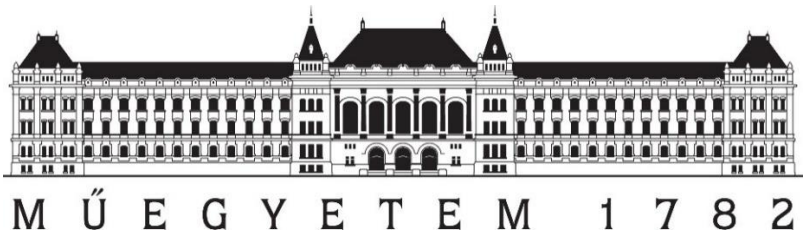
Budapesti Műszaki és Gazdaságtudományi Egyetem

Villamosmérnöki és Informatikai Kar



A B92 KVANTUMOS KULCSELOSZTÁSI PROTOKOLL VIZSGÁLATA ZAJOS KÖRNYEZETBEN

Készítették:

Csaplár Miklós és Kemecsei Kornél

Czuczor Gergely Bencés Gimnázium, Győr
12. évfolyam

Témavezetők:

Imre Sándor

Egyetemi tanár (BME)

Tóth Kristóf

Matematika- és fizikatanár
(Czuczor Gergely Bencés Gimnázium)
Doktorandusz (ELTE)

Hálózati Rendszerek és Szolgáltatások Tanszék

Tartalom

1. Absztrakt

Az utóbbi néhány évtizedet szokás második kvantumos forradalomnak hívni, mert felismerte az emberiség a kvantummechanika alkalmazásának egy új mérnöki lehetőségét. Ezt az új tudományágat összefoglalóan kvantum-számítástechnikának hívjuk. TDK kutatásunk is ebbe a témakörbe esik, a B92 kulcselosztási protokollt vizsgáltuk.

Első körben elvégeztünk egy kb. 3 hónapos szakkört, így elsajátítva a kvantummechanika alapjait fotonpolarizáción keresztül. Ezt követően önállóan utánajártunk és megértettük a titkosítási eljárásokat, így eljutva a B92 protokoll megismeréséhez, mely kézenfekvő hiszen ez az eljárás az általunk ismert fotonok polarizációs állapotait használja fel.

Kutatási projektünk eredményeképpen szimulációs környezetet fejlesztettünk Python programozási nyelven a B92 protokoll vizsgálatához. A programozás során elemeztük két kommunikáló fél, Anna és Béla kommunikációját zajtalan, illetve zajos környezetben is. A zajt a közvetítőközeg fotonok állapotára gyakorolt hatásaként építettük be, amely kis mértékben megváltoztatja a kvantumbiteket reprezentáló fotonok állapotát, így Béla mérési valószínűségeit is. Vizsgáltuk, hogy egy harmadik, külső, támadó fél (Éva) hogyan zavarja meg Anna és Béla kommunikációját azzal, hogy mérési beavatkozásával megváltoztatja a fotonok (kvantumbitek) állapotát. Éva támadását zajmentes és zajos környezetben is vizsgáltuk. Megnéztük, hogy mennyi az optimális kvantumbit-szám, amelyet Annának és Bélának érdemes ellenőrizni annak érdekében, hogy Éva támadásáról megbizonyosodjanak.

2. Bevezetés

A 20. század elején felfedezett kvantummechanika napjainkban megkerülhetetlenné vált, az ipari és mérnöki életbe is leszivárogtak az atomi méretskálájú jelenségek. Gondoljunk csak például a gyógyszeriparra, az orvosi diagnosztikára, a nukleáris iparra és a félvezetőkre. A 20. század végén az egyedi kvantumrendszereken végzett kísérletek [1-5] ismét egy új fejezetet nyitottak, létrejött a kvantummechanika új alkalmazási területe, a kvantum-számítástechnika. Felmerült a kérdés, vajon képes-e az emberiség új alapokra helyezni a számítógépek működését, lehetséges-e a gyakorlati életben is jól használható kvantumszámítógép építése? Ennek motivációját az adta, hogy számos kvantummechanikai rendszer szimulálása klasszikus számítógéppel túlzottan bonyolultnak bizonyult. Feynman vetette fel elsőként, hogy kvantumrendszert szimuláljunk kvantumszámítógéppel [6]. A kvantumszámítógépek kérdésköre még izgalmasabbá vált, amikor 1994-ben Peter Shor kitalálta a róla elnevezett Shor-algoritmust [7], amely során egy megfelelő méretű kvantumszámítógép képes a gyors prímtényezős felbontásra, mellyel a mai titkosítási rendszerek alapjait adó RSA kódolás feltörhetővé válna. Idő közben azonban Charles Bennett és Gilles Brassard 1984-ben kitalálták az első kvantummechanika törvényeit felhasználó titkosítási eljárást, a BB84 protokollt [8], amely során természeti törvények védik a biztonságos kommunikáció alapját adó titkos kulcs megosztását, így a kommunikáció még egy kvantumszámítógéppel sem lesz feltörhető. Az ezeket a témákat átölelő új diszciplína robbanásszerű feltörését szokás második kvantumos forradalomnak hívni. [9]

Kutatásunk témája a kvantumtitkosítási eljárások témakörébe esik, A BB84-hez hasonló, eddig kevésbé vizsgált B92 protokollt elemezzük Python környezetben, mely 1992-ben kitalált kvantumkriptográfiai eljárás szintén Charles Bennett nevéhez köthető [10]. Témánkat aktualizálja az is, hogy az EU 2023 januárjában elkezdi kiépíteni a páneurópai kvantumos optikai hálózatot, és 2-3 éven belül tervezi fellőni a műholdakat a kvantumos kulcsmegosztás érdekében [11-12]. Kutatásunk témájaként tehát egy új tudományterület frontját választottuk, írásunk az első magyar nyelvű ismertető a B92 eljárásról és annak elemzéséről.

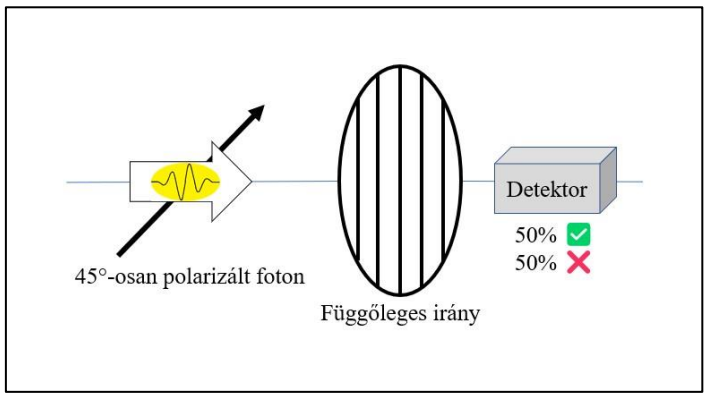
A következő fejezetben bemutatjuk a kutatásunk során felhasznált kvantummechanikai összefüggéseket, majd a folytatásban a B92 protokoll egyes eseteit vázoljuk fel, melyek szükségesek az elmélet megértéséhez. Az 5. fejezetben tárgyaljuk a további összes bekövetkezhető esetet a program könnyebb átláthatóságának érdekében. A 6. fejezetben lesz szó a programhoz használt fontos információkról, illetve magáról a programról. A 7. fejezetben grafikonok segítségével bemutatjuk a program által szimulált eseteket és következtetéseinket.

3. A kvantummechanika alapjai

A kvantumfizika tanulmányaink első lépése volt a *foton*, mint elemi fénykvantum megismerése. A fotonok felfedezését Einstein nevéhez kötjük, aki a fotoeffektus jelenségével kísérleti úton bizonyította létezésüket. Számításai szerint a fény nem egyenletes eloszlásban, hanem adagokban szállítja az energiát. Ezért a felfedezéséért 1921-ben fizikai Nobel-díjat kapott. [13]

A folytatásban megismerkedtünk a fotonok egyedi eseményeinél fellépő *valószínűséggel*. A mikrovilágban az állapot ismerete mellett is elkerülhetetlen a valószínűség használata és ezt kísérletileg is igazolták. „Az Úristen tényleg kockajátékos", ezért járt 2022-ben a fizikai Nobel-díj. [14]

Ezt követően megértettük a kvantummechanika matematikai alapjait. Először szakkör keretében elsajátítottuk egy fotonpolarizációra épülő tananyagot, melyet röviden az alábbi cikk mutat be [15]. A későbbiek során felhasznált ismereteinket egy konkrét példával demonstráljuk, melyet az *1. ábra* mutat be. Essen egy függőleges irányú polarizátorlemezre egy 45°-osan polarizált foton. Mivel a foton és a lemez által bezárt szög 45°, ezért az áthaladás, vagy elnyelődés valószínűsége 50-50%. Ezt követően a foton állapota megváltozik. Az áthaladásnak függőleges, az elnyelődésnek pedig a vízszintes polarizáció felel meg.



