen, a kvantummechanika szabályai szerint nem fog tudni másolatot készíteni róluk.

Végül, Aliznak és Bobnak meg kell győződnie arról, hogy nem hallgatták le őket. Ezt úgy tehetik meg, ha a megtartandó bitek egy részét publikussá teszik és megvizsgálják hányad részük egyezik meg. Ha egy bizonyos küszöböt meghalad azoknak a biteknek a száma, amelyek különbözőek, akkor a felek tudják, hogy valaki hallgatózott és nem tarthatnak meg egyetlen bitet sem. Minden olyan bit, amivel Éva kapcsolatot létesített torzulhatott és így hozzájárulhatott a hibás bitek számához. A küszöbszámot meg lehet határozni ha feltesszük, hogy Éva optimálisan viselkedik [7].

Bár a protokoll feltétel nélkül biztonságos [8, 9], a fizikai megvalósítása lehetőséget teremt támadásra [10]. Ezért indult meg az a törekvés, hogy ezeket a protokollokat eszközfüggetlen módon valósítsák meg. A cikk utolsó nagyobb fejezete ezzel kapcsolatos eredményekkel foglalkozik.

MÉG INKÁBB KVANTUM: BBM92, E91

A BB84 protokoll a Heisenberg-féle határozatlansági elven (egy rendszer megfigyelése hatással van a rendszerre) alapul, együtt a nem-klónozhatósági tétellel. A kvantummechanikának van egy másik sajátsága, ami segíthet abban, hogy a klasszikus védettségnél biztonságosabbá tegyünk egy kommunikációs csatornát.

A kvantummechanikai összefonódottság fogalma azt takarja, hogy kvantum rendszerek egyes részei kapcsolatban állhatnak egymással, de egy olyan értelemben, ami túlmutat a klasszikus kapcsolat fogalmán. A következő képen lehet ezt elképzelni egy ilyen nemklasszikus kapcsolatot két olyan érme esetén, amelyek ilyen kapcsolatban állnak: Ha feldobom az egyik érmét és a dobás eredménye fej, akkor a másik érmét feldobva, a dobás eredménye szintén fej lesz. Ugyan ez igaz az írásra is: Ha feldobjuk az egyik érmét és a dobás eredménye írás, akkor a másik érme feldobása is írást fog eredményezni. A két érme vagy egyszerre fog fejet vagy egyszerre fog írást mutatni, de soha nem fog az megtörténni, hogy az egyik fejet, míg a másik írást mutat. Ha fogunk két ilyen nem-klasszikus módon összekötött érmét és nagyon messze elvisszük őket egymástól, a hatás ugyan az marad, a távolságtól függetlenül. Ez az ötlet zavarta Albert Einsteint és ezért kollégáival Boris Podolskyval és Nathan Rosen-nel egy gondolatkísérletet javasolt, amivel a kvantummechanika hiányosságára szeretett volna rámutatni. Ami akkor egy gondolatkísérletet volt, ma mindennapos rutin a fizika laborokban. Az olyan jellegű kvantum biteket, amelyek rendelkeznek ezzel a nem-klasszikus kapcsolattal gyakran EPR pároknak nevezzük.

Artur K. Ekert [11] bevezetett egy protokollt, amit ma E91-nek neveznek és ami az összefonódottságon alapul. A módszer Bell tételét használta, amely arra szolgál, hogy az összefonódottság miatt keletkezett nem-klasszikus korrelációt számszerűen jellemezze és ezzel mérhetővé tegye.

A protokoll a következőképpen működik. EPR párok egy megbízható forrása a pár egyik kvantum bitjét elküldi Aliznak, a másikat Bobnak. A forrás minden EPR párt úgy állít elő, hogy az négy kívánatos állapot egyikében legyen, például úgy, hogy a párt alkotó bitek tökéletesen korreláltak legyenek. A fentebb említett tárcsa analógiát használva azt látnánk, hogy ha ránéznénk az egyik bitre a párból és a mutatója észak-dél irányú lenne, akkor megvizsgálva a pár másik bitjét, szintén egy észak-dél irányú mutatót látnánk. De ha ránézve az egyik bitre egy kelet-nyugat irányú mutatót látunk, akkor megvizsgálva a másik bitet, szintén egy kelet-nyugati irányú mutatót látnánk.

