Projekt KEGA
Vyučovanie fyziky programovaním modelov fyzikálnych javov
a pomocou interaktívneho softvéru

Kvantová kryptografia

GYMNÁZIUM
arm. gen. L. Svobodu
HUMENNÉ

Martin Furman
Slavomír Tuleja

Humenné 2006

Autori: Martin Furman
Editor: RNDr. Slavomír Tuleja, PhD.

Preprint 2006 (LaTeXverzia)

Moderné informačno-komunikačné technológie a status preprintu tejto publikácie nám dovoľuje obrátiť sa s prosbou na našich kolegov, spolupracovníkov v oblasti didaktiky fyziky a nielen v nej o zaslanie svojich komentárov a názorov, resp. upozornení na zistené chyby a nedostatky.

Na základe tejto širšej spätnej väzby bude možné v časovom horizonte jeden rok a za nižších nákladov pripraviť, resp. rozšíriť tento preprint do akceptovatelnejšej a kvalitnejšej formy a obsahu v porovnaní so štandardným publikovaním. Informácie o presnom dátume prvého vydania žiadajte na emailovej adrese <stuleja@gmail.com>.

Gymnázium arm. gen. L. Svobodu
Humenné

Táto publikácia vznikla s prispením grantovej agentúry MŠ SR KEGA v rámci projektov 3/3005/05 *Vyučovanie fyziky programovaním modelov fyzikálnych javov a pomocou interaktívneho softvéru.*

Obsah

Úvod

Je elektronické bankovníctvo bezpečné? Nemôže niekto pri našich online nákupoch zneužiť citlivé informácie, ktoré zadávame počítaču pri komunikácii s bankou? Odpoveď je naporúdzi: Môže. No iba pod podmienkou, že *prelomí* šifrovanie, ktorým je komunikácia s bankou chránená. Šanca, že sa to niekomu podarí, je *mizivá*. Existuje však jeden spôsob komunikácie, pri ktorom je táto šanca *nulová*. Volá sa kvantová kryptografia.

Prvý bankový transfer v histórii s využitím kvantovej kryptografie uskutočnila skupina vedcov vedená prof. Antonom Zeilingerom z Viedenskej univerzity v spolupráci s ARC Seibersdorf research GmbH dňa 21. apríla 2004 [1]. Bankový transfer prebehol medzi Vienna City Hall – Steinsaal a pobočkou Schottengasse banky Bank Austria Creditanstalt. Bol ním prevedený dar 3 000 € na účet laboratória prof. Zeilingera. Kvantový prenos umožnili páry kvantovo previazaných fotónov.

Keď sme o kvantovej kryptografii počuli prvýkrát, neverili sme, že niečo také môže existovať. Po niekoľkých mesiacoch štúdia tých zdanlivo najnelogickejších vecí, aké sme kedy počuli, sme o existencii niečoho takého stratili pochybnosti. Kvantová kryptografia na nás urobila taký dojem, že sme sa rozhodli, že sa o to, čo sme sa naučili podelíme a napíšeme túto prácu. Rozhodli sme sa, že v nej o kvantovej kryptografii uvedieme to, čo je podľa nás najdôležitejšie a stanovili sme si tieto ciele:

1. Vysvetliť, čo to vlastne kryptografia je a stručne opísať princípy najznámejších kryptografických metód, ktoré sa používali v minulosti i dnes.

2. Jednoduchým, no zároveň kvantovomechanickým spôsobom popísať základné zákony popisujúce správanie sa atómov striebra so spinom 1/2. Urobiť to takým spôsobom, aby v záujme zjednodušenia pochopenia popisu nedošlo ku skresleniu informácií—ukázať to tak, ako to je v skutočnosti.

3. Opísať podmienky EPR experimentu, ktorý kvantovokryptografický protokol priamo využíva, jeho pôvodný účel a jeho dopad na chápanie sveta.

4. Popísať kvantovokryptografický protokol a napísať program v jazyku *Java*, ktorý by uľahčil pochopenie kvantového sveta záujemcom o fyziku, ale aj laikom.

Podľa týchto cieľov bola zvolená aj štruktúra práce. Každému cieľu zodpovedá jedna kapitola.

V prvej kapitole, *Každý má svoje tajomstvá*, sa venujeme stručnému vysvetleniu terminológie používanej v kryptografii a dotýkame sa aj historicky najznámejších spôsobov šifrovania. V tejto kapitole vysvetľujeme aj podstatu Vernamovej šifry, ktorá tvorí jeden z pilierov kvantovej kryptografie.

Druhá kapitola, *Pohľad do mikrosveta*, sa zaoberá základnými vlastnosťami atómov striebra so spinom 1/2. Na základe myšlienkových experimentov so Stern-Gerlachovými prístrojmi sú v nej zavedené pojmy kvantovomechanický stav a kvantovomechanická amplitúda.

Tretia kapitola, *Hrá Boh v kocky?*, rozoberá Einsteinov-Podolskeho-Rosenov myšlienkový experiment a jeho vylepšenú verziu navrhnutú Johnom Bellom. Táto vylepšená verzia je druhým pilierom, na ktorom stojí kvantová kryptografia. Naviac táto kapitola odvodzuje dôležitý výsledok—atómy, ktoré v EPR experimente letia zo zdroja do ľavého a pravého detektora *neobsahujú* až do okamihu detekcie ani náznak informácie o tom, ktorými otvormi prístrojov vyletia. Toto sa ukáže vo štvrtej kapitole ako dôležitý faktor, ktorý znemožňuje odpočúvať kvantový prenos.

Štvrtá kapitola, *Superbezpečná komunikácia*, popisuje detailne kvantovokryptografický protokol. Ukazuje, že šance, že pri distribúcii tajného kľúča môže dôjsť k odpočutiu treťou osobou a my si to nevšimneme, vieme zredukovať prakticky k nule. V tejto kapitole je stručne popísaná *Java* aplikácia, ktorú sme vytvorili ako doplnok tejto práce, a ktorá by mala pomôcť k lepšiemu pochopeniu kvantovej mechaniky a kvantovej kryptografie u prípadných záujemcov.

Skôr než budeme pokračovať chceli by sme sa poďakovať človeku, bez ktorého by sme túto prácu nikdy nenapísali, pretože bez neho by sme nikdy netušili, ako zvláštne sa príroda v skutočnosti správa. Je ním RNDr. Slavomír Tuleja, učiteľ matematiky a fyziky na našej škole, ktorý bol konzultantom tejto práce a obetoval mnohé utorkové popoludnia na to, aby nás na fyzikálnom krúžku zoznámil so základmi kvantovej mechaniky. Okrem toho nám pomohol zorientovať sa v programovacom jazyku Java, ktorý nám počas písania tejto práce priniesol veľmi *zábavné* momenty.

Okrem toho by sme chceli vyjadriť vďačnosť aj ľuďom, ktorí po prečítaní tejto práce vyjadrili svoj názor na ňu, a tak nám pomohli urobiť túto prácu zrozumiteľnejšou. Sú nimi RNDr. Jozef Hanč, PhD. z Ústavu fyzikálnych vied Prírodovedeckej fakulty Univerzity Pavla Jozefa Šafárika v Košiciach a náš spolužiak Peter Ondáč.

Kapitola 1

Každý má svoje tajomstvá

Už v časoch, keď na čele každého národa stál kráľ, začal mať človek potrebu chrániť si svoje tajomstvá. Táto potreba sa stala ešte naliehavejšou po tom, čo medzi národmi začali vznikať rôzne konflikty. Vtedy najväčší myslitelia tých čias prišli s úžasným nápadom—posielať informácie tak, aby ich nepriateľ nemohol prečítať. Objavili kryptografiu.

1.1 Základné kryptografické pojmy

Pri popise tajnej výmeny informácií je zvykom spomínať tri osoby—*Alicu*, *Boba* a *Evu*. Alica bude osoba, ktorá bude šifrovanú informáciu odosielať. Bob bude osoba, ktorá bude tajnú informáciu prijímať. A napokon Eva[1] bude osobou, ktorá sa bude pokúšať (ilegálne) dešifrovať tajnú informáciu, ktorú bude posielať Alica Bobovi, a ktorá bude chcieť zostať neodhalená.

Okrem týchto troch osôb budeme v práci spomínať aj slová ako *informácia*, *kľúč* a *šifra*. Ich použitie nemusí byť celkom jasné (napr. pod pojmom kľúč si môžeme predstaviť množstvo vecí), a tak ich tiež stručne vysvetlíme. Dalo by sa to zobraziť takto:

$$\text{informácia} + \text{kľúč} = \text{šifra}$$

Inak povedané, informácia je to, čo chceme, aby niekto vedel. Kľúč je zase to, čo použijeme na ochranu danej informácie. A šifra je to, čo z toho vznikne.

1.2 História kryptografie

Počas dlhej existencie si kryptografia vytvorila mnoho tvárí—spôsobov akými chránila informácie. Tie môžeme rozdeliť do dvoch veľkých skupín, ktorými sú *transpozícia* a *substitúcia* [2]. V každej skupine je veľké množstvo tých najrôznejších druhov ochrany informácií. Zhrnieme tu iba tie, ktoré boli najdôležitejšie, a ktoré v dejinách kryptografie (i mimo nej) zohrali najväčšiu rolu.

Do skupiny transpozície (čo je vlastne zámena poradia písmen) patrí napríklad šifrovanie, ktoré je založené na veľmi jednoduchom princípe—šifrovanie pomocou

---

[1] Meno vzniklo z anglického slova *eavesdropper* - človek, ktorý odpočúva.

Normálna abeceda	A	B	C	D	E	F	...	Y	Z
Posun o 3 písmená	C	D	E	F	G	H	...	A	B

Tabuľka 1.1: Posunutie abecedy o tri znaky využívané pri Cézarovej zámene.

papierika navinutého na drevený valček. Princíp spočíval v tom, že sa na valček špirálovito navinul dlhý, úzky papierik podobne, ako keby ste obväzovali ranu. Potom sa na papierik napísala po dĺžke valčeka správa a papierik sa odvinul. Takto napísaný odkaz sa dal dešifrovať iba opätovným navinutím papierika na taký istý valček, aký bol použitý pri šifrovaní.

Šifrovanie známe ako Cézarova zámena patrí už do skupiny substitúcie—zámeny písmena za iné písmeno. Táto šifra spočívala v posune abecedy. Ak by niekto chcel zašifrovať napríklad slovo ABECEDA, toto slovo by po zašifrovaní pomocou Tabuľky 1.1 malo tvar CDGEGFC. Túto šifru je veľmi ľahké prelomiť pomocou frekvenčnej analýzy znakov, založenej na tom, že pre daný jazyk sa v bežnom texte vyskytuje každé písmeno s jeho charakteristickou početnosťou, nezávislou na obsahu textu.

