Kvantová kryptografie

Jan Horáček

České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská

Obsah prezentace

Úvod do užité kvantové mechaniky

- chování částic v kvantové mechanice
- princip superpozice

Obsah prezentace

Úvod do užité kvantové mechaniky

- chování částic v kvantové mechanice
- princip superpozice

Kvantové kryptování

- principy kvantového kryptování
- protokol BB84
- protokol E91

Chování částic v kvantové mechanice

- nelze změřit vlastnosti částice bez jejího ovlivnění
- chování lze určit jen s jistou pravděpodobností
- nelze určit přesně rychlost a zároveň polohu částice

Princip superpozice

Vlastnosti superponované částice

- nachází ve více stavech zároveň
- měření způsobí kolaps do jediného náhodného stavu

K měření dochází

- při měření člověkem
- při náhodném působení částic

Základní principy

- Kvantové kryptování řeší, pomocí poznatků kvantové mechaniky, problém bezpečné distribuce klíčů
- Kanál neslouží k přenosu tajné informace, ale k výrobě a přenosu dokonale náhodného klíče
- Kryptovací kanál není utajený, ale odposlech není schopen rekonstruovat celý klíč a zároveň je detekován

Princip přenosu

- Protokol BB84 využívá polarizace fotonů v přímočaré rovině ($+$) a v rovině diagonální ($\times$).
- Fotony jsou vysílány ve 4 polarizačních stavech pootočených od sebe o 45° ($\uparrow$, $\nearrow$, $\rightarrow$, $\searrow$).
- Foton polarizovaný v rovině filtru projde.

Bitové stavy fotonu :

Rovina	0	1
$+$	$\uparrow$	$\rightarrow$
$\times$	$\nearrow$	$\searrow$

Příklad přenosu

Alicin náhodný bit	0	1	1	0	1	0	0	1
Alicina náhodná polar. rovina	+	+	×	+	×	×	×	+
Pol. Alicina vyslaného fotonu	↑	→	↘	↑	↘	↗	↗	→
Bobova náhodná polar. rovina	+	×	×	×	+	×	+	+
Polar. fotonu naměřená Bobem	↑	↗	↘	↗	→	↗	→	→
Veřejná domluva užitých polarizačních rovin								
Sdílený tajný klíč	0		1			0		1

Detekce odposlechu

Alicin náhodný bit	0	1	1	0	1	0	0	1
Alicina náhodná vysílací rovina	+	+	×	+	×	×	×	+
Pol. Alicina vyslaného fotonu	↑	→	↘	↑	↘	↗	↗	→
Evina náhodná přijímací rovina	+	×	+	+	×	+	×	+
Pol. fotonu naměř. a vysl. Evou	↑	↗	→	↑	↘	→	↗	→
Bobova náhodná přijímací rovina	+	×	×	×	+	×	+	+
Polar. fotonu naměřená Bobem	↑	↗	↗	↘	→	↗	↑	→
Veřejná domluva užitých polarizačních rovin								
Sdílený tajný klíč	0		1			0		1
Chyby v klíči	✔		✗			✔		✔

Výhody a nevýhody BB84

Výhody :

- lze vysílat po optickém kabelu
- fotony lze snadno polarizovat a měřit

Nevýhody :

- foton nemusí dorazit k příjemci
- foton nemusí být detekován

Princip přenosu

- Jsou vytvořeny 2 fotony v korelované superpozici (mají každý opačný spin, ale je mezi ně rozdělen náhodně)
- Po změření spinu fotonu příjemce ví, že protistrana dostala opačnou hodnotu
- Odposlech naruší kvantovou korelaci a začnou platit klasické Bellovy nerovnosti
- Vysílající a příjemce si vymění několik bitů a porovnáním objeví případný odposlech

Výhody a nevýhody E91

Výhody :

- Měření není závislé na rovinách měření (nemusíme zahazovat bity)

Nevýhody :

- Superponovaný stav podléhá rychle dekoherenci
- Dekoherence se může jevit jako odposlech
- Tvorba korelovaných superponovaných fotonů je náročnější, než jejich polarizace u protokolu BB84

Literatura

CZ Wikipedia
http://cs.wikipedia.org/wiki/Kvantová_kryptografie

US Wikipedia
http://en.wikipedia.org/wiki/Quantum_cryptography