Kvantové komunikačné protokoly

Martin Piják

1. 5. 2009

Kvantové komunikačné protokoly

Diplomová práca

Martin Piják

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
KATEDRA INFORMATIKY

Diplomový vedúci
Mgr. Mário Ziman PhD.
Bratislava 2009

Prehlásenie

Prehlasujem, že som diplomovú prácu vypracoval samostatne s odbornou pomocou školiteľa a s použitím uvedenej literatúry.

Abstrakt

V tejto práci sa zaoberáme modifikáciami kvantových komunikačných protokolov BB84 a B92.

Kľúčové slová: BB84, B92, modifikácie

Obsah

Úvod

Kvantové komunikačné protokoly sú novou oblasťou kryptológie. Bezpečnosť týchto protokolov sa zakladá priamo na kvantovej fyzike a to je celkom výnimočný jav. Znamená to asi toľko, že správne realizovaný kvantový komunikačný protokol bude bezpečný až dovtedy, kým nebude kompromitovaná kvantová fyzika. A to je zaujímavý predpoklad. Naproti tomu dnes asi najviac rozšírený kryptografický štandard RSA poskytuje bezpečnosť, ktorá sa zakladá na predpoklade, že faktorizácia veľkých čísel je „ťažký“ problém. V prípade RSA môže nastať problém, ak nájdeme niekoho, pre koho to nebude až taký „ťažký“ problém. Zatiaľ čo v prípade kvantových protokolov by niekto šikovný musel vyvrátiť kvantovú fyziku a to sa z určitého pohľadu môže javiť ťažší ako „ťažký“ problém.

Cieľ práce

Cieľom tejto práce je poskytnúť prehľad základných vlastností protokolov BB84 a B92, ďalej preskúmať konštrukciu týchto protokolov, a na základe zistených informácii navrhnúť ich modifikáciu. Nasledujúcim krokom bude overenie bezpečnosti modifikovaných protokolov.

Členenie práce

Neoddeliteľnou šúčasťou kvantových komunikačných protokolov sú základy kvantovej fyziky. Preto ak ich chceme bližšie pochopiť, musíme sa najskôr pozrieť na základy kvantovej fyziky. Stručný prehľad nám prináša prvá kapitola tejto práce. Druhá kapitola sa zameriava na konštrukciu a priebeh protokolu BB84. Získané informácie potom použijeme v tretej kapitole pri návrhu modifikácie BB84. Obdobný postup sme zvolili aj pri skúmaní protokolu B92. Postupne prejdeme cez originálny návrh B92 (štvrtá kapitola), vylepšenie (piata kapitola) až po nami navrhnuté modifikácie, ktoré sú v šiestej kapitole. Na záver práce zhodnotíme dosiahnuté výsledky.

Postup

Základna modifikácia protokolu BB84 spočíva v zmene jednej z báz, tak aby zvierali iný ako $\frac{\pi}{4}$ uhol. Tento prístup môže byť zaujímavý aj z praktického hľadiska, pretože meracie a vysielacie zariadenia obvykle pracujú s určitou odchýlkou. Pri modifikácii B92 budeme postupovať podobne.

Základné princípy

Označenie používané v kvantovej fyzike

Fyzici používajú tzv. Diracovu alebo bra-ket notáciu. Túto notáciu vytvoril britský teoretický fyzik Paul Adrien Maurice Dirac. Výhodou Diracovej notácie je, že prináša zjednodušený zápis často používaných fyzikálnych operácií.

Diracova notácia

$$|\psi\rangle = (a_1, .., a_n)^T,$$
$$\langle\psi| = (a_1^*, .., a_n^*)$$

Operácia „$*$“ označuje komplexné združenie.

V kvantovej teórii infromácie sa používa najmä dvojrozmerný komplexný priestor, takže pod označením $|\psi\rangle$ si môžeme predstaviť vektor $(a_1, a_2)^T$, pričom $a_1, a_2 \in \mathbb{C}$.

V angličitne sa niekedy $\langle\psi|$ nazýva bra vektor a $|\psi\rangle$ ket vektor.

V podstate ide o slovnú hračku, odvodenú z anglického názvu zátvorky bracket. Bra-vektor, označuje prvú časť zátvorky $\langle a,$ a ket-vektor druhú časť zátvorky $, b\rangle$ čiže dokopy máme skalárny súčin $\langle a, b\rangle$.

Diracova notácia sprehľadňuje zápis skalárneho súčinu, lineárneho operátora, projekčného operátora... Nižšie si môžete pozrieť detaily týchto operácií.

Skalárny súčin: nech $|\psi\rangle$ a $|\phi\rangle$ sú vektory ich skalárny súčin označujeme $\langle\psi|\phi\rangle$.

Lineárny operátor: nech H je Hilbertov priestor, ak $|\psi\rangle$ je bra-vektor a $\langle\phi|$ je ket-vektor, potom ich vonkajší produkt je lineárny operátor, ktorý označujeme $|\psi\rangle\langle\phi|$.

Projekčný operátor: nech $|\psi\rangle$ je ket-vektor s normou 1, ortogonálna projekcia je $|\psi\rangle\langle\psi|$.

Stredná hodnota pozorovania: nech A je operátor a nech je systém v stave $|\psi\rangle$ potom stredná hodnota pozorovania je $\langle\psi|A|\psi\rangle$.

Princípy kvantovej fyziky

Kvantová teória je matematickým modelom fyzikálneho sveta. Aby sme mohli charakterizovať tento svet, potrebujeme zaviesť základné pojmy t.j.: stavy, pozorovateľné veličny, merania.

Skalárny súčin je definovaný ako funkcia na vektorovom priestore $\mathbb{V}$ nad poľom $\mathbb{F}$,

$$\langle ., . \rangle : \mathbb{V} \times \mathbb{V} \mapsto \mathbb{F},$$

ktorá spĺňa nasledujúce axiómy pre všetky $x, y, z \in \mathbb{V}, a, b \in \mathbb{F}$

1. $\langle x, y \rangle = \langle y, x \rangle^*$ symetria;
2. $\langle x, ay \rangle = a\langle x, y \rangle$,
3. $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$ linearita;
4. $\langle x, x \rangle > 0, \forall x \neq 0, \langle x, x \rangle = 0 \iff x = 0$ pozitivita;

$*$ označuje komplexné združenie.

Skalárnym súčinom vektorov $|\psi\rangle = (a_1, \ldots, a_n)^T, |\phi\rangle = (b_1, \ldots, b_n)^T$
kde $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{C}$ je táto funkcia,

$$\langle \psi | \phi \rangle = \sum_i^n a_i^* b_i$$

Čo?

S čím budeme pri kvantových komunikačných protokoloch narábať? Budú to stavy kvantových systémov alebo presnejšie povedané čisté kvantové stavy. Stav kvantového systému má pre nás veľký význam, pretože je to nosič informácie. Pozrime sa, ako opisuje stavy fyzikálny formalizmus.

Stav

Stav je úplným opisom fyzikálneho systému. Poznáme dva druhy stavov: čistý a zmiešaný. Čistý stav je normovaným vektorom Hilbertovho priestoru.
Pozrime sa najprv na čistý stav. Neskôr keď získame niekoľko základných pojmov, tak si zavedieme aj zmiešaný stav a to pomocou matice hustoty.
Čistý stav je normovaný vektor z Hilbertovho priestoru, čiže normovaný ket-vektor $|\psi\rangle$.
Označuje sa aj qbit (kvantový bit - základná jednotka informácie v kvantovej teórii informácie).
Na vyjadrenie čistých stavov (qbitov) sa používa ortonormálna báza označovaná $\{|0\rangle, |1\rangle\}$.

$$|\psi\rangle = a|0\rangle + b|1\rangle, |a|^2 + |b|^2 = 1, a, b \in \mathbb{C}$$

Hovoríme, že stavy $|\psi\rangle, e^{i\alpha}|\psi\rangle$ opisujú rovnaký stav, ak $|e^{i\alpha}| = 1$. Skalár $e^{i\alpha}$ nazývame aj fázovým faktorom.

Kvantové protokoly, ktorými sa budeme v tejto práci zaoberať používajú iba čisté stavy. Čisté stavy sa dajú reprezentovať aj pomocou matice hustoty, podobne ako zmiešané stavy.

Spin

Pre fyzika predstavuje každý stav aj určitý spin. Napríklad ortonormálna báza $\{|0\rangle, |1\rangle\}$ reprezentuje spin hore $|\uparrow\rangle$ a spin dole $|\downarrow\rangle$ pozdĺž nejakej osi, v našom prípade osi z. Dve reálne čísla charakterizujúce qbit (komplexné čísla a, b modulo normalizácia a fázový faktor) opisujú orientáciu spinu v trojrozmernom priestore (polárny uhol θ a azimutálny uhol ϕ). Neskôr v sekcii Blochova sféra si presne ukážeme, ako sú θ a ϕ definované a ako si môžeme spin predstaviť.

Kde?

Už vyššie pri stavoch bolo spomenuté, že stav je vektor Hilbertovho priestoru. Teória kvantovej informácie sa odohráva v tomto priestore. Pozrime sa na jeho definíciu a niektoré zaujímavé vlastnosti.

Hilbertov priestor

Hilbertov priestor je zovšeobecnením Euklidovského priestoru. Je nazvaný podľa nemeckého matematika Davida Hilberta. Zovšeobecňuje pojem priestoru, ktorý rozširuje metódy vektorovej algebry z dvojrozmerného priestoru a trojrozmerného priestoru na nekonečnorozmerný priestor.

Komplexný Hilbertov priestor je:

a) Vektorový priestor nad komplexnými číslami $\mathbb{C}$. Vektory označujeme $|\psi\rangle$ (Diracova notácia);

b) Jeho vnútorný produkt vektorov $\langle\psi|\phi\rangle$, ktorý mapuje usporiadané dvojice vektorov do $\mathbb{C}$ je definovaný takýmito vlastnosťami:

   (i) Pozitivita: $\langle\psi|\psi\rangle > 0$ ak $|\psi\rangle \neq 0$

   (ii) Linearita: $\langle\psi|(a|\phi_1\rangle + b|\phi_2\rangle) = a\langle\psi|\phi\rangle + b\langle\psi|\phi\rangle$

   (iii) Antisymetria: $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$

c) Je úplný normovaný priestor s normou: $||\psi|| = \langle\psi|\psi\rangle^{\frac{1}{2}}$

Hilbertov priestor môže byť konečno alebo nekonečnorozmerný. Takisto môže byť reálny alebo komplexný.
Keď sa v tejto práci odvolávame na Hilbertov priestor, myslíme tým dvojrozmerný komplexný Hilbertov priestor.

Ako?

Teraz sa bližšie pozrieme na operácie, ktoré môžeme vykonávať na kvantových stavoch. Operátory nám určujú operácie na kvantových stavoch. Už na tomto mieste si treba uvedomiť, že samotná

matematická teória nám umožňuje realizovať akúkoľvek operáciu. Ale fyzikálne realizovateľné operácie sú iba podmnožinou všetkých operácií na systéme. Poďme sa pozrieť, o ktoré ide.