Do skupiny substitúcie patrí aj šifrovanie pomocou veľmi známeho zariadenia využívaného počas druhej svetovej vojny nemeckými vojskami. Tým zariadením je *Enigma*. Prístroj bol založený na troch otáčavých kotúčoch, z ktorých každý sa dal nastaviť do 26 rôznych polôh. Každé nastavenie kotúčov určovalo, ktoré písmeno bude priradené ľubovoľnému písmenu abecedy. Po napísaní každého písmena tajnej správy sa prvý kotúč posunul o jednu pozíciu. Ak sa otočil o celú otáčku dookola, posunul o jednu pozíciu druhý kotúč. Ak sa aj ten otočil o celú otáčku, posunul o jednu pozíciu tretí kotúč. Každé nastavenie kotúčov zmenilo tabuľku priradení. To viedlo k zvýšeniu bezpečnosti prenosu informácií a nemožnosti použiť frekvenčnú analýzu na dešifrovanie správy. Napriek tomu našli poľskí matematici spôsob ako túto šifru prelomiť.

Štvrtým a zároveň najnovším druhom je šifrovanie pomocou RSA. Toto šifrovanie spočíva na princípe využívania jednosmerných matematických funkcií, založených na operáciách s obrovskými prvočíslami. V súčasnosti je štandardom pri prenose tajných informácií cez internet, pretože dnešné počítače takto šifrované informácie (bez poznania kľúča) nedokážu v rozumnom čase dešifrovať.[2]

Všetky tieto druhy šifrovania, či to už bola Cézarova šifra, alebo RSA majú spoločnú jednu vlastnosť. Dajú sa (aspoň v princípe) prelomiť. Inými slovami—všetky predchádzajúce druhy šifier sa dali dešifrovať aj bez poznania kľúča—dali sa dešifrovať ilegálne. Je tu však jeden spôsob, ako úplne zaručiť bezpečnosť údajov, súkromných informácií, či iných maličkostí, ktoré by pri styku s okolitým svetom mohli vyvolať búrlivú reakciu. Nazýva sa Vernamova šifra.[3]

---

[2] Keď informáciu konečne dešifrujú, jej obsah bude už dávno nepodstatný.

[3] V angličtine sa často nazýva aj *one-time pad*, teda blok na jedno použitie, čo súvisí s tým, že jeden kľúč možno bezpečne použiť len raz. Pri viacnásobnom použití toho istého kľúča sa dá toto šifrovanie prelomiť.

Alica				
správa	A	H	O	J
kľúč	3	5	2	7
šifra	D	M	Q	Q

Bob				
šifra	D	M	Q	Q
kľúč	3	5	2	7
správa	A	H	O	J

Tabuľka 1.2: Správu AHOJ Alica pomocou kľúča zašifruje na DMQQ. Túto šifru môže bezpečne poslať Bobovi verejným kanálom. Bob správu rozšifruje pomocou toho istého kľúča. Na rozdiel od Alice Bob posúva písmená v abecede doľava.

1.2.1 Vernamova šifra

Princíp tejto šifry (viď Tab. 1.2) spočíva v tom, že Alica každé písmeno správy v abecede náhodne posunie doprava o istý počet znakov. To, o koľko znakov ho posunie, určuje kľúč, ktorý sa skladá z toľkých čísel, koľko znakov má správa. Bob potom pomocou tohto kľúča znaky šifry posunie späť a získa pôvodnú správu. Na posúvanie v abecede môžu používať jednoduchú pomôcku—dva kotúče s abecedou, ktoré možno voči sebe natáčať (viď Obr. 1.1). Túto šifru nie je možné prelomiť, keďže napr. dvadsať-písmenová zašifrovaná správa môže zodpovedať čomukoľvek, čo sa dá zapísať dvadsiatimi písmenami.

(a) posunutie +1 (b) posunutie +2 (c) posunutie +3

Obrázok 1.1: Posunutia abecedy pri rôznych hodnotách kľúča, označených číslom pod každým obrázkom. Ak chceme zistiť, aké písmeno priradiť napríklad písmenu H, natočíme vnútorný kotúč o toľko znakov ako určuje kľúč, nájdeme na ňom písmeno H a prečítame aké písmeno mu zodpovedá na vonkajšom kotúči.

Prečo sa Vernamova šifra potom nepoužíva? Súvisí to s jej nepraktickosťou. Ak ju chceme použiť, musíme zabezpečiť, aby Alica aj Bob mali *ten istý* náhodný kľúč. Ale ako dosiahneme aby ho mali obaja? Musia si ho poslať. Ale to nie je bezpečné, pretože ho niekto môže zachytiť. Preto ho musia poslať zašifrovaný... Je to teda bludný kruh.

Tu prichádza na scénu kvantová mechanika, ktorá ponúka spôsob, ako zabezpečiť, aby Alica aj Bob mali ten istý náhodný kľúč, o ktorom si môžu byť istí, že ho okrem nich nikto nepozná. Spôsob, ktorým sa to dosiahne, sa nazýva kvantovokryptografický protokol.[4]

Skôr než však budeme môcť povedať, ako tento protokol vlastne funguje, je potrebné zoznámiť sa s prostredím, z ktorého vychádza. Je to svet taký malý, že nikto z nás ho doteraz nevidel na vlastné oči a máloktorí z nás si ho v bežnom živote uvedomujú—je to svet atómov. Aj napriek tomu, že tento svet nemôžeme pozorovať priamo, vieme o ňom dosť—dosť na to, aby sme to mohli využiť vo svoj prospech.

---

[4] Vtedy sa používa binárna verzia Vernamovej šifry, s ktorou sa stretneme v 4. kapitole.

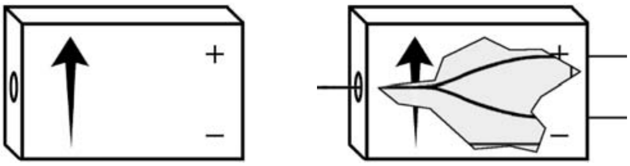
Kapitola 2

Pohľad do mikrosveta

Aby sa tento svet dal ľahšie pochopiť, rozhodli sme sa ho opísať pomocou experimentov a rôznych situácií, ktoré pri nich môžu nastať. Inšpirovali sme sa pri tom *Feynmanovými prednáškami z fyziky* [4].

Všetky nasledujúce (myšlienkové) experimenty sú veľmi podobné reálnym experimentom. Tie však väčšinou obsahujú množstvo komplikácií, ktoré museli ich pôvodní tvorcovia odstrániť. Ako sme však už spomenuli—toto budú myšlienkové experimenty, a tak sa týmito komplikáciami nemusíme zaoberať.

V prvom experimente využijeme prístroj, ktorý sa nazýva podľa svojich objaviteľov—Stern-Gerlachov prístroj (pozri Obr. 2.1). Podstatou tohto prístroja je to, že atómy striebra, ktoré doň vstúpia sa ocitnú v nehomogénnom magnetickom poli (označené šípkou), v dôsledku čoho sa rozdelia na dve skupiny a z prístroja vyletia jedným z dvoch otvorov—buď „+“ alebo „–“.[1]



Obrázok 2.1: Jednoduchý Stern-Gerlachov prístroj a pohľad do jeho vnútra. Čierna šípka na bočnej stene prístroja má smer nehomogénneho magnetického poľa a zároveň ukazuje smer, v ktorom toto pole narastá.

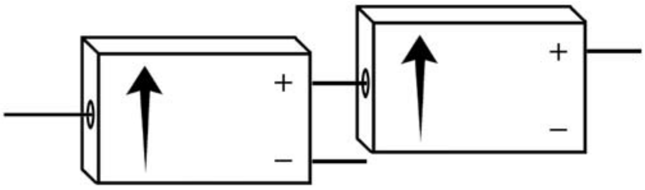
Predstavme si teraz, že cez prístroj necháme prechádzať zväzok atómov. Ak by sme teraz počas experimentu odstránili bočnú stenu prístroja a pozreli sa dovnútra, videli by sme zväzok atómov, ktorý sa počas prechodu prístrojom rozdeľuje na dva zväzky tak, ako to vidíme na Obr. 2.1. Pritom, ak by sme tento experiment nechali *bežať* dostatočne dlho, zistili by sme, že cez každý otvor prechádza asi polovica atómov.

---

[1] Toto správanie sa atómov striebra je spôsobené tým, že každý z nich sa v istom zmysle podobá na maličký magnet. Táto predstava však pri použití *klasických* predpokladov (ako je predpoklad, že magnet má konkrétnu orientáciu, že má konkrétnu polohu a pod.) nevedie pre tento experiment k správnej predpovedi a preto ju nebudeme podrobnejšie rozvíjať [3].

Ak necháme cez prístroj letieť *len jeden* atóm, atóm si náhodne vyberie otvor, ktorým vyletí. Pravdepodobnosť, že vyletí otvorom „+“ je 1/2 a pravdepodobnosť, že vyletí otvorom „−“ je tiež 1/2. Toto správanie sa atómu je ilustráciou pravdepodobnostného charakteru kvantovomechanického popisu. Kvantová mechanika nevie predpovedať, ktorým otvorom atóm vyletí. Vie predpovedať len *pravdepodobnosti* výletu jednotlivými otvormi.

Skúsme si teraz predstaviť situáciu podobnú tej na Obr. 2.2. Atómy, ktoré vstúpia do prvého prístroja vyletia buď cez „+“, alebo cez „−“ otvor. Pri tomto experimente atómy, ktoré vyletia cez „−“ otvor ignorujeme a do druhého prístroja necháme vstúpiť iba atómy, ktoré z prvého prístroja vyleteli cez „+“ otvor. Po prelete cez druhý prístroj pozorujeme, že všetky atómy vyletia cez otvor „+“.



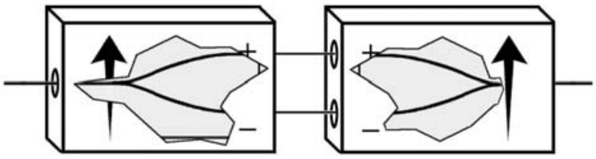
Obrázok 2.2: Dva Stern-Gerlachove prístroje.

Znamená to, že atómy si svoj stav pamätajú, a ak boli zmerané a vyšli cez otvor „+“, tak aj pri nasledujúcom meraní takým istým prístrojom budú znovu zaradené do „+“.

Takýto výsledok experimentu nám teda hovorí, že otvorením iba jedného otvoru sme vytvorili zväzok, ktorého správanie v prístroji rovnakého typu, ako bol pôvodný prístroj, je možné predpovedať. Všetky atómy v takomto zväzku sú v rovnakom stave. Takýto zväzok potom nazývame polarizovaný zväzok.

