Kvantová kryptografie

T. Benedikt, Gymnázium Rokycany, Tom.Benedikt@seznam.cz
T. Liepoldová, Gymnázium F. X. Šaldy Liberec, Mecnet@seznam.cz
J. Lukeš, Gymnázium Českolipská Praha 9, Lukes.Jakub@gmail.com

Abstrakt

Seznámili jsme se s vlastnostmi kvantové mechaniky a jejím užití ke kódování informací.Toto jsme demonstrovali na příkladu kvantových peněz a zjistili jsme míru pravděpodobnosti jejich padělání.

1. Úvod

Kryptografie je věda, která se zabývá šifrováním zpráv. Toto kódování je natolik dokonalé, že je čitelné jenom se speciální znalostí. Kvantová kryptografie je metoda pro bezpečný utajený přenos informací. Její bezpečnost je garantována fundamentálními zákony kvantové fyziky. V naší práci jsme se zaměřili především na princip polarizačního kódování a pravděpodobnost se kterou můžeme daný kód rozšifrovat. Dále jsme se zabývali přenosem šifrovaných zpráv a jejich možným odposlechem.

Nejprve se budeme zabývat principy kvantové fyziky a potom ji budeme aplikovat na principy kvantové kryptografie.

2. Kvantová kryptografie

Kvantová kryptografie je založena na vlastnostech kvantové mechaniky. K porozumění, jak tedy skutečně kvantová kryptografie funguje, je nezbytné říci si něco o zákonech a principech, kterými se kvantové fyzikální objekty řídí. Pro co nejsrozumitelnější výklad se omezíme na nejjednodušší kvantový fyzikální systém: qubit.

Qubit je označení pro kvantový fyzikální systém, který může nabývat dvou základních (bazických) kvantových stavů. Příkladem qubitů můžou být třeba dvě různé orientace spinu elektronu, horizontální a vertikální polarizace fotonu, atom v základním a excitovaném stavu, atd. Nejde tak ani o konkrétní realizaci qubitu, ale o fakt, že existují dva různé zcela odlišitelné stavy kvantového systému.

Člověk znalý klasické fyziky by mohl namítnout, že takovéto stavy se nacházejí také v klasické fyzice. V čem tedy spočívá rozdíl? Podstatným rozdílem je, že se quibit se nemusí nacházet pouze v těchto dvou základních stavech, ale i v libovolné superpozici (lineární kombinaci) těchto dvou základních stavů. Nyní pro lepší pochopení si uvedeme příklad dvou stavů. Polarizovaný foton se může nacházet nejen ve stavu vertikální polarizace $|\updownarrow\rangle$ nebo horizontální polarizace $|\leftrightarrow\rangle$, ale i v libovolné lineární kombinaci těchto dvou bazických stavů $|\psi\rangle \equiv \alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle \quad \alpha, \beta \in C$.

Jak tedy rozumět tomuto stavu? Jde o zcela nový stav, kde amplitudy α a β určují, že s pravděpodobností $|\alpha|^2$ nalezneme qubit ve stavu $|\updownarrow\rangle$ a s pravděpodobností $|\beta|^2$ ve stavu $|\leftrightarrow\rangle$. Z pravidel pro pravděpodobnost plyne, že součet $|\alpha|^2$ a $|\beta|^2$ je roven 1. Příkladem těchto superpozic jsou stavy

$$|A\rangle = \frac{1}{\sqrt{2}}|\updownarrow\rangle + \frac{1}{\sqrt{2}}|\leftrightarrow\rangle$$

$$|B\rangle = \frac{1}{\sqrt{2}}|\updownarrow\rangle - \frac{1}{\sqrt{2}}|\leftrightarrow\rangle$$

Měřili bychom nyní polarizovaný foton (qubit) ve stavu $|A\rangle$ polarizačním filtrem orientovaným svisle, máme pravděpodobnost $\frac{1}{2}$, že foton projde (je ve stavu $|\updownarrow\rangle$) a pravděpodobnost $\frac{1}{2}$ že neprojde (je ve stavu $|\leftrightarrow\rangle$) . Obdobné pozorování bychom obdrželi, kdybychom stejným způsobem měřili polarizovaný foton ve stavu $|B\rangle$. Výsledek tohoto měření tedy nelze dopředu určit, je zcela náhodné a pro foton v obou stavech $|A\rangle$ i $|B\rangle$ shodné. V čem se tedy tyto dva stavy liší? Natočením polarizačního filtru o 45 stupňů lze tyto dva stavy zcela odlišit. V tomto měření foton ve stavu $|A\rangle$ s pravděpodobností 1 projde a foton ve stavu $|B\rangle$ s jistotou neprojde. Stavy $|A\rangle$ a $|B\rangle$ jsou tedy zcela rozlišitelné a opět tvoří jinou bázi, v které lze každý stav polarizovaného stavu vyjádřit jako lineární kombinaci těchto bazických stavů. Jednoduchou algebrou se snadno přesvědčíme, že

$$|\updownarrow\rangle = \frac{1}{\sqrt{2}}|A\rangle + \frac{1}{\sqrt{2}}|B\rangle$$

$$|\leftrightarrow\rangle = \frac{1}{\sqrt{2}}|A\rangle - \frac{1}{\sqrt{2}}|B\rangle$$

