Kvantová kryptografia

Dušan Kladivík

395642

Vernamova šifra

- Gilbert Vernam, 1917
- Najdôležitejšia šifra pre kvantovú kryptografiu
- Šifrovanie:
  - Každé písmeno správy posunieme o daný počet znakov kľúča.
- Dešifrovanie:
  - Opačný postup

Vlastnosti

- Bez znalosti kľúča – nemožné prelomiť
- Nepodmienená bezpečnosť
- Neprelomiteľnosť – exaktne matematicky dokázaná
- Akákoľvek množina znakov

- Podmienky
  - Kľúč je rovnako dlhý ako prenášaná správa.
  - Kľúč je dokonale náhodný.
  - Kľúč nemožno použiť opakovane.

Príklady

- Koniec abecedy, odznova

- kľúč (3, 5, 2, 7),
  - slovo DMQQ bude dešifrované ako AHOJ
- kľúč (2, 1, 8, 6),
  - slovo DMQQ bude dešifrované ako BLIK
- kľúč (2, 21, 3, 2),
  - Slovo DMQQ bude dešifrované ako BRNO

Prax

- Kľúč - rovnako dlhý ako správa
- Zložité generovanie – dokonale náhodný.
- Znalosť kľúča – iba A a B.
  - Bezpečný spôsob distribúcie kľúča
- Neefektívnosť – 2MB kľúč, 2MB data
- Zriedkavé použitie

Kvantová mechanika

- Princípy
  - Dokonalá náhodnosť
  - Meranie ovplyvňuje stav (Heisenberg)
  - Nemožnosť merania určitých párov veličín súčasne
- Výroba a distribúcia kľúča
- Vernamova šifra – nezabezpečený kanál
- Odpočúvanie nieje neodhaliteľné

Komunikácia

- Kvantový systém (fotóny), polarizácia (meranie)
- Odpočúvanie kanála – meranie veličín.
  - Akékoľvek meranie systém ovplyvňuje, mení jeho stav
    - detekcia odpočúvania

- Postup:
  - Odosielateľ nastaví fyzický systém do známeho kvantového stavu a pošle ho príjemcovi.