Kryptografie, kvantová mechanika a jak to souvisí

J. Jelínek, Z. Farana
Katedra fyziky, Břehová 7, Praha 1
kni.zka@seznam.cz, byf@seznam.cz

Abstrakt

Práce se týká užití kvantových vlastností částic v bezpečné datové komunikaci. Obsahuje popis kvantového EPR protokolu spolu se zamyšlením nad jeho bezpečností.

1. Úvod

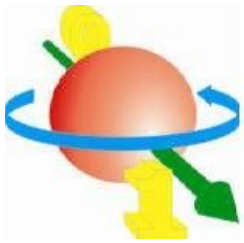
Všichni se neradi dělíme o své soukromí. Proto máme zámky na dveřích, PINy v telefonech a hesla v počítačích. Jsme nedůvěřiví. Právem. Se stejným úsilím, se kterým se snažíme své soukromí skrýt, pokoušíme se cizí soukromí odkrýt. Tato rozpolcenost nás provází již od nepaměti. Snaha zamaskovat pravý význam určitého sdělení a naopak snaha rozluštit je dala vzniknout dvěma vědním oborům: *kryptografii* a jejímu protějšku *kryptoanalýze*. Dnes se budeme zabývat kryptografií. Existuje mnoho druhů šifer, od *substitučních*[1], přes *transpoziční*[2] až po *symetrické* a *hashovací*. Moderní fyzika nám přinesla nové možnosti a to konkrétně v oblasti kvantové mechaniky. V této oblasti předběhla teorie praxi.

Šifrovat lze pomocí veřejného, či soukromého šifrovacího kliče. Nadále se budeme věnovat problematice bezpečného přenosu soukromého kliče. Zde je totiž hlavní kámen úrazu standardních šifrovacích metod. Jestliže si dotyčné osoby chtějící si vytvořit bezpečný komunikační kanál nepředají soukromý klíč osobně, nemohou si být jisti, že ho třetí osoba nezachytí a nezneužije pro odposlechnutí komunikace.

Právě *kvantová kryptografie* řeší problém bezpečné distribuce klíčů mezi dvěma osobami na úrovni fyzikálních zákonů kvantové mechaniky. Poté lze pomocí bezpečně předaného soukromého šifrovacího klíče zakódovat pomocí *one-time pad*[3] šifry.

2. Kvantový svět

Základním rysem kvantové mechaniky je *linearita*. Tento pojem vyjadřuje skutečnost, že pokud může být částice ve stavu |0> nebo |1>, může být i v libovolné *superpozici*[4] těchto stavů. Příkladem takových dvou stavů můžou být například dva navzájem kolmé spinové stavy nebo polarizace fotonů. Vzhledem k jejich blízké analogii s klasickými bity, nazýváme tyto systémy *qubity*. Qubity chápeme jako základní nositele informace, kterým linearita propůjčuje zvláštní vlastnosti. Mohou nabývat mnoha stavů, které od sebe nelze obecně odlišit. Z toho plyne, že



Obr. 1 qubit

1 užívají nahrazování každého znaku jiným znakem dle určitého klíče
2 tzv. přesmyčka - změna pořadí znaků dle urč. klíče
3 jednorázová tabulková šifra, též známá jako Vernamova šifra
4 lineární kombinaci

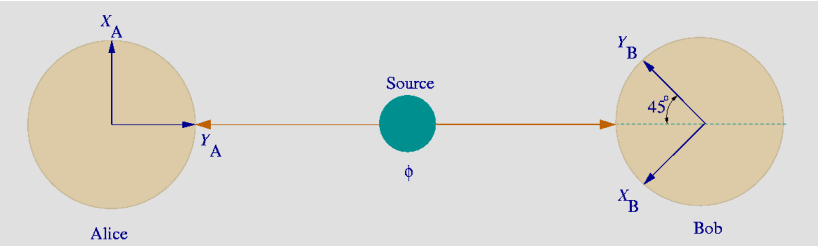
informaci, kterou qubity nesou, nelze zkopírovat.

