Kvantumkriptográfia, kvantumos titkosítás kétállapotú kvantumrendszerrel

Klasszikus kriptográfia

Egy szöveg rejtjelezése a titkosírás vagy idegen szóval kriptográfia régóta használatos üzenetek küldésésre, kommunikációra. A kvantummechanika kétállapotú rendszerei pl. fotonok polarizációja erre egy érdekes lehetőséget nyújt. Mielőtt ezt tárgyalnánk röviden ismertetjük az úgynevezett klasszikus titkos kulcsú titkosírás módszerét. A szöveg titkosítást egy kulcs segítségével végezzük, amely az egyes betűket számokkal helyettesíti. Pl::

A	*Á*	*B*	*C*	*D*	*E*	*É*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15

N	*O*	*Ö*	*P*	*Q*	*R*	*S*	*T*	*U*	*Ü*	*V*	*W*	*X*	*Y*	*Z*
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Helyettesítsünk minden betűt 5-tel nagyobb számmal Mod 30. Ekkor A KOCKA EL VAN VETVE szöveg így néz ki: E ÖSGÖE IP AER AIXAI. Az üzenet olvasásához kulcsot ismernie kell küldőnek és a fogadónak is, de másoknak nem. Egy ilyen egyszerű módon kódolt szöveg azonban gyorsan feltörhető és vagyis a kulcs megfejthető.

Azonban ha a betűt kódoló számhoz más és más véletlenszerűen generált számot adunk, majd az így kapott szöveget írjuk le, az már nem lesz megfejthető, csak annak számára aki a kulcsot is ismeri. Ez utóbbi a Vernam kód, Gilbert Vernam amerikai kutató nevéről, aki ezt a módszert 1918-ban javasolta. A kulcsot azonban időről időre változtatni kell, mert egyébként az is megfejthető. Be lehet ugyanis bizonyítani, ez 1925 körül történt, hogy a biztonságos továbbításhoz, vagyis a megfejthetetlenséghez az kell, hogy a kulcs és a kódolandó szöveg hossza azonos legyen. Ezt a kulcsot egyszeri blokknak (one time pad) szokás nevezni. Ilyen titkosírással üzent Che Guevara a boliviai őserdőkből Fidel Castronak, illetve Dr. Sorge a szovjet elhárítás Japánban kémkedő tisztje a II. világháborúban. Ő pl. Németország statisztikai évkönyvének előre megbeszélt számtáblázatait használta a kódolásra. Általában a kulcs azonosságának a biztosítása a kritikus pont a küldő és a fogadó részéről. Megjegyezzük, hogy manapság pl. banki adatok továbbítására más módszert használnak, egy úgynevezett nyilvános kulcsú titkosírást, amely valójában szintén alkalmaz egy gyakorlatilag megfejthetetlen, titkos kulcsot is. (Ennek az un. RSA algoritmuson alapuló módszernek a leírása megtalálható pl. a http://hu.wikipedia.org/wiki/RSA-eljárás

Létezik azonban olyan kvantumos módszer, amellyel elvileg is titkosan lehet egy kulcsot készíteni két fél Aliz és Bob számára. Ezt kvantumos kulcstovábbításnak, vagy újabban kvantumos kulcsgenerálásnak szokás nevezni, ez az alapja a kvantumos titkosírásnak a kvantumkriptográfiának.

Kvantumkriptográfia és a BB84 protokoll

A két fél: Aliz (A) és Bob (B) üzenetei nyilvánosak lehetnek, de a kódoláshoz és a visszafejtéshez titkos kulcsot használnak, amelyet csak ők ismernek. A kvantumos módszer valójában a titkos kulcs átviteléhez szükséges A és B között, ezért a módszert kvantumos kulcstovábbításnak (vagy kulcs-szétosztásnak) szokás nevezni. Az angol quantum key distribution szavak rövidítéseként QKD módszerről illetve protokollról is szoktak beszélni. A kulcsot mint megfelelő qubitek sorozatát juttatják el egymáshoz, így ha azokon egy harmadik,

illetéktelen személy, mérést hajtana végre, akkor elrontja az eredeti állapotot, amit a két fél statisztikai módszerek alapján észre tud venni.