2.1 Pokusy so Stern-Gerlachovými prístrojmi

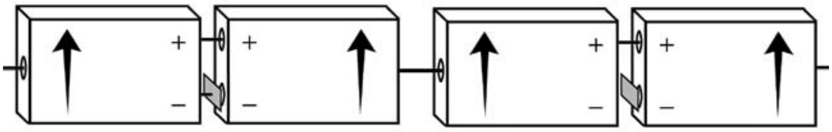
Pre ďalšie pokusy si Stern-Gerlachov prístroj trochu upravíme—bude o niečo zložitejší, no nasledujúce pokusy tým značne zjednodušíme. Náš nový prístroj, ktorý je zobrazený na Obr. 2.3, budú tvoriť dva zrkadlovo otočené Stern-Gerlachove prístroje.



Obrázok 2.3: Zložený Stern-Gerlachov prístroj.

Atómy, ktoré do nášho prístroja vletia budú jeho prvou časťou rozdelené do dvoch skupín, podobne ako v predchádzajúcich experimentoch. Keď však vyletia cez otvory „+“ a „−“, vletia do otvorov „+“ a „−“ druhej časti prístroja. Druhá časť prístroja bude pôsobiť presne opačne ako prvá a rozdelené zväzky atómov znovu spojí do jedného zväzku.

Vkladaním prekážky medzi prvú a druhú časť prístroja (čím zablokujeme jeden z otvorov) budeme môcť vybrať stav, v akom bude atóm po tom, čo opustí náš zložený prístroj. Aj tu platí, že atómy si svoj stav budú pamätať, a ak postavíme dva zložené prístroje za sebou, môže nastať situácia ako je na Obr. 2.4.



Obrázok 2.4: Dva zložené Stern-Gerlachove prístroje za sebou.

V prvom zloženom Stern-Gerlachovom prístroji sme zablokovali kovovou platničkou otvor „−“, a tak všetky atómy, ktoré prejdú cez prvý prístroj sú v stave, ako keby prešli cez jednoduchý prístroj cez otvor „+“. V druhom prístroji bol tiež zablokovaný otvor „−“, no keďže sú atómy po prejdení prvým zloženým prístrojom polarizované, tak druhým zloženým prístrojom prejdú (hornou „+“ vetvou) všetky.

Zobrazenie vylepšeného Stern-Gerlachovho prístroja je dosť zložité. Preto si pre zvýšenie prehľadnosti zavedieme symbol, ktorý bude reprezentovať takýto vylepšený prístroj.

$$\underset{S}{\left\{\begin{matrix}+\\-\end{matrix}\right\}} \tag{2.1}$$

Tento symbol (označujúci prístroj S) však bude vyjadrovať nielen samotný prístroj, ale aj to, či je v tomto prístroji zablokovaná niektorá z vetiev. Ak bude zablokovaná vetva „+“, do symbolu pridáme za znamienko „+“ zvislú čiaru. Podobne to bude pri vetve „−“. V nasledujúcich experimentoch budeme využívať nasledujúce tri symboly:

Zablokované vetvy	žiadna	vetva „+“	vetva „−“
Označenie	$\left\{\begin{matrix}+\\-\end{matrix}\right\}$	$\left\{\begin{matrix}+\mathbf{|}\\-\end{matrix}\right\}$	$\left\{\begin{matrix}+\\-\mathbf{|}\end{matrix}\right\}$

Ak budeme mať, tak ako na Obr. 2.4, dva prístroje, kde v oboch bude priechodná iba „+“ vetva, pomocou symbolov ich zobrazíme takto:

$$\underset{S}{\left\{\begin{matrix}+\\-\mathbf{|}\end{matrix}\right\}} \; \underset{S'}{\left\{\begin{matrix}+\\-\mathbf{|}\end{matrix}\right\}} \tag{2.2}$$

Pri tomto experimente cez druhý prístroj vystúpia všetky atómy, ktoré doň z prvého prístroja vstúpili (budú si *pamätať*, ako boli zmerané v prvom prístroji). Ak však zostavíme prístroje nasledovne

$$\underset{S}{\left\{\begin{matrix} + \\ -\rule{2pt}{1.6ex} \end{matrix}\right\}} \quad \underset{S'}{\left\{\begin{matrix} +\rule{2pt}{1.6ex} \\ - \end{matrix}\right\}} \tag{2.3}$$

z druhého prístroja nevystúpi žiaden atóm—všetky pôjdu v druhom prístroji vrchnou vetvou, kde budú zachytené (napr. kovovou platničkou). Žiadne atómy neprejdú druhým prístrojom ani pri pokuse:

$$\underset{S}{\left\{\begin{matrix} +\rule{2pt}{1.6ex} \\ - \end{matrix}\right\}} \quad \underset{S'}{\left\{\begin{matrix} + \\ -\rule{2pt}{1.6ex} \end{matrix}\right\}} \tag{2.4}$$

No pri pokuse

$$\underset{S}{\left\{\begin{matrix} +\rule{2pt}{1.6ex} \\ - \end{matrix}\right\}} \quad \underset{S'}{\left\{\begin{matrix} +\rule{2pt}{1.6ex} \\ - \end{matrix}\right\}} \tag{2.5}$$

prejdú druhým prístrojom všetky atómy.

2.2 Stavy a amplitúdy

Popíšeme teraz štyri posledné experimenty (experiment 2.2, 2.3, 2.4 a 2.5) kvantovomechanickým spôsobom. No na to, aby sa tieto pokusy kvantovomechanickým spôsobom dali popísať, je potrebné uviesť úplné základy tohto druhu popisu. Pri popise budeme využívať Diracovu notáciu, ktorá je v kvantovej mechanike bežná [4]. V tomto druhu notácie sa stavy atómov označujú nasledovne: ak atóm prešiel cez prístroj

$$\underset{S}{\left\{\begin{matrix} + \\ -\rule{2pt}{1.6ex} \end{matrix}\right\}}$$

(musel prejsť jeho „+“ vetvou, pretože vetva „−“ bola zablokovaná) jeho stav po tom, ako vyletí z prístroja označíme $|{+S}\rangle$. Naopak, ak by v prístroji bola zablokovaná vetva „+“, atóm by prešiel vetvou „−“ a jeho stav by bol $|{-S}\rangle$.

Atóm, ktorý je v istom stave $|a\rangle$ môžeme namerať s istou pravdepodobnosťou v inom stave $|b\rangle$. Mierou tejto pravdepodobnosti je *kvantovomechanická amplitúda*, ktorú označíme ako $\langle b|a\rangle$ (koncový stav vľavo, začiatočný stav vpravo—ako v hebrejčine). Amplitúda $\langle b|a\rangle$ je komplexné číslo, ktorého veľkosť umocnená na druhú $|\langle b|a\rangle|^2$, predstavuje pravdepodobnosť toho, že atóm v stave $|a\rangle$ nájdeme v stave $|b\rangle$.

Teraz už môžeme určiť, aké amplitúdy budú prislúchať k jednotlivým experimentom. Pri experimente 2.2 atóm po prechode prvým prístrojom vyletel otvorom „+“, a teda jeho stav bol $|{+S}\rangle$. Potom vždy prešiel druhým prístrojom a jeho stav sa nijako nezmenil. Pravdepodobnosť, že nájdeme atóm, ktorý bol pôvodne v stave $|{+S}\rangle$ znovu v stave $|{+S}\rangle$, je 1. Môžeme napísať:

$$\langle +S| + S\rangle = 1$$

Pri experimente 2.3 však z druhého prístroja nevyšli žiadne atómy a preto:

$$\langle -S | +S \rangle = 0$$

Podobne pri experimente 2.4 dostávame

$$\langle +S | -S \rangle = 0$$

a pri experimente 2.5 je to zase

$$\langle -S | -S \rangle = 1$$

Tieto výsledky môžeme zapísať do matice a dostaneme:

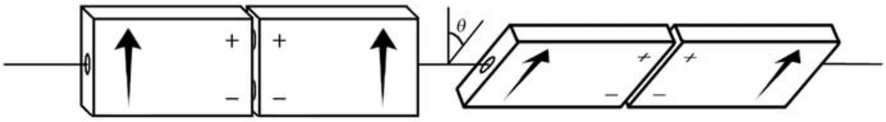
$$\begin{array}{c|cc} & +S & -S \\ \hline +S & 1 & 0 \\ -S & 0 & 1 \end{array} \tag{2.6}$$

V kvantovej mechanike nazveme súbor stavov $|+S\rangle$ a $|-S\rangle$ *bázové stavy.*

2.3 Existujú aj iné stavy?

Môžeme si však položiť otázku: Existujú aj nejaké iné stavy ako $|+S\rangle$ a $|-S\rangle$? Doteraz sme pracovali iba so stavmi $|+S\rangle$ a $|-S\rangle$, pretože všetky atómy prechádzali cez prístroj S. Čo by sa však stalo, ak by sme si do experimentu zaradili nejaký iný prístroj, ktorý by sa od prístroja S v niečom odlišoval.

Skúsme si predstaviť situáciu, že bude druhý prístroj voči prvému pootočený o istý uhol (označme si tento uhol gréckym písmenom θ). Vznikne nám situácia podobná tej na Obr. 2.5. Prvý prístroj je rovnaký ako tie, ktoré sme používali doteraz. Preto si ho aj označíme ako prístroj S. Druhý sa však už v niečom odlišuje (v uhle natočenia). Preto ho označíme inak—napr. T.



Obrázok 2.5: Dva zložené Stern-Gerlachove prístroje; druhý je voči prvému pootočený o uhol θ.

Aj pre druhý prístroj použijeme už opísaný symbol—zmení sa však jeho označenie. Rovnako ako pri predchádzajúcich prístrojoch, aj tu môžeme oddeliť atómy tým, že necháme prechodnú iba jednu vetvu. Môžeme si teda zostaviť nasledujúci experiment:

$$\underset{S}{\left\{\begin{matrix} + \\ -\rule{2pt}{8pt} \end{matrix}\right\}} \quad \underset{T}{\left\{\begin{matrix} + \\ -\rule{2pt}{8pt} \end{matrix}\right\}} \tag{2.7}$$

alebo aj experiment

$$\underset{S}{\begin{Bmatrix} + \\ -\rule{3pt}{10pt} \end{Bmatrix}} \quad \underset{T}{\begin{Bmatrix} +\rule{3pt}{10pt} \\ - \end{Bmatrix}} \tag{2.8}$$

Čo sa stane, ak takéto experimenty *spustíme*? Ak by sme nechali napríklad bežať experiment 2.7, zistili by sme, že aj keď do druhého prístroja vstúpili atómy po tom, ako všetky prešli vetvou „+“ prvého prístroja (teda pred vstupom do druhého prístroja sú v stave $|{+S}\rangle$), nie všetky atómy, ktoré do druhého prístroja vstúpili z neho aj vyleteli. Znamená to, že niektoré z nich museli letieť spodnou vetvou a zastaviť sa na prekážke, ktorá blokovala otvor „−“. Podobne pri experimente 2.8 sa všetky atómy v druhom prístroji nezastavia na prekážke a niektoré z neho vyletia.

To nám dosť jasne dokazuje, že ak sú atómy v určitom stave vzhľadom na S, nie sú v tomto stave vzhľadom na T (napr. ak by v experimente 2.7 boli atómy v stave $|{+T}\rangle$ vyleteli by všetky, no v skutočnosti vyleteli iba niektoré).