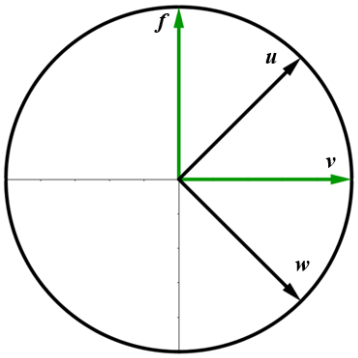
1. ábra: A 45°-osan polarizált foton 50% eséllyel áthalad a polarizátorlemezen, ekkor polarizációja függőleges lesz és a detektor érzékeli. Továbbá 50% valószínűséggel nyelődik el a foton, melyet elképzelhetünk úgyis, mintha a foton a vízszintes polarizációba esne bele, amely az elnyelődésnek felel meg.

Reprezentáljuk egy foton polarizációs állapotát egy tetszőleges $\boldsymbol{u}$ kétdimenziós egységvektorral. Ez az egységvektor szemléletesen azt jelenti, hogy milyen irányban polarizáltak a fotonok. Ekkor az $\boldsymbol{u}$ egységvektor felírható a polarizátorlemez által kijelölt (lásd *1. ábra*) függőleges ($\boldsymbol{f}$) és vízszintes ($\boldsymbol{v}$) egységvektorok lineáris kombinációjaként:

$$\boldsymbol{u} = \psi_1 \boldsymbol{v} + \psi_2 \boldsymbol{f}, \tag{1}$$

ahol ψ_1 és ψ_2 a lineáris kombináció együtthatója. Tapasztalati tény, hogy egy foton nem csak a mérhető állapotokban (a fenti példában ez $\boldsymbol{v}$ és $\boldsymbol{f}$) lehet, hanem azok lineáris kombinációja is lehetséges állapot (ilyen a 45°-osan polarizációs állapot is). Ezt nevezzük a *szuperpozíció elvének.* A kvantummechanikában a valószínűségi leírás oka tehát a szuperpozíció elve. A lineáris kombinációban az együtthatóknak, fizikai jelentése is van. A ψ_1^2 a $\boldsymbol{v}$ bázisállapot, ψ_2^2 az $\boldsymbol{f}$ bázisállapot mérési valószínűsége. A valószínűségi értelmezésből következik, hogy $\psi_1^2 + \psi_2^2 = 1$, azaz az állapotvektorok szükségképpen 1 hosszúak. Ez alapján felírható a példában szereplő 45°-os polarizációjú foton ($\boldsymbol{u}$), az $\boldsymbol{f}$ és $\boldsymbol{v}$ állapotvektorokra vonatkoztatva:

$$\boldsymbol{u} = \frac{1}{\sqrt{2}}\boldsymbol{v} + \frac{1}{\sqrt{2}}\boldsymbol{f}. \tag{2}$$



2. ábra: A fotonok polarizációs állapotvektora ábrázolható egy egységkörön, melyet állapotkörnek nevezünk [16]. Az ábrán bejelöltük a dolgozatunkban megjelenő legfontosabb állapotokat (***f***, ***u***, ***v***, ***w***). A ***w*** állapot a -45°-os polarizációnak felel meg. Az azonos színnel jelölt vektorok egy lehetséges mérési bázist adnak, ezek merőlegesek egymásra.

A szuperpozíció szemléletesen azt jelenti, hogy egy részecske állapota kettős. Egy 45°-osan polarizált fotonra nem lehet azt mondani, hogy csak vízszintes, vagy csak függőleges polarizációjú, mindkettő mérési eredmény lehetősége keveredik benne.

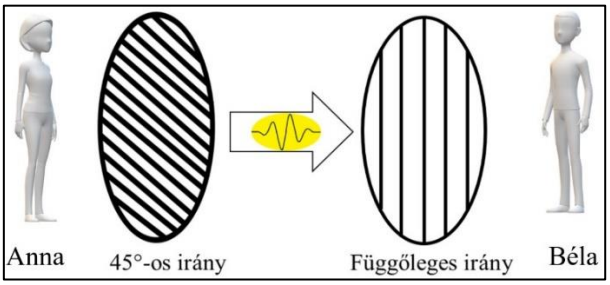
A szuperpozícióban megjelenő bázisállapotok nem csak az iskolában megszokott vízszintes és függőleges bázisok lehetnek, hanem bármilyen egymásra merőleges két irány. Ezeket a bázisokat érdemes a feladathoz mérten választani. Például, ha egy +45°-os ($\boldsymbol{u}$) irányú polarizátorlemezre esik egy vízszintesen polarizált foton, akkor a szuperpozíciót a mérhető $\boldsymbol{u}$ és $\boldsymbol{w}$ bázisokban érdemes felírni:

$$\boldsymbol{v} = \frac{1}{\sqrt{2}}\boldsymbol{u} + \frac{1}{\sqrt{2}}\boldsymbol{w}. \tag{3}$$

4. A B92 protokoll elméleti bemutatása

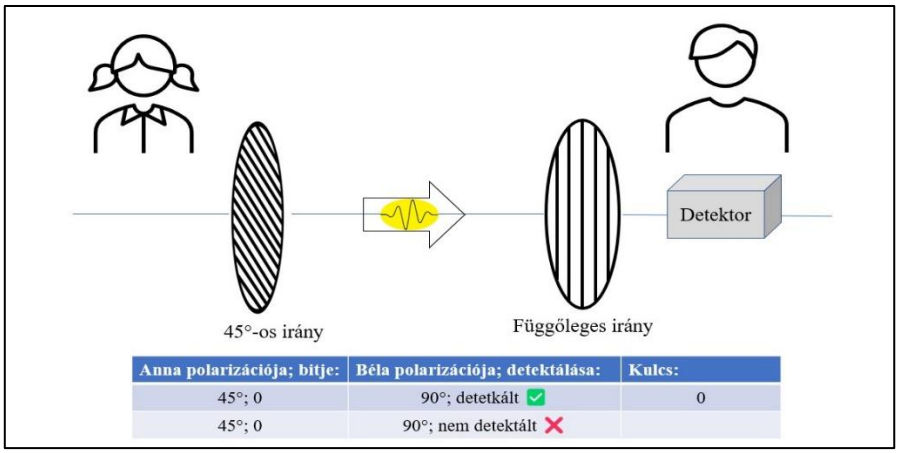
A protokoll alapja az előző fejezetben már ismertetett 4 polarizációs állapot, ***v***, ***f***, ***u*** és ***w***. Az egyik kommunikáló fél, Anna, véletlenszerűen ***v*** és ***u*** állapotokban küld fotonokat a másik félnek, Bélának, aki megpróbálja a fotonokat detektálni. Béla annak érdekében, hogy kitalálja, hogy a fotonok milyen állapotúak voltak, ***f*** vagy ***u*** állapotokat áteresztő polarizátorlemezt használ. A polarizátorlemez kiválasztása véletlenszerű. Ezt a konkrét példát a *3. ábra* mutatja be.

A *3. ábrán* látjuk, hogy ha Anna ***u*** állapotú fotont küld és Béla ***f*** irányú polarizátorlemezzel mér, akkor a foton detektálási valószínűsége 50%. Ha viszont Béla ***w*** irányú polarizátorlemezzel próbálna detektálni, akkor a foton biztosan elnyelődne a polarizátorlemezen. Így Béla amennyiben detektált fotont, tud következtetni Anna állapotára. Az ***f*** állapotot átengedő polarizátorlemezen történő áthaladás esetén Anna csakis ***u*** állapotú fotont küldhetett (***v***-t nem). Ehhez hasonlóan, amennyiben Anna ***v*** állapotú fotont küld, azt Béla ***f*** irányú polarizátorlemezzel sosem, de ***w*** irányú polarizátorlemezzel 50% eséllyel detektálja.



3. ábra: Anna véletlenszerűen küld egy fotont (legyen most ez ***u*** állapotú), Béla véletlenszerűen kiválasztja a függőleges irányú polarizátorlemezt. Amennyiben a foton áthalad, Béla biztos lehet abban, hogy Anna ***u*** állapotú fotont küldött.