Operátor je také zobrazenie, ktoré nejakej funkcii f priraďuje funkciu g to označíme $A(f) = g$, pričom A je operátor.

Lineárny operátor je operátor, ktorý má takéto vlastnosti:

1. $A(f(x) + g(x)) = A(f(x)) + A(g(x))$,
2. $A(cf(x)) = cA(f(x))$.

Unitárny operátor je operátor spĺňajúci tieto podmienky:

$$U^\dagger U = 1, UU^\dagger = 1.$$

Iba unitárne transformácie sú fyzikálne realizovateľné.

Projekčný operátor je každý operátor, ktorý má túto vlastnosť;

$$P = P^\dagger = P^2.$$

nazývame ho projekčným operátorom.

Hermitovský operátor je lineárny operátor, pre ktorý platí naledovné

$$\langle\psi|A|\phi\rangle = \langle\phi|A|\psi\rangle^*.$$

Pozitívny operátor je špeciálny typ operátora. Nech A je operátor na priestore $\mathbb{C}^n$, potom A je pozitívny operátor vtedy a len vtedy, ak platí;

$$\forall|\psi\rangle \in \mathbb{C}^n, \langle\psi|A|\psi\rangle \geq 0.$$

Z vyššie uvedenej vlastnosti vyplýva tento vzťah

$$B^\dagger = B \wedge B^2 = A.$$

Stopa (trace) štvorcovej matice A rozmerov $n \times n$ je suma jej diagonálnych prvkov, značíme

$$tr(A) = a_{11} + a_{22} + \cdots + a_{nn} = \sum_i a_{ii}.$$

Vo fyzike sa používa definícia cez ortonormálnu bázu priestoru, kde $|e_k\rangle$ sú bázové ortonormálne vektory a A je operátor na priestore $\mathbb{H}$

$$tr(A) = \sum_k \langle e_k|A|e_k\rangle,$$

Niektoré z vlastností trace sú

$$tr(A+B) = tr(A) + tr(B),$$
$$tr(cA) = c.tr(A)$$

pre všetky matice A a B a všetky skaláre c.
Keďže hlavná diagonála štvorcovej matice sa transpozíciou nemení, tak matica a jej transpozícia majú rovnakú stopu

$$tr(A) = tr(A^T).$$

Ak A je matica tvaru $m \times n$ a B je matica tvaru $n \times m$, potom oba produkty AB a BA sú štvorcové a naviac platí

$$tr(AB) = tr(BA).$$

Nech je matica A operátorom a nech U je unitárny operátor, potom platí

$$tr(U^\dagger AU) = tr(A) \iff \sum_k \langle e_k|U^\dagger AU|e_k\rangle = \sum_k \langle f_k|A|f_k\rangle.$$

Dôsledkom tohto tvrdenia je, že je jedno, v akej báze zisťujeme stopu, bude stále rovnaká.

Zmiešaný stav

Zmiešaný stav si môžeme predstaviť ako zmes čistých stavov, používa sa na opis kvantových systémov, ktoré sú buď

- zložené z viacerých systémov alebo
- nevieme s určitosťou povedať akým spôsobom bol náš stav pripravený.

Matica hustoty je hermitovská, pozitívne semidefinitná matica (môže byť nekonečnorozmerná) so stopou jedna, ktorá opisuje štatistický stav kvantového systému. Je označovaná ako ρ.

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|,$$

kde p_i sú nezáporné koeficienty, ktoré sa sumujú na 1 a $|\psi_j\rangle$ je čistý stav. Matica hustoty reprezentuje štatistickú zmes čistých stavov.

Pomocou matice hustoty sa dá vyjadriť aj čistý stav. V takom prípade platí, že matica hustoty opisuje čistý stav vtedy a len vtedy, ak

$$\rho = \rho^2.$$

Ak by sme mali čistý stav $|\psi\rangle$, jeho matica hustoty by vyzerala takto,

$$\rho = |\psi\rangle\langle\psi|.$$

Overme vyššie uvedenú vlastnosť pre túto maticu hustoty čistého stavu

$$\rho = \rho^2 \iff |\psi\rangle\langle\psi| = (|\psi\rangle\langle\psi|)^2 \iff |\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|\psi\rangle\langle\psi|.$$

Keďže čistý stav je normovaný vektor, tak skalárny súčin $\langle\psi|\psi\rangle = 1$, z tejto vlastnosti dostávame rovnosť

$$|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| \iff |\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|.$$

Tenzorový súčin je operáciou na zovšeobecnení vektorov a matíc (tenzoroch).

Všeobecný vzorec na výpočet komponentov súčinu dvoch a viacerých tenzorov. Ak U a V sú dva kovariantné tenzory s m alebo n komponentami, potom komponenty ich tenzorového súčinu sú

$$(U \otimes V)_{i_1 i_2 \ldots i_{m+n}} = U_{i_1 i_2 \ldots i_m} V_{i_{m+1} i_{m+2} i_{m+3} \ldots i_{m+n}}.$$

Jednotlivé komponenty tenzorového súčinu dvoch tenzorov sú obyčajným produktom komponentov tenzorov.

Pripomeňme, že počet potrebných ukazovateľov (rank) sa spočítava,

$$\text{rank}(U \otimes V) = \text{rank}(U) + \text{rank}(V)$$

Príklad

$$U \otimes V = \begin{bmatrix} u_{11}V & u_{12}V & \cdots \\ u_{21}V & u_{22}V & \\ \vdots & & \ddots \end{bmatrix} = \begin{bmatrix} u_{11}v_{11} & u_{11}v_{12} & \cdots & u_{12}v_{11} & u_{12}v_{12} & \cdots \\ u_{11}v_{21} & u_{11}v_{22} & & u_{12}v_{21} & u_{12}v_{22} & \\ \vdots & & \ddots & & & \\ u_{21}v_{11} & u_{21}v_{12} & & & & \\ u_{21}v_{21} & u_{21}v_{22} & & & & \\ \vdots & & & & & \end{bmatrix}$$

Špeciálnym podprípadom tenzorového súčinu je súčin dvoch tenzorov s rankom 2, čiže vektorov. Tento súčin sa označuje aj ako diadický. Nech u a v sú vektory, potom $\mathbb{P}$ je ich diadický súčin, značíme

$$\mathbb{P} = u \otimes v.$$

S ohľadom na zvolenú bázu $\{e_i\}$, môžu byť komponenty P_{ij} diadickéhu produktu $\mathbb{P} = u \otimes v$ definované ako

$$P_{ij} = u_i v_j.$$

Kde

$$u = \sum_i u_i e_i, v = \sum_j v_j e_j$$

$$\mathbb{P} = \sum_{i,j} P_{ij} e_i \otimes e_j$$

Príklad

$$\mathbf{u} \otimes \mathbf{v} \rightarrow \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} = \begin{bmatrix} u_1 v_1 \\ u_1 v_2 \\ u_1 v_3 \\ u_2 v_1 \\ u_2 v_2 \\ u_2 v_3 \\ u_3 v_1 \\ u_3 v_2 \\ u_3 v_3 \end{bmatrix}$$

Pozrime si nejaké zaujímavé vlastnosti tenzorového súčinu. Nech u, v sú tenzory a nech $\{e_j\}, \{f_k\}$ sú ich ortonormálne bázy.

$$\langle u \otimes v | u' \otimes v' \rangle = \langle u | u' \rangle \langle v | v' \rangle$$

Z tejto vlastnosti vyplýva,

$$\langle \psi | \psi' \rangle = \sum \psi^*_{jk} \langle e_j \otimes f_k | e_l \otimes f_m \rangle \psi'_{lm} = \sum \psi^*_{jk} \langle e_j | e_l \rangle \langle f_k | f_m \rangle \psi'_{lm} = \sum \psi^*_{jk} \delta_{jl} \delta_{km} \psi'_{lm} = \sum \psi^*_{jk} \psi'_{jk}$$

Je to vďaka tomu, že $\{e_j\}$ je ortonormálnou bázou, takže $\langle e_j | e_l \rangle = 1$ iba ak $j = l$ inak $\langle e_j | e_l \rangle = 0$, čiže môžeme písať $\langle e_j | e_l \rangle \equiv \delta_{jl}$. Obdobné tvrdenie platí aj pre $\langle e_j | e_l \rangle$.

Je kvantová fyzika nepochopiteľná?

Významný americký fyzik dvadsiateho storočia Richard Feynmann povedal „, kvantová fyzika je nepochopiteľná a kto tvrdí, že jej rozumie, klame.“ Pozrime sa bližšie na niektoré fakty, pri ktorých zostáva „klasický“ rozum stáť.

Dostávame k veľmi dôležitej vlastnosti kvantovej informácie. Tá sa nazýva: **neklonovateľnosť** a hovorí, že kvantový stav sa nedá klonovať. Túto teorému formuloval Wootters, Zurek a Dieks v roku 1982.
Neklonovateľnosť je niečo, čo si v našom každodennom svete dokážeme iba ťažko predstaviť. Napriek tomu to skúsme. Predstavme si, že sme našli fotón a z neznámeho dôvodu nám pripomína veľmi pekný objekt - trebárs vázu. Chceli by sme si urobiť presne takú istú a všetko, čo máme, je táto jedna, ktorá nám bude slúžiť ako vzor. S odhodlaním sa pustíme do práce. Aký bude výsledok? Nielenže nezískame rovnakú novú vázu, ale zničíme aj tú, ktorú sme mali.

Dôkaz: Majme kvantový systém $|\psi\rangle$, ktorý chceme skopírovať. Za účelom kopírovania stavu $|\psi\rangle$, zoberme prázdny stav $|R\rangle$ z rovnakého priestoru. O stave $|\psi\rangle$ nemáme žiadnu vedomosť. Zložením našich dvoch stavov je ich tenzorový produkt:

$$|\psi\rangle \otimes |\psi\rangle = |\psi\rangle|\psi\rangle.$$

Uvažujme unitárnu operáciu (iba unitárne operácie sú fyzikálne realizovateľné) U, ktorá vykonáva klonovanie. Potom musí pre ľubovoľné $|\psi\rangle, |\phi\rangle$ platiť toto,

$$|\psi\rangle|R\rangle \overset{U}{\mapsto} |\psi\rangle|\psi\rangle,$$

$$|\phi\rangle|R\rangle \overset{U}{\mapsto} |\phi\rangle|\phi\rangle.$$

Z definície unitárnej transformácie vieme, že zachováva skalárny súčin. To znamená, že musí platiť táto rovnosť:

$$\langle R|\langle\phi|U^\dagger U|\psi\rangle|R\rangle = \langle\phi|\langle\phi|\psi\rangle|\psi\rangle.$$

Nakoľko $U^\dagger U = 1$, máme

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2.$$

Ale to je možné vtedy a len vtedy, ak $\langle\phi|\psi\rangle = 0 \vee \langle\phi|\psi\rangle = 1$. Čiže buď $|\phi\rangle = |\psi\rangle$, alebo $|\phi\rangle, |\psi\rangle$ sú ortogonálne. To znamená, že operácia klonovania nezachováva skalárny súčin, preto nie je unitárna, a teda nie je fyzikálne realizovateľná.