Tu sa vynára zaujímavá otázka: Čo stane s atómom v stave $|{+S}\rangle$ ak ho prístroj T nameria v stave $|{-T}\rangle$? Bude si pamätať, že niekedy bol v stave $|{+S}\rangle$? Odpoveď nám poskytne nasledujúci experiment:

$$\underset{S}{\begin{Bmatrix} + \\ -\rule{3pt}{10pt} \end{Bmatrix}} \quad \underset{T}{\begin{Bmatrix} +\rule{3pt}{10pt} \\ - \end{Bmatrix}} \quad \underset{S'}{\begin{Bmatrix} + \\ -\rule{3pt}{10pt} \end{Bmatrix}} \tag{2.9}$$

Tretí prístroj S' je úplne rovnaký ako prístroj S. Chceme vedieť, či si atómy, ktoré prechádzajú tretím prístrojom *spomenú* na to, že už niekedy prešli prístrojom S cez otvor „+“. Ak áno, tak by všetky atómy, ktoré vyletia z prístroja T mali prejsť prístrojom S'.

Výsledok: Neprejdú. Iba určité množstvo z tých atómov, ktoré prejdú prístrojom T prejde aj prístrojom S'. To znamená, že stav $|{+S}\rangle$, ktorý atóm nadobudol pri prejdení cez prístroj S bol nahradený stavom $|{-T}\rangle$ po prejdení prístroja T. Tiež hovoríme, že stav $|{+S}\rangle$ *skolaboval* pri meraní prístrojom T do stavu $|{-T}\rangle$.

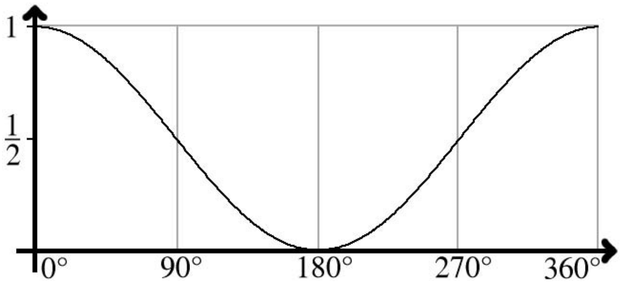
Nakoniec ešte uvedieme tabuľku podobnú tabuľke v rovnici (2.6). Sú v nej uvedené amplitúdy toho, že atóm, ktorý sa nachádza v niektorom zo stavov $|{+S}\rangle$, alebo $|{-S}\rangle$ voči prvému prístroju S, zmeria prístroj T v niektorom zo stavov $|{+T}\rangle$, alebo $|{-T}\rangle$. Pre rozsiahlosť jej odvodenia sme si ju len *požčiali* z literatúry [4]:

	$+S$	$-S$
$+T$	$\cos(\theta/2)$	$\sin(\theta/2)$
$-T$	$-\sin(\theta/2)$	$\cos(\theta/2)$

(2.10)

Na Obr. 2.6 je znázornené ako závisí pravdepodobnosť toho, že atóm v stave $|{+S}\rangle$ nameria natočený prístroj T v stave $|{+T}\rangle$, od uhla natočenia θ. Táto pravdepodobnosť bola vypočítaná pomocou amplitúdy $\langle +T | +S \rangle$.

Matica (2.10) je veľmi prirodzená, o čom svedčí napríklad to, že pre uhol $\theta = 0°$, keď atóm prechádza dvoma *rovnakými* prístrojmi, musí druhým vyletieť tým istým otvorom. Preto sa vtedy pravdepodobnosť výletu otvorom „+“ rovná 1. Navyše pri uhle $\theta = 180°$ je pravdepodobnosť, že atóm vyletí z druhého prístroja cez „+“ otvor



Obrázok 2.6: Graf závislosti pravdepodobnosti $|\langle +T| + S\rangle|^2$ toho, že atóm, ktorý je v stave $|+S\rangle$ voči prístroju S, nameria aj pootočený prístroj T v stave $|+T\rangle$, od uhla θ.

nulová, pretože prístroje sú navzájom opačne natočené—všetky atómy vyletia v druhom prístroji otvorom „–“. No a nakoniec, ak uhol prístrojov je $\theta = 90°$, tak je rozumné očakávať, že atóm si s rovnakou pravdepodobnosťou bude vyberať „+“ aj „–“ otvor. Preto sa pravdepodobnosť výletu otvorom „+“ rovná 1/2.

Kapitola 3

Hrá Boh v kocky?

Albert Einstein je známy svojou nechuťou ku kvantovej mechanike. Táto jeho nechuť je zhmotnená v jeho slávnom výroku [5]: *„Boh nehrá v kocky.“* Einstein ním chcel vyjadriť svoj odmietavý postoj k tvrdeniu kvantovej mechaniky, že fyzikálne vlastnosti fyzikálnych systémov vznikajú až pri ich meraní a nie sú objektívne prítomné už pred meraním, a už vôbec nie nezávisle od merania [6].

Snáď najtvrdší Einsteinov útok na kvantovú mechaniku predstavuje jeho článok z roku 1935, ktorý napísal spolu s Borisom Podolskym a Nathanom Rosenom [7]. Zverejnili v ňom argument, ktorý podľa ich slov dokazoval, že kvantová mechanika zlyháva pri podávaní kompletného popisu reality. O niekoľko rokov neskôr (1964) navrhol John Bell experiment [8], ktorý by umožnil zistiť, či má pravdu Einstein, alebo zástancovia kvantovej mechaniky. Trvalo skoro ďalších 20 rokov, pokým bol takýto experiment zrealizovaný [9].

3.1 EPR experiment

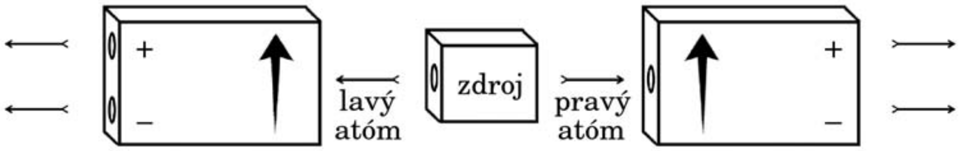
Na zdôvodnenie svojho postoja Einstein, Podolsky a Rosen navrhli slávny Einsteinov-Podolskeho-Rosenov myšlienkový experiment.[1] V experimente sú využité tri prístroje—dva jednoduché Stern-Gerlachove prístroje, ktoré sú zrkadlovo natočené oproti sebe a jeden zdroj, ktorý vystreľuje páry atómov smerom k prístrojom (pozri Obr. 3.1). Zdroj vysiela k detektorom atómy v špeciálnom, *kvantovo previazanom stave*,[2] ktorého matematický popis uvedieme neskôr. Experimentátorku, ktorá obsluhuje ľavý prístroj nazveme Alica a experimentátora pri pravom prístroji nazveme Bob. Zdroj nemusí byť nutne v strede medzi prístrojmi, môže byť bližšie k jednému z nich. Budeme kvôli konkrétnosti predpokladať, že zdroj je o niekoľko centimetrov bližšie k Alici. Atómy letia zo zdroja rovnako rýchlo, a tak ako prvá zaregistruje svoj atóm Alica, a až o istý čas po nej zaregistruje svoj atóm aj Bob.

Kvantová mechanika pre takýto experiment predpovedá, že ak ľavý atóm vyletí z ľavého prístroja cez otvor „+“, tak vieme s istotou povedať, že pravý atóm vyletí z pravého prístroja cez otvor „−“, resp. ak by ľavý atóm vyletel pri Alici cez otvor

---

[1] Používa sa skrátený názov „EPR experiment“.

[2] Vedecký termín pre takýto stav je *entanglovaný stav* z anglického *entangled state*. V tejto práci sme použili slovenský ekvivalent, hoci odborníci sa viac pridŕžajú anglického.



Obrázok 3.1: Schéma usporiadania prístrojov v pôvodnom EPR experimente. Oba prístroje sú orientované v rovnakom zvislom smere. Pri ľavom prístroji je Alica a pri pravom Bob. Medzi prístrojmi je zdroj párov atómov striebra v špeciálnom previazanom stave, z ktorých každý letí do jedného z prístrojov. Predpokladáme, že zdroj nie je presne v strede, ale je o niekoľko cm bližšie k Alici.

„−“, tak pravý by potom zaručene vyletel pri Bobovi cez otvor „+“.

Keďže obidva prístroje sú orientované tým istým smerom, môžno ich oba označiť rovnakým symbolom S. Predpoveď kvantovej mechaniky sa teraz dá formulovať takto: Ak Alica zaregistruje ľavý atóm v stave $|+S\rangle$, tak Bob pravý atóm nameria s istotou v stave $|-S\rangle$. A ak Alica nameria svoj atóm v stave $|-S\rangle$, tak Bob nájde svoj zaručene v stave $|+S\rangle$. Pritom do stavu $|+S\rangle$, alebo $|-S\rangle$ atómy prejdú ihneď po tom, čo prebehne Alicino meranie.

Ako môže byť stav atómu na jednom mieste (pri Bobovi) okamžite ovplyvnený tým, že na inom mieste (pri Alici) bolo uskutočnené meranie na *inom* atóme? Takéto správanie sa atómov porušuje *princíp lokálnosti*, ktorý hovorí, že ak sa pri Alici niečo stane, môže to ovplyvniť udalosti pri Bobovi, ale *nie okamžite*. Informácia o tom, že sa pri Alici niečo stalo, musí *postupne* prejsť od Alice k Bobovi. Informáciu môžu niesť napríklad elektromagnetické vlny, alebo iné *hmotné* nosiče. Navyše Einsteinova špeciálna teória relativity je v tomto neúprosná: Maximálna rýchlosť šírenia sa takejto informácie je c, rýchlosť svetla vo vákuu.

Presne toto trápilo aj Einsteina—dokonca tieto deje aj pomenoval *strašidelné pôsobenie na diaľku.*[3] Einsteinova predstava o fyzike bola založená na predpoklade, že to, čo *reálne existuje* pri Bobovi (teda konkrétna tendencia atómu[4] vyletieť nejakým konkrétnym otvorom—buď „+“ alebo „−“, teda to, čo sme volali doteraz *stav atómu*) by nemalo závisieť na tom, aký je výsledok Alicinho merania niekde inde. Tiež by to malo byť nezávislé na tom, či vôbec nejaké meranie Alica uskutočnila.

Einstein sa pridŕžal tejto svojej predstavy a navrhol jediné vysvetlenie javov predpovedaných v EPR experimente kvantovou mechanikou, ktoré mohlo byť s jeho predstavou konzistentné. Podľa neho *musí* byť u ľavého aj pravého atómu už dávno pred prechodom prístrojmi *reálne prítomná* tendencia vyletieť nejakým konkrétnym otvorom. Dá sa povedať, že musia mať každý „jasno“ v tom, ktorými otvormi vyletia. Už zo zdroja si každý z nich so sebou ponesie skrytú *inštrukciu* kadiaľ má vyletieť. To, aby vylietali rôzne označenými otvormi možno zariadiť tak, že ich inštrukcie budú opačné (viď Tab. 3.1). Problém s komunikáciou ľavého a

---

[3] Spooky actions at a distance.