A jövőben létrehozni kívánt titkos kulcs, az Anna által Bélának küldött 0-ás és 1-es kvantumbitek egy részéből fog állni. Az egyes kvantumbiteket a fotonok állapotai reprezentálják. Az Anna által ***v*** állapotban küldött fotonokat 0 bitnek, az ***u*** állapotban küldött fotonokat 1 bitnek vesszük. Mint azt már említettük, Béla csak bizonyos esetekben detektálja az Anna által küldött fotonokat és csak ilyenkor lehet biztos az Anna által küldött fotonok állapotában (így a küldött kvantumbitekben). Annak érdekében, hogy Anna tudja, mikor detektált Béla, ezeket a detektálási eseményeket Béla közli egy nyilvános csatornán, és mind a 2-en felírják ezeket a közös a biteket. Anna tudja mit küldött, Béla pedig következtetni tud a saját bázisában történő detektálás alapján, így ugyan azt a kulcsot kell kapniuk anélkül, hogy akár 1 db bitet is elárultak volna a nyílt kommunikációs csatornán.



Anna polarizációja; bitje:	Béla polarizációja; detektálása:	Kulcs:
45°; 0	90°; detetkált ✅	0
45°; 0	90°; nem detektált ❌	

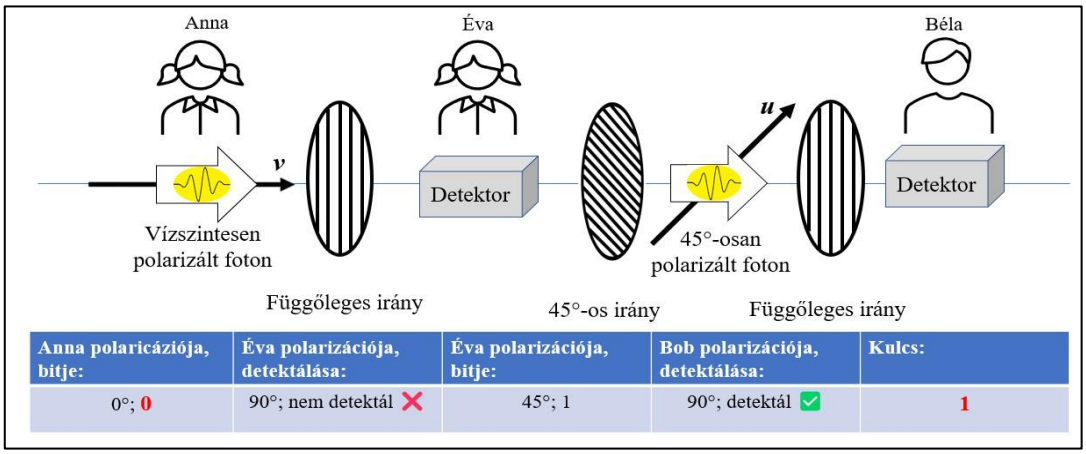
4. ábra: Anna 45°-os polarizáltságú fotonokat küld Bélának, aki függőleges irányú polarizátorlemezt használva az esetek közel felében detektálja azt, az esetek másik részében nem.

A probléma akkor jön, amikor belép a képbe Éva, aki le szeretné hallgatni az Anna által Bélának küldött biteket, csakhogy ő se tudja, hogy Anna milyen állapotban küld, mert Anna véletlenül változtatja azt. Tegyük fel, hogy Éva Béla polarizátorlemez állásait használja a lehallgatás során.

Írjuk fel a legalapvetőbb lehetőségeket:

1. Anna ***v***-t küld és Éva ***w*** állapotot áteresztő polarizátorlemezt használ, melyen a foton áthalad és ezt detektálja. Ekkor nincsen semmi gondja, biztos lehet abban, hogy Anna ***v*** állapotú fotont küldött. Ezért pusztán annyi a feladata, hogy küld egy ugyanolyan fotont, mint amilyet Anna eredetileg is küldött. Ha szerencséje van, Béla detektálni fogja ezt az Éva által küldött fotont, és tud következtetni, milyen kvantumbitet kapott. Béla közli a sorszámát egy nyilvános csatornán, azaz szól, hogy felírhatják a bitet a kulcsba, akkor Évának megvan 1 elem a titkos kulcsból és az üzengetők nem jöttek rá, hogy valaki belehallgatott a kulcs átadásába.
2. Anna ***v***-t küld és Éva nem detektálja. Ilyenkor jön Éva számára a probléma, ugyanis nem tudja kitalálni, milyen állapotú fotont küldött Anna. Ezért véletlenszerűen küld egy, ***v*** vagy ***u*** állapotú fotont Bélának. Ha ***u***-t küld és Béla nem detektál, akkor semmi nem történik, hiszen Béla ilyenkor nem közli a nyilvános csatornán mérésének sorszámát. Ekkor Éva kiléte titokban marad, azonban információhoz sem jutott hozzá.
3. Tegyük fel, hogy Anna továbbra is ***v***-t küld és Éva a tudáshiányából adódó véletlenszerű választása most az ***u*** állapotra esett. Tegyük fel továbbá, hogy ezt az Éva által küldött ***u*** állapotot Béla detektálta egy ***f***-et áteresztő polarizátorlemezzel. Ekkor Béla közli a nyilvános csatornán, hogy detektált. Anna, mivel a ***v***-t, azaz a 0 bitet küldte felírja a 0-t a kulcsba. Béla azonban mérési eredményéből arra következtet, hogy Anna ***u***-t küldött és felírja az 1-et a kulcsba. Jól

látható, hogy ekkor Anna és Béla megbizonyosodhat arról, hogy valaki belepiszkált a rendszerbe.



Anna polaricáziója, bitje:	Éva polarizációja, detektálása:	Éva polarizációja, bitje:	Bob polarizációja, detektálása:	Kulcs:
0°; **0**	90°; nem detektál ❌	45°; 1	90°; detektál ✅	**1**

5. ábra: A 3. eset szemléltetése: Anna elküldi a ***v*** állapotú fotont, Éva ezt nem detektálja az ***f*** irányú polarizátorlemezen keresztül, rosszul tippel és ***u*** állapotú fotont küld Bélának. Béla szintén ***f*** irányú polarizátorlemezt választott és detektálja a fotont, viszont a leírt kvantumbit nem közös az Anna által leírt kvantumbittel.

Annak érdekében, hogy Anna és Béla meggyőződjenek arról, hogy a kulcsot senki sem hallgatta le ellenőrzést hajtanak végre. A nyílt csatornán Anna és Béla random kiválasztanak ellenőrzésre néhány bitet, ugyan arról a helyről a kulcsból és megvizsgálják azokat. Ha minden ellenőrzött bitjük ugyanaz, akkor biztonságosnak ítélik, ha viszont a 3. eset előfordul és észreveszik, akkor tudják, hogy valaki lehallgatta őket, hiszen Béla nem detektálhatta volna az Anna által választott polarizációban elküldött fotont.

A fentiek szerint, ha az ellenőrzés során Anna és Béla hibát találnak, az csakis Éva miatt fordulhat elő. A gyakorlatban azonban a kommunikációs csatorna zajos, méréseiknek hibája van. Azaz előfordulhat, hogy Béla akkor is rossz bitet ír fel, ha Éva nem hallgatja le őket. A zaj, akárcsak Éva megváltoztatja a foton polarizációját, így a detektálás, elnyelődés valószínűséget is a polarizátorlemezen. Kutatásunk témája éppen ez. Azt vizsgáljuk, hogy ha a Béla által detektált bitek bizonyos százaléka megváltozik a kommunikációs csatorna zaja miatt, akkor amellett mennyire vehető észre Éva lehallgatása, illetve, hogy Éva hányszor hallgathat bele, hogy észrevétlen maradjon.

A B92 protokollt az [17] online elérhető szimuláció szemléletesen bemutatja, azonban a szimulációba nincs beépítve zaj, nem tudjuk szabályozni, hogy Éva hányszor próbáljon fotont detektálni, illetve nem tudjuk szabályozni az ellenőrzött bitek számát sem.

5. A B92 protokoll gyakorlati használata

Az elméleti bemutatásnál már felírtunk néhány lehetőséget példa gyanánt, de fontos tisztáznunk az összes esetet, ami Anna, Éva és Béla között megtörténhet, illetve, hogy egy adott eset végén Béla mekkora eséllyel fogja detektálni a fotont:

1. Éva nem néz bele:

Anna	Béla	Detektálás valószínűsége
v	***f***	0%
v	***w***	50%
u	***f***	50%
u	***w***	0%

1. táblázat: Anna és Béla kommunikációjának összes esete. A vörös színnel jelölt részek azt jelentik, hogy a küldött foton állapota és a Béla által választott polarizátorlemez állapota egymásra merőleges.