Vidíme tedy, že měřením polarizačních stavů $|\leftrightarrow\rangle$ a $|\updownarrow\rangle$ v bázi stavů $|A\rangle$, $|B\rangle$ (polarizačním filtrem orientovaným pod úhlem 45 stupňů od svislé osy) bychom dostali stavy $|A\rangle$ a $|B\rangle$ každý s pravděpodobností $\frac{1}{2}$. Obecně lze říci, že měření mění stav fyzikálního systému a kvantový systém se po takovémto měření nachází ve stavu, v jakém jsme ho naměřili. Popis výsledků budeme nadále v textu využívat, shrňme si je proto do následující tabulky.

	Měření v bázi $\|\updownarrow\rangle, \|\leftrightarrow\rangle$		Měření v bázi $\|A\rangle$, $\|B\rangle$	
	$\|\updownarrow\rangle$	$\|\leftrightarrow\rangle$	$\|A\rangle$	$\|B\rangle$
$\|\updownarrow\rangle$	1	0	$\frac{1}{2}$	$\frac{1}{2}$
$\|\leftrightarrow\rangle$	0	1	$\frac{1}{2}$	$\frac{1}{2}$
$\|A\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	1	0
$\|B\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	1

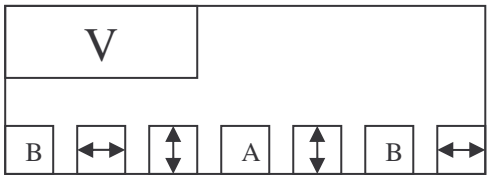
Na nejjednodušším kvantovém systému – qubitu, jsme si vysvětlili popis kvantových stavů, princip superpozice a možnosti měření v různých bází.

Na závěr této krátké exkurze do kvantové mechaniky zmiňme ještě jednu důležitou vlastnost kvantových stavů a sice, že není možné klonovat neznámé navzájem ne zcela rozlišitelné stavy kvantového systému.

3. Kvantové peníze

Kořeny kvantové kryptografie se datují do 60. let 20. století. Tehdy byla poprvé publikována myšlenka na kvantové peníze, které není možné padělat. Tento nápad S. Wiesnera byl však natolik revolucionářský, že nebyl podporován a nemohl se tedy dále rozvíjet.

Přenesme se teď ale do 21. století, kdy se myšlenka kvantové kryptografie a kvantových peněz stává aktuální myšlenkou. Pojďme teď společně nahlédnout do tajů kvantových peněz. Také vás napadá myšlenka, jak takové peníze asi vypadají? A jakým způsobem to funguje? Kvantová bankovka má své vlastní identifikační číslo (V).



Při výrobě bankovky přiřadí banka řadě qubitů právě jedno identifikační číslo V a proto banka ví, jak jsou fotony v bankovce polarizované a jaká báze byla k polarizaci použita. Pokud bychom chtěli bankovku padělat, museli bychom náhodně tipovat bázi, na které k polarizaci došlo. Pravděpodobnost, že se nám podaří padělat jeden qubit se dá lehce vypočítat a činí 75% neboli $\frac{3}{4}$. Při vrůstajícím počtu qubitů se pravděpodobnost padělání exponenciálně snižuje tzn.při *n* qubitech se pravděpodobnost vypočítá jako $\left(\frac{3}{4}\right)^n$. Uveďme si konkrétní příklad, bankovka má 5 qubitů, poté je šance na neodhalené padělání bankovky 23,73%, ale pokud banka použije qubitů 20 pak se šance sníží na 0,32%. Z toho vyplývá, že kódování bankovek pomocí kvantové kryptografie by bylo účinným prostředkem proti padělání peněz.

4. Shrnutí

Díky našemu miniprojektu jsme se dozvěděli jaký je rozdíl mezi kvantovou a klasickou fyzikou. Zabývali jsme se principy a zákony kvantové kryptografie, díky kterým jsme nahlédli do záhad kvantového polarizačního kódování. Jedním z cílů bylo polarizační kódování kvantových bankovek. Zjistili jsme, že pravděpodobnost padělání bankovky exponenciálně klesá s rostoucím počtem fotonů v bankovce.

Poděkování

Děkujeme FJFI za realizaci fyzikálního týdne. Dále děkujeme sponzorům. Zvláštní poděkování patří našemu supervisorovi za odhalení této problematiky a za trpělivost, kterou nám věnoval, a humor, který vnesl do práce ☺.

Reference

http://cml.fsv.cvut.cz/~kupca/qc/node7.html
http://cs.wikipedia.org/wiki/Kryptografie
optics.upol.cz/download/vyzkum/prezent-krypto.pdf