[4] Vo fyzike sa tejto tendencii atómu hovorí priemet magnetického momentu atómu do zvislej osi. Pre atómy striebra nadobúda len dve hodnoty, $\pm m_{\mathrm{B}}$, podľa toho, či je atóm v stave $|+S\rangle$, alebo $|-S\rangle$. Pritom $m_{\mathrm{B}} = 9,27 \cdot 10^{-24}\mathrm{J.T}^{-1}$ je Bohrov magnetón.

pravého atómu nadsvetelnou rýchlosťou sa tým pádom vyrieši, lebo každý z nich je potom „samostatný“ a nemusí sa „pozerať“ čo robí ten druhý. Takže komunikovať nepotrebujú. Navyše pri takejto predstave výsledok Alicinho merania neovplyvňuje výsledok Bobovho merania, lebo už od samého začiatku je tento výsledok predurčený. Einsteinovo vysvetlenie využívajúce skryté inštrukcie teda uspokojivo vysvetľovalo predpoveď kvantovej mechaniky pre EPR experiment.

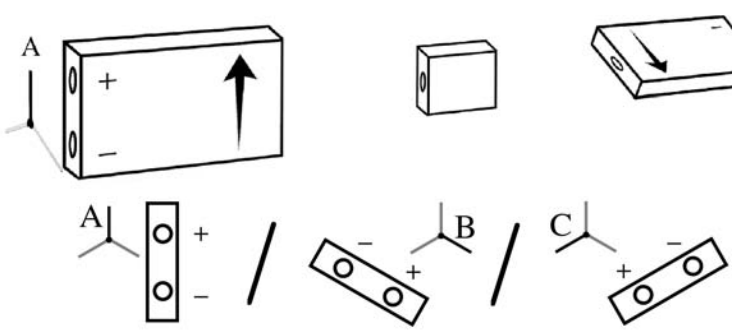
$(+) \leftrightarrow (-)$
$(-) \leftrightarrow (+)$

Tabuľka 3.1: Možné dvojice inštrukcií pre ľavý a pravý atóm pri EPR experimente. Napríklad dvojica „$(+) \leftrightarrow (-)$“ znamená, že ľavý atóm vyletí otvorom „+“ a pravý otvorom „−“.

V apríli 1948 Einstein optimisticky napísal Maxovi Bornovi [6], že aj keď uvažuje všetky jemu dovtedy známe fyzikálne javy popisované tak úspešne kvantovou mechanikou, stále *nemôže nikde nájsť žiaden fakt*, vďaka ktorému by mohlo začať byť pravdepodobné, že požiadavku nezávislej existencie fyzikálnej reality treba opustiť. O 16 rokov neskôr takýto fakt našiel John Bell.

3.2 Fakt sa našiel – Bellov teorém

Bell navrhol pôvodný EPR myšlienkový experiment trochu pozmeniť. Namiesto pôvodných pevných Stern-Gerlachových prístrojov navrhol využiť prístroje, ktoré sa môžu otáčať okolo svojej pozdĺžnej osi do troch smerov: Do smeru A, ktorý je zhodný so zvislým smerom, do smeru B, ktorý so zvislým smerom zviera uhol $\theta = 120°$ a do smeru C, ktorý so zvislým smerom zviera uhol $\theta = 240°$ (pozri Obr. 3.2).



Obrázok 3.2: Vylepšený EPR experiment, ktorý navrhol Bell. Ľavý aj pravý detektor sú otočné okolo pozdĺžnej osi. Možno ich každý nezávisle natočiť do jedného zo smerov A, B a C.

Keď prístroj zmení smer, stáva sa z neho *iný* Stern-Gerlachov prístroj. Kvôli jednoduchosti budeme v ďalšom prístroje Alice a Boba označovať podľa ich smerov ako A, B alebo C. Potom keď atóm vyletí z „+“ otvoru prístroja B, bude v stave $|{+}B\rangle$, keď z „−“ otvoru prístroja A, bude v stave $|{-}A\rangle$ a pod.

Zdroj vystrelí pár atómov v previazanom stave k Alicinmu a Bobovmu prístroju. Ešte predtým ako atómy doletia k prístrojom, Alica aj Bob *náhodne* natočia svoje prístroje do niektorého z troch smerov A, B a C. Potom pozorujú, ktorými otvormi atómy z ich prístrojov vyletia.

Kvantová fyzika pre tento experiment predpovedá, že ak budú Alicin aj Bobov prístroj nastavené do *rovnakých smerov* (AA, BB, CC), tak ľavý aj pravý atóm budú vylietať vždy z *rôzne* označených otvorov (ľavý „+“ a pravý „−“ alebo ľavý „−“ a pravý „+“), čo je v zhode s pôvodným EPR experimentom. Ak však budú Alicin a Bobov prístroj nastavené do *rôznych* smerov (AB, AC, BA, BC, CA, CB), tak sa môže stať, že *niekedy* ľavý atóm pri Alici a pravý atóm pri Bobovi vyletia z *rovnako* označeného otvoru (ľavý „+“ a pravý „+“ alebo ľavý „−“ a pravý „−“).

Ak sú prístroje nastavené do rovnakých smerov, je aj v tomto experimente výsledok merania na pravom prístroji okamžite ovplyvnený výsledkom merania na ľavom prístroji. Preto ak aj tento experiment chceme vysvetliť v zhode s Einsteinovou predstavou o fyzike, musia aj v tomto experimente atómy opúšťať zdroj s inštrukciami, z ktorého otvoru majú vyletieť. Tentoraz však pri vzniku páru atómov nie je jasné, v ktorom smere bude natočený Alicin a Bobov prístroj v okamihu preletu. Preto musí každý z atómov niesť so sebou pre istotu *tri inštrukcie*, ktoré mu povedia, ktorým otvorom má vyletieť, ak nájde svoj prístroj natočený do smeru A, B, alebo C. Hovoríme, že atómy so sebou nesú *inštrukčné sady*. Napríklad ľavý atóm s inštrukčnou sadou $(+-+)$ pri natočení Alicinho prístroja do smeru A vyletí cez otvor „+“, pri natočení do smeru B vyletí cez otvor „−“, a pri natočení do smeru C vyletí znovu cez otvor „+“. Ak sú prístroje natočené rovnako, atómy musia vyletieť opačnými otvormi. Preto musia byť inštrukčné sady atómu letiaceho k ľavému prístroju a atómu letiaceho k pravému prístroju navzájom opačné. Prehľad všetkých možných dvojíc inštrukčných sád je znázornený v Tab. 3.2.

$(+++) \leftrightarrow (---)$	$(-++) \leftrightarrow (+--)$
$(++-) \leftrightarrow (--+)$	$(--+) \leftrightarrow (++-)$
$(+-+) \leftrightarrow (-+-)$	$(-+-) \leftrightarrow (+-+)$
$(+--) \leftrightarrow (-++)$	$(---) \leftrightarrow (+++)$

Tabuľka 3.2: Zoznam možných dvojíc inštrukčných sád pre ľavý a pravý atóm.

Bell si dal otázku, **ako často budú** v tomto experimente za horeuvedených predpokladov **vyletovať Alicin a Bobov atóm z *rôzne* označených otvorov?** Ako sa neskôr ukáže, práve toto bola cesta ako nájsť rozpor medzi Einsteinovým klasickým popisom a kvantovou mechanikou.

3.2.1 Predpoveď pravdepodobnosti s využitím inštrukčných sád

Na to, aby sme mohli určiť, aká je pravdepodobnosť toho, že atómy opustia prístroje rôzne označenými výstupmi, si vypíšme všetky možné kombinácie výsledkov, ktoré môžeme dostať (viď Tab. 3.3).

	AA	AB	AC	BA	BB	BC	CA	CB	CC	P
$(+++) \leftrightarrow (---)$	$+-$	$+-$	$+-$	$+-$	$+-$	$+-$	$+-$	$+-$	$+-$	1
$(++-) \leftrightarrow (--+)$	$+-$	$+-$	$++$	$+-$	$+-$	$++$	$--$	$--$	$-+$	5/9
$(+-+) \leftrightarrow (-+-)$	$+-$	$++$	$+-$	$--$	$-+$	$--$	$+-$	$++$	$+-$	5/9
$(+--) \leftrightarrow (-++)$	$+-$	$++$	$++$	$--$	$-+$	$-+$	$--$	$-+$	$-+$	5/9
$(-++) \leftrightarrow (+--)$	$-+$	$--$	$--$	$++$	$+-$	$+-$	$++$	$+-$	$+-$	5/9
$(-+-) \leftrightarrow (+-+)$	$-+$	$--$	$-+$	$++$	$+-$	$++$	$-+$	$--$	$-+$	5/9
$(--+) \leftrightarrow (++-)$	$-+$	$-+$	$--$	$-+$	$-+$	$--$	$++$	$++$	$+-$	5/9
$(---) \leftrightarrow (+++)$	$-+$	$-+$	$-+$	$-+$	$-+$	$-+$	$-+$	$-+$	$-+$	1

Tabuľka 3.3: Prehľad výsledkov experimentov pre rôzne orientácie ľavého a pravého prístroja pri použití všetkých možných inštrukčných sád. V poslednom stĺpci sú pravdepodobnosti toho, že pri danej inštrukčnej sade vyletia atómy rôznymi otvormi.

Z Tab. 3.3 môžeme zistiť aká je pravdepodobnosť vyletenia atómov rôzne označenými otvormi pre každú možnú inštrukčnú sadu. Pre danú inštrukčnú sadu ju určíme ako podiel počtu orientácií prístrojov ktoré vedú k tomu, že atómy vyletia cez rôzne otvory a počtu všetkých rôznych orientácií prístrojov (tých je 9). Vidíme, že pre všetky sady okrem prvej a poslednej je to $\frac{5}{9}$. Pri prvej a poslednej sade je to 1. To, aká bude pravdepodobnosť toho, že ľavý aj pravý atóm vyletia rôzne označenými otvormi, závisí od zdroja atómov, presnejšie od toho, akými inštrukčnými sadami a ako často sú vystreľované páry atómov vybavované. Isté ale je, že sa bude pohybovať niekde medzi $\frac{5}{9}$ a 1.