2. Éva belenéz:

Anna	Éva mér	Éva küld	Béla	Detektálás valószínűsége
v	***f***	***v***	***f***	0%
v	***f***	***v***	***w***	50%
v	***f***	***u***	***f***	50%!
v	***f***	***u***	***w***	0%
v	***w***	***v***	***f***	0%
v	***w***	***v***	***w***	50%
v	***w***	***u***	***f***	50%!
v	***w***	***u***	***w***	0%
u	***f***	***v***	***f***	0%
u	***f***	***v***	***w***	50%!
u	***f***	***u***	***f***	50%
u	***f***	***u***	***w***	0%
u	***w***	***v***	***f***	0%
u	***w***	***v***	***w***	50%!
u	***w***	***u***	***f***	50%

u	***w***	***u***	***w***	0%
v	***f***	***v***	***f***	0%

2. táblázat: Anna, Éva és Béla közti kommunikáció összes esete. A vörös szín azt jelenti, hogy az Éva által küldött foton polarizációja és a Béla által választott foton polarizátorlemez állapota egymásra merőleges. A felkiáltó jellel jelölt részek azt mutatják, amikor Béla polarizátorlemeze az Anna által küldött fotonnak a polarizációjával merőleges állapotban van, mégis detektálhatja azt 50%-os eséllyel.

Az előzőek alapján ki tudjuk számolni, hogy például *N* elküldött foton esetében mennyi hiba keletkezet Anna és Béla ellenőrzésekor olyan környezetben, ahol nincs zaj. Tételezzük fel, hogy Éva mindig próbálja detektálni Anna elküldött fotonjait. Ekkor az esetek közel felében 50%-os eséllyel fog detektálni fotont Béla, vagyis azt várjuk, hogy a kulcs közel *N*/4 kvantumbit hosszú lesz.

Éva 2 polarizátorlemez-irányt használhat Anna fotonjainak állapotának lehallgatására. A detektálásra, akárcsak Bélának, 25% esélye van, ami azt jelenti, hogy az esetek közel negyedében az Anna által küldött állapotban küld fotont. Ha ez nem sikerül neki, akkor 2 lehetőség közül kell választani (***v*** és ***u***), így 50% valószínűséggel Bélának olyan polarizációban fog fotont küldeni, mint Anna. Az esetek maradék 25%-ban pedig az Annáéval 45°-ban eltérő állapotot választ, Ezt nevezzük a későbbiekben „rossz választásnak”.

Az *1. táblázat* nem csak Anna és Béla lehetőségeit mutatja be, hanem Éva és Béla lehetőségeit is. Ebből kiderül, hogy Béla az Éva által „rosszul választott” fotonokat az esetek felében 50% valószínűséggel detektálja, szóval a 25%-kal bekövetkező „rossz választást” 25% eséllyel detektálja. Az Anna és Béla általi ellenőrzésben a hiba tehát 25% · 25% = 6,25% körül lesz.

6. A B92 protokoll programkódjának ismertetése

A B92 protokoll vizsgálatára a Python nyelvet használtuk. Az elkészített munkánk a [18]-as linken keresztül érhető el. Ebben a programozási nyelvben, lehetőségünk van pseudo random számok generálására. A valószínűségeket egy 0 és 1 közötti tizedes tört generálásával szimuláljuk. Ha egy esemény valószínűsége 50%, akkor a szimulációban ez akkor történik meg, ha a generált számunk nagyobb mint 0,5. Az így létrehozható 50%-os valószínűséget használjuk fel a kvantumos mérési kimenetelek modellezésére.

Anna adott számú vízszintesen (***v***) vagy +45°-osan (***u***) polarizált fotonokat preparál. A ***v*** állapotú fotonokat 0-s, az ***u*** állapotú fotonokat 1-es bitnek feleltetjük meg, s programkódunkban a fotonok állapotát reprezentáló biteket pszeudo randomszám-generátorral sorsoljuk ki a fent említett módon, 50-50%-os valószínűséggel.

A B92 protokoll programozásának megvalósítása a következő:

- Béla véletlenszerűen választja az ***f*** függőleges és ***w*** -45°-os irányú polarizátorlemez állások egyikét (50-50%-os valószínűséggel). Ezeket a fent említett módon modellezzük: véletlenszerűen generált 0-s (***w***) és 1-es (***f***) bitekkel.
- Ha Béla random választott (***f*** vagy ***w***) irányú polarizátorlemeze 45°-os szöget zár be Anna fotonjának polarizációs állapotával (kettejük random generált száma megegyezik), akkor Anna fotonjának van esélye (50%) áthaladni Béla polarizátorlemezén. Azt, hogy a foton ténylegesen áthalad-e ismételten randomszám generálással sorsoljuk ki, ezzel lemodellezve, hogy Béla polarizátorlemezén át megy-e Anna fotonja.
- Amennyiben Béla, Anna fotonjára merőleges polarizációjú lemezt választott, a foton biztosan nem megy át a lemezen, ekkor mivel Béla nem detektál fotont, nem ír fel semmit, a programban ekkor tehát nincs dolgunk.
- Béla detektálás esetén nyílt kommunikációs csatornán elmondja Annának, hogy detektált fotont, majd Anna, felírja, hogy ő milyen bitet küldött. Ezt a programban egy új tömb feltöltésével tesszük meg. Annak a fotonnak a hozzárendelt értékét, (0, 1) amelyen a szimulációt végezzük hozzá adjuk Anna új tömbjéhez.
- Ezt követően az egészet újra kezdjük, Béla, Anna soron következő fotonjához újra sorsol egy polarizátorlemez irányt.

Most tekintsük azt az esetet, amikor egy harmadik támadó fél (Éva) belehallgat Anna és Béla kommunikációjába, így a mérés végeredménye bizonyos esetekben változhat. Ha Éva detektál fotont, abból következtetni tud arra, hogy Anna milyen polarizációjú fotont küldött, ezért képes arra, hogy ugyan abban a polarizációban küldjön egy fotont Bélának, mint azt Anna tette. Azaz

ekkor észrevétlen marad. Ezt ugyan úgy szimulálhatjuk mintha a mérés Éva nélkül történne: Anna polarizációjához hasonlítjuk Béláét, ha megegyezik 50% eséllyel detektál és nem találnak egymás kulcsa között különbséget.

Ha Éva nem detektál fotont, akkor nem tudja milyen bitet (fotont) küldött Anna, ezért muszáj tippelnie (50%-os valószínűséggel). Ha szerencséje van és olyan bitet (fotont) küld el Bélának, mint Anna tette akkor úgy megy a szimuláció, mint amikor Éva nem hallgat bele a kommunikációba.

Ha Éva nem detektál fotont és Annától eltérő irányú polarizációt küld, akkor Bélának 25%-os esélye lesz, hogy olyan bitet detektáljon melyet nem lenne neki szabad, hiszen Annára merőleges polarizációban mért. Ennek az a következménye, hogy Anna és Béla ellentétes bitet ír fel, amely csakis a lehallgatás következménye lehet. A programban ezt úgy szimuláljuk, hogy Anna felírja az éppen soron lévő bitjét, ha az 1 akkor Béla felír egy 0-t, ha 0 akkor pedig egy 1-est.

A kommunikációs csatorna tökéletlensége miatt zaj lép fel, azaz a fotonok polarizációs állapota kis mértékben módosul, így a detektálási valószínűségek is változnak. Ezt szintén valószínűségi alapon implementáltuk. Egy húsz százalékos zaj azt jelenti, hogy az esetek közel 1/5-ében Béla rosszul mér, azaz olyankor is detektál fotont mikor nem kéne, illetve előfordul, hogy a foton elnyelődik a polarizátorlemezen akkor is, amikor annak zajmentes környezetben át kéne haladnia. Ez a következőképpen lett szimulálva:

Először kisorsoltuk, hogy Béla olyan polarizátorlemezt használt, amin a fotonnak van esélye áthaladni, majd Béla detektál. Ezt követően generálunk egy random számot 0 és 1 között mely, ha nagyobb, mint a zajnak meghatározott értéke (0 és 1 közötti érték, ahol a 0,2 20%-os zajt jelent) akkor ugyan úgy folytatjuk a szimulációt, mint ha nem lenne egyáltalán zaj. Ha azonban a random számunk kisebb, mint a zaj „mértéke” akkor a beérkező bittel ellentétesnek szimuláljuk detektálását. Elképzelhető az is, hogy Éva rossz, Anna bitjével ellentétes bitet küld, de zaj miatt végeredményben Béla mégis csak jó bitet fog érzékelni.