Kvantový stav $|\psi\rangle$ môže byť naklonovaný $|\psi\rangle|R\rangle \mapsto |\psi\rangle|\psi\rangle$ vtedy a len vtedy, ak poznáme bázu $|\psi\rangle$.

Na rozdiel od klasického sveta, pozorovateľ v kvantovom svete nenávratne ničí celý systém iba jeho pozorovaním. A dokonca získa iba zlomok z celej kvantovej informácie. Kvantová informácia sa nedá klonovať bez toho, aby nebola aspoň jej časť zničená. Výsledky meraní kvantových stavov sú vo všeobecnosti náhodné.

Blochova sféra slúži v kvantovej fyzike na vizualizáciu stavov. Každý čistý stav $|\psi\rangle = a|0\rangle + b|1\rangle$ si môžeme predstaviť ako spin v smere (θ, ϕ). Tieto uhly sú definované ako

- $a = \cos(\frac{\theta}{2})$
- $b = e^{i\phi}\sin(\frac{\theta}{2})$

Z vyššie uvedeného vyplýva, že a musí byť reálne. Toto vieme dosiahnuť tým, že stav $|\psi\rangle$ prenásobíme komplexným skalárom s absolútnou hodnotou 1, tiež nazývaným fázovým faktorom. Fázový faktor nie je pozorovateľný, takže sa aj po prenásobení jedná o ten istý stav. Reprezentujme si tento jav na príklade.
Nech $|\psi'\rangle = a'|0\rangle + b'|0\rangle, a' = r + si, s \neq 0$, potom, aby a' bolo reálne, stačí stav $|\psi'\rangle$ prenásobiť konjugovaným komplexným číslom $a'^* = r - si$.
Dostávame

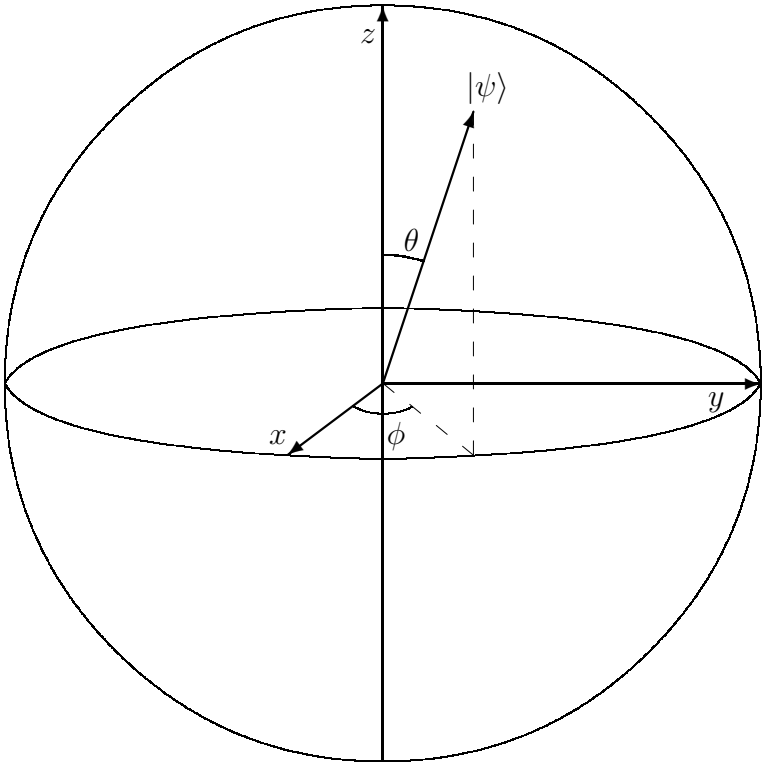
$$a'^*|\psi'\rangle = a'a'^*|0\rangle + b'a'^*|1\rangle = (r+si)(r-si)|0\rangle + b'a'^*|1\rangle = (r^2 - s^2)|0\rangle + b'a'^*|1\rangle.$$

$(r^2 - s^2)$ je reálne číslo, $b'a'^*$ je komplexné číslo. Norma nového vektora nie je rovná 1. Celý vektor musíme prenásobiť reálnou konštantou c, takou aby $||ca'^*|| = 1$. Takže ca'^* je normovaný skalár s absolútnou hodnotou 1 alebo fázovým faktorom. Potom vektor $ca'^*|\psi'\rangle$ je normovaný, pretože sme ho prenásobili skalárom s absolútnou hodnotou 1.

$|\psi\rangle$ môže byť reprezentovaný v trojrozmernom priestore ako normovaný vektor:
$(\cos(\phi)\sin(\theta), \sin(\phi)\sin(\theta), \cos(\theta))$, tento vektor sa tiež nazýva Blochov vektor.

Poznámka: Vďaka triku s fázovým posunom dokážeme reprezentovať dvojrozmerný komplexný stav v trojrozmernom priestore. Stav by inak bolo možné reprezentovať iba v štvorrozmernom priestore.

Pozornému čitateľovi istotne neuniklo paradoxné označenie Blochova „sféra“. Toto označenie je zavádzajúce, pretože nejde o kružnicu (sféru), ale o guľu.



Blochova sféra

Kvantové merania

Aby sme kvantové javy mohli využívať, musíme ich vedieť rozoznať. Na to potrebujeme spôsob, ako ich merať. Princíp neurčitosti nám dáva hranicu, koľko informácie dokážeme získať z kvantového systému. Najskôr sa pozrieme na pokus Stern-Gerlach, potom si predstavíme projekčné meranie a nakoniec zovšeobecnené meranie POVM.

Stern-Gerlach

V roku 1922 realizoval Otto Stern a Wilhelm Gerlach meranie na prúde elektrónov. Po nich je tento pokus pomenovaný.

Stern a Gerlach realizovali svoj pokus s dvoma opačne nabitými magnetmi. Tieto magnety boli tvarované tak, aby medzi nimi vzniklo nerovnomerné magnetické pole. Týmto magnetickým

poľom nechali prúdiť zväzok elektrónov. Klasická teória predpokladala, že takýto prístroj rozdelí zväzok elektrónov rovnomerne. Výsledok merania bol prekvapivý. Elektróny sa sústredili iba na dve časti, bez toho aby sa rozptyľovali. Klasická teória si s týmto výsledkom nedokázala poradiť. Preto s vysvetlením pomohla kvantová teória, ktorá hovorí, že elektróny sa rozdelili podľa spinu na dve časti.

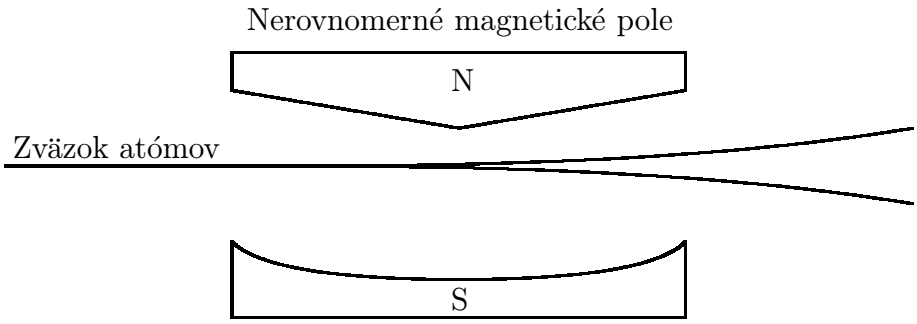


Schéma Stern-Gerlachovho merania

Nastavenie meracieho prístroja sa dá predstaviť ako lineárna kombinácia operátorov

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ak meriame pomocou operátora $\sigma^* = \overrightarrow{a}.\overrightarrow{\sigma}$, (ktorý je nejakou kombináciou vyššie uvedených operátorov), výsledok merania získame pomocou nasledujúcej operácie:

$$\langle\psi|\sigma^*|\psi\rangle = S,$$

pričom S nám označuje strednú hodnotu, z nej sa dá ľahko vypočítať pravdepodobnosť jednotlivých výsledkov. Je to možné vďaka tomu, že pri Stern-Gerlachovom zariadení máme iba dva

možné výsledky merania. Nech sú výsledkami merania $\{1, -1\}$.

$$S = 1p + (-1)(1-p), p = \frac{S+1}{2}$$

Ak by bol stav (vektor) $|\psi_j\rangle$ vlastným vektorom operátora σ^*, tak výsledok merania bude prislúchajúca vlastná hodnota h_j s pravdepodobnosťou 1.

Stern-Gerlach je realizáciou projekčného merania. Pozrime sa bližšie, aké má toto meranie vlastnosti a limity.

Projekčné meranie

Projekčné meranie je množina usporiadaných dvojíc $\hat{O} = \{(h_j, |\psi_j\rangle)\}$. $h_j \in \mathbb{R}$ označuje výsledok merania a $|\psi_j\rangle$ označuje stav, podľa ktorého meriame. $\{|\psi_j\rangle\}$ sú navzájom kolmé.
Pravdepodobnosť výsledku h_j pri meraní stavu $|\phi\rangle$ je

$$P_{|\phi\rangle}(h_j) = \frac{|\langle\psi|\phi\rangle|^2}{\langle\phi|\phi\rangle}.$$

Z predpokladu, že stav je normovaný, dostávame $\langle\phi|\phi\rangle = 1$. A teda pravdepodobnosť merania je,

$$P_{|\phi\rangle}(h_j) = |\langle\phi|\psi_j\rangle|^2.$$

Keďže stavy, podľa ktorých meriame, musia byť navzájom kolmé, tak súčet súm výsledkov meraní a vonkajšieho súčinu kolmých stavov, podľa ktorých meriame, tvorí hermitovský operátor.

$$\hat{O} = \sum_j h_j |\psi_j\rangle\langle\psi_j|.$$

Z jeho konštrukcie vidíme, že $|\psi_j\rangle$ sú vlastné vektory a h_j sú vlastné čísla. Čiže pre meranie platí:

$$\{(h_j, |\psi_j\rangle)\} \equiv \hat{O}.$$

Ak je výsledok merania h_j, potom je kvantový systém po meraní v stave:

$$|\phi\rangle = |\psi_j\rangle,$$

takže akékoľvek ďalšie meranie pomocou $\hat{O}$ prinesie rovnaký výsledok h_j. Táto vlastnosť sa nazýva kolaps vlnovej funkcie. Vlnová funkcia po meraní skolabovala (ak meranie dalo výsledok h_j) na stav $|\psi_j\rangle$.

Spomeňme si na definíciu čistého stavu (vyjadreného v ortonormálnej báze): $|\psi\rangle = a|0\rangle + b|1\rangle$, kde $a, b \in \mathbb{C}$ a $|0\rangle, |1\rangle$ je ortonormálna báza.
Môžeme urobiť meranie, ktoré projektuje stav $|\psi\rangle$ na bázu $|0\rangle, |1\rangle$. Výsledok merania bude nedeterministický, s pravdepodobnosťou $|a|^2$ dostaneme stav $|0\rangle$ a s pravdepodobnosťou $|b|^2$ dostaneme $|1\rangle$.