3.2.2 Predpoveď pravdepodobnosti s využitím kvantovej mechaniky

Na to, aby sme Bellov experiment vedeli popísať kvantovomechanickým spôsobom potrebujeme vedieť popísať *stav páru atómov*. Predpokladajme na chvíľu, že Alicin aj Bobov prístroj sú oba nastavené do smeru A. Ak by opúšťal pár atómov zdroj v stave $|+A,-A\rangle$, tak by bolo *isté*, že ľavý atóm vyletí cez otvor „+“ a pravý cez otvor „−“. Podobne, ak by opúšťal pár atómov zdroj v stave $|-A,+A\rangle$, tak by bolo *isté*, že Alicin atóm vyletí cez otvor „−“ a Bobov cez otvor „+“. Takéto vyjadrenia stavu páru atómov teda nepredstavujú nami spomínaný *previazaný* stav.

V odbornej literatúre [6] sa pre previazaný stav páru atómov uvádza nasledujúci vzťah:[5]

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|+A,-A\rangle - \frac{1}{\sqrt{2}}|-A,+A\rangle \tag{3.1}$$

---

[5] Vo všeobecnosti môže mať pár atómov stav:

$$|\Psi\rangle = a\,|+A,+A\rangle + b\,|+A,-A\rangle + c\,|-A,+A\rangle + d\,|-A,-A\rangle\,,$$

kde a, b, c a d sú amplitúdy pravdepodobnosti, že atómy nájdeme v stavoch $|+A,+A\rangle$, $|+A,-A\rangle$, $|-A,+A\rangle$ a $|-A,-A\rangle$. Pritom musí platiť, že $|a|^2+|b|^2+|c|^2+|d|^2=1$.

Ak pár atómov opúšťa zdroj v takomto stave, tak ho Alicin aj Bobov prístroj (oba natočené do smeru A) namerajú s pravdepodobnosťou 1/2 v stave $|+A,-A\rangle$ a s rovnakou pravdepodobnosťou v stave $|-A,+A\rangle$. Ďalej vidíme, že vždy, keď pri Alici vyletí atóm cez otvor „+“, musí previazaný stav $|\Psi\rangle$ skolabovať do stavu $|+A,-A\rangle$. V opačnom prípade musí skolabovať do stavu $|-A,+A\rangle$.

Teraz už nechýbajú žiadne informácie na to, aby sme si zostavili tabuľku pravdepodobností pre Bellov experiment (viď Tab. 3.4). Pre každé nastavenie prístrojov (spolu deväť) môžu nastať štyri situácie: aj ľavý, aj pravý atóm môže vyletieť cez „+“, ľavý môže vyletieť cez „+“ a pravý cez „−“, ľavý cez „−“ a pravý cez „+“, alebo oba cez „−“. V tabuľke budeme mať teda 36 pravdepodobností. Pravdepodobnosť skončenia atómov v určitom stave si vypočítame tak, že najprv vypočítame amplitúdu toho, že previazaný stav $|\Psi\rangle$ nájdeme v danom stave, a potom určíme druhú mocninu jej veľkosti.

Napríklad pre koncový stav $|+B,-C\rangle$ zodpovedajúci tomu, že ľavý atóm vyletí z prístroja orientovaného do smeru B cez „+“ otvor a pravý atóm vyletí z prístroja natočeného do smeru C cez „−“ otvor ju vypočítame takto:

$$\langle +B,-C|\Psi\rangle = \langle +B,-C| \left[\frac{1}{\sqrt{2}} |+A,-A\rangle - \frac{1}{\sqrt{2}} |-A,+A\rangle \right] =$$

$$= \frac{1}{\sqrt{2}} \langle +B,-C| +A,-A\rangle - \frac{1}{\sqrt{2}} \langle +B,-C| -A,+A\rangle =$$

$$= \frac{1}{\sqrt{2}} \langle +B| +A\rangle \langle -C| -A\rangle - \frac{1}{\sqrt{2}} \langle +B| -A\rangle \langle -C| +A\rangle$$

Podľa vzťahov (2.10) môžeme nahradiť amplitúdy nasledujúcimi hodnotami:

$$\frac{1}{\sqrt{2}} \cos(120^\circ/2) \cos(240^\circ/2) - \frac{1}{\sqrt{2}} \sin(120^\circ/2) \left[-\sin(240^\circ/2)\right]$$

Za uhol θ, ktorý vo vzťahoch (2.10) vystupuje, dosádzame uhol, ktorý zvierajú medzi sebou prístroje A a B alebo A a C (v našom prípade teda 120° alebo 240°). Po úprave získame výsledok

$$\langle +B,-C|\Psi\rangle = \frac{1}{2}\frac{1}{\sqrt{2}}$$

Pravdepodobnosť javu, že pri orientácii prístrojov do smerov B a C vyletia atómy cez otvory „+“ a „−“ bude

$$|\langle +B,-C|\Psi\rangle|^2 = \frac{1}{8}.$$

Takýmto spôsobom sa dá doplniť celá tabuľka 3.4.

Teraz pomocou tejto tabuľky zistíme odpoveď na otázku, ktorú si položil Bell: Aká je pravdepodobnosť, že ľavý a pravý atóm vyletia z rôzne označených otvorov?

Predstavme si, že Alica a Bob zopakujú svoj pokus 9 000 000 krát. Každá z možných deviatich orientácií prístrojov bude použitá v priemere rovnako často, teda 1 000 000 krát. Z Tab. 3.4 vidíme, že ak sú orientácie prístrojov Alice a Boba

	AA	AB	AC	BA	BB	BC	CA	CB	CC
$++$	0	3/8	3/8	3/8	0	3/8	3/8	3/8	0
$+-$	1/2	1/8	1/8	1/8	1/2	1/8	1/8	1/8	1/2
$-+$	1/2	1/8	1/8	1/8	1/2	1/8	1/8	1/8	1/2
$--$	0	3/8	3/8	3/8	0	3/8	3/8	3/8	0

Tabuľka 3.4: Tabuľka pravdepodobností výletov rôznymi dvojicami otvorov pre rôzne natočenia prístrojov, predpovedaná kvantovou mechanikou.

rovnaké, vyletia atómy rôzne označenými otvormi *vždy*. Ak sú orientácie prístrojov rôzne, vyletia atómy rôzne označenými otvormi v $1/8 + 1/8 = 1/4$ prípadov.

Spočítame teraz, koľko z 9 000 000 opakovaní experimentu povedie k výletu atómov opačne označenými otvormi: Orientácie prístrojov budú rovnaké pri 3 000 000 opakovaní, z ktorých výlet opačne označenými otvormi nastane pri všetkých. Zarátame preto 3 000 000. Orientácie prístrojov budú rôzne pri 6 000 000 opakovaní, z ktorých výlet opačnými otvormi nastane u jednej štvrtiny. Zarátame teda 1 500 000 pozitívnych výsledkov. Spolu nastane skúmaný jav v priemere pri 4 500 000 opakovaní experimentu, čo je polovica všetkých opakovaní. Jeho pravdepodobnosť musí teda byť 1/2.

Kvantová mechanika predpovedá, že pravdepodobnosť, že ľavý a pravý atóm vyletia rôzne označenými otvormi je $\frac{1}{2}$. Teória inštrukčných sád, na rozdiel od toho, predpovedá, že táto pravdepodobnosť má byť väčšia ako $\frac{5}{9}$. Obe teórie sú takto v spore. To, ktorá z nich nie je správna, môže rozhodnúť experiment.

3.3 Čo hovorí experiment?

Analogické experimenty, ktoré vykonal Alain Aspect [9] ukazujú, že pravdepodobnosť toho, že atómy vychádzajú rôznymi otvormi je naozaj $\frac{1}{2}$. Z argumentácie Johna Bella teda vyplýva, že atómy, pritom, ako letia zo zdroja do detektorov, nemajú žiadne inštrukčné sady.[6] Tým pádom **počas letu atómov k prístrojom nie je predurčené, ktorými otvormi vlastne vyjdú, a preto atómy nenesú žiadnu informáciu o svojom budúcom správaní sa v detektoroch. Táto informácia sa tvorí až pri meraní na prístrojoch.** Bell naviac ukázal, že atómy sa naozaj nesprávajú lokálne deterministicky[7] a daný stav nadobúdajú až keď sú zmerané. Einsteinova snaha udržať doktrínu, že fyzikálne vlastnosti vecí

---

[6] Existujú viaceré zložitejšie variácie takýchto experimentov, pri ktorých je rozdiel predpovedí kvantovej mechaniky a teórie inštrukčných sád oveľa väčší [3]. Pri niektorých sa dokonca predpovede líšia až do takej miery, že zatiaľ čo kvantová mechanika predpovedá pravdepodobnosť 1, teória inštrukčných sád predpovedá nulu—experimenty znovu dokazujú zhodu s kvantovou mechanikou.

[7] Napriek tomu, že pri jednoduchom EPR experimente, pri ktorom je ľavý prístroj bližšie pri zdroji atómov ako pravý, experimentátor pri ľavom prístroji vie hneď po tom, ako zaregistruje ľavý atóm, ako vyletí z pravého prístroja pravý atóm, nevie to experimentátor pri pravom prístroji. Musí si počkať na výsledok experimentu. Preto sa nedá hovoriť, že by sa medzi experimentátormi šírila informácia nadsvetelnou rýchlosťou. Einsteinova špeciálna teória relativity teda nie je narušená.

sú vo všeobecnosti objektívne reálne a nezávislé od pozorovania, sa tak ukázala ako neudržateľná. Ako povedal Pascual Jordan [10]

> Pozorovanie nielen že ovplyvňuje to, čo chceme odmerať, ono to vytvára … Sme to my, kto prikazuje elektrónu, aby zaujal konkrétnu polohu … Sami produkujeme výsledky meraní.

Kapitola 4

Superbezpečná komunikácia

4.1 Kvantovokryptografický komunikačný protokol

Už v úvode práce sme spomenuli, že komunikácia pomocou kvantovokryptografického protokolu je nezlomiteľná—inými slovami, nedá sa odpočúvať. Ako je to však možné? A ako bude prebiehať samotná komunikácia?

Dajme tomu, že Alica chce poslať Bobovi informáciu v tvare: „*a*“ (správu tvorí jedno malé písmeno a). Použije binárnu verziu už spomínanej Vernamovej šifry. Prvou vecou, ktorú musí Alica urobiť, je preklad správy do binárnej sústavy (napríklad pomocou tabuľky ASCII—pozri priložené CD). Správa v binárnej sústave vyzerá takto: 1100001.

Ďalším krokom bude, že sa každá číslica zašifruje pomocou náhodnej zmesi núl a jedničiek (kľúča), a to nasledujúcim spôsobom: Nula ponecháva šifrovanú číslicu v pôvodnom stave; jednička mení číslicu na opačnú, teda 0 na 1 a 1 na 0 (viď Tab. 4.1). Teraz už môže Alica odoslať šifru (zašifrovanú informáciu), pričom sa nemusí obávať toho, že ju niekto zachytí, pretože bez kľúča šifru nedešifruje nikto.

A tu sa dostávame k ďalšiemu problému. Bez kľúča šifru nemôže dešifrovať nikto—teda ani Bob. Alica mu nemôže poslať kľúč, pretože by ho musela znovu zašifrovať, a to by Bobovi veľmi nepomohlo. Potrebujeme teda vyriešiť **problém distribúcie kľúča**.