Az első QKD protokoll, a BB84-nek nevezett módszer, amelyet C. Bennett és Brassard javasolt 1984-ben. Ez két nem ortogonális állapotot használ a kód előállítására. A BB84 a következőképpen működik. A előállít egy *klasszikus* véletlen bitsorozatot, melynek k-adik tagja legyen a_k. Ennek a bitsorozatnak egy alkalmas részsorozata lesz majd a titkos kulcs. Ezt fogja A kódolni egy $|\varphi_k\rangle$ kvantumálapot sorozattal, amelyek egy kétdimenziós tér elemei. Ezeket a klasszikus bitekkel szemben kvantumos biteknek *qubitek*nek szokás nevezni. A kódolás módjának meghatározásához egy *másik* véletlen *klasszikus* bitsorozatot a'_k-t használ a következőképpen: a_k-t attól függően kódolja *két különböző bázisban*, hogy mi az a'_k értéke. Fizikailag, a tekintett qubiteket fotonok polarizációs állapotainak tekintjük, a jelenleg már kereskedelmi forgalomban is kapható kvantumtitkosító berendezésekben valóban ezeket is használják.

A két bázist a következőképpen választjuk. Az egyiket Z bázisnak nevezzük, amelynek bázisvektorai $|\leftrightarrow\rangle$ és $|\updownarrow\rangle$ a horizontálisan, (azaz vízszintesen) illetve vertikálisan (azaz függőlegesen) polarizált fotonállapotot jelentik. Ezeket ortonormáltnak tekinthetjük, mivel $\langle\leftrightarrow|\updownarrow\rangle = 0$, $\langle\leftrightarrow|\leftrightarrow\rangle = \langle\updownarrow|\updownarrow\rangle = 1$. A Z bázis elemei legyenek $|\leftrightarrow\rangle$ vagy $|\updownarrow\rangle$ Eszerint, ha $a'_k = 0$, akkor a Z bázist használja, amelynek elemei $|\leftrightarrow\rangle$ vagy $|\updownarrow\rangle$ vagyis ha ha $a_k = 0$ akkor $|\varphi_k\rangle = |\leftrightarrow\rangle$ illetve, ha $a_k = 1$, akkor $|\varphi_k\rangle = |\updownarrow\rangle$. Viszont, ha $a'_k = 1$, akkor az X bázist használja, és ekkor, ha $a_k = 0$ akkor, $|\varphi_k\rangle = |\nearrow\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle + |\updownarrow\rangle)$=$|\nearrow\rangle$ illetve ha $a_k = 1$, akkor $|\varphi_k\rangle = |A\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle - |\updownarrow\rangle) = |\nwarrow\rangle$. Ezután A átküldi a $|\varphi_k\rangle$ kvantumos véletlen kódsorozatot B-nek, aki mérést hajt végre a $|\varphi_k\rangle$ állapotokon. Mérőberendezését ő is véletlenszerűen állítja be Z vagy X irányba egy általa választott b'_k klasszikus bitsorozat segítségével, ugyanazon előírás szerint mint A. Vagyis, ha $b'_k = 0$ akkor B is Z irányban mér, míg ha $b'_k = 1$, akkor X irányban. A mérés eredményétől függően ő is létrehozza saját *klasszikus* b_k bitsorozatát ugyanazon előírás szerint ahogyan A, azaz ha a mérési eredmény a Z beállítás során H, akkor $b_k = 0$, ha V akkor $b_k = 1$, illetve ha a z Világos, hogy ha B éppen véletlenül azonos bázisban mért mint amelyben A kódolt, akkor az eredmény elvileg egységnyi valószínűséggel ugyanaz mint amit A kódolt. Ha viszont B nem azonos bázisban mért mint amelyben A kódolt, akkor az eredménye csak 1/2 valósznűséggel esik egybe a_k-val. Az alább látható táblázatban összefoglalva láthatók a lehetséges kimenetelek, a táblázat 3-6 sorában a 4–7 oszlopokban a megfelelő mérési valószínűségeket adtuk meg:

		$\|\varphi_k\rangle$	$b'_k = 0$		$b'_k = 1$	
			$\|\leftrightarrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$
$a'_k = 0$	$a_k = 0$	$\|\leftrightarrow\rangle$	1	0	1/2	1/2
$a'_k = 0$	$a_k = 1$	$\|\updownarrow\rangle$	0	1	1/2	1/2
$a'_k = 1$	$a_k = 0$	$\|\nearrow\rangle$	1/2	1/2	1	0
$a'_k = 1$	$a_k = 1$	$\|\nwarrow\rangle$	1/2	1/2	0	1
			$b_k = 0$	$b_k = 1$	$b_k = 0$	$b_k = 1$

