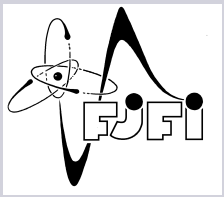

České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská
Katedra fyziky

Kvantová kryptologie

Autor: Brus Adam

24.4.2014 Praha

Obsah

Proč kvantová kryptologie

Proč kvantová kryptologie

1. Náhodné procesy
2. „Bezpečné“ protokoly

Axiomy kvantové mechaniky

1. Každému kvantovému systému přísluší komplexní Hilbertuv prostor, který nazveme **stavovým prostorem** daného systému.
2. Každému stavu uvažovaného systému odpovídá nějaký **paprsek**, tj. jedno-rozměrný podprostor v stavovém prostoru.
3. Každé pozorovatelné daného kvantového systému odpovídá nějaký samosdružený operátor na stavovém prostoru

Axiomy kvantové mechaniky

1. Možné výsledky měření veličiny A jsou body spektra operátoru A.

2. Po naměření hodnoty a veličiny A se systém ocitne ve stavu odpovídajícímu nějakému paprsku, který náleží do vlastního podprostoru operátoru A příslušícímu vlastnímu číslu a.

Důsledky kvantové mechaniky

Důsledky kvantové mechaniky

Existence q-bitu (kvantové bity) jako klasické bity mohou nabývat stavu $|0\rangle$ a $|1\rangle$, ale mohou nabývat i superpozice: $\alpha|0\rangle + \beta|1\rangle$, měřením takovéhoto stavu v bázi $(|0\rangle, |1\rangle)$ dostaneme vždy jen stavy $|0\rangle$ s pravděpodobností $|\alpha|^2$ a $|1\rangle$ s pravděpodobností $|\beta|^2$ ($|\alpha|^2 + |\beta|^2 = 1$).

Fyzikální realizaci q-bitu lze provádět například pomocí lineárně polarizovaného fotonu.

Důsledky kvantové mechaniky

Obecně nelze kopírovat neznámý stav. Útočník má tedy jen jeden pokus na prolomení protokolu.

Důsledky kvantové mechaniky

Měření ovlivní stav, je tedy poznat, že se někdo pokusil nabourat do protokolu.

Příklad Kvantového protokolu.

Protokol BB84 (C.H.Bennett,G.Brassard)

1. Alice si vezme dvě náhodné binární posloupnosti a_k a b_k o délce $(4+\delta)n$.

2. Alice si zvolí dvě báze $X = (|0\rangle, |1\rangle)$ a $Z = (|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = (\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$

3. Alice zakóduje posloupnost a_k v bazi X a Z v závislosti na posloupnosti b_k jako posloupnost $(4+\delta)n$ q-bitu. Pokud člen b_k je 0 užije bazi X, jinak Z.

4. Vzniklou zprávu a báze X, Z pošle Bobovi.

Příklad Kvantového protokolu.

1. Bob každý q-bit přijaté zprávy měří náhodně v bázi X nebo Z a zveřejní fakt, že zprávu přijal.
2. Alice následně zveřejní posloupnost b_k
3. Alice a Bob zahodí všechny bity, kdy Bob měřil v jiné bázi, než v jaké byly připraveny. Z vysokou pravděpodobností se Alice a Bob shodli alespoň v $2n$ případech (jinak přeruší protokol). Ponechají si $2n$ bitu
4. Alice nyní zvolí n kontrolních bitu, které slouží pro kontrolu, zda protokol nebyl napaden a zdělí Bobovi, které bity vybrala.

Příklad Kvantového protokolu.

1. Alice a Bob si porovnají hodnoty na kontrolních bitech. Pokud se víc, než akceptovatelná část bitu neschoduje pak přeruší protokol.

2. Alice a Bob si nyní předávají informaci za pomocí zbylých n bitů.

Vliv kvantové mechaniky na klasickou kryptografii

Kvantové počítače, přinášejí lepší algoritmy na řešení některých problému, na kterých jsou založeny klasické protokoly.

Např. **Shorův** algoritmus na faktorizaci celých čísel. Faktorizuje v polynomiálním čase $\mathbf{O}((logN)^3)$

Je tedy nutné zohlednit existenci takovýchto algoritmů při vytváření nových kryptografických protokolů.

Závěr

Kvantová mechanika přináší:

1. Náhodné procesy
2. „Bezpečné“ protokoly
3. Nové algoritmy pro řešení klasických problému za pomocí kvantových počítačů.

Závěr

Děkuji za pozornost!