Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

Mérési útmutató (felkészülés)

KVANTUM-ALAPÚ HÁLÓZATOK: BEVEZETÉS MÉRÉSHEZ

A mérést kidolgozta:
Bacsárdi László, Galambos Máté, Imre Sándor
Mérésvezető:
Solymos Balázs, `solymosb@hit.bme.hu`

Adminisztráció és mérési anyagok

A méréshez használható felhő eléréséhez BME Címtár azonosítóra van szükség - aki még nem aktiválta magának a korábbi félévekben, tegye meg a mérés kezdetéig!
"A BME Címtár elsődleges feladata egy központi azonosítási szolgáltatás nyújtása minden egyetemi polgár részére. Minden személy, aki felhasználóval rendelkezik a Neptunban, automatikusan kap címtáras azonosítót is. Ahhoz, hogy ezt használatba vehesse, be kell állítania egy címtáras jelszót, mivel ezt biztonsági okokból nem vesszük át a Neptunból. A jelszó beállítását a felhasználói adminisztrációs oldalon lehet elvégezni: `https://login.bme.hu/` "

A méréshez szükséges három programot külön is elérhetővé tettük, amennyiben nem virtuális gépen, hanem a saját gépen szeretné valaki futtatni, ezen a linken érhető el és telepíthető saját gépre: `http://www.hit.bme.hu/~bacsardi/mcl/kvantum_meres_programok.zip`

Jegyzőkönyv

A mérésről készült jegyzőkönyveket a `solymosb@hit.bme.hu` e-mailre várjuk, „kvantummeres" tárggyal. A jegyzőkönyv sablonja a `http://www.hit.bme.hu/~bacsardi/mcl/kvantummeres/` oldalról érhető el.

Bevezetés

A mérés fő célja az alapvető kvantuminformatikában használt jelenségek bemutatása, valamint a témakörben felmerülő hallgatói kérdésekre történő válaszadás. Ennek tudatában ajánlott jelen mérési útmútatóban lévő feladatokat az alkalom előtt átnézni, elvégezni, hogy később minél kevesebb időt kelljen fordítani a demonstrációs programok használatára, a kvantumos jelenségek tényleges vizsgálatával ellentétben.

A kvantumbit

Kvantuminformatikai alkalmazásokban az információt jellemzően kicsi, kvantummechanikai szabályoknak megfelelően viselkedő fizikai egységek hordozzák. Ennek következtében az ezekkel való dolgozás során lehetőség nyílik (egyben szükséges is) kvantumos jelenségek használatára, ennek minden előnyével és nehézségeivel. Jellemző ilyen fizikai hordozók pl.: fotonok polarizációja, elektronok spinje, egyes ionok stb.. A továbbiakban optikai megoldások távközlésben való elterjedsége miatt alapértelmezésben tekintsük fotonok polarizációját az információ hordozójaként (matematikai leírás szempontjából a tényleges fizikai megvalósítás egyébként is a legtöbb esetben közömbös).

Klasszikusan egy bitünk két fajta értéket tárolhat attól függően, hogy hogyan állítottuk be. Ehhez természetesen szükséges, hogy a hordozónak legyen két egyértelműen megkülönböztethető állapota, hogy a tárolt információt később ki is tudjuk olvasni. Foton polarizációja esetén ilyen lehet két egymásra merőleges polarizációs sík (merőlegesnek kell lenniük az egyértelmű kiolvasáshoz). Valóságban azonban a polarizáció nem csak két féle lehet. Kvantumos állapotoknál ez meg van

engedve, így a tényleges állapot az eredeti két merőleges állapotunk tetszőleges keveréke is lehet. (Vegyük észre, hogy két merőleges állapot keverésével előállítható a többi lehetséges polarizációs állapot.) Ezt a jelenséget szokás szuperpozíciónak nevezni. Természetesen ebből az engedményből az is következik, hogy ismeretlen kvantumbitről nem tudunk teljes információt kinyerni kiolvasásnál. Általánosan kvantumbitek és viselkedésük diszkrét időben leírható egy viszonylag egyszerű matematikai modellel, melynek ide tartozó része a következő:

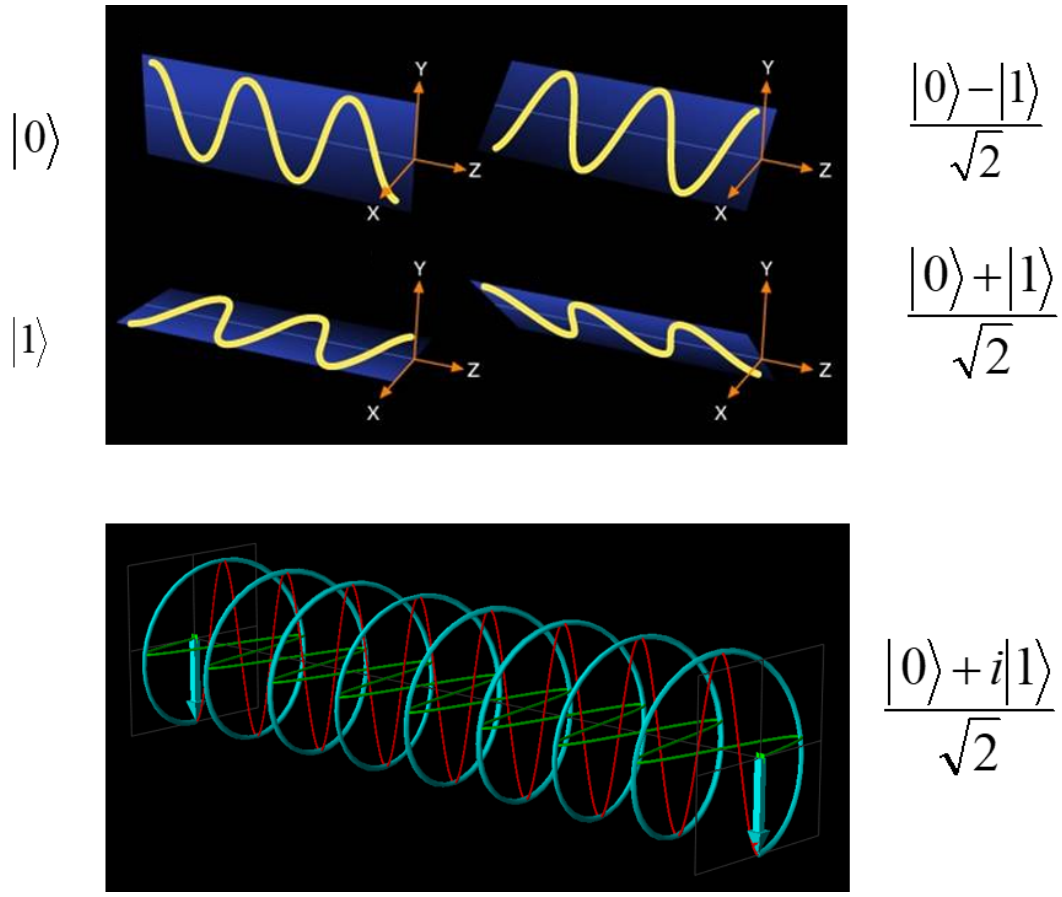
Kvantumbit matematikai modellje

Egy zárt fizikai rendszer éppen aktuális állapota leírható egy **V** Hilbert-térbeli egységhosszú, komplex együtthatós állapotvektorral. Hilbert-tér például egy komplex lineáris vektortér, amire értelmezve van a belső szorzat (skalárszorzat). Vegyünk példának egy két dimenziós Hilbert-teret, ami egy egyszerű zárt fizikai rendszert jelképez (pl.: foton polarizációja). A rendszer állapotát le lehet írni egy **v** kétdimenziós vektorral, ahol:

$$v = \begin{bmatrix} a \\ b \end{bmatrix} = a\mathbf{0} + b\mathbf{1} \text{ ,ahol } \mathbf{0} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{1} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, a, b \in C$$

Itt **0** és **1** az orthonormális (ortogonális és egységhosszú) bázisvektorok. Mivel az állapotvektor egységhosszú, ezért ki kell még kötni, hogy $|a|^2+|b|^2 = 1$. Az együtthatókra szokás még valószínűségi amplitúdóként is hivatkozni, mivel az egyes állapotokhoz tartozó mérési valószínűségek ebben az alap bázisban $|a|^2$ és $|b|^2$. A két bázisvektort a szakirodalomban általában $|0\rangle$ és $|1\rangle$ jelöli. [1]

[1] Jelölés: A kvantumbitek (vagy qubitek) leírására leggyakrabban a Bra-ket, vagy más néven Dirac jelölés használt (Ezt a jelölést Dirac vezette be, ezért Dirac jelölésként is ismert). A rendszer egy állapotát általában ennek megfelelően $|\varphi\rangle$ jelöli, ami egy komplex oszlopvektor. A $\langle\varphi|$ jelőlés ,a $|\varphi\rangle$ transzponáltjának konjugáltja, vagyis komplex adjungáltja.



1. ábra. *Foton polarizációja mint kvantumos állapot.*

Műveletek kvantumbiteken

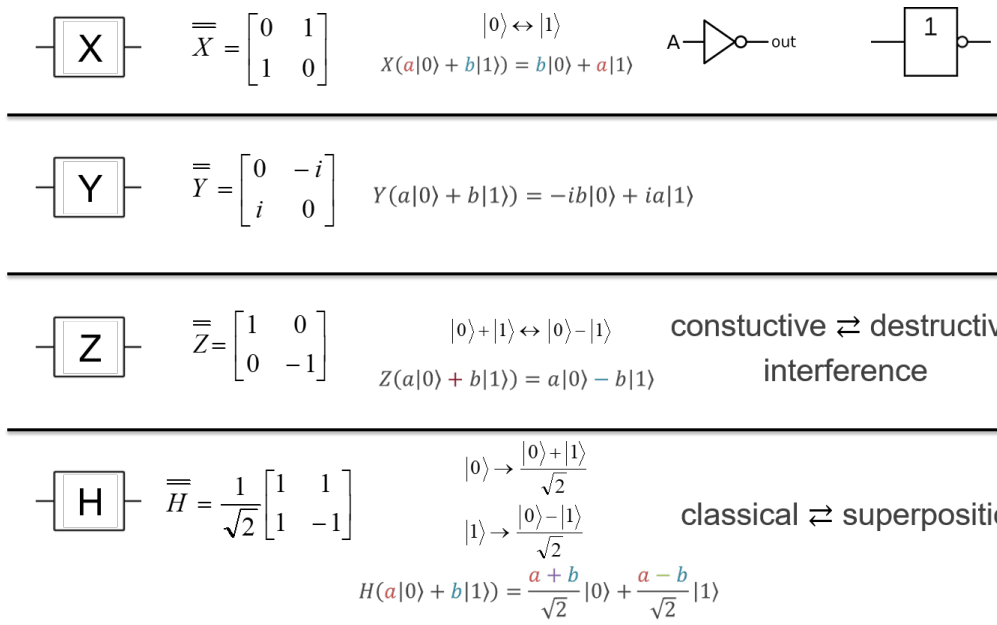
Klasszikus esethez hasonlóan, a bitjeinken végezhetünk különböző műveleteket. A valóságban ezt fotonok esetén különböző optikai elemek valósítják meg. Mérnökként legtöbbször elég csak a kezdeti és végállapot közötti kapcsolattal foglalkoznunk, ami a modellünkben a következőt jelenti:

Zárt fizikai rendszer időbeli fejlődése leírható csak a változás kezdő- és végpontjától függő unitér transzformációval. Az előbbi jelölésrendszer segítségével leírva:

$$v'(t_2) = U(t_1, t_2)v(t_2), v' \in V$$

U unitér operátor lineáris algebrai reprezentációja egy **U** kvadratikus mátrix, melynek U_{ij} elemei a bemeneti **j** orthonormális bázisvektor **i** vektorral való kapcsolatát jelképező valószínűségi amplitúdókat jelölik.

Különbség klasszikus kapukhoz képest (pl.: „és” és „vagy” kapuk), hogy minden esetben a bemenetek és kimenetek száma egyező, az egyes műveletek inverzét megfelelő sorrendben végrehajtva visszajuthatunk a kiinduló állapotba. Unitér mátrixok (transzponált konjugáltja egyben inverze is) esetében ez kifejezettek előnyős, mivel az általunk vizsgált gyszerű kapuk sokszor önmaguk inverzei is. Ezen egyszerű kapuk a következők:



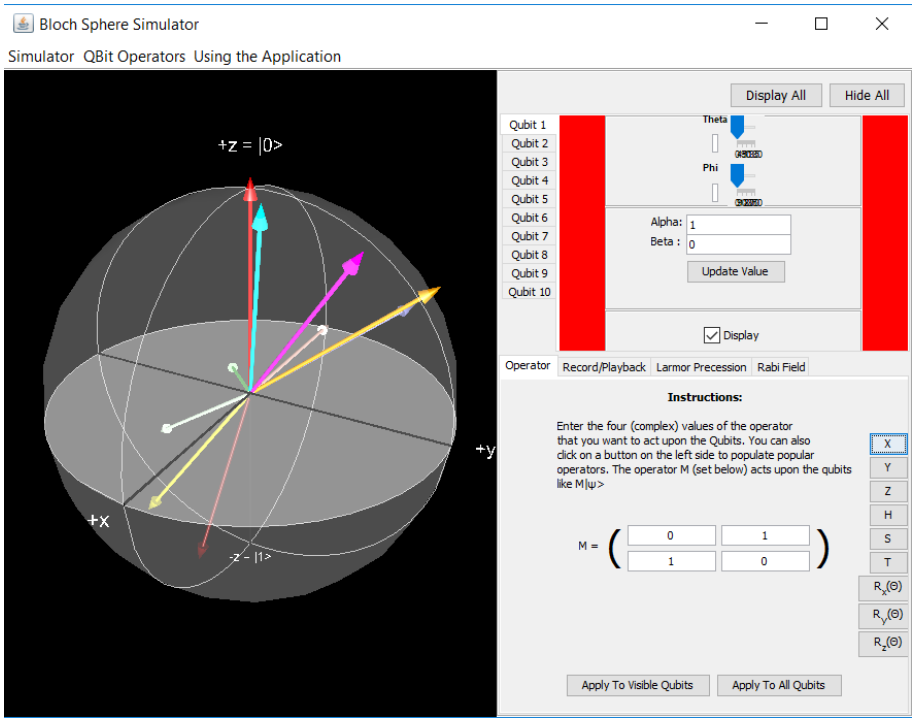
2. ábra. *X, Y, Z és H kapu.*

Kalandozások a Bloch-gömbön

Kvantumbitek egy lehetséges megjelenítési formája a Bloch-gömb, ahol egy állapot következő módon történő átírásán alapul:

Vegyük észre, hogy csak 3 paraméter van használva. Vajon miért?

A következő feladatokhoz a `Bloch3dApp` program szükséges. Ennek a kezelőfelülete látható az alábbi ábrán:



3. ábra. *Bloch3dApp program*

- Bal oldalt a Bloch-gömbön éppen megjelenített állapotok láthatóak különböző színekkel. Kezdésként javasolt egy `Hide All`-t nyomni, hogy ne 10 véletlenszerűen választott állapotot

lássunk.

- `Qubit 1-10` fülek segítségével lehet megjelenítendő állapotok tulajdonságait állítani. `Alpha` és `Beta` segítségével a **0** és **1** bázisokhoz tartozó amplitúdók állíthatóak. A `Display` négyzettel lehet állítani, hogy az éppen állított állapot a gömbön látszódjék-e vagy sem.

- Műveletek a jobb alsó kvadránsban található M = (mátrix) segítségével lehet megadni. Jobb oldalt az „X, Y, Z, H, stb..” segítségével ismertebb kapuk mátrixai tölthetőek be. A műveleteket az alsó két gomb segítségével lehet végrehajtatni a gömbön.

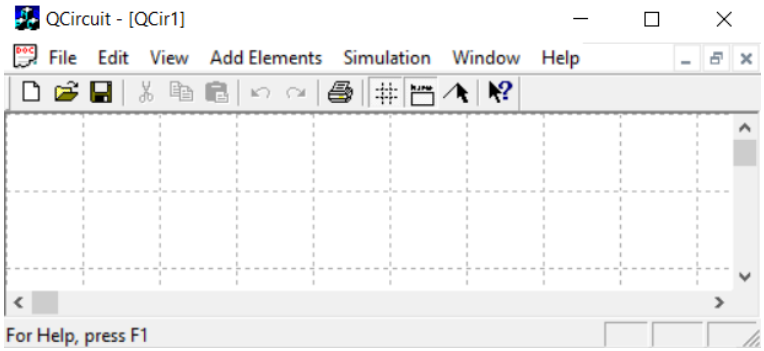
Feladatok:

1. Vizsgáljuk meg hogyan jelennek meg egyes állpotok a gömbön. Ehhez vegyen fel legalább 4 állapotot, melyek közül az első kettő a **0** és **1** (Alpha vagy Beta 0, a másik 1) legyen. (Ajánlott további állapotok még, ahol alpha és beta egyenlőek, valamint legalább egy teljesen szabadon választott.). Hogyan jelenik meg a gömbön, ha két állapot ortogonális? Milyen régió tartozik a gömbön egy bizonyos mérési eredményhez (pl.: 50-50% hogy 1-et vagy 0-át mérek)?

2. X,Y,Z kapuk vizsgálata: Milyen műveletet hajtanak végre a gömbön ezen a kapuk, vajon miért éppen az a nevük ami (elég választani egyet)? H kapu vizsgálata: Mit csinál a H kapu? Igazoljuk, hogy HXH=Z.

Kvantumáramkör-szimulátor

A következő feladatokhoz a `QCircuit` program szükséges. Ennek a kezelőfelülete látható az alábbi ábrán:



4. ábra. *QCircuit program*

- Elemeket az Add Elements menüpont alatt lehet hozzáadni. `Gates` menüpont alatt az X, Y, Z kapuk a Pauli Operators almenüben vannak. Mérésekből csak az `orthogonal` mérést használjuk, ennél a `number of qubits` azt állítja, hány vezeték legyen a bemenete. Az `Inputs` alatt kezdeti bemeneteket választhatunk itt a $|0\rangle$ és $|1\rangle$ a két eddigi bázisvektorunk megfelelője. `Watches` alatt a rendszer belső állapotát megfigyelő elemeket lehet beilleszteni. `Subsystem Watch`-al egy dobozt rakhatunk le, ami a bele kötött vezetékek állapotát tudja megfigyelni, a `Cut Watch` pedig az összes rajta áthaladó vezeték állapotát figyeli. `Outputs`-ra a kimeneti vezetékek elnyelése céljából van szükség (szimulációnál az ide érkező eredményeket kapjuk meg).

- Miután leraktuk a szükséges építőelemeket a `Connect elements` (Vonalra mutató nyíl `Window` alatt) segítségével alakíthatunk ki kapcsolatokat közöttük.

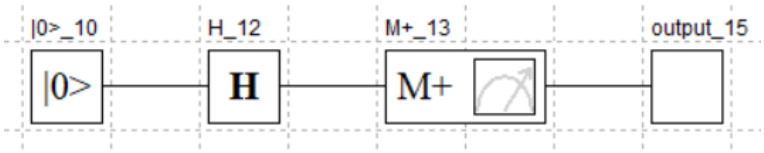
- Szimulációt a `Simulation` alatt tudjuk elindítani. Mivel a mérés kimenete valószínűségi jellegű, ezért a szimulációnál többször futtatásból származó statisztikát nézünk. Futások számát 1000 körülire állítani ajánlott.

- A teleportációs áramkörnél szükséges mind egyedi bemenet, mind irányított kapuk alkalmazása. Ezt az adott elemre (input, vagy kapu) jobb egérgombbal kattintva elérhető properties gombbal tehetjük meg. Egyedi bemenetnél adható saját név (name és label), valamint egyedi állapot (define a unit vector or density matrix). Állapot választásnál arra kell ügyelni, hogy tizedespont használat magyar szokást követ (tizedesvessző: ,), valamint a normálást nem végzik el automatikusan a program. Itt 0,6 és 0,8 például egy jó választs lehet majd. Irányított kaput az adott kapu properties menüjében a `number of control qubits` számláló változtatásával lehet készíteni.

Feladatok:

A feladatok elvégzése során a vázolt áramköröket a hallgató minden esetben `watch` elemekkel szabadon bővítheti, a pontosabb megértéshez ez még ajánlott is. A mérés során IMSc pontot lehet szerezni ezen program használatával amennyiben itt nem sorolt valamilyen probléma megoldására képes áramkört tervez a hallgató és ezt megfelelően bemutatja. Így a feledat két részből áll: probléma valódiságának megindoklása (sales pitch) és ezt megoldani képes áramkör készítése. Ebből adódóan kísérletezést elősegítendó a jegyzőkönyvben az alap áramkörök működést nem változtató bővitett verzió is elfogadhatóak.

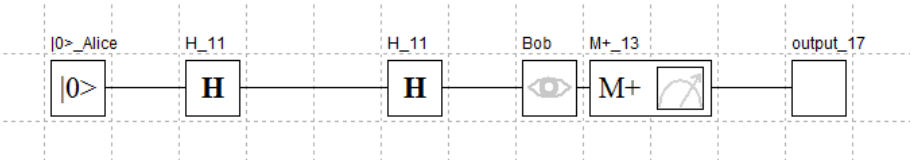
1. Készítsük el az alábbi véletlenszámgenerátort megvalósító áramkört:



5. ábra. *1. áramkör*

Vizsgáljuk a működését. Ezután helyezzünk be a már meglévő mérésünk után egy újabb mérést és hasonlítsuk össze a mérések eredményeit. Mit tapasztalunk? Mi a második mérés előtt a rendszer belső állapota (amit a watch-okkal lehet figyelni)?

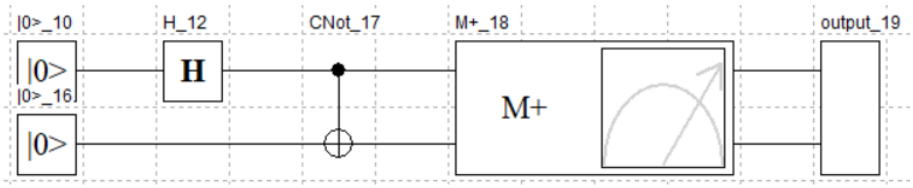
2. Vizsgáljuk a következő kiegészített áramkört:



6. ábra. *2. áramkör*

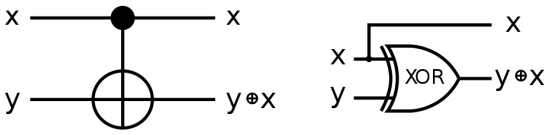
Tételezzük fel, hogy az Alice és Bob-al jelölt részekkel két külön helyen (köztük egy optikai kábel) rendelkezik két résztvevőnk, Alíz és Bob. Alíz kedve szerint 0-át vagy 1-et küld. Mit mér ilyenkor Bob? Mit mér az az aljas támadó aki le akarja hallgatni a vezetéket (Betesz egy mérést a két résztvevőnk közé.) ? Alkalmazható-e ez a konstrukció biztonságos kommunikációra?

3. Építsük meg a következő áramkört:



7. ábra. *3. áramkör*

A feladathoz egy eddig nem ismertetett kaput, a CNOT kaput kell alkalmazni. Ez a kapu lényegében egy irányított nem kapu: ha a felső vezetéken 0 jön, akkor az alsón nem változtat, ha 1, akkor az alsót invertálja. Kvantumosan az egyetlen érdekesség, hogy a felső vezetéken érkezhet 0 és 1-es állapot keveréke is. Ebben az esetben is szuperpozíciót alkalmazva egyszerűen előállítható a kimenet.



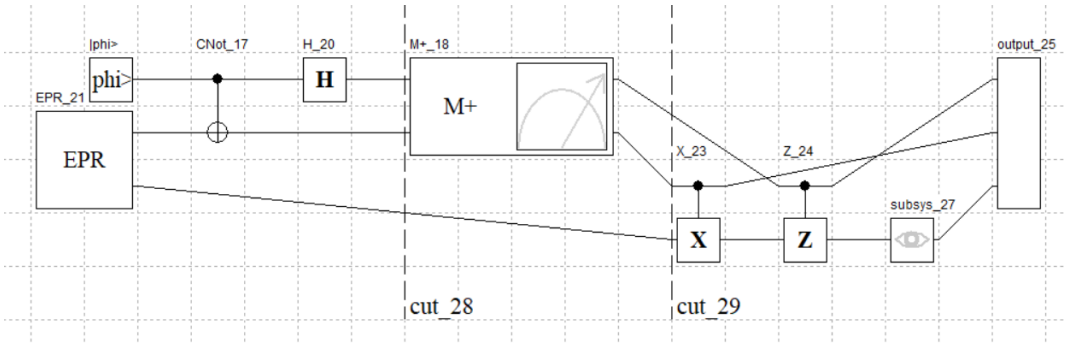
input		output	
x	y	x	y+x
|0⟩	|0⟩	|0⟩	|0⟩
|0⟩	|1⟩	|0⟩	|1⟩
|1⟩	|0⟩	|1⟩	|1⟩
|1⟩	|1⟩	|1⟩	|0⟩

input		output	
x	y	x	y+x
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

8. ábra. *CNOT kapu működése és klasszikus párja.*

Vizsgáljuk meg a mérési eredményeket. Függetlenek-e egymástól a két vezetéken keletkező eredmények? Felhasználható-e ez a jelenség kommunikációra?

4. Építsük meg a kvantumteleportáció protokollt megvalósító áramkört.

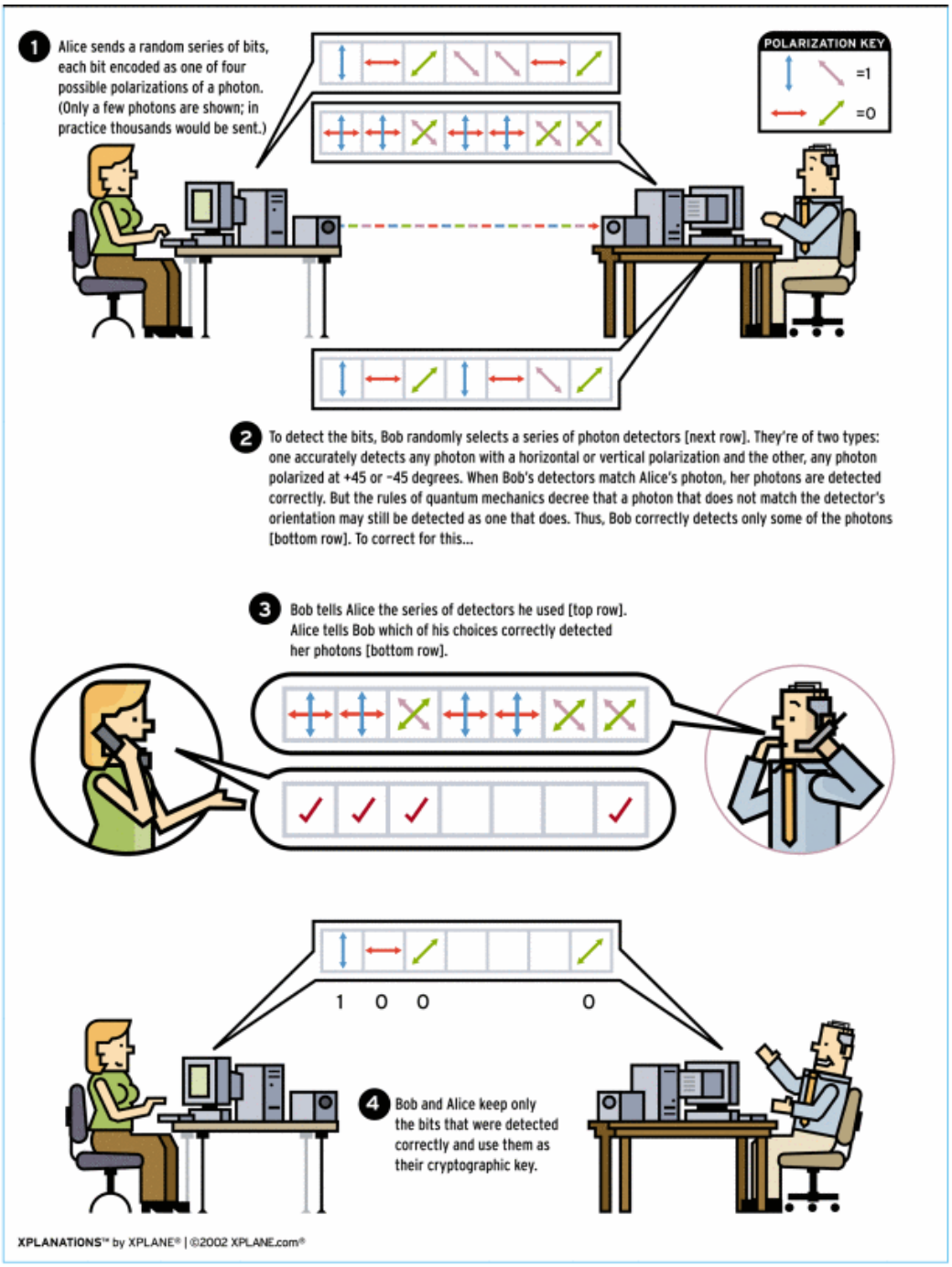


9. ábra. *Teleportáció protokollt megvalósító áramkör.*

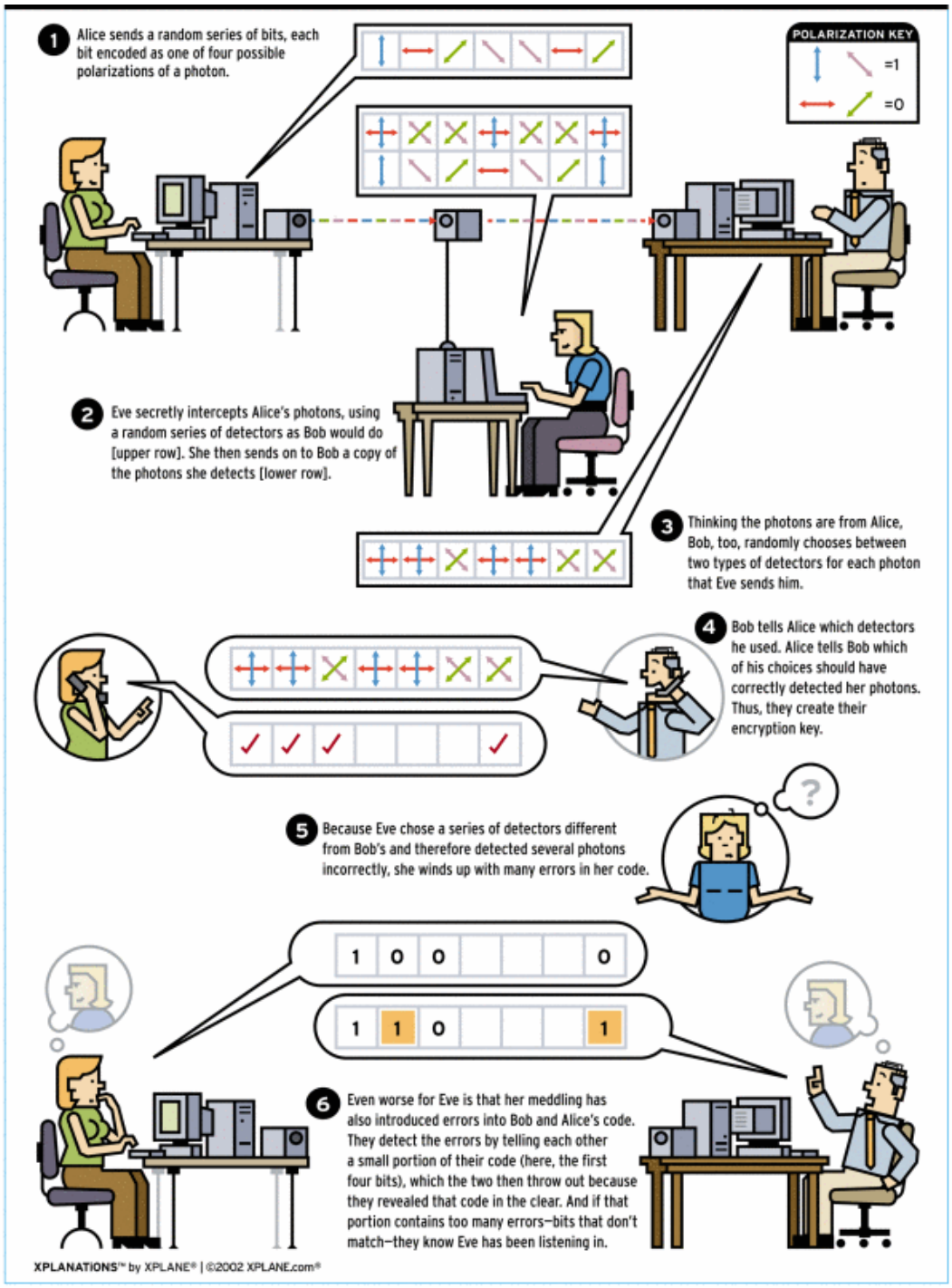
A $|phi\rangle$-vel jelölt elembe állítsunk be egyedi bemenet, az áramkör bemenetének mint teleportálandó ismeretlen állapot (0,6 és 0,8 egy jó választás amplitúdópárnak). A bemenetként használt EPR-pár egy az előző feladatban megvalósított áramkört realizál, aminek a kimenetei összefonódott párok ($|00\rangle+|11\rangle$). Vizsgáljuk meg, hogy sikeresen megkaptuk-e az általunk beállított állapotot az alsó vezetéken, illetve vizsgáljuk a rendszer mérés utáni állapotát!.

BB84 kvantumkulcsszétosztó protokoll

A kvantumkulcsszétosztás a kvantumkommunikáció egyik legfejletteb és gyakorlatban legkeresettebb felhasználása (2000-es évek közepe óta bárki számára megvásárolható megoldások a piacon). Az első és legegyszerűbb ilyen protokoll az 1984-es BB84, aminek rövid áttekintését adják a következő ábrák:



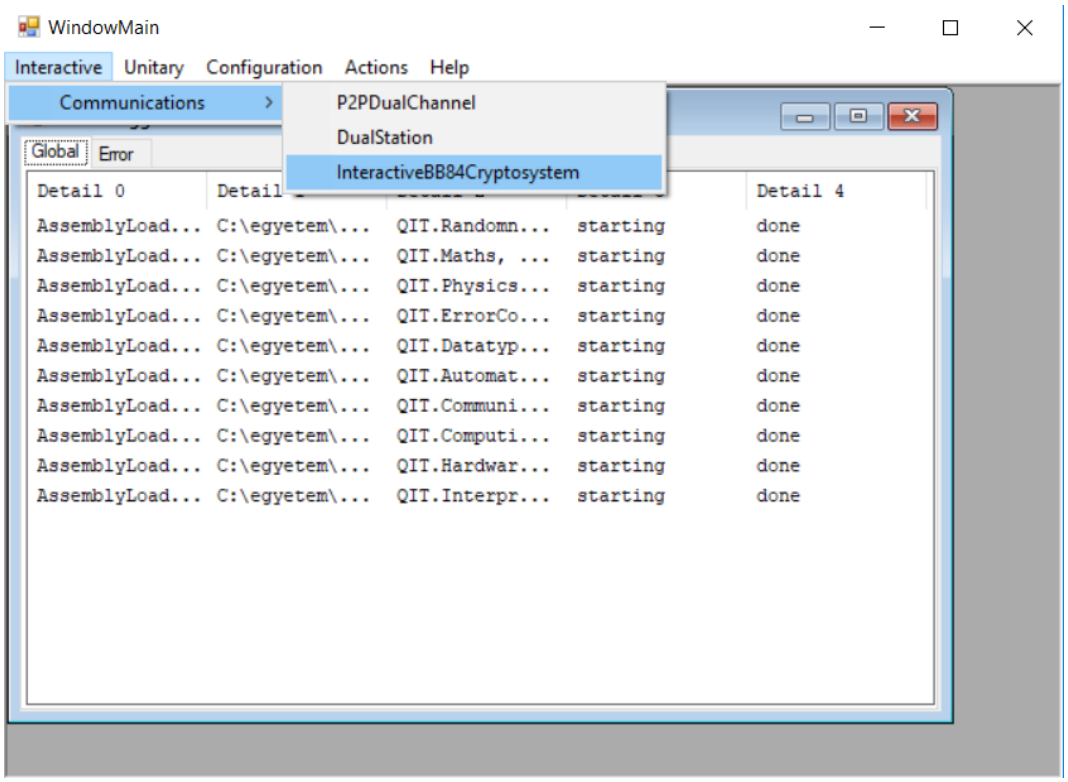
10. ábra. *BB84-protokoll támadó nélkül.*



11. ábra. *BB84-protokoll támadóval.*

Miként jelenik meg a támadó a hálózatban a komunikáló felek számára? Az elküldött bitek mekkora részéből lesz hasznos kulcs?

A protokoll működését lépésről lépésre a `QIT` program `InteracticeBB84Cryptosystem` opciójával lehet lépésről lépésre végigkövetni.



12. ábra. *QIT program BB84 protokoll szimulátora*

A mérés során ezen feladatok vezetett formában részletesebb tárgyalásra is kerülnek majd, azonban otthoni áttekintésük, hálózatok megépítése ajánlott a vezetett szekció pontosabb és gyorsabb megértéséhez.