Aliznak is és Bobnak is van három-három maszkja. Az egyszerűség kedvéért a maszkokra az iránypárok helyett csak egyetlen iránnyal utalunk. Aliz maszkjai keletre, északkeletre és északra mutatnak, míg Bob maszkjai északkeletre, északra és északnyugatra. Mindketten, egymástól és a korábbi mérési eredményektől függetlenül választanak maszkot, minden egyes megfigyelés előtt. Mindketten megvizsgálják a bitet, amit kaptak és lejegyzik a megfigyelésüket, valamint a használt maszkot. Amint végeztek az összes tervezett méréssel publikussá teszik a mérések során használt maszkok sorozatát egy olyan klasz-

szikus csatornán, ami, ismét, lehallgatható, de meggátolja a közvetített információ megváltoztatását. A kapott információ alapján mindketten két csoportra bontják a méréseiknek az eredményét: Az első csoportba kerülnek azok az eredmények, amelyeknél azonos maszkokat használtak, a másik csoportba azok, ahol a maszkok különbözőek voltak.

Ezek után nyilvánosságra hozzák a második csoportba tartozó mérési eredményeket, azaz amikor különböző maszkokat használtak. Az így beszerzett információ alapján ki tudják számítani a mérések közötti korrelációt. Ha Éva megpróbál beavatkozni a folyamatba úgy, hogy az összefonódott párokat bármilyen módon manipulálja, akkor a kiszámított korrelációs érték el fog térni a kvantummechanika által meghatározottól és ezzel Éva felfedi magát.

Ch. H. Bennett, G. Brassard (akikről a BB84 van elnevezve) és N. David Mermin [12] előálltak egy protokollal (BBM92 a neve ma), amelyik a Bell tétel nélkül is működik: Éva nem nyer információt abból, ha megfigyeli a EPR pár bitjeit miközben azok átkerülnek Alizhoz és Bobhoz, mivel információ mérés előtt nem létezik. Amit tehet az, hogy megváltoztatja, mondjuk, Aliz bitjét saját igényei szerint, de ez kiderül a mért korreláció csökkenéséből és így Éva lebukik.

Egyik járhatónak tűnő út Éva számára az, ha lecseréli az EPR párok forrását egy olyanra, amelyben a legyártott EPR párokat titokban összefonja egy kvantum bittel, amelyik csak az övé. A cikkükben Bennett, Brassard és Mermin megmutatja, hogy még ebben az esetben sem tud Éva információhoz jutni úgy, hogy közben rejtve marad: Az egyetlen módja annak, hogy rejtve maradjon az, ha a saját bitjét függetleníti az EPR pártól. Bármilyen extra összefonódás rá fogja nyomni a bélyegét a mérési eredményekre.

Továbbá, az is megmutatható, hogy a BBM92 protokoll ekvivalens a BB84 protokollal, ha a kommunikáló felek közül legalább az egyikük azonnal elvégzi a mérést a kapott kvantum biten. Ha egy összefonódáson alapuló protokoll esetén a méréseket nem végzik el rögtön, hanem csak akkor, amikor szükség van rá a kulcs generálásához, akkor a beérkezett biteken végrehajtott változtatás továbbra is kimutatható a mérésekben. Például, ha egy betörő bejut abba az irodába ahol a beérkezett kvantum biteket tárolják és módosítja azokat, akkor ez a tette napvilágra kerül a mérés során. Ugyanez nem igaz a BB84-re, mert ebben az esetben Aliz klasszikusan tárolja a saját információját.

ESZKÖZFÜGGETLEN MEGVALÓSÍTÁS

Ahogy említettük korábban, egyes kutatók [10] rámutattak a fizikai megvalósításból származó sebezhetőségre. Az összefonódottságon alapuló protokollok még akkor is biztonságosan működhetnek, ha az eszközt magát egy ellenséges fél szolgáltatja, mindaddig amíg az eszköz megfigyelhetően a kvantummechanika törvényei szerint működik: Az előző fejezetben kiderült, hogy a kvantummechanika törvényei teszik lehetetlenné Éva, a lehallgató, számára a rejtett megfigyelést.