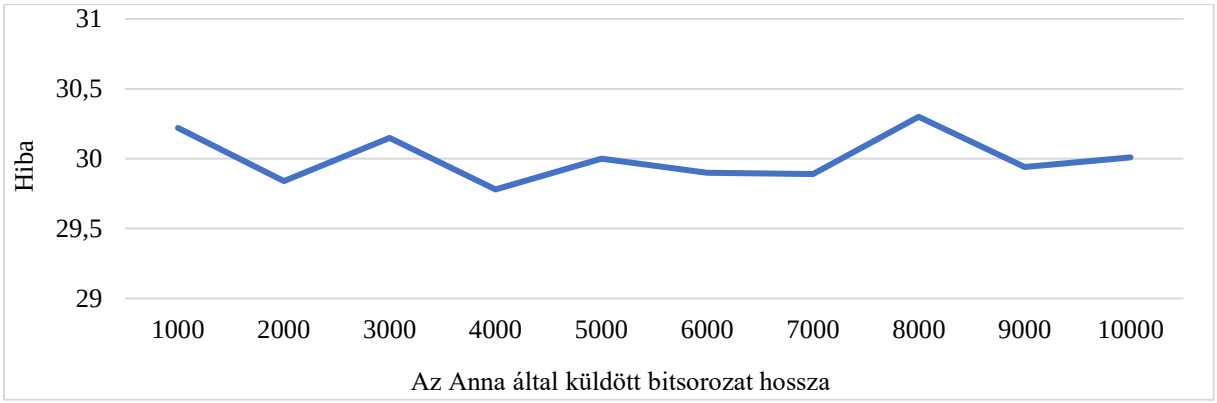
A mérések után 0 és Anna leírt bitjeinek hossza között, egy megadott mennyiségű random számot generálunk. Ezek a számok határozzák meg annak a helyét, ahol Anna és Béla összehasonlítják bitjeiket egymással, majd „kidobják” azokat (törlik a tömbjükből).

Ideális környezetben nem találnak hibát így a kommunikációt sikeresnek könyvelik el. Zajos esetben csak a zaj mértékének megfelelő hiba lép fel. Éva „támadásának” esetén tehát, ha a mért hiba jelentősen eltér a zaj miatt várt mennyiségtől Anna és Béla tudni fogja, hogy lehallgatták őket.

7. Levont következtetések

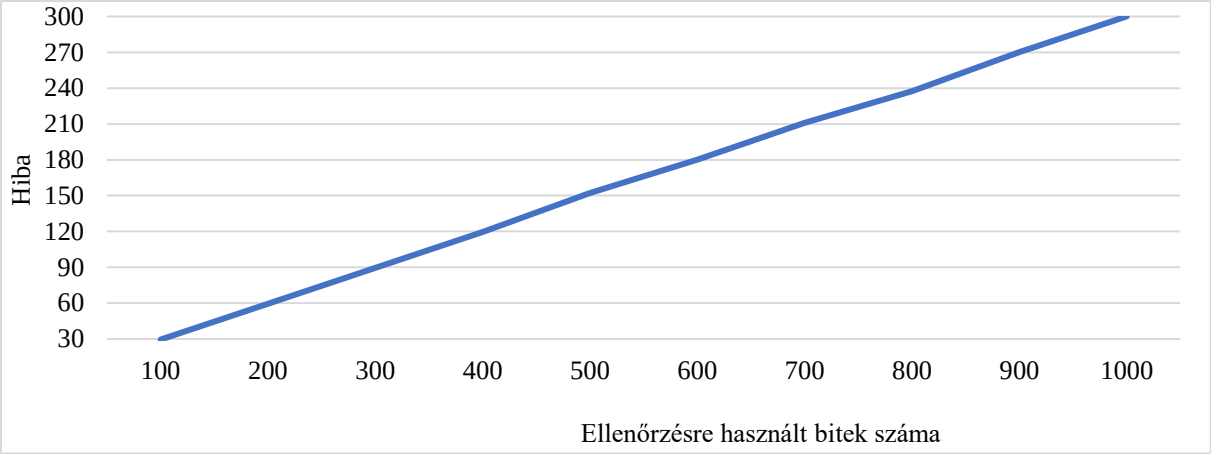
Tegyük fel, hogy Éva Anna minden egyes bitjét megpróbálja lehallgatni és Anna és Béla 100 bitet használnak arra, hogy kiderítsék Éva lehallgatja-e őket. A korábbi fejezetek alapján, Béla átlagosan minden negyedik fotont fogja detektálni. Ezért, ha Anna túl kevés bitet küldene, akkor előfordulhat az, hogy Bélának nem lesz 100 detektált bitje az ellenőrzéshez. Azaz érdemes Annának elég sok bitet küldenie.

Tegyük fel, hogy Anna elég sok bitet küldött, ezért Bélának biztosan lesz 100 detektált bitje. Kutatásunk eredménye az, hogy az Anna által küldött bitek hossza egy idő után már semmiféle előnnyel nem jár. Az Éva felderítésére használt 100 bitben talált hibák mennyisége nem függ az Anna által küldött bitek számától (*6. ábra*). Azaz, Annának fölösleges túl sok bitet küldeni, ha közben a támadó fél lehallgatásának kimutatására felhasznált bitek számát nem növeljük. Ez csak terhelné a kommunikációs csatornát és a gépigényt.



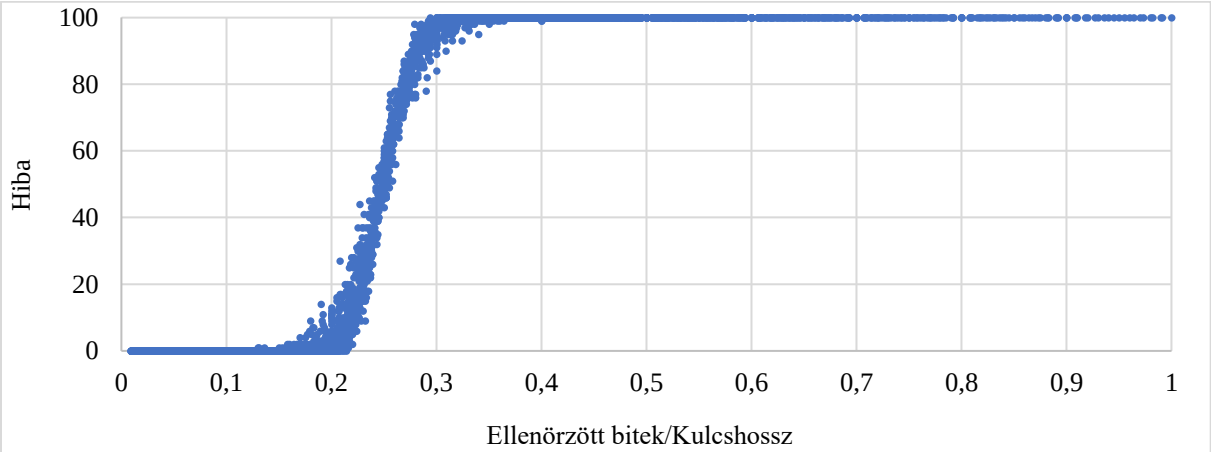
6. ábra: A grafikon azt mutatja be, hogy ha Anna és Béla 100 bitet használ ellenőrzésre, akkor mennyi az 1000 szimulációban talált hibák átlaga. A függőleges tengelyen az Anna és Béla által ellenőrzött bitek között talált hibák számának átlagát látjuk. A vízszintes tengelyen az Anna által küldött bitek hosszát láthatjuk. A grafikonon jól látszik, hogy a hibák átlaga csak csekély mértékben változik a várt 30-hoz képest, ami a kvantummechanika statisztikus jellegéből, és nem a küldött bitek hosszából fakad.

A hiba mennyisége egyenesen arányos az ellenőrzött bitek mennyiségével, arányuk nem változik jelentősen, ha csak az ellenőrzött bitek számát növeljük (*7. ábra*).