Linearita kvantové mechaniky je odpovědná i za další kvantový jev zvaný *provázání*[5]. Uvažujme pro jednoduchost dva qubity ve stavech |00>[6], |01>, |10> a |11>. Z principu linearity vyplývá, že dva qubity se mohou nacházet i v libovolné superpozici těchto čtyř stavů. Existují ale i superpozice, které nelze rozložit na stavy jednotlivých qubitů a těm pak říkáme provázané stavy neboli *ebity*. Provázanost je *monogamní* a tudíž, pokud se dva qubity prováží maximálně, nemohou se již provázat se třetím. Příkladem silně provázaného stavu je tzv. *EPR*[7] stav:

$$\mathrm{EPR} = \frac{|00> + |11>}{\sqrt{2}}$$

Důležitou vlastností je, že qubity v tomto stavu jsou silně *korelovány*. Představme si, že Alice měří, zdali je její qubit ve stavu |0> nebo |1>. Takové měření je možné zkonstruovat a kvantová mechanika předpovídá, že s pravděpodobností 50% naměří stav |0> a s pravděpodobností 50% naměří stav |1>. Výsledek je tedy čistě náhodný. Silná korelace zde znamená, že po jejím měření bude Bobův qubit ve stejném stavu jako Aliččin.

Korelace mezi výsledky měření existují i v klasické fyzice. Kvantové korelace se však ukazují mnohem silnější. Jak tedy rozpoznat, zda jde o klasickou nebo kvantovou korelaci? Pro zkoumání síly korelací lze použít Bellovy nerovnosti



Obr. 2: Ilustrace Bellova testu pro částice se spinem 1/2. Zdroj vyrábí provázané páry a jeden qubit pošle Alici, druhý Bobovi. Oba provedou měření.

$$p(Q=q, R=r, S=s, T=t)$$

A	**B**
$Q=\pm 1$	$S=\pm 1$
$R=\pm 1$	$T=\pm 1$

$$QS + RS + RT - QT = (Q+R)S + (R-Q)T = \pm 2$$

$$E(QS + RS + RT - QT) = \sum_{q,r,s,t=\pm 1} p(Q=q, R=r, S=s, T=t) \leq 2$$

Bellovy nerovnosti

Při zkoumání EPR stavu vychází Bellovy nerovnosti $\leq 2\sqrt{2}$, čímž jsou porušeny. Interval $\langle 2, 2\sqrt{2} \rangle$ je dostatečně veliký, abychom mohli vyloučit statistickou chybu. EPR stav je kvantově korelován.

---

5 anglicky *entanglement*
6 oba qubity jsou ve stavu |0>
7 Einstein-Podolsky-Rosen

3. EPR kryptografický protokol

Tato metoda je založena na kvantové propletenosti dvou částic. Určitý zdroj bude generovat ebity v EPR stavu. Předpokládejme, že Alice sdílí s Bobem n EPR párů $\frac{|00>+|11>}{\sqrt{2}}$. Vždy jeden qubit z dvojice vlastní Alice a Bob. Alice a Bob nyní provedou měření v bázi stavů |0> a |1> na každém svém qubitu. Výsledky těchto měření jsou naprosto náhodné. V případě, že Alice nebo Bob naměří stav |0>, zaznamenají si 0 do šifrovacího klíče, v opačném případě zapíšou 1. Silná korelace v EPR páru nám zajišťuje, že jejich klíče budou shodné.

Jak lze bezpečnost narušit? Hlavní nebezpečí spočívá v možnosti zachycení qubitů Evou[8]. Ta může změřit hodnoty qubitů, které zachytila, poslat Bobovi jiné qubity nebo částečně navázat další částici, kterou si ponechá[9]. Ve všech zmíněných případech ale dojde k úplnému zničení provázání nebo alespoň k výraznému zeslabení. Důležitým bezpečnostním prvkem tedy je počkat, až bude mít každý z nich svou sadu n qubitů. Následně se pomocí veřejného kanálu domluví na vybrané posloupnosti párů, které obětují a na nichž provedou Bellův test síly provázání. V případě, že výsledky odpovídají kvalitě kanálu, mohou zahájit generování kódu pomocí individuálních měření

4. Shrnutí

Kvantová kryptografie nabízí vysoce bezpečný přenos šifrovacích klíčů. K tomu využívá principy kvantové teorie, jako je linearita, provázání a Bellovy nerovnosti. Problémem je zejména fyzická realizace distribučního kanálu a přístrojů.

Poděkování

Děkujeme supervizorovi J. Novotnému a organizátorům Fyzikálního týdne

Reference

[1] Michael A. Nielsen a Isaac L. Chuang: *Quantum Computation and Quantum Information*
[2] *Kryptografie* http://cs.wikipedia.org/wiki/Kryptografie
[3] *Kvantová kryptografie* http://cs.wikipedia.org/wiki/Kvantov%C3%A1_kryptografie
[4] *Bell's inequality* http://en.wikipedia.org/wiki/Bell%27s_inequality
[5] *Qubit image* http://acqp.physi.uni-heidelberg.de/inside_the_atomchip.php

8 podle anglického eavesdropping
9 tím se ale korelace oslabí