Našťastie je tu jedno riešenie. Spomeňme si na to, keď sme opisovali vylepšený EPR experiment (časť 3.2, str. 16). V tomto experimente atómy pri rovnakom natočení prístrojov vychádzali vždy rôznymi otvormi, pričom to, ktorým otvorom

Alica	
správa	1100001
kľúč	1101001
šifra	0001000

Bob	
šifra	0001000
kľúč	1101001
správa	1100001

Tabuľka 4.1: Správu 1100001 Alica pomocou kľúča 1101001 zašifruje na 0001000. Túto šifru môže bezpečne poslať Bobovi verejným kanálom. Bob správu rozšifruje pomocou toho istého kľúča.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
a_1	B	B	C	A	C	B	B	B	A	C	A	B	A	B	B	A	B	A	A	A
a_2	$-$	$-$	$+$	$+$	$+$	$+$	$-$	$+$	$+$	$-$	$-$	$-$	$-$	$+$	$+$	$-$	$-$	$-$	$+$	$-$
a_3	0	0	1	1	1	1	0	1	1	0	0	0	0	1	1	0	0	0	1	0
b_1	A	B	B	B	C	B	A	C	B	C	C	C	C	B	C	A	C	B	A	A
b_2	$-$	$+$	$+$	$-$	$-$	$-$	$-$	$-$	$-$	$+$	$-$	$-$	$-$	$-$	$+$	$+$	$+$	$-$	$-$	$+$
b_3	1	0	0	1	1	1	1	1	1	0	1	1	1	1	0	0	0	1	1	0
k		0			1	1				0				1		0			1	0

Tabuľka 4.2: Záznam údajov, ktoré si pre prvých 20 vygenerovaných párov zaznamenajú Alica a Bob. V prvom riadku tabuľky sú poradové čísla párov atómov, v riadku a_1 sú uvedené smery Alicinho prístroja, v riadku a_2 sú zaznačené otvory, ktorými vyšiel na prístroji atóm a v riadku a_3 je preklad jej výsledkov merania do jednotiek a núl. Podobný význam majú riadky b_1, b_2 a b_3, ktoré sa týkajú Boba. Posledný riadok k predstavuje kľúč.

ten ktorý atóm vyletí, bolo určené až keď atómy vstúpili do prístrojov a boli zmerané. Predstavme si teda, že Alica bude mať jeden Stern-Gerlachov prístroj a Bob bude mať druhý. Medzi nimi bude—podobne ako v experimente—zdroj atómov v previazanom stave. Čo musia Alica a Bob urobiť, aby obaja získali kľúč, ktorý bude slúžiť na šifrovanie a dešifrovanie informácií? Ukážeme si to na konkrétnom príklade dvadsiatich vygenerovaných párov atómov (viď Tab. 4.2).

1. Po vygenerovaní každého páru Alica aj Bob náhodne natočia svoje prístroje, každý do jedného z troch smerov, pričom si každý z nich zaznamená tri veci: (1) poradové číslo páru atómov, (2) smer natočenia svojho prístroja a (3) číslo 1 alebo 0 podľa nasledujúcich pravidiel: Ak na Alicinom prístroji vyletí atóm cez „+“ otvor Alica si zaznačí 1. Ak vyletí cez „−“ otvor zaznačí si číslo 0. Podobne bude postupovať Bob, len s tým rozdielom, že on si zaznačí čísla opačne. Ak Bobov atóm vyletí cez otvor „+“, zaznačí si 0 a ak cez otvor „−“, zaznačí si 1 (viď Tab. 4.2).

2. Po nameraní 20 atómov Alica pošle verejným kanálom (napr. obyčajným telefónom) Bobovi zoznam poradových čísel s prislúchajúcimi natočeniami svojho prístroja, teda v našom prípade zoznam

$$BBCACBBBACABABBABAAA.$$

   Bob jej obratom cez verejný kanál pošle zoznam poradových čísel párov, pri ktorých sa natočenie jeho prístroja zhodovalo s jej natočením, teda zoznam $2, 5, 6, 10, 14, 16, 19, 20$ (viď Tab. 4.2). Ak náhodou verejný kanál odpočúva Eva, znalosť týchto informácií jej nijako nepomôže poznať kľúč. Teraz Alica aj Bob zoberú svoje jednotky a nulky z týchto pozícií a vytvoria z nich kľúč. V našom prípade získajú 01101010. Tak získajú zoznam jednotiek a núl, ktorý majú obaja spoločný.

3. Na záver si ešte Alica a Bob cez verejný kanál porovnajú náhodne vybranú polovicu bitov kľúča, aby sa ubezpečili, že ich Eva neodpočúvala (pozri nasledujúcu časť). Napríklad Alica zavolá Bobovi a povie mu: „Pošli mi tretí, štvrtý, šiesty a siedmy bit kľúča.“ Bob jej do telefónu oznámi, že tieto bity sú 1,0,0 a 1. Alica tieto bity porovná so svojimi a keďže sú rovnaké, uzavrie, že ich nikto neodpočúval. Takto zverejnené 4 bity teraz zahodia a použijú zvyšné 4 bity: 0110. Tieto jednotky a nulky teraz môžu použiť ako kľúč pri komunikácii, ktorú sme už popísali. Ak by Alica pri tomto porovnaní bitov zistila, že jej a Bobove bity sa nezhodujú, bol by to znak toho, že ich Eva odpočúva. Preto by vygenerovaný kľúč s Bobom nepoužili a skúsili by ho generovať znovu, prípadne by sa pokúsili nájsť Evu.

Je zrejmé, že na vygenerovanie dostatočne dlhého náhodného kľúča treba generovať veľmi veľa párov atómov. Z nich zhruba $\frac{1}{6}$ bude využitá na získanie kľúča, keďže Alicin a Bobov detektor budú mať rovnaké smery v priemere v jednej tretine prípadov a z nich polovica sa použije na porovnanie. V ďalšej časti sa pozrieme na to, ako ovplyvní situáciu Eva, keď sa bude snažiť odpočúvať distribúciu kľúča.

4.2 Aké sú Evine šance?

Ak chce Eva rozšifrovať správu, ktorú posiela Alica Bobovi, musí poznať kľúč. Nezostáva jej teda nič iné ako „načúvať“ pri procese distribúcie kľúča. Vezme preto svoj Stern-Gerlachov prístroj a umiestni ho medzi zdroj previazaných párov atómov a Alicin prístroj, tak, aby všetky atómy, ktoré letia k Alici preleteli cez jej prístroj. Predpokladajme pre jednoduchosť, že ho natočí do smeru A[1].

Zámerom Evy je pomocou svojho prístroja zistiť, ako vyletí atóm z Alicinho prístroja. Hlavným výsledkom Kapitoly 3 bolo to, že keď ľavý a pravý atóm páru letia k prístrojom, *nevedia ešte* ktorými otvormi vyletia. Táto informácia vzniká až pri detekcii v prístrojoch Alice a Boba. Tu vidieť, že Evina snaha získať túto informáciu ešte predtým, ako atómy zaregistrujú Alica a Bob, je márna. Eva ju bude svojím meraním vytvárať a ako uvidíme, nebude ťažké, aby si to Alica a Bob všimli.

Teraz podrobnejšie. Ak majú náhodou Alica aj Bob svoje prístroje nastavené obaja do smerov A, tak sa Eve podarí získať informáciu o tom, ktorým otvorom vyletí atóm pri Alici. Vytvorí ju totiž sama Eva. Ak by napríklad Eva zaregistrovala ľavý atóm v stave $|+A\rangle$, tak by musel preletieť Aliciným prístrojom cez otvor „+“. Pravý atóm by musel Bobovým prístrojom preletieť cez otvor „−“. Pôvodný previazaný stav atómov $|\Psi\rangle$ by tak Eva svojím meraním zmenila na stav $|+A,-A\rangle$. Ak by Eva zaregistrovala ľavý atóm v stave $|-A\rangle$, pôvodný stav $|\Psi\rangle$ by skolaboval na stav $|-A,+A\rangle$. Teda Eva dokáže nepozorovane prečítať tie bity kľúča, ktoré vzniknú z orientácií oboch prístrojov do smeru A. V Tab. 4.2 to zodpovedá 16. a 20. páru atómov.

Ak by mali Alica aj Bob orientované svoje prístroje obaja do smeru B, situácia by sa zmenila v neprospech Evy. Predpokladajme, že by Eva zaregistrovala ľavý

---

[1] Vo všeobecnosti ho môže mať natočený do ľubovoľného smeru, keďže nevie, ktoré tri smery si vybrali Alica a Bob na komunikáciu.

atóm v stave $|{+A}\rangle$. Pôvodný previazaný stav $|\Psi\rangle$ by potom skolaboval na stav $|{+A},{-A}\rangle$. Vypočítame teraz, aká je pravdepodobnosť toho, že Alica nájde ľavý atóm v stave $|{+B}\rangle$ a Bob nájde pravý atóm v stave $|{-B}\rangle$. Keby sa to totiž stalo, Eve by sa podarilo odpočuť práve prenášaný bit kľúča a Alica ani Bob by o tom nevedeli (atómy by u nich vyšli z rôznych otvorov).

Najprv vypočítame amplitúdu $\langle{+B},{-B}|+A,-A\rangle$. Budeme postupovať rovnako ako v Kapitole 3.

$$\begin{aligned}\langle{+B},{-B}|+A,-A\rangle &= \langle{+B}|+A\rangle\,\langle{-B}|-A\rangle = \\ &= \cos{(120^\circ/2)}\cos{(120^\circ/2)} = \frac{1}{4}\end{aligned}$$

Pravdepodobnosť potom bude 1/16.

Alica a Bob by nevedeli, že ich Eva odpočúva ani v prípade, že by Alica našla svoj atóm v stave $|{-B}\rangle$ a Bob svoj atóm v stave $|{+B}\rangle$. Lenže v tomto prípade by Eva získala odpočúvaním opačný bit ako oni, čo by jej nepomohlo.

Vo zvyšných dvoch prípadoch, keď by Alica našla svoj atóm v stave $|{+B}\rangle$ a Bob svoj atóm v stave $|{+B}\rangle$, alebo keď by Alica našla svoj atóm v stave $|{-B}\rangle$ a Bob svoj atóm v stave $|{-B}\rangle$, by mohli Alica a Bob vzájomným porovnaním svojich bitov zistiť, že sú rôzne, čo by svedčilo o prítomnosti Evy. Pritom v prvom z týchto prípadov by Eva uhádla správny bit Alicinho kľúča a v druhom nie.