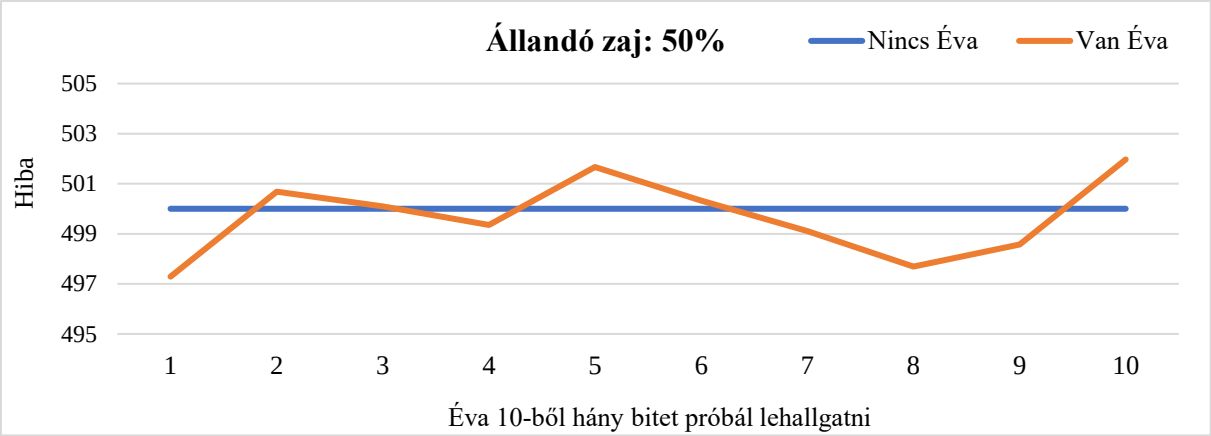
7. ábra: Ha Anna eredeti kulcsa 10 000 bit hosszúságú, akkor 100-zal több bit ellenőrzése esetén átlagosan 30-cal több hibát észlelünk.

Az ellenőrzött bitek számának kisebbnek kell lennie, mint az Anna által küldött bitek 30%-a, különben az esetek nagyon nagy részében több bitet akarunk ellenőrizni, mint amennyi rendelkezésünkre áll. Ajánlott 10 és 20 százalék között megválasztani ezt az értéket, ekkor ugyanis csak kis valószínűséggel lesz elégtelen hosszúságú a Béla által detektált bitekből alkotott kulcs, marad a titkos kulcshoz is bit, de nem is ellenőrzünk túl kevés bitet így Éva támadását könnyebben felfedezhetjük. Ezt az eredményt mutatja be a *8. ábra*.



8. ábra: A grafikon vízszintes tengelye az ellenőrzött bitek és az Anna által küldött bitek hosszának aránya. A függőleges tengely azt mutatja, hogy Béla kulcsa 100 alkalomból, hányszor volt rövidebb, mint amennyi bitet ellenőrizni szerettek volna Annával.

Ha 50%-os (vagy attól kis mértékben 1-2% eltérő) a zaj, nem tudjuk eldönteni, hogy Éva támadott-e vagy sem, teljesen függetlenül attól, hogy az esetek hány százalékában hallgat bele a kommunikációba.



9. ábra: A grafikon azt mutatja, hogy 50%-os zajnál Éva mérésének gyakoriságát növelve 1%-os hibahatárral ugyan azt a hiba mennyiséget kapjuk, mint azt Éva nélkül várnánk. Mivel a zaj sem lesz mindig pontosan ugyan annyi a kettő megkülönböztethetetlen.

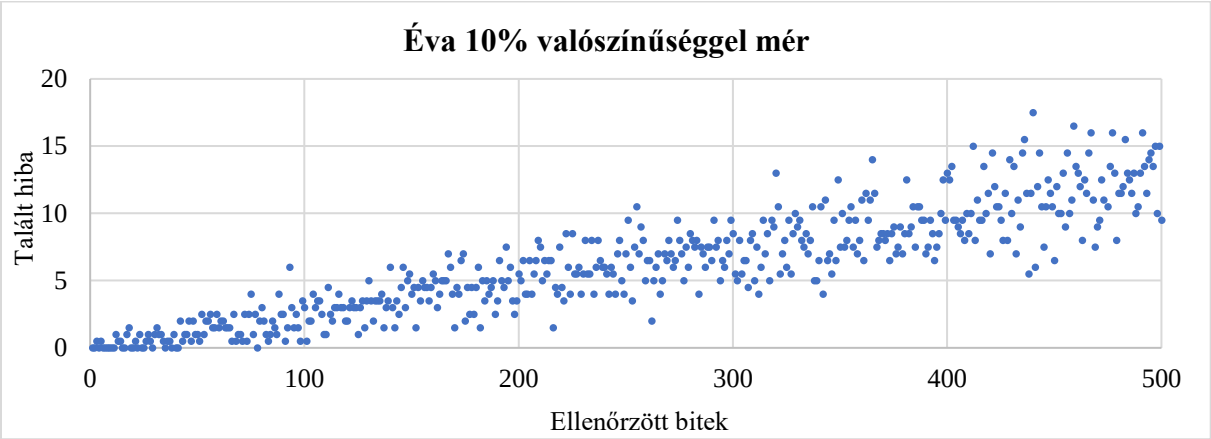
Az ideális kulcshossz

Egy ma is használt titkosítási módszerben, az RSA titkosításban minimum 0,5 Kb hosszú titkos kulcsot használnak [19]. Mivel a B92 használatával kulcsunkat csak kitalálni tudják, (nincsenek prímtényezői, hiszen ez egy másféle titkosítás) ezért itt elegendő egy rövidebb kulcs is. Egy 128 bit hosszú végső/titkos kulcs esetén $2^{128} = (2^{10})^{12,8} \approx 1000^{12,8} \approx 10^{38}$ féle kulcslehetőségünk van.

Az *Our World in Data* [20] szerint 442 kvadrillió ($442 \cdot 10^{15}$) műveletet tudott elvégezni a világ leggyorsabb szuperszámítógépe 2021-ben. Ez egy pár éven belül el fogja érni a 10^{18} műveletet mellyel $\frac{2^{128}}{10^{18}} = 3{,}4 \cdot 10^{38}$ lehetőséget $\frac{3.4 \cdot 10^{38}}{60 \cdot 60 \cdot 24 \cdot 365} = 10^{13}$ év alatt tud végig próbálni. Ezen ~~a~~ gondolatmenet szerint 256 bit hosszú kulcsot 10^{51} év alatt lehetne feltörni. Ezek alapján egy 128 és 256 bit közötti hosszúságú kulcs bőven megfelelő a számunkra, szinte lehetetlen azt feltörni. Amennyiben nincs zaj, 1000 bit küldése esetén átlagosan 250 bitet fog Béla detektálni. Ez már elég hosszú ahhoz, hogy biztonságosan kommunikálhassanak.

A *10. ábra* azt az eredményünket mutatja, hogy Éva észrevételéhez elég kb. 200-300 bitet ellenőriznünk még akkor is, ha Éva csak minden 10 alkalommal próbál biteket lehallgatni Anna üzenetéből (ennél lényegesen kevesebbel nincs értelme foglalkoznunk hiszen akkor Éva szinte semmilyen információhoz nem jut a kulccsal kapcsolatba). Ahhoz, hogy 100-200 bitünk maradjon a titkos kulcshoz, legalább ezerötszáz-kétezer bitet érdemes küldenie Annának hiszen ennek átlagosan csak a negyedét fogja Béla detektálni. Így az ellenőrzésre kidobott bitek közül várhatóan fog még maradni a titkos kulcshoz elegendő. Kettőezer bit küldése esetén 500 bitet

detektálunk átlagosan melyből 300 bit ellenőrzése esetén körülbelül 200 bitünk marad végleges kulcsként.

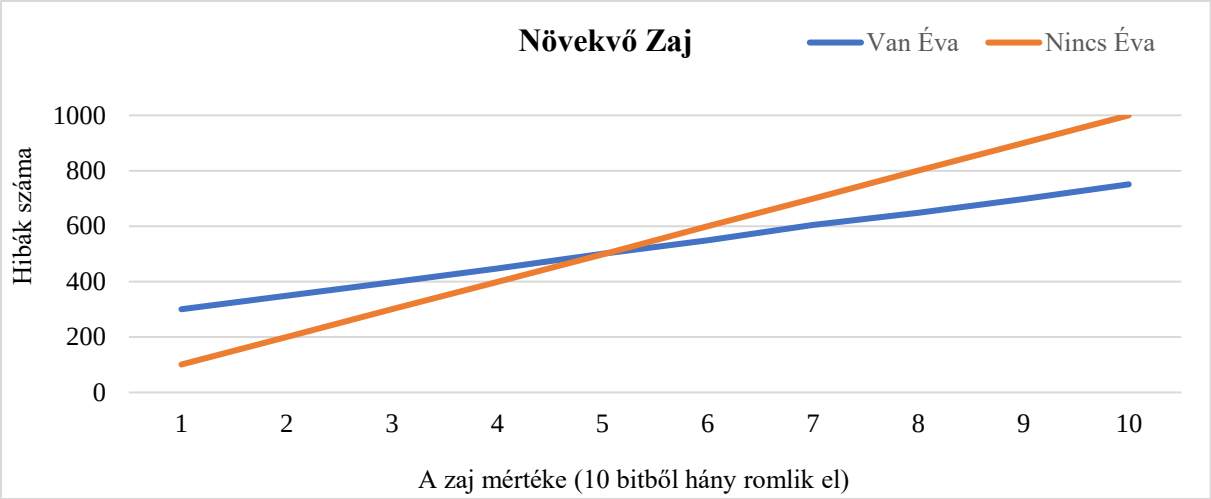


10. ábra: A grafikonon azt láthatjuk, hogy az ellenőrzött bitek mennyiségének növelésével mennyi hibát talál Anna és Béla, ha Anna egy 10 000 bit hosszú kulcsot küld el Bélának és Éva a kommunikációban 10% valószínűséggel mér. (Ahol nulla vagy ahhoz közeli értéket látunk a függőleges tengelyen ott a kommunikációban résztvevő felek nem ellenőriztek megfelelő mennyiségű bitet, hiszen mi tudjuk, hogy Éva belehallgatott a kommunikációjukba, ők viszont nem.)