Ak potrebujeme odlíšiť dva kolmé stavy, projekčné meranie nám ich rozlíši so 100 %-nou pravdepodobnosťou. Čo však v prípade, že máme dva stavy, ktoré zvierajú uhol $0 < \theta < \frac{\pi}{2}$? Bude projekčné meranie optimálne? Pozrime sa na takýto prípad bližšie.

Nech $|\psi\rangle$ a $|\phi\rangle$ zvierajú uhol $\frac{\pi}{4}$, pričom meraný stav môže byť každom stave s pravdepodobnosťou $\frac{1}{2}$. Potom najlepším spôsobom ako tieto dva stavy rozlíšiť bude meranie.

$$\{(1, |\psi^T\rangle), (1, |\phi^T\rangle)\}.$$

Pre stavy $|\psi^T\rangle$ a $|\phi^T\rangle$ platí,

$$\langle\psi|\psi^T\rangle = 0, |\psi\rangle \perp |\psi^T\rangle, \langle\phi|\phi^T\rangle = 0, |\phi\rangle \perp |\phi^T\rangle$$

Pri meraní bude platiť, ak budeme merať pomocou $|\phi^T\rangle$ stav $|\psi\rangle$ a výsledok merania bude 1, budeme vedieť, že sme merali stav $|\psi\rangle$. Ak bude výsledok 0, nebudeme vedieť, aký stav sme merali. Podobne pri výsledku 1 merania $|\psi^T\rangle$ stavu $|\phi\rangle$ vieme, že sme merali stav $|\phi\rangle$. S použitím predpokladu, že stav môže byť v jednom, alebo v druhom stave s pravdepodobnosťou $\frac{1}{2}$ odvodíme, že úspešnosť merania je,

$$P = \frac{1 - |\langle\phi|\psi\rangle|^2}{2} = \frac{1 - (\frac{1}{\sqrt{2}})^2}{2} = \frac{1}{4} = 25\%$$

Zovšeobecnené kvantové meranie, POVM

POVM je skratkou výrazu Positive Operator Valued Measure, definované ako množina Hermitovských, nezáporných, semidefinitných operátorov $\{F_j\}$ na Hilbertovom priestore H, ktoré sa sumujú na identitu.

$$\sum\nolimits_{i=1}^{n} F_i = I_H$$

Táto vlastnosť pripomína dekompozíciu Hilbertovho priestoru na množinu ortogonálnych projektorov s tým rozdielom, že prvky v POVM na seba nemusia byť kolmé.

POVM dosahuje lepšie výsledky pri rozlišovaní stavov, ktoré na seba nie sú kolmé. Pozrime sa, ako to funguje na predchádzajúcom príklade. Stavy $|\psi\rangle$ a $|\phi\rangle$ zvierajú uhol $\frac{\pi}{4}$. Potom POVM, ktoré tieto stavy najlepšie rozlišuje, sa skladá z nasledujúcich operátorov:

$$\widehat{F}_\psi = \frac{1 - |\phi\rangle\langle\phi|}{1 + |\langle\phi|\psi\rangle},$$
$$\widehat{F}_\phi = \frac{1 - |\psi\rangle\langle\psi|}{1 + |\langle\phi|\psi\rangle},$$
$$\widehat{F}_{nerozh.} = 1 - \widehat{F}_\psi - \widehat{F}_\phi.$$

Ak použijeme projektor $\widehat{F}_\psi$ a dostaneme výsledok 1, znamená to, že systém bol s určitosťou v stave $|\psi\rangle$. Ak použijeme projektor $\widehat{F}_\phi$, tak výsledok 1 znamená, že systém bol v stave $|\phi\rangle$. $\widehat{F}_{nerozh.}$ vymedzuje nerozhodnuteľný výsledok. Táto stratégia merania vedie k úspešnej detekcii s pravdepodobnosťou

$$P = 1 - |\langle\psi|\phi\rangle| = 1 - \frac{1}{\sqrt{2}} \approx 29,3\%.$$

Tento výsledok je z pohľadu teoretickej kvantovej fyziky optimálny. Lepšie meranie nedokážeme realizovať. Treba povedať aj to, že POVM vyžaduje náročnejšie meracie prístroje ako jednoduchšie projekčné meranie.

Kryptologické princípy

Komunikácia s útočníkom je taká komunikácia medzi Alicou a Bobom, pri ktorej sa nachádza niekde medzi nimi Eva, ktorá môže zachytávať ich vzájomnú komunikáciu.

Vernamova šifra (one-time pad) je šifra vyvinutá Gilbertom Vernamom v roku 1917. Bola vyvinutá pre potreby armády v laboratóriách AT&T. Kľúč (zhluk náhodných bitov) tejto šifry má dĺžku šifrovaného textu. Šifrovanie (dešifrovanie) je jednoduchý paritný súčet kľúča s otvoreným textom (šifrovaným textom). Sila tejto šifry sa zakladá na entropii náhodného zhluku bitov, táto náhodnosť dokáže odstrániť redundanciu z otvoreného textu. Niekedy sa o tejto šifre hovorí, že je to jediná šifra, o ktorej je dokázané, že je bezpečná.

Jednou zo zásad použitia tejto šifry je, že nesmie byť použitá viackrát. Ak by sme ju použili viackrát, podstúpili by sme veľké riziko, ako ukazuje nižšie uvedená demonštrácia.

Nech O_1 je otvorený text, ktorý zašifrujeme Vernamovým kľúčom K a nech O_2 je druhým otvoreným textom šifrovaným rovnakým kľúčom. Potom dostávame dva šifrové texty $O_1 \oplus K, O_2 \oplus K$. Ak na tieto dva šifrové texty aplikujeme paritný súčet, dostaneme $O_1 \oplus K \oplus O_2 \oplus K$. Keďže paritný súčet je komutatívny, máme $O_1 \oplus K \oplus K \oplus O_2$. Paritný súčet dvoch rovnakých textov je prázdny text, takže výsledkom je paritný súčet dvoch otvorených textov $O_1 \oplus O_2$. Takýto súčet už nie je náhodný, prejavuje sa v ňom štatistický výskyt znakov prirodzeného jazyka a dá sa rozšifrovať.

Ukážka šifrovania pomocou Vernamovej šifry

šifra	1	0	1	0	0	1	0	1	0	1	0	1
otvorený text	1	1	1	1	1	1	0	0	0	0	0	0
šifrovaný text	0	1	0	1	1	0	0	1	0	1	0	1

Autorizovaný kanál je taký, o ktorom vieme prehlásiť, kto je na jeho koncoch. Všetky kvantové protokoly spomínané v tejto práci vyžadujú použitie autorizovaného kanála na zverejnenie báz merania a vysielania.

Kerckhoffsov princíp (tiež označovaný ako Kerckhoffsova domnienka, pravidlo alebo axióma) formuloval holandský lingvista a kryptológ August Kerckhoffs v 19. storočí, kryptosystém musí zostať bezpečný, aj ak je okrem kľúča celý verejne známy.
Neskôr tento princíp preformuloval Claude Shannon na výrok „útočník pozná systém“. Je to základný predpoklad pri analýze bezpečnosti verejných kryptografických systémov.

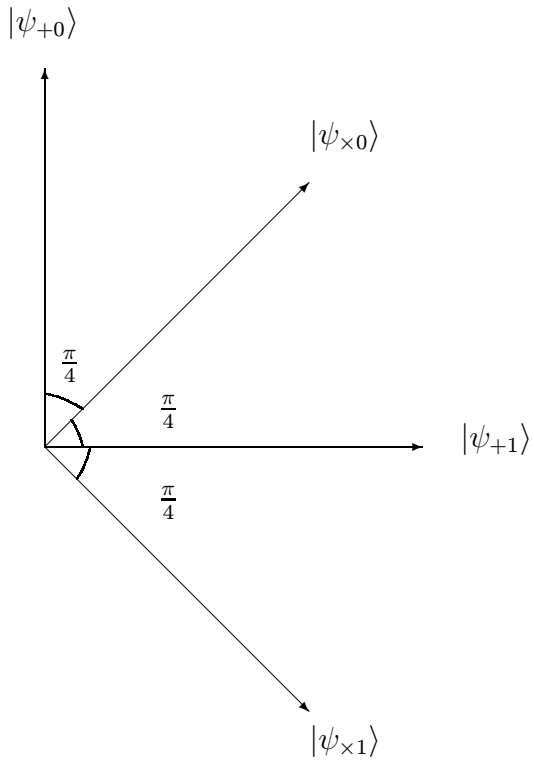
Kvantové komunikačné protokoly

V tejto sekcii opíšeme ako fungujú najbežnejšie kvantové protokoly BB84 a B92. Oba protokoly slúžia na bezpečnú distribúciu kľúča. Následná bezpečná komunikácia prebieha s pomocou tohto kľúča. Kvantový kanál nie je použitý na samotnú komunikáciu.

BB84

Protokol BB84 (ktorý vytvoril Charles Bennett a Gilles Brassard v roku 1984) využíva základné javy kvantovej fyziky. Najdôležitejšie je, aby sme si uvedomili, že kvantové stavy sa nedajú klonovať a teda útočník nemôže použiť klasický spôsob útoku, pretože by tým zničil informáciu.

Klasický návrh protokolu BB84 počíta so štyrmi qbitmi (čistými stavmi), pričom každá dvojica je v inej báze a navzájom sú kolmé.
$|\psi_{+0}\rangle = |0\rangle$ neskôr je v demonštrácii reprezentovaný ako $|\uparrow\rangle$
$|\psi_{+1}\rangle = |1\rangle \equiv |\downarrow\rangle$
$|\psi_{\times 0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |\nearrow\rangle$
$|\psi_{\times 1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |\searrow\rangle$
$+$ a $\times$ označujú vektorové bázy (pozri obrázok nižšie). $+ = \{|\psi_{+0}\rangle, |\psi_{+1}\rangle\}, \times = \{|\psi_{\times 0}\rangle, |\psi_{\times 1}\rangle\}$
Báza $+$ je niekedy označovaná ako rektilineárna a báza $\times$ ako diagonálna alebo duálna.