Ha Aliz és Bob egy ilyen eszköz mellett döntenek, akkor meg kell győződniük valamilyen módon, hogy amit kaptak egy valódi kvantum eszköz. Ezt például úgy lehet elérni, hogy az eszköznek két üzemi állapota van: Kulcsgeneráló és teszt üzemmód [13]. Aliz és Bob egymással „körökben” kommunikál. Minden egyes kör lehet kulcsgeneráló kör vagy teszt kör. Az egyik ilyen megvalósítás esetén ([14]), Bob bizonyos valószínűséggel eldönti,

hogy az adott kör vajon egy kulcsgeneráló vagy teszt kör és erről tájékoztatja Alizt. A kulcsgeneráló körben Aliz és Bob egy E91 jellegű vagy ennél egyszerűbb protokollal generál biteket amelyeket később a tényleges kulcs létrehozására használnak.

A teszt körben viszont egy játékot játszanak. A játék neve CHSH vagy Clauser–Horne–Shimony–Holt játék [15]. A játékot két együttműködő játékos játssza egy bíró közreműködésével, akit általában Charlie-nak hívnak és itt is ezt fogjuk használni. A játékosok, Aliz és Bob, a játék során nem kommunikálhatnak egymással, de a játék előtt megbeszélhetik milyen stratégia szerint fognak játszani, valamint megoszthatnak egy EPR párt, mivel ezeken a párokon keresztül nem lehet kommunikálni direkt módon. Charlie választ két számot: Az első számnak 0-t vagy 1-et választ ugyanakkora valószínűséggel és ugyanezt teszi a második szám esetén. Az első számot elküldi Aliznak, a másodikat Bobnak. Amint Aliz megkapja a számot Charlie-től, egy megfelelő stratégiát követve, visszaküld egy 0-st vagy egy 1-est Charlie-nak. Ugyanezt teszi Bob is. Charlie bíráskodik: Végrehajt egy logikai ÉS műveletet azokon a számokon, amelyeket kiküldött Aliznak és Bobnak és egy modulo 2 összeadást a két biten, amit a játékosok küldtek vissza. Ha a számítások eredményei megegyeznek akkor Aliz és Bob nyer.

A játék klasszikus, lokális változatában, azaz amikor EPR pár nem kerül felhasználásra, átlagosan, az esetek legfeljebb 75%-ban nyerhetnek a játékosok. Ha használják az EPR párt úgy, hogy mérést végeznek rajta, akkor a nyerési esély felmegy nagyjából 85%-ra. Ha az EPR pár hamis vagy meg lett bolygatva, akkor a nyerési esély visszább megy.

Lehetséges, hogy Éva hallgatózik, de ez nem gond: A CHSH játék esetén számszerűen meg lehet határozni mennyi információ szivárog ki Éva felé abból, ahogyan csökken a játék nyerési valószínűsége. Ha a kiszivárgott információ mennyiség elfogadható vagy van valami módszerük arra, hogy a problémát megkerüljék (például ilyen megoldás a „titoktartás erősítése", *privacy amplification*, lásd [14, 16, 17]), akkor még mindig kinyerhetnek egy titkos kulcsot az adatokból, amit Éva nem fog ismerni.

Úgy tűnik, hogy a kutatóknak végre sikerült legyőzni a jelenlegi technológia adta akadályokat: A [14, 16, 17] cikkek, amelyek közel egy időben jelentek meg, arról számolnak be, hogy sikerült valódi eszközfüggetlen kulcs-elosztást megvalósítani.

KONKLÚZIÓ

Van egy pár kérdés, amit érdemes feltenni. Mi a helyzet akkor, ha a kvantummechanika nem érvényes minden körülmények között vagy létezik valami olyan postkvantum fizika amely lehetővé teszi egy fejlett civilizációnak, hogy lehallgasson bennünket. A jó hír az [18], hogy Jonathan Barrett, Lucien Hardy és Adrian Kent szerint egyszerűen csak egy fizikára van szükségünk, amely kizárja a fénysebességnél gyorsabb kommunikációt.

Ebben a cikkben és úgy általában az irodalomban (lásd például [19]) gyakran használunk olyan kifejezéseket, hogy „Aliz kiválaszt egy ábrázolást" vagy „Bob kiválaszt egy maszkot". Mi történik abban az esetben, ha a fizika nem engedi meg a szabad vagy független választást? Mi van akkor, ha a szuperdeterminizmus igaz és a jelenlegi döntéseink mind összefüggenek vagy korreláltak? A szuperdeterminizmus [20] a Bell tétel egy kiskapuja és természetesen nem egy új probléma. John Bell elismerte a létezését és foglalkozott a kérdéssel [21]. A vita még nincs lezárva, de úgy tűnik, hogy a válasz nem változtat igazán semmit a mindennapokban használt modellek jellegén.