Ha a rendszerben zaj van (mely 50%-tól eltér), akkor a talált hibák mennyisége Éva mérési gyakoriságától függően fog eltérni a szimplán zajtól várt hiba mennyiségétől. A hiba mennyisége Éva támadásával kis zaj esetén nő, nagy (több mint 50%) esetén pedig csökken, azaz a zaj valójában 50% felett tükrözve van önmagára így Éva nagy, mondjuk 80% feletti zaj esetén sem tud elbújni. (90%-os zaj esetén a megtalált hibáink az ellenőrzött bitek 90%-nál kisebbek lesznek, 20%-os zaj esetén pedig az ellenőrzött bitek 20%-nál nagyobbak). Tehát ha elég hosszú kulcsunk van, hogy a mérések statisztikai mivoltából adódó eltéréseket meg tudjuk különböztetni Évától, akkor nem kell változtatnunk a zaj nélküli kulcshosszunkon. Ezek alapján egy ideális kulcshossz lehet egy 1000 vagy annál nagyobb bites Anna által létrehozott eredeti kulcs (1-2 Kb).

Zaj hatása

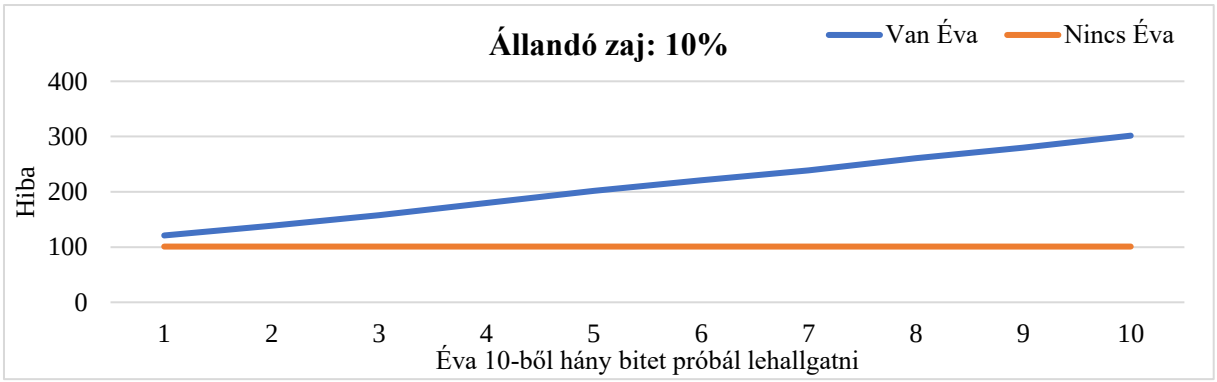
A zaj megváltoztatja a hibák számát. 50%-ig egyre nehezebben különböztethetjük meg a zajt és Évát, majd 100% felé haladva újra egyre könnyebben (*11. ábra*).

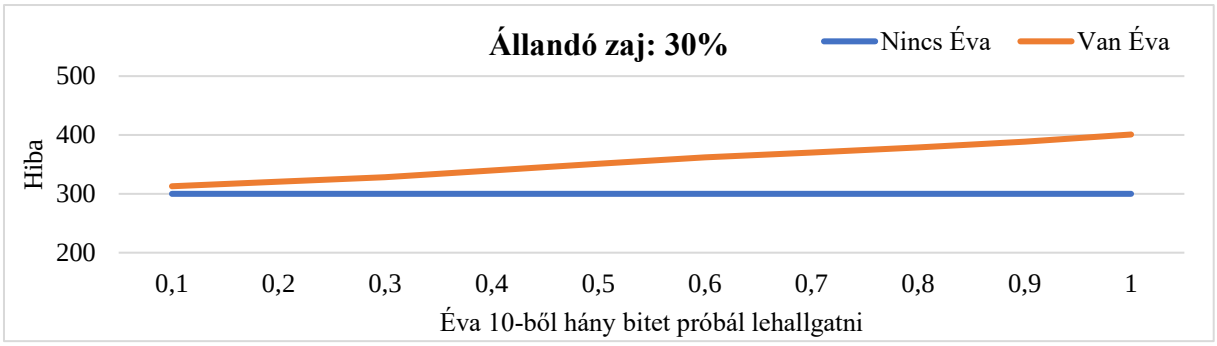


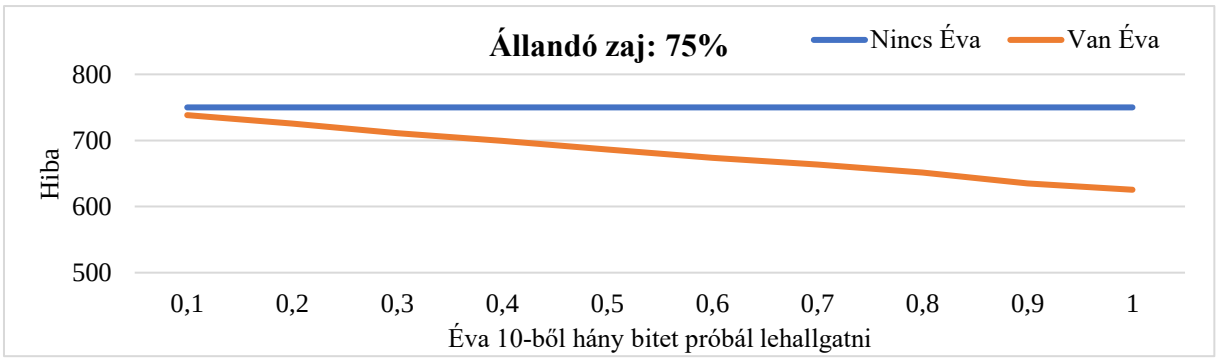
11. ábra: A grafikon azt mutatja, hogy hogyan változik a hiba mértéke a zaj lépésenként 10%-os növelésével, amikor Éve nem hallgat bele a kommunikációba és mikor mindig belehallgat. Az 50%-os zajt megközelítve a zaj Éva nélkül és a zaj Évával együtt okozott hiba mennyisége közötti különbség egyre kisebb. Majd a 100% felé haladva egyre nagyobb. A méréseket egy eredetileg 10 000 bit hosszúságú kulccsal és abból 1000 bitnek az ellenőrzésével végeztük.