Stavy, ktoré používa BB84

Pozrime sa na merania, ktoré môžeme robiť, ale ešte predtým si pripomeňme, že $P_{\psi+0}(0)$ je pravdepodobnosť, že výsledok merania na stave $|\psi_{+0}\rangle$ bude 0. Ak budeme merať stav $|\psi_{+0}\rangle$ v prislúchajúcej báze + (tj. pomocou jedného zo stavov $\{|\psi_{+0}\rangle, |\psi_{+1}\rangle\}$), potom pre meranie pomocou $|\psi_{+0}\rangle$ dostávame,

$$P_{\psi+0}(0) = |\langle\psi_{+0}|\psi_{+0}\rangle|^2 = 1$$

A pre meranie pomocou $|\psi_{+1}\rangle$,

$$P_{\psi+0}(0) = |\langle\psi_{+0}|\psi_{+1}\rangle|^2 = 0$$

Analogicky potom dostávame toto,

$$P_{\psi+1}(0) = |\langle\psi_{+1}|\psi_{+0}\rangle|^2 = 0, P_{\psi+1}(0) = |\langle\psi_{+1}|\psi_{+1}\rangle|^2 = 1.$$

Ak by sme merali pomocou dvojice $\{0, |\psi_{+0}\rangle\}$, potom výsledky budú $P_{\psi+0}(0) = 1$ a $P_{\psi+1}(0) = 0$. Podobne pri meraní $\{0, |\psi_{+1}\rangle\}$ budú výsledky $P_{\psi+0}(0) = 0$ a $P_{\psi+1}(0) = 1$. Z toho je zrejmé, že pri meraní stavov $|\psi_{+0}\rangle$ a $|\psi_{+1}\rangle$ v báze + vieme bezpečne rozlíšiť, o aký stav ide.
Podobne dokážeme rozlíšiť stavy $|\psi_{\times 0}\rangle$ a $|\psi_{\times 1}\rangle$ pri meraní v báze $\times$.

Pozrime sa teraz na meranie stavu $|\psi_{+0}\rangle$ v duálnej báze,

$$P_{\psi+1}(0) = |\langle\psi_{+0}|\psi_{\times 0}\rangle|^2 = |\langle 0|\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|^2 = |\frac{1}{\sqrt{2}}(\langle 0|0\rangle + \langle 0|1\rangle)|^2 = \frac{1}{2}$$

Ak meriame v báze $\times$ jeden z dvojice stavov $|\psi_{+0}\rangle, |\psi_{+1}\rangle$, tak s pravdepodobnosťou $\frac{1}{2}$ dostávame výsledok 0 a s rovnakou pravdepodobnosťou aj opačný výsledok 1. To znamená, že výsledok takéhoto merania je náhodný. Rovnaké tvrdenie platí, keď meriame v báze $+$ jeden z dvojice stavov $|\psi_{\times 0}\rangle, |\psi_{\times 1}\rangle$.

Poznámka: práve zo vzťahov medzi stavmi vyplýva bezpečnosť protokolu BB84. Bázy $+$ a $\times$ sú skonštruované tak, aby pri meraní stavu z inej bázy bol výsledok merania náhodný.

Priebeh protokolu

1. Alica sa náhodne rozhodne, v ktorej báze bude vysielať a či bude vysielať 0 alebo 1.
2. Bob sa náhodne rozhodne, v ktorej báze bude merať. Ak si Bob zvolí rovnakú bázu ako Alica, tak vznikne časť kľúča, ktorú budú môcť neskôr použiť na zašifrovanie správy. Ak si Bob zvolí odlišnú bázu, jeho meranie bude dávať náhodný výsledok (pravdepodobnosti sú uvedné v nižšie uvedenej tabuľke).
3. Bob zverejní bázu, v ktorej meral.
4. Alica aj Bob zahodia všetky bity, pri ktorých nemali zhodné bázy (ak by ich nezahodili, výsledky by boli náhodné).
5. Alica aj Bob si navzájom ukážu časť kľúča, aby zistili, či kanál niekto neodpočúva.

Pravdepodobnosti merania v závislosti od vysielaného stavu

Vysielaný stav	$+$		$\times$	
$\|\psi_{+0}\rangle$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$
$\|\psi_{+1}\rangle$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$
$\|\psi_{\times 0}\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0
$\|\psi_{\times 1}\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$

Ukážka distribúcie kľúča pomocou BB84

náhodné bity, ktoré vytvorila Alica	0	1	0	0	1	0	0	1	1	1	0	1
vysielaný stav	$\nearrow$	$\searrow$	$\uparrow$	$\nearrow$	$\downarrow$	$\nearrow$	$\uparrow$	$\searrow$	$\searrow$	$\downarrow$	$\uparrow$	$\searrow$
báza vysielania	$\times$	$\times$	$+$	$\times$	$+$	$\times$	$+$	$\times$	$\times$	$+$	$+$	$\times$
báza merania	$+$	$\times$	$\times$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$+$	$\times$	$+$
meranie u Alice	0	1	1	1	1	0	0	1	1	1	0	0
zhodné bázy		$\surd$			$\surd$	$\surd$			$\surd$	$\surd$		
kľúč		1			0	1			1	1		
zverejnenie časti kľúča						1			1			
výsledný kľúč		1			0					1		

Pri obsluhe kvantového kanála je veľmi dôležité načasovanie. Komunikujúce strany sa musia dohodnúť na presnej časovej schéme, aby sa komunikácia vôbec mohla uskutočniť. Rozmedzie

niekoľkých milisekúnd je vo všeobecnosti postačujúce. Šum na dnešných kvantových kanáloch môže spôsobiť, že protistrana, s ktorou komunikujeme, vôbec nezaregistruje vysielaný stav. Tento problém rieši správne načasovanie. V praxi to znamená, že Bob má k dispozícii pri oznamovaní bázy merania tri možnosti - meranie v bázach $+, \times$ alebo neznámy. Neznámy znamená, že Bob nezistil žiadnu časticu (fotón).

Detekcia útočníka

Ak je na komunikačnom kanáli útočník (Eva), môže sa pokúsiť odchytávať komunikáciu od Alice. Potom si náhodne vyberie bázu a v nej uskutoční meranie. Na základe výsledku merania určí stav, ktorý bude vysielať.

Poznámka: Pri tomto type útoku predpokladáme, že útočník má rovnako nastavené meracie zariadenie a meria v rovnakých dvoch bázach ako Alica a Bob (tento predpoklad vyplýva z Kerkhoffovho princípu). Tento spôsob útoku nie je jediným možným. Pri odpočúvaní sa dá použiť aj koherentný útok. Tento sa snaží unitárnou tranformáciou skopírovať zo stavu čo najviac informácie a potom takto zmenený stav posiela Bobovi.

Na to aby vedela Alica a Bob zistiť, či počas distribúcie kľúča boli odpočúvaní, si potrebujú zverejniť časť nazdieľaného kľúča.

Ukážka detekcie útočníka s použitím BB84

náhodné bity, ktoré vytvorila Alica	0	1	0	0	1	0	0	1	1	1	0	1
vysielaný stav	$\nearrow$	$\searrow$	$\searrow$	$\downarrow$	$\downarrow$	$\nearrow$	$\nearrow$	$\downarrow$	$\searrow$	$\downarrow$	$\nearrow$	$\downarrow$
báza vysielania	$\times$	$\times$	$+$	$\times$	$+$	$\times$	$+$	$\times$	$\times$	$+$	$+$	$\times$
báza merania u Evy	$+$	$\times$	$\times$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$+$	$\times$	$+$
meranie u Evy	0	1	0	0	1	0	0	1	1	1	0	1
stavy vysielané Evou	$\uparrow$	$\searrow$	$\nearrow$	$\uparrow$	$\downarrow$	$\nearrow$	$\nearrow$	$\downarrow$	$\searrow$	$\downarrow$	$\nearrow$	$\downarrow$
bázy merania u Boba	$\times$	$\times$	$+$	$+$	$\times$	$+$	$\times$	$\times$	$+$	$\times$	$+$	$+$
meranie u Boba	0	1	1	0	1	0	0	1	1	1	1	1
zhodné bázy Alice a Boba	$\surd$	$\surd$	$\surd$					$\surd$			$\surd$	
kľúč u Alice	0	1	0					1			0	
kľúč u Boba	0	1	1					1			1	
zverejnenie časti kľúča			?								?	

Problém, ktorému útočník čelí, je takýto. Pravdepodobnosť, že uhádne bázu, v ktorej bol vysielaný stav, je $\frac{1}{2}$. A pravdepodobnosť, že útočníkom vysielaný stav bude zmeraný v rovnakej ako útočníkovej a vysielateľovej báze, je $\frac{1}{8}$. Takže úspešnosť distribúcie kľúča zrazu klesne z 50 % na 25 %. Vďaka tomuto javu sa podarí odhaliť útočníka.

Získanie maximálneho objemu informácií

Najlepšie meranie na extrahovanie maximálnej možnej informácie o každom jednom qbite sa dá dosiahnuť pomocou merania v Breidbartovej báze:

$$\{\cos(\frac{\pi}{8})|0\rangle + \sin(\frac{\pi}{8})|1\rangle, -\sin(\frac{\pi}{8})|0\rangle + \cos(\frac{\pi}{8})|1\rangle\}$$

Úspešnosť merania je uvedená v tabuľke dole. Meranie v Breidbartovej báze pre Evu maximalizuje množstvo získanej informácie. [6]

výsledok merania	0	1
$\|\psi_{+0}\rangle$	$\cos(\frac{\pi}{8})^2$	$\sin(\frac{\pi}{8})^2$
$\|\psi_{+1}\rangle$	$\sin(\frac{\pi}{8})^2$	$\cos(\frac{\pi}{8})^2$
$\|\psi_{\times 0}\rangle$	$\frac{1}{2}(\cos(\frac{\pi}{8}) + \sin(\frac{\pi}{8}))^2$	$\frac{1}{2}(\cos(\frac{\pi}{8}) - \sin(\frac{\pi}{8}))^2$
$\|\psi_{\times 1}\rangle$	$\frac{1}{2}(\cos(\frac{\pi}{8}) - \sin(\frac{\pi}{8}))^2$	$\frac{1}{2}(\cos(\frac{\pi}{8}) + \sin(\frac{\pi}{8}))^2$

V percentuálnom vyjadrení to znamená, že Eva dokáže každý bit prečítať s pravdepodobnosťou 85%. V praxi to znamená, že viac ako polovica kľúča musí byť zverejnená (respektíve kompromitovaná), aby sme dokázali eliminovať riziko odpočúvania. Napriek tomu, že tento poznatok je už dlho známy, niekedy sa pri implementácii nezohľadňuje, čo môže viesť k nízkej bezpečnosti.

Koherentné útoky

Koherentné útoky sú útoky, ktoré majú odlišnú stratégiu ako vyššie spomínané typy útokov. Tieto útoky sa snažia skopírovať vysielaný stav a merať až po zverejnení bázy vysielania. Z prvej kapitoly vieme, že klonovanie stavu nie je možné. Ale ešte stále máme k dispozícii pomerne efektívne prostriedky, ako získať čo najviac informácie. Problémom je, že čím viac informácie zo stavu získame, tým viac ho meníme, a teda zvyšujeme šancu odhalenia útoku.

Existuje celý rad koherentných útokov, my sa pozrime na univerzálne symetrické klonovanie, ktoré je optimálne (v prípade, že o kvantovom stave nemáme nijakú ďalšiu informáciu).

Operáciu optimálneho symetrického klonovania vytvorili Bužek a Hillery [3]. Jedná sa o klonovanie, ktoré vyžaduje jeden qbit a produkuje dve kópie rovanké kópie s najvyššou možnou presnosťou.

Ak by sme ho aplikovali na bázu $\{|0\rangle, |1\rangle\}$, vyzeralo by takto. $|R\rangle$ je prázdny referenčný stav. $|M\rangle$ je pomocný stav alebo klonovací prístroj.

$$|0\rangle|R\rangle|M\rangle \mapsto \sqrt{\frac{2}{3}}|0\rangle|0\rangle|1\rangle - \sqrt{\frac{1}{3}}|\Psi^+\rangle|0\rangle$$

$$(-|1\rangle)|R\rangle|M\rangle \mapsto \sqrt{\frac{2}{3}}|1\rangle|1\rangle|0\rangle - \sqrt{\frac{1}{3}}|\Psi^+\rangle|1\rangle$$

Kde $|\Psi^+\rangle = \frac{1}{\sqrt{2}}[|1\rangle|0\rangle + |0\rangle|1\rangle]$. Keďže toto klonovanie je symetrické, parciálne stavy kópie a originálu sú rovnaké, a to

$$\rho_O = \rho_K = \frac{5}{6}|0\rangle\langle 0| + \frac{1}{6}|1\rangle\langle 1|.$$

Ide o univerzálne klonovanie, a teda použiteľné pre ľubovoľný stav. Každý stav použitý v BB84 môžeme klonovať s úspešnosťou $\frac{5}{6}$, čo je približne 83 %, takže približne rovnaký objem informácie ako meranie v Breidbartovej báze.

Poznámka: Zvolená stratégia klonovania je vhodná, ak nemáme nijakú ďalšiu informáciu o klonovanom stave. V BB84 máme dodatočnú informáciu. Vieme, že všetky používané stavy sú v rovine. Vďaka tomuto faktu existuje aj efektívnejšia stratégia klonovania stavov BB84.

Útočníkova informácia

Pri analýze bezpečnosti sa používa fiktívna tretia strana nazývaná *Big Brother* (veľký brat). Predpokladáme, že Eva namiesto toho, aby uskutočnila niektorý z útokov, pošle qbit tretej strane *Big Brother* uskutoční meranie a pošle nový qbit Bobovi. Bob na novom qbite odmeria chybný výsledok s pravdepodobnosťou $0,1243$. V skutočnosti nijakého *Big Brother* nepoznáme. Táto konštrukcia je iba čisto teoretická a robí horný odhad množstva informácie, ktoré má Eva k dispozícii.

Povedzme, že chceme mať kľúč bezpečný s pravdepodobnosťou 95%(môžeme si zvoliť ľubovoľnú presnosť, dokonca asymptoticky absolútnu). Vypočítajme, akú veľkú časť kľúča by sme mali zverejniť. Predpokladáme, že Eva posielala všetky qbity tretej strane a tá vykonávala merania. Pri prvom zverejnení bitu nazdieľaného kľúča odhalia Alica a Bob útočníka s pravdepodobnosťou $0,1243$.

$$A_1 = 0,1243$$

Pri zverejnení druhého bitu odhalíme útočníka s pravdepodobnosťou A_1 a k tomu pridáme pravdepodobnosť, že pri prvom zverejnení sme útočníka neodhalili a odhalili sme ho až v druhom kroku.

$$A_2 = A_1 + (1 - A_1)A_1 \approx 0,2331$$

Dostávame sa k výrazu, ktorý nám výpočíta pravdepodobnosť odhalenia útočníka,

$$A_{n+1} = A_n + (1 - A_n)A_1$$

Požadujeme, aby pravdepodobnosť, že náš kľúč nebol kompromitovaný bola 95%.

$$A_{22} \approx 0,9461, A_{23} \approx 0,9528$$

To znamená, že Bob a Alica si musia zverejniť aspoň 23 bitov z distribuovaného kľúča. Ak by sa zverejnenie kľúča konalo predvídateľne, potom by útočník mohol predvídať, ktoré časti kľúča sa zverejnia a tie neodpočúvať. Preto musí byť každý bit kľúča zverejnený s rovnakou pravdepodobnosťou.

Poznámka: Kvantový kanál má v reálnom svete pomerne nízku úspešnosť prenosu bezpečných bitov. Kapacita dnešných kvantových kanálov je na úrovni 100 až 1000 bezpečných bitov za sekundu.

Je to iba zlomok (približne jedna stomilióntina) kapacity klasického kanála. Pri použití protokolu BB84 je teoretická hranica využitia na úrovni 25%. Qbity nie je možné nijakým spôsobom ovplyvňovať a teda ani zosilňovať (inak by sme poškodili informáciu), preto je vzdialenosť komunikácie limitovaná kvalitou kanála. Kvantový kanál, ktorý prenáša bity vzduchom má vyššiu prenosovú kapacitu, ale nižší dosah (menej ako jeden kilometer). Naproti tomu kvantový kanál realizovaný optickým vláknom má nižšiu prenosovú kapacitu, ale vyšší dosah (viac ako sto kilometrov).

Modifikácia BB84

Pri modifikáciách môžeme zvažovať viac zmien. Dá sa uvažovať aj zmena vysielaných stavov. Ak by sme k tomu pristúpili, stratila by sa ortonormalita a vysielané stavy by už netvorili bázu Hilbertovho priestoru. Tento prístup nepovažujeme za výhodný, nakoľko by sa znížila úspešnosť merania v príslušnej báze. Nameraná informácia by už nebola perfektne korelovaná na oboch stranách kvantového kanála pri použití rovnakého merania. Preto pristúpme k odlišnej modifikácii.

V navrhovanej modifikácii zmeníme vzťah medzi množinou vektorov $\{|\psi_{+0}\rangle, |\psi_{+1}\rangle\}$ a druhou množinou $\{|\psi_{\times 0}\rangle, |\psi_{\times 1}\rangle\}$. Modifikácia sa týka zmeny uhlov, ktoré tieto dve množiny zvierajú. V pôvodnom návrhu tieto dve bázy zvierajú uhol $\frac{\pi}{4}$. Pozrime sa, ako bude fungovať BB84, keď tento uhol zmeníme.

Aby sme preskúmali fungovanie zmenených báz, stačí meniť jednu bázu. Nechajme prvú bázu $\{|\psi_{+0}\rangle, |\psi_{+1}\rangle\}$ nezmenenú a skúsme zmeniť druhú bázu $\{|\psi_{\times 0}\rangle, |\psi_{\times 1}\rangle\}$. Takýto prístup je postačujúci, pretože správanie protokolu ovplyvňuje najmä uhol, ktorý zvierajú dve bázy.

Vektory musia byť normované, preto sa ako vhodná zmena vektorov ponúka množina tvaru $(\cos(\phi), \sin(\phi))$ pre ľubovoľné ϕ.

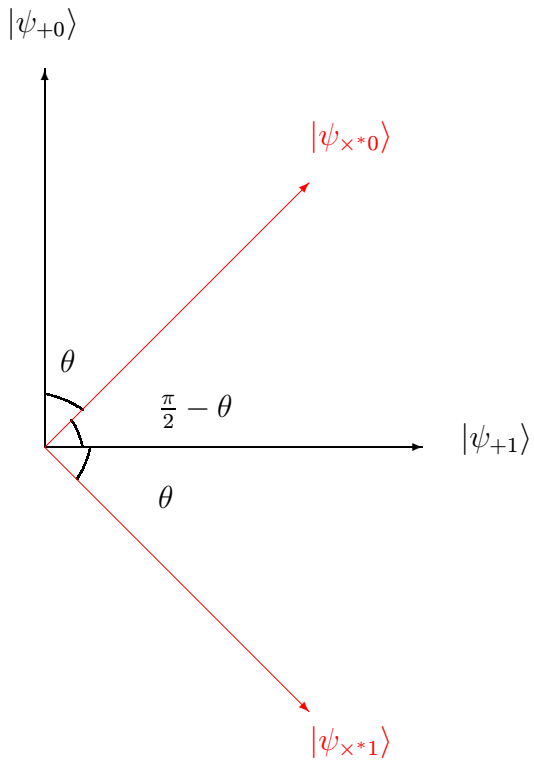
Nech $|\psi_{\times^* 0}\rangle = \cos(\phi)|0\rangle + \sin(\phi)|1\rangle$, potom aby sme získali ortonormálnu bázu, musí platiť toto:

$$\langle\psi_{\times^* 0}|\psi_{\times^* 1}\rangle = 1, \langle\psi_{\times^* 0}|\psi_{\times^* 0}\rangle = \langle\psi_{\times^* 1}|\psi_{\times^* 1}\rangle = 1.$$

Takže nová ortonormálna báza σ^* je

$$\{|\psi_{\times^* 0}\rangle, |\psi_{\times^* 1}\rangle\} = \{\cos(\phi)|0\rangle + \sin(\phi)|1\rangle, -\sin(\phi)|0\rangle + \cos(\phi)|1\rangle\}$$

Pre lepšiu predstavu si ju môžeme pozrieť na nižšie uvedenej schéme. Červenou sú znázornené stavy, ktoré boli zmenené.



Stavy, ktoré používa modifikovaný BB84

Pozrime sa bližšie na jej vlastnosti. Parameter ϕ bude mať zásadný vplyv na modifikovaný protokol. Ak $\phi = \frac{\pi}{4}$, tak máme k dispozícii originálny návrh protokolu, pretože

$$\cos(\frac{\pi}{4}) = \sin(\frac{\pi}{4}) = \frac{1}{\sqrt{2}}.$$

Ak by $\phi = 0$, tak by sme mali k dispozícii dve zhodné bázy. Pretože

$$\cos(0) = 1, \sin(0) = 0, |\psi_{\times^*0}\rangle = |0\rangle = |\psi_{+0}\rangle, |\psi_{\times^*1}\rangle = |1\rangle = |\psi_{+1}\rangle.$$

Takže na odlíšenie akéhokoľvek stavu by stačilo jediné meranie. V dôsledku toho by takto modifikovaný BB84 neposkytoval nijakú bezpečnosť potrebnú na distribúciu kľúča.