ÖSSZEFOGLALÓ

Amint a kvantum számítógépek megjelennek a hétköznapokban, veszélyt fognak jelenteni a jelenlegi titkosítási módszerekre. Jó tudni, hogy ugyan ez a technológia válasszal tud szolgálni a problémára és a segítségével, úgy tűnik, meg fogjuk tudni őrizni a számunkra fontos adataink biztonságát.

FELHASZNÁLT IRODALOM

[1] D. Castelvecchi, "The race to save the Internet from quantum hackers", *Nature, vol.* 602, no. 7896, 198–201, 2022.
[2] Ch. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", *Conf. on Computers, Systems and Signal Processing* (Bangalore, India), pp. 175-179, 1984.
[3] Ch. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Theoretical Computer Science* vol. 560, 7-11, 2014, DOI https://doi.org/10.1016/j.tcs.2014.05.025. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.
[4] Ch. Paar and J. Pelzl, "Understanding cryptography: a textbook for students and practitioners", Springer Science & Business Media, 2009.
[5] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, and J. Rothe, "Quantum cryptography: A survey", ACM Computing Surveys (CSUR) vol. 39, no. 2, 1–31, 2007.
[6] A. Kumar and S. Garhwal, "State-of-the-Art Survey of Quantum Cryptography", *Archives of Computational Methods in Engineering,* vol. 28, no. 5, 3831–3868, 2021.
[7] Ch. A. Fuchs, N. Gisin, R. B. Griffiths, Ch-Sh. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy", *Physical Review A,* vol. 56, no. 2, 1163, 1997.
[8] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", *Physical review letters,* vol. 85, no. 2, 441, 2000.
[9] H-K. Lo, "A simple proof of the unconditional security of quantum key distribution", *Journal of Physics A: Mathematical and General,* vol. 34, no. 35, 6957, 2001.
[10] V. Scarani and Ch. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems", *Theoretical Computer Science,* vol.560, 27–32, 2014.
[11] A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett*. vol. 67, 661-663, 1991.
[12] Ch. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem", *Physical review letters,* vol. 68, no. 5, 557, 1992.
[13] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and Th. Vidick, "Practical device-independent quantum cryptography via entropy accumulation", *Nature communications,* vol. 9, no. 1, 1–11, 2018.
[14] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J-D. Bancal, "Device-independent quantum key distribution", arXiv preprint arXiv:2109.14600, 2021.
[15] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories", *Physical review letters,* vol. 23, no. 15, 880, 1969.

[16] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, V. Scarani, Ch. C-W. Lim, and H. Weinfurter, "Experimental device-independent quantum key distribution be-tween distant users", arXiv preprint arXiv:2110.00575, 2021.
[17] W-Zh. Liu, Y-Z. Zhang, Y-Zh. Zhen, M-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J-W. Pan, "High-speed device-independent quantum key distribution against collective attacks", arXiv preprint arXiv:2110.01480, 2021.
[18] J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution", *Physical review letters,* vol. 95, no. 1, 010503, 2005.
[19] A. Ekert and R. Renner, "The ultimate physical limits of privacy", *Nature,* vol. 507, no. 7493, 443–447, 2014.
[20] J-A. Larsson, "Loopholes in Bell inequality tests of local realism", *Journal of Physics A: Mathematical and Theoretical,* vol. 47, no. 42, 424003, 2014.
[21] J. S. Bell, "Free variables and local causality", *Quantum mechanics, high energy physics and accelerators. Selected papers of John S. Bell (with commentary),* 1995.
[22] M. Rorvig, "Cryptographers Achieve Perfect Secrecy With Imperfect Devices" (February 25, 2022), https://www.quantamagazine.org/cryptographers-achieve-perfect-secrecy-with-imperfect-devices-20220225/. Accessed March 13, 2022.
[23] N. Nyári, "The Impact of Quantum Computing on IT Security", *Biztonságtudományi Szemle,* vol. 3, no. 4, 25-37, 2021.
[24] Buttyán L. és Vajda I., „Kriptográfia és alkalmazásai", Typotex Kiadó, 2005.