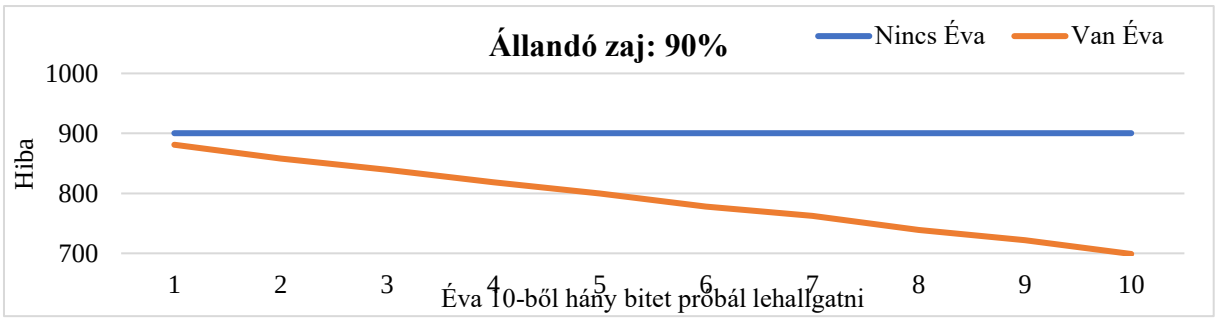
Éva stratégiája

Éva úgy lesz egyre kevésbé észrevehető, ha a zaj mértéke közelít az 50%-hoz vagy ha Éva csak ritkán (pl.: az esetek 10%-ban) mér. Azonban utóbbi, csak kis mennyiségű ellenőrzött bitszámnál releváns hiszen, ha több bitet ellenőrzünk több hibát fogunk kapni, viszont a várt hibától való eltérés nagysága nem fog annyit változni. Azaz, tegyük fel, hogy 100 bit ellenőrzése esetén Anna és Béla a csatorna 10%-os zaja miatt 10 bit hibát vár. A kvantummechanika statisztikus jellege miatt a valóságban az is előfordulhat, hogy Éva belehallgatása nélkül akár 5% vagy 15% is lehet a hiba. Így, ha Éva minden 10-ikre hallgat bele a kommunikációba akkor ő a hibát 2,5%-kal változtatja. Tehát azt várnánk, hogy 10 várt hiba helyett 7,5 és 12,5 hibát találunk. Ekkor még bőven hihetjük azt, hogy a bithiba pusztán a zajból ered, ezért Éva észrevétlen marad, amit a zaj elfed. Sőt, ilyenkor még zaj nélküli esetben is nagyon sokszor előfordulhat, hogy Anna és Béla nem is talál hibát. Azonban, ha az ellenőrzött biteket mondjuk 10 000-re növeljük, akkor egy kicsit ugyan nő a hibahatárunk, azaz 1 000 hiba várásakor akár még 950-1 050 hiba közötti hibaszámok is sokszor előfordulhatnak. Azonban, még akkor is, ha Éva továbbra is csak minden 10-dik alkalommal mér akkor az általa okozott hiba 2,5%-a az ellenőrzött biteknek, azaz 250 bitnyi eltérés a várt értéktől. Ez már lényegesen túl fog lógni a várt hibahatáron, így Évát észrevesszük.









A grafikonok azt mutatják, hogy 10%-os zaj esetén, Anna és Béla mennyi hibát talál, ha Éva nem hallgat bele a kommunikációba. Továbbá, ha lépésenként 10%-kal egyre többször hallgat bele. A méréseket egy 10 000 bit hosszúságú eredeti kulccsal és abból 1000 bitnek az ellenőrzésével végeztük. Az eredmények a szimuláció százszor való lefuttatásának átlagait mutatják.

8. Összefoglalás

A *kvantummechanika alapjai* fejezetben szó esett azon tanulmányainkról, melyek elengedhetetlenek voltak a B92 protokollhoz és a programunk megírásához. Az állapotok reprezentálása egységvektorokkal, valamint a szuperpozíció elve kulcsfontosságú volt a folytatásban.

A B92 protokoll elvének bemutatása volt a következő fejezetek témája, mely tisztázza az általunk használt fogalmakat és lerakja az építő alapköveket a programozáshoz. Saját ábrák és táblázatok segítségével írjuk le egyes folyamatok lehetőségeit.

A programkód bemutatásnál ismét elővesszük a legfontosabb tudnivalókat, amik alapján elkészítettük a szimulációt. Az esetek végbemenetelének valószínűsége és az azokból vont következtetések képezik a kód alapjait.

Végül a már kész alapokon nyugvó ház falait építettük fel azzal, hogy változatos beállításokkal futtattuk a programot és szűrtünk le olyan következtetéseket, mint:

- az ellenőrzött bitek során keletkezett hibák száma nem függ az Anna által küldött bitek számától, amennyiben a keletkezett kulcs elég hosszú, hogy tudjuk ellenőrizni és marad megfelelő mennyiségű bit az ellenőrzés után.
- az ideális kulcshossz annak érdekében, hogy az Anna és Béla kommunikációja során keletkezett kulcsot ne lehessen feltörni, de ne is terheljük feleslegesen a rendszert (nagyjából 1-2 Kb).
- a zaj hogyan befolyásolja az Éva által keltett hibákat. Itt röviden azt vettük észre, hogy 50%-os zaj felett Éva belehallgatása miatt kevesebb hibát találunk az ellenőrzés során, mint tisztán a zaj miatt.
- az Éva által használható legjobb stratégia, amikor 50%-ig minél nagyobb zaj mellett minél kevesebb alkalommal hallgat bele (nagyjából minden 8-10. alkalom már kevésnek számít). Azonban vigyáznia kell arra is, hogy ha kevesebb alkalommal hallgat bele a beszélgetésbe, akkor kevesebb eleme lesz meg a kulcsból.

9. Továbblépés

Ha a jövőben kiépülnek a kvantumkommunikációs csatornák akkor azokkal szeretnénk, hogy viszonylag biztonságosan tudjunk kommunikálni, de ne használjon fel a kommunikáció túl sok erőforrást feleslegesen.

Erre lehetne megoldás egy olyan programnak az írása mely egy adott rendszer számára megmondja az optimális kulcshosszt (melyet Annának kell generálnia) és azt, hogy ebből hány bitet ellenőrizzenek Bélával attól függően, hogy a felhasználó mekkora kockázatot szeretne vállalni (azaz mekkora eséllyel tud Éva úgy részleteket szerezni a kulcsból, hogy ők azt ne vegyék észre) és mekkora a zaj mértéke. Túl nagy zaj vagy túl kevés kockázatvállalás esetén a program azt is javasolhatná, hogy a felhasználó általa megadott elvárások teljesítéséhez szinte nagyon sok qubit vagy az éppen legtöbb qubittel rendelkező számítógépnél is erősebb kellene, ezért növelje a vállalt kockázatot vagy csökkentse a zajszintet.

10. Irodalomjegyzék

[1] A. Einstein, B. Podolsky, and N. Rosen (1935) Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? Physical Review 47, 777 https://doi.org/10.1103/PhysRev.47.777

[2] J. Bell (1964) On the Einstein–Poldolsky–Rosen paradox. *Physics* 1 3, 195–200 https://cds.cern.ch/record/111654/files/vol1p195-200_001.pdf

[3]J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt (1970) Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters.* **23** 880 https://doi.org/10.1103/PhysRevLett.23.880

[4] A. Aspect, P. Grangier, G. Roger (1982) Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. Physical Review Letter 49 (2) 91 https://doi.org/10.1103/PhysRevLett.49.91

[5] D. Bouwmeester, J-W Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger (1997) Experimental quantum teleportation. *Nature* **390**, 575-579 https://doi.org/10.1038/37539

[6] R. P. Feynman (1982) Simulating Physics with Computers. *International Journal of Theoretical Physics.* 21 (6–7). 467–488. https://doi.org/10.1007/BF02650179

[7] P. W. Shor (1994) Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 124-134 doi: 10.1109/SFCS.1994.365700

[8] C. H. Bennett, and G. Bassard (1984) Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the International Conference on Computers, Systems & Signal Processing*, Bangalore, India 175-179.

[9] Quantum Flagship webpage, an European open portal 2020 https://qt.eu/

[10] C. H. Bennett (1992) Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters*, **68**, 3121. http://dx.doi.org/10.1103/PhysRevLett.68.3121

[11] 2023-2027 EU secure connectivity programme: Building a multi-orbital satellite constellation https://www.europarl.europa.eu/thinktank/hu/document/EPRS_BRI(2022)729442 (2022.10.29.)

[12] The Quantum Internet Alliance will build an advanced European quantum internet ecosystem 14.10.2022 https://quantum-internet.team/2022/10/14/the-quantum-internet-alliance-will-build-an-advanced-european-quantum-internet-ecosystem/ (2022.10.29.)

[13] Halász T., Jurisits J. és Szűcs J. (2015): Fizika 11-12. Közép- és emelt szintű érettségire készülőknek. *Mozaik Kiadó,* Szeged.

[14] The Nobel Prize in Physics 2022 https://www.nobelprize.org/prizes/physics/2022/summary/ (2022.10.19.)

[15] Tóth K. (2021) Modell kvantummechanika középiskolában. *Fizikai Szemle*. 209-214. **71**(6)

[16] Chris Bernhardt (2019) Quantum Computing for Everyone. *The MIT Press*. Cambridge.

[17] University of St Andrews: QuVis: Quantum key distribution using two non-ortogonal states https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-b92/B92_photons.html (2022.10.19.)

[18] Csaplár Miklós, Kemecsei Kornél (2022.10.30) B92 protokoll programkódja: https://github.com/Harcipan/B92_Protocol

[19] IBM: Size consideration for public and private keys. 2021.03.03. https://www.ibm.com/docs/en/zos/2.3.0?topic=certificates-size-considerations-public-private-keys (2022.10.29.)

[20] Our World in Data: Computational capacity of the fastest supercomputers https://ourworldindata.org/grapher/supercomputer-power-flops (2022.10.19.)