Pravdepodobnosti pri zmene jednej bázy

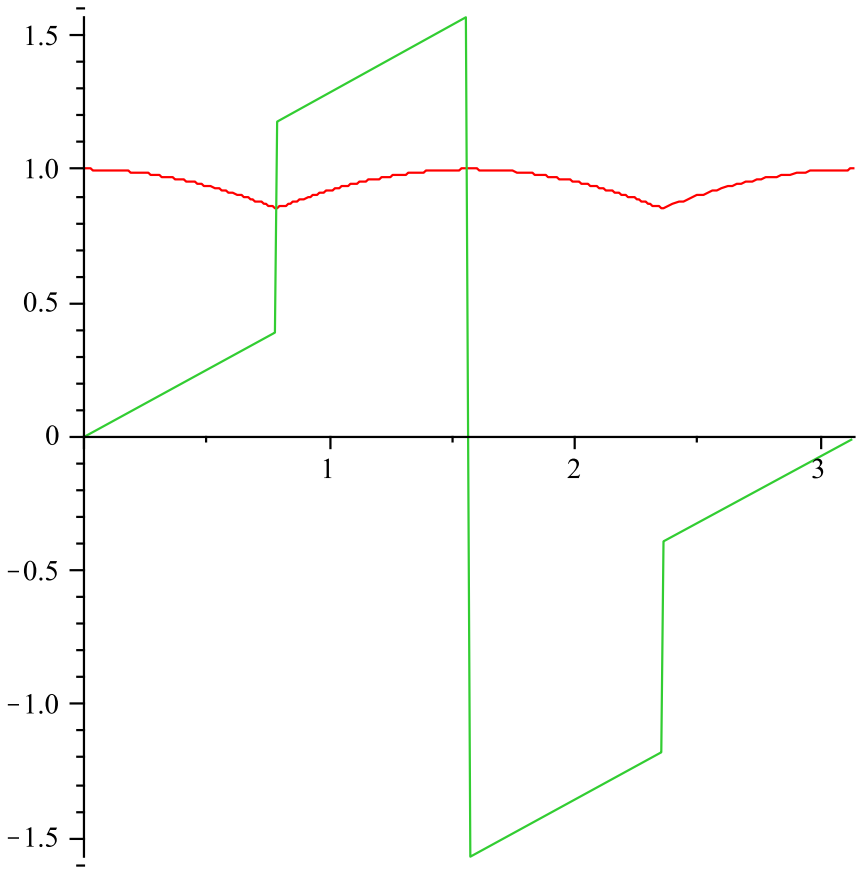
Vysielaný stav	+		× modifikovaná	
$\|\psi_{z0}\rangle$	$\frac{1}{2}$	0	$\frac{(\cos(\phi))^2}{2}$	$\frac{(\sin(\phi))^2}{2}$
$\|\psi_{z1}\rangle$	0	$\frac{1}{2}$	$\frac{(\sin(\phi))^2}{2}$	$\frac{(\cos(\phi))^2}{2}$
$\|\psi_{x0}\rangle$	$\frac{(\cos(\phi))^2}{2}$	$\frac{(\sin(\phi))^2}{2}$	$\frac{1}{2}$	0
$\|\psi_{x1}\rangle$	$\frac{(\sin(\phi))^2}{2}$	$\frac{(\cos(\phi))^2}{2}$	0	$\frac{1}{2}$

Analýza bezpečnosti

V grafe je znázornené, koľko informácie vie útočník získať z merania vysielaných stavov. Na osi x je hodnota ϕ na intervale $(0, \pi)$, ako bolo vyššie spomenuté v prípade, že $\phi = 0$, protokol neposkytuje nijakú bezpečnosť, v prípade $\phi = \frac{\pi}{4}$ ide o originálny protokol.

Červená krivka reprezentuje, koľko informácie môže získať útočník, ak použije optimálne meranie. Hodnoty tejto krivky sa pohybujú v rozmedzí $(0, 85; 1)$. Hodnota $0, 85$ dosahuje na dvoch miestach $\frac{\pi}{4}, 3\frac{\pi}{4}$ reprezentuje objem informácie, ktorá je získaná pri meraní v Breidbartovej báze.

Zelená krivka reprezentuje hodnotu ϕ optimálneho merania. Pohybuje sa v rozmedzí $(-\frac{\pi}{2}, \frac{\pi}{2})$. Funkcie cos, sin sú periodické, vďaka tomu existuje nekonečne veľa optimálnych meraní odlišujúcich sa fázovou konštantou. V grafe sú načrtnuté hodnoty najbližšie k hodnote 0.



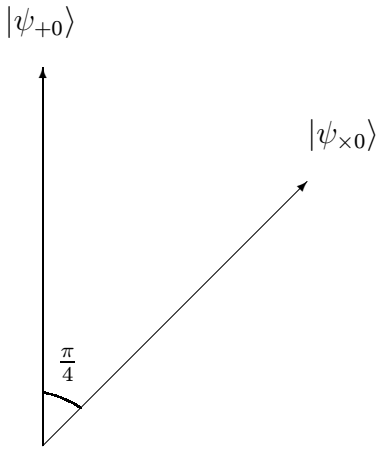
Obr. 1: krivka hore: objem informácie, krivka dole: parameter ϕ bázy merania

Ak chcú Alica a Bob bezpečne komunikovať pomocou modifikovaného BB84, musia zverejniť väčšiu časť kľúča ako pri klasickom návrhu.

B92

Tento protokol používa rovnaký princíp ako BB84. Vytvoril ho Bennett v roku 1992. Protokol je vlastne zjednodušenou verziou BB84. Namiesto štyroch stavov používa na distribúciu kľúča iba dva stavy. Tieto dva stavy nie sú ortogonálne, a preto neexistuje meranie, ktoré by ich s istotou rozlíšilo. Napriek príťažlivosti sa toto jednoduché riešenie v praxi nepoužíva. Dokonca sa v praxi ukazuje ako veľmi nebezpečný protokol. Avšak principiálne riešenie tohto protokolu si zaslúži, aby sme o ňom uvažovali.

Na realizáciu protokolu sa dajú použiť dva stavy z BB84.
$|\psi_{+0}\rangle = |0\rangle$ neskôr je v demonštrácii reprezentovaný ako $|\uparrow\rangle$
$|\psi_{\times 0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |\nearrow\rangle$



Stavy, ktoré používa B92

V B92 reprezentuje $|\uparrow\rangle$ bit 0 a $|\nearrow\rangle$ bit 1.

Protokol prebieha takto:

1. Alica sa náhodne rozhodne pre jeden zo stavov $|\uparrow\rangle$ a $|\nearrow\rangle$, ktorý pošle Bobovi.
2. Bob si zvolí bázu merania buď + alebo $\times$.
3. Bob nameria buď a) 0 s pravdepodobnosťou $\frac{3}{4}$ alebo
   b) 1 s pravdepodobnosťou $\frac{1}{4}$. Ak dáva meranie výsledok 0, tak to znamená, že Bob nedokáže určiť, o aký stav išlo (pozri tabuľku). Ak je výsledok merania 1, tak si Bob na základe bázy merania zapíše v prípade bázy + 1 a v prípade bázy $\times$ 0.
4. Na konci protokolu Bob prezradí, ktoré merania nadobudli hodnotu 1. To umožní Alici vybrať všetky prenosy, ktoré tvoria kľúč.

5. Zverejnenie časti kľúča. Bob aj Alica si prezradia časť distribuovaného kľúča.

Pravdepodobnosti merania v závislosti od vysielaného stavu

Vysielaný stav	Meranie v báze σ_z (+)		Meranie v báze $\sigma_x(\times)$	
$\|\psi_{z0}\rangle$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$
$\|\psi_{x0}\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0

Z tabuľky je vidno, že protokol B92 potrebuje dva krát viac prenesených qbitov na to, aby preniesol rovnaký objem informácie ako BB84.

B92 s použitím POVM

Od vyššie opísaného protokolu sa líši najmä použitím iného druhu merania. Na rozdiel od predchádzajúceho má merania použité v tomto protokole tri možné výsledky. Vďaka tomu prijímateľ meria v jedinej báze.
Alica vysiela dva kvantové stavy $|\theta\rangle, |\bar{\theta}\rangle$ s nasledujúcimi vlastnosťami

1. $|\theta\rangle = -|\bar{\theta}\rangle$,
2. $|\theta\rangle$ a $|\bar{\theta}\rangle$ spolu zvierajú uhol $2\theta, 0 < \alpha < \frac{\pi}{4}$.

Z vlastností stavov $|\theta\rangle$,$|\bar{\theta}\rangle$ vidíme, že sú neortogonálne. Dva neortogonálne stavy nedokážeme rozlíšiť nijakým meraním.

Bennett navrhol meranie s projekčnými operátormi

$$P_\theta = 1 - |\theta\rangle\langle\theta|, P_{|\bar{\theta}\rangle} = 1 - |\bar{\theta}\rangle\langle\bar{\theta}|$$

Pri Bennettovom meraní je pravdepodobnosť detegovania vysielaného stavu

$$\frac{1 - ||\langle\theta|\bar{\theta}\rangle||^2}{2}$$

kde

$$||\langle\theta|\bar{\theta}\rangle|| = \cos(2\theta)$$

Pravdeposť namerať neznámu hodnotu je

$$\frac{1 + ||\langle\theta|\bar{\theta}\rangle||^2}{2}$$

Ekert navrhol efektívnejšie meranie pozostávajúce z POVM operátorov

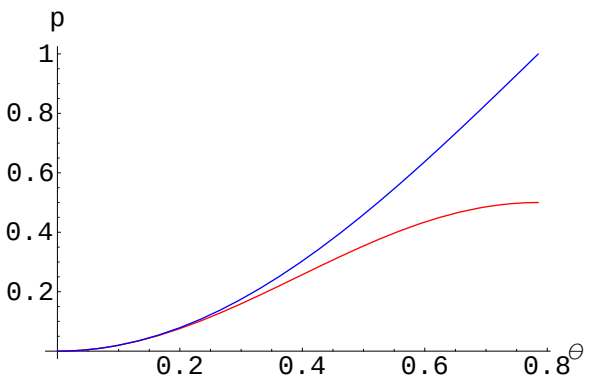
$$A_\theta = \frac{P_\theta}{1 + ||\langle\theta|\bar{\theta}\rangle||} \quad A_{\bar{\theta}} = \frac{P_\theta}{1 + ||\langle\theta|\bar{\theta}\rangle||} \quad A_? = 1 - A_\theta - A_{\bar{\theta}}$$

Pri tomto meraní je pravdepodobnosť namerať neznámu hodnotu

$$||\langle\theta|\bar{\theta}\rangle|| = \cos(2\theta).$$

Voľba stavu θ bližšie k 0 má za následok zvýšenie pravdepodobnosti detekcie neurčitého výsledku. Čím je θ bližšie k $\frac{\pi}{4}$, tým je pravdepodobnosť detekcie stavu vyššia (pozri grafy). Je zrejmé, že meranie navrhnuté Ekertom je efektívnejšie.

Uhol, ktorý v tomto protokole zvierajú stavy, ktoré prenášajú informáciu, je ponechaný v rozmedzí 0 až $\frac{\pi}{2}$. Manipulácia medzi týmito hranicami nám smerom k 0 znemožňuje rozlíšenie stavov, a tým zvyšuje náročnosť komunikácie na kvantovom komunikačnom kanále. Ak by sme uhol posúvali smerom k hodnote $\frac{\pi}{2}$, rozlíšiteľnosť týchto dvoch stavov by stúpala a tým by sa zvyšoval aj objem komunikácie na kvantovom kanáli.



Obr. 2: **Priebeh pravdepodobnosti detekcie stavu pre Bennettove (červená) a Ekertove (modrá) meranie**

Modifikácie B92

Z prevedenia B92 je jasné, že neortogonálne vektory, ktoré sa používajú pri jeho realizácii, sa dajú rôzne meniť.

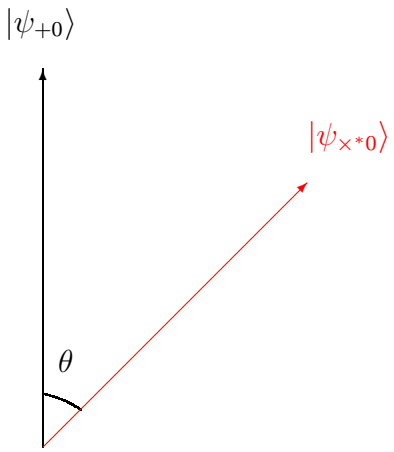
Skúsme vysielané vektory a bázy ich merania zmeniť.