Mohli by sme teraz vypočítať aj pravdepodobnosti spomínaných troch prípadov. Tabuľka 4.3 uvádza prehľad výsledkov takýchto výpočtov. Je z nej vidieť, *že nezávisle na tom, aký bit nameria Eva*, platí, že ak Alica a Bob nasmerujú obaja svoje prístroje do smeru A (pravdepodobnosť 1/3), získajú rôzne bity s pravdepodobnosťou 0. Ak prístroje nastavia obaja do smeru B (pravdepodobnosť 1/3), tak získajú rôzne bity s pravdepodobnosťou 3/8. No a nakoniec, ak prístroje nastavia obaja do smeru C (pravdepodobnosť 1/3), tak získajú rôzne bity znovu s pravdepodobnosťou 3/8. Z tabuľky vyplýva, že pri Evinom nepretržitom odposluchu bude pravdepodobnosť toho, že Alica a Bob *nezaznamenajú* rovnaký bit

$$\frac{1}{3}\cdot 0+\frac{1}{3}\cdot\frac{3}{8}+\frac{1}{3}\cdot\frac{3}{8}=\frac{1}{4}$$

	A	B	C
$\lvert\langle{+S},{+S}\rvert+A,-A\rangle\rvert^2$	0	$\frac{3}{16}$	$\frac{3}{16}$
$\lvert\langle{+S},{-S}\rvert+A,-A\rangle\rvert^2$	1	$\frac{1}{16}$	$\frac{1}{16}$
$\lvert\langle{-S},{+S}\rvert+A,-A\rangle\rvert^2$	0	$\frac{9}{16}$	$\frac{9}{16}$
$\lvert\langle{-S},{-S}\rvert+A,-A\rangle\rvert^2$	0	$\frac{3}{16}$	$\frac{3}{16}$

	A	B	C
$\lvert\langle{+S},{+S}\rvert-A,+A\rangle\rvert^2$	0	$\frac{3}{16}$	$\frac{3}{16}$
$\lvert\langle{+S},{-S}\rvert-A,+A\rangle\rvert^2$	0	$\frac{9}{16}$	$\frac{9}{16}$
$\lvert\langle{-S},{+S}\rvert-A,+A\rangle\rvert^2$	1	$\frac{1}{16}$	$\frac{1}{16}$
$\lvert\langle{-S},{-S}\rvert-A,+A\rangle\rvert^2$	0	$\frac{3}{16}$	$\frac{3}{16}$

Tabuľka 4.3: Prehľad pravdepodobností rôznych možných koncových stavov páru atómov v prípade, že Eva nameria ľavý atóm v stave $|{+A}\rangle$ (vľavo) resp. v stave $|{-A}\rangle$ (vpravo) a Alica a Bob majú svoje prístroje natočené obaja do rovnakého smeru S, kde S je buď A, B, alebo C.

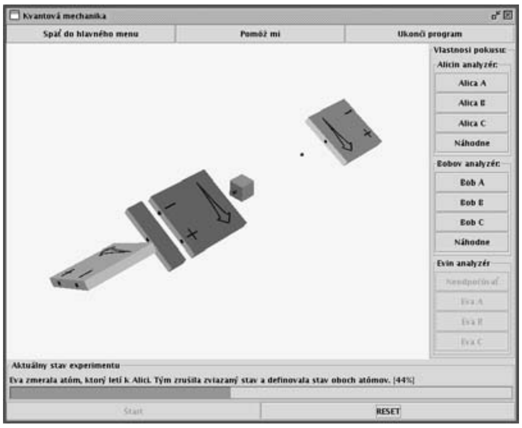
Teda v priemere štvrtina bitov kľúča, ktorý získajú Alica a Bob sa nebude u Alice a Boba zhodovať.

Vieme, že v poslednej fáze distribúcie kľúča si Alica a Bob navzájom porovnajú len náhodne vybranú polovicu bitov kľúča. Aká je pravdepodobnosť, že by pri tom *neodhalili* Evu? Ak si porovnajú n bitov, tak táto pravdepodobnosť bude

$$\left(1 - \frac{1}{4}\right)^n$$

Vidíme, že bude tým menšia, čím dlhší kľúč generujú. Ak by vygenerovali 2 000 bitový kľúč a z neho si porovnali 1 000 bitov, bola by pravdepodobnosť, že pri tom neodhalia Evu $0,75^{1000} \approx 1,15 \cdot 10^{-125}$, čo je prakticky nula. Vidíme, že použitím kvantovokryptografického protokolu nevieme odpočúvaniu zabrániť, ale vieme ho rozoznať.

4.3 Java applet



Eva zmerala atóm, ktorý letí k Alici. Tým zrušila zviazaný stav a definovala stav oboch atómov. [44%]

Obrázok 4.1: V okne aplikácie sa zobrazujú simulácie experimentov.

Keďže v súčasnosti sa o ochrane prenášaných informácií hovorí najmä v súvislosti s internetom a počítačmi, rozhodli sme sa ako súčasť tejto práce vytvoriť počítačový program (applet) v jazyku *Java*, ktorý by simuloval deje prebiehajúce v mikrosvete atómov. Tento program sa zaoberá dvoma základnými témami— kvantovou mechanikou a kvantovou kryptografiou. Ďalej je program rozdelený na jednotlivé časti, ktoré sa potom zaoberajú samotnými experimentami. Ku všetkým častiam sa pristupuje priamo z hlavného menu.

Prvá časť je simulácia pokusu, ktorý využívali vo svojom argumente Einstein, Podolsky a Rosen. V tejto časti vás program oboznámi s úplnými základmi tej časti kvantovej mechaniky, ktorej sa týkala táto práca.

Druhá časť sa zaoberá experimentom, ktorý navrhol John Bell. Od predchádzajúcej časti sa líši aj tým, že pri tomto experimente sa môže stať experimentátorom každý, pretože program ponúka možnosť zmeniť natočenie oboch prístrojov, a to buď do zadaného smeru, alebo náhodne.

Tretia časť patrí už do kvantovej kryptografie. V tejto časti vám simulácia dovolí nahliadnuť do tej časti kvantovej kryptografie, ktorá je spojená s kvantovou mechanikou. Aj tu môžete priebeh experimentu riadiť, a tak *nasimulovať* rôzne situácie a pozorovať výsledky vašej práce.

Každá z týchto častí obsahuje možnosť automaticky uskutočniť viac experimentov, pričom po ich uskutočnení vám program zobrazí výsledky všetkých experimentov a početnosť jednotlivých výsledkov.

A na záver je tu aj posledná časť aplikácie, v ktorej si budete môcť vyskúšať (aspoň virtuálne), aké je to byť Alicou, Bobom, či dokonca Evou. Touto časťou je hra, ktorá sa síce na problém kvantovej kryptografie pozerá trochu z nadhľadu, ale pritom sa nijako neodkláňa od kvantovomechanických zákonov. Snažili sme sa ju napísať tak, aby dokázala vzbudiť záujem o kvantovú kryptografiu aj u tých, ktorý majú k fyzike trochu *ďalej*.

Celá aplikácia sa dá spustiť priamo z priloženého CD. Hneď po spustení sa zobrazí už spomínané hlavné menu. Ovládanie aplikácie je intuitívne, no ak by ste si z ňou náhodou nevedeli rady, môžete si pomôcť pomocníkom, v ktorom je podrobne popísané ovládanie každej časti programu.

Na záver by sme radi podotkli, že všetky mená, internetové a emailové adresy, použité v hre sú fiktívne a prípadná podobnosť je čisto náhodná.

Záver

Na záver zhrnieme, čo všetko sa nám podarilo v práci dosiahnuť:

1. Oboznámili sme sa s najznámejšími druhmi kryptografie, ktoré sa využívali v minulosti, a ktoré sa využívajú v súčasnosti.
2. Zoznámili sme sa s kvantovomechanickým popisom atómov striebra so spinom 1/2.
3. Popísali sme EPR experiment a tiež jeho zdokonalenú verziu. Zoznámili sme sa s Bellovým dôkazom toho, že ľavý a pravý atóm si pri lete zo zdroja nenesú inštrukčné sady a teda nemajú žiadnu hodnotu priemetu magnetického momentu. Tú získavajú až pri meraní na ľavom a pravom prístroji.
4. Na základe tohoto experimentu sme popísali kvantovokryptografický protokol a vypočítali sme pravdepodobnosť toho, že Eva zostane pri použití tohto protokolu neodhalená.
5. Na základe vytvorenej teórie sme vytvorili aplikáciu v programovacom jazyku *Java*, ktorá záujemcom pomôže lepšie preniknúť do situácií, ktoré nastávajú pri experimentoch opísaných v tejto práci.

Splnili sme teda všetky ciele, ktoré sme si dali v úvode práce. Pritom práca má aj praktický úžitok, keďže spolu s interaktívnym Java programom môže slúžiť ako učebný text k netradičnému zoznámeniu sa s kvantovou mechanikou, ktorý môžu použiť vedúci fyzikálnych krúžkov, prípadne učitelia na seminároch z fyziky.

Úplne na záver by sme chceli vyjadriť ešte jedno naše želanie do budúcnosti. Svoju činnosť v tejto oblasti by sme chceli zakončiť vytvorením a spravovaním internetovej stránky, ktorá bude pomáhať žiakom a študentom so záujmom o získanie nových informácií z takého lákavého sveta, akým svet kvantovej mechaniky celkom určite je.

Literatúra

[1] *World Premiere: Bank Transfer via Quantum Cryptography Based on Entangled Photons* [online]. [cit. 2006-02-04]. Dostupné na internete: <`www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf`>.

[2] Singh, S.: *The Code Book CD-ROM*[online]. [cit. 2006-02-04]. Dostupné na internete: <`http://www.simonsingh.net/Code_Book_Download.html`>.

[3] Styer, D. F.: *The Strange World of Quantum Mechanics.* Cambridge: Cambridge University Press 2000.

[4] Feynman, R., Leighton, R., Sands, M.: *Feynmanove prednášky z fyziky, 5. diel.* Bratislava: Alfa 1990.

[5] Born M., *The Born-Einstein Letters.* New York: Walker 1971.

[6] Mermin, N. D.: *Is the Moon There When Nobody Looks? Reality And Quantum Theory.* In: Physics Today, roč. 38, apríl 1985, č. 4, s. 38-47.

[7] Einstein, A., Podolsky, B., Rosen, N.: *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* In: Physical Review, roč. 47, máj 1935, s. 777-780.

[8] Bell, J. S.: *On the Einstein Podolsky Rosen Paradox.* In: Physics, 1964, č. 1, s. 195-200.

[9] Aspect, A., Dalibard, J., Roger, G.: *Experimental Test of Bell's Inequalities Using Time-Varying Analyzers.* In: Physical Review Letters, roč. 49, december 1982, č. 25, s. 1804-1807.

[10] Citované v Jammer, M.: *The Philosophy of Quantum Mechanics.* New York: Wiley 1974, s. 151.

[11] Christian, W.: *Open Source PHYSICS: A User's Guide with Examples.* San Francisco: Pearson Addison Wesley 2006.

Zoznam príloh

1. CD, na ktorom sa nachádza Java applet a elektronická verzia tejto práce vo formáte *Portable Document Format* (*.pdf).