Ezek után B egy nyilvános csatornán közli A-val az ő b'_k sorozatát, de titokban tartja b_k-kat. A

most már meg tudja mondani B-nek, hogy melyek voltak ezek közül olyanok, amelyekkel az ő kódolási módja megegyezett, azaz kiválasztják azokat a vesszőtlen elemeket, amelyekre a vesszősek megegyeztek. Látható, hogy ha $b'_k = a'_k$ akkor $b_k = a_k$ egységnyi valószínűséggel. Az ezeknek a k-nak megfelelő biteket megtarthatják mint titkos kulcsot, ekkor ugyanis a kiválasztott a_k-k részhalmaza megegyezik a megfelelő b_k halmazával a másik oldalon. Ha valaki viszont csak a vesszős bitsorozatról szerez tudomást, számára az a_k (és b_k-k is) egyforma, azaz 1/2 valószínűséggel lehetnek 0-k vagy 1-ek . Hiába tudja meg valaki a nyilvános csatorna lehallgatásával a b'_k-k értékét, annak alapján pontosan 1/2 annak a valószínűsége, hogy a_k értéke 0 volt vagy 1, azaz nem jut információhoz.

Valójában azonban A és B nem lehetnek biztosak abban, hogy a két megtartott bitsorozat pontosan azonos, aminek két fő oka lehet. Egyrészt lehetséges, hogy maga a qubiteket átvivő csatorna nem tökéletes, azaz zajos, másrészt előfordulhat, hogy van egy harmadik személy, aki lehallgatja az átvitt információt. Ezt a személyt E-nek szokás nevezni az angol ”eavesdropper” (hallgatózó) szó miatt. Természetesen E-nek az az érdeke hogy A és B ne vegyék észre, hogy ő lehallgatta az üzenetet. A kvantumos csatorna használata miatt azonban A tudomást szerezhet arról, hogy a csatornát lehallgatják. Hogy ezt hogyan tehetik meg, az alábbiakban tárgyaljuk.

E két módon próbálhat tudomást szerezni arról, hogy milyen $|\varphi_k\rangle$ qubit állapot ment át A és B között. Egy primitív módszer lehet ha E mérést hajt végre a qubiteken. Tudjuk azonban, hogy a kvantummechanikában egy mérés általában befolyásolja az állapotot kivéve, ha E abban a bázisban mér, amelyben A kódolt. Noha E esetleg tudja azt, hogy A melyik két bázisban (az X vagy a Z bázisban) kódolt, mivel ez véletlenszerűen történik, E még e tudás birtokában is átlagosan csak méréseinek felében nem fogja megváltoztatni az eredményt. Maguknak a választott bázisoknak a száma is lehet több stb. Egyébként, ha a kvantumos információátvitel egyes fotonokkal történik a közbeavatkozás nyomán a foton elnyelődik és meg sem érkezik B-hez.

Egy ravaszabb módszer lehet emiatt, ha E megpróbálja lemásolni az átvitt qubit értékét egy általa külön erre a célra használt kvantumregiszterbe. Meg lehet azonban mutatni, hogy kvantumállapotokat másolni 100 % -os hitelességgel elvileg is lehetetlen. Ez az un. nemklónozhatósági tétel.

Tehát látjuk, hogy vagy a csatorna zajossága miatt vagy E közbevatkozása miatt az átvitt qubitrendszer megváltozik. Erről A és B olymódon vehet tudomást, hogy föláldozza a megtartott és a közbeavatkozás nélkül biztosan megegyezőnek gondolt bitjeinek egy részét, és ezeket nyilvánosan egyeztetik. Meg lehet mutatni, hogy annak a valószínűsége, hogy a titkosan tartott bitek között nem egyezők vannak arányos a nyilvánosan egyeztetett és eltérőnek talált bitek arányával. Ha ez utóbbi kicsi, tehát a nyilvánosan egyeztetett bitek lényegében megegyeznek a két oldalon, akkor ugyanez igaz a titkosan tartott bitekre is.

Megjegyezzük még, hogy az itt ismertetett BB84 protokollon kívül számos más kvantumos titkosítási protokoll is létezik.