Zmena bázy merania a vysielaných stavov

Nakoľko B92 vychádza z BB84, použime rovnakú modifikáciu, ako sme použili pri BB84. Takže naša nová báza bude

$$\{|\psi_{\times^*0}\rangle, |\psi_{\times^*1}\rangle\} = \{\cos|0\rangle + \sin(\phi)|1\rangle, -\sin(\phi)|0\rangle + \cos(\phi)|1\rangle\}.$$

Pozrime si, ako budú vyzerať zmenené stavy



Stavy, ktoré používa modifikovaný B92

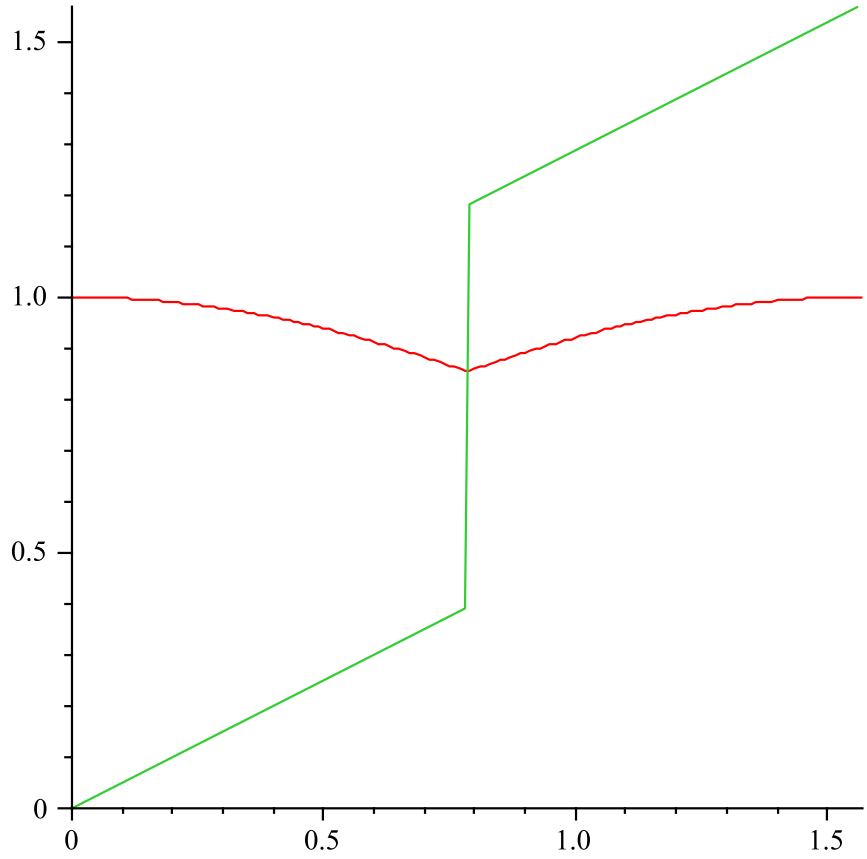
Celá pravdepodobnostná tabuľka bude závisieť od parametra ϕ. Má zmysel pozrieť sa na pravdepodobnosť meraní, keď je ϕ v rozmedzí $(0, \frac{\pi}{2})$. Periodickosť funkcií $\sin, \cos$ zabezpečí, že nemá zmysel uvažovať iné rozmedzie hodnôt ϕ. Opäť ako pri modifikácii BB84 hraničné hodnoty neposkytujú nijakú bezpečnosť. Pri hodnotách $0, \frac{\pi}{2}$ je báza $+$ zhodná s bázou $\times^*$.

Pravdepodobnosti merania v závislosti od vysielaného stavu

Vysielaný stav	Meranie v báze $+$		Meranie v báze $\times^*$	
$\|\psi_{+0}\rangle$	$\frac{1}{2}$	0	$\frac{(\cos(\phi))^2}{2}$	$\frac{(\sin(\phi))^2}{2}$
$\|\psi_{\times^*0}\rangle$	$\frac{(\cos(\phi))^2}{2}$	$\frac{(\sin(\phi))^2}{2}$	$\frac{1}{2}$	0

Analýza bezpečnosti takejto modifikácie je zhodná s analýzou BB84. Ak vezmeme do úvahy, že meraním v Breidbartovej báze by útočník získal 85% vysielanej informácie, tak sa zdá, že nie je vhodné meniť bázu vysielaných stavov. A ak, tak potom iba vo veľmi malej miere. Zmena by mala byť v okolí bodu $\frac{\pi}{4}$. A tejto zmene je treba prispôsobiť aj proces zverejňovania nazdieľaného kľúča.

V nasledujúcom grafe červená krivka označuje informáciu, ktorú útočník dokáže získať. Zelená krivka vizualizuje nastavenie meracieho zariadenia. Ide o analogický graf, aký sme videli pri analýze bezpečnosti modifikovaného BB84.



Obr. 3: **Objem informácie získanej útočníkom pre rôzne ϕ**

Zmena vysielaných stavov bez zmeny báz merania

V tejto sekcii uvažujeme zmenu vysielaných stavov bez zmeny báz merania.

Problém tejto modifikácie je, že zvyšuje pravdepodobnosť zlej detekcie. Realizácia tejto modifikácie by znamenala, že napriek tomu, že by sme namerali hodnotu 1, nemali by sme istotu, že sme merali v správnej báze. Teda už tento teoretický návrh by zaviedol do merania „šum“. Preto zrejme nemá zmysel uvažovať tento návrh a analyzovať jeho vlastnosti.

Pravdepodobnostná tabuľka by vyzerala takto.

Pravdepodobnosti merania v závislosti od vysielaného stavu

Vysielaný stav	Meranie v báze σ_z (+)		Meranie v báze $\sigma_x(\times)$	
$\|\phi\rangle$	$\frac{1-\cos(2\phi)}{4}$	$\frac{1+\cos(2\phi)}{4}$	$\frac{1+\sin(2\phi)}{4}$	$\frac{1-\sin(2\phi)}{4}$
$\|\phi\rangle$	$\frac{1-\cos(2\phi)}{4}$	$\frac{1+\cos(2\phi)}{4}$	$\frac{1+\sin(2\phi)}{4}$	$\frac{1-\sin(2\phi)}{4}$

Túto modifikáciu si môžeme pozrieť ako príklad neúspešnej modifikácie. Ak by sme totiž zmenili iba stavy bez zmeny bázy, tak sme už nedostali výsledok merania 1 iba pri meraní v „správnej“ báze. Čiže napriek správnej detekcii by sme si nemoli byť istí, že kľúč budeme môcť použiť. Samozrejme chyba by sa dala znížiť na veľmi malé pecento, ale teoretický návrh s chybnou detekciou nemôžeme považovať za dobrý. Najmä ak máme k dispozícii protokol, ktorý má teoreticky 100 %-nú úspešnosť pri meraní v príslušnej báze.

Záver

Spotreba qbitov

Parameter, ktorým sa na záver zaoberáme, je spotreba qbitov na distribúciu 1 bitu kľúča. BB84 dosahuje lepší pomer prenesených qbitov k správne detegovaným qbitom (takým, ktoré tvoria kľúč). Teoretický návrh BB84 spotrebuje 2 qbity na prenesenie 1 qbitu utajenej informácie (surového kľúča). Samozrejme na overenie odpočúvania si musia obe strany zverejniť časť kľúča. Preto treba na 1 bit kľúča aspoň 4 qbity. V prípade nemodifikovaného B92 je tento pomer až 8:1. Je to preto, že prijímateľ si volí bázu merania s pravdepodobnosťou $\frac{1}{2}$, ale aj v správnej báze merania nameria požadovaný výsledok iba s pravdepodobnosťou 50 % a potom sa časť klúča musí zverejniť. Predpokladáme, že zverejnená bude až polovica bitov surového kľúča.

V sekcii „Útočníkova informácia“ sme vypočítali, že ak chceme nájsť útočníka s pravdepodobnosťou aspoň 95%, tak minimálny počet zverejnených bitov je 23. Takisto sme zistili, že každý bit kľúča musí byť zverejnený s rovnakou pravdepodobnosťou.

Spotreba qbitov potrebných na prenesenie jedného bitu kľúča

	Vyslané qbity	Správne detegované qbity	Dĺžka kľúča
BB84	4	2	1
B92	8	2	1
B92*	7	2	1

* B92 realizovaný pomocou POVM s Eckertovým meraním

Dosiahnuté výsledky

Nami preskúmané možnosti modifikácií kvantových protokolov nám ukázali, že originálne návrhy sú z teoretického hľadiska optimálne. Prípadne ich už na optimálnu úroveň vylepšili predchádzajúci kritici. Napriek tomu však v praxi môžeme naraziť na problémy pri ich realizácii. Preto je dobré vedieť, akým obmedzeniam čelíme a do akej miery sú reálne používané protokoly bezpečné. Ukazuje sa, že je možné realizovať bezpečný kvantový protokol odlišný od originálneho návrhu, avšak za cenu nárastu objemu komunikácie. Nakoľko aj nepatrné zmeny vo vzťahu dvoch báz v BB84 nám prinášajú zvýšený objem informácie pre útočníka. A tým pádom nutnosť zverejniť väčšiu časť nazdieľaného kľúča, čiže znižovať využitie kvantového komunikačného kanála.

Zhrnutie

Kvantové protokoly majú veľký potenciál rozvoja. V tejto práci sme skúmali protokoly, ktoré využívajú čisté stavy. Ďalšou veľkou triedou kvantových protokolov sú tie, ktoré využívajú entanglované stavy. Aj v tejto oblasti je čo skúmať. Môžeme konštatovať, že kvantový svet môže ponúknuť kryptografii veľmi veľa. Je to vďaka unikátnym vlastnostiam kvantových mikrosvetov.

Literatúra

[1] Lecture Notes for Physics 229: Quantum Information and Computation, John Preskill (1998)

[2] Quantum Cryptography: Uncertainty in the Service of Privacy Science, Charles H. Bennett (1992)

[3] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, Quantum Cloning, Rev. Mod. Phys. 77, 1225-1256 (2005), arXiv:quant-ph/0511088v1

[4] Tassos Nakassis, J.C. Bienfang, P. Johnson, A. Mink, D. Rogers, X. Tang, C.J. Williams, Has Quantum cryptography been proven secure?

[5] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, Hugo Zbinden, Quantum Cryptography, (2001), arXiv:quant-ph/0101098v2

[6] Bennett, C.- H., Bessette, F., Brassard, G., Salvail, L. and Smolin, L., Journal of Cryptology, 5, no. 1, 3-28. (1992)

[7] Quantum Cryptography Security, http://www.cki.au.dk/experiment/qrypto/doc/secAnalysis/, Salvail (2001)

[8] Mathematical Dictionary, mathworld.wolfram.com

[9] Wikipedia The Free Encyclopedia, en.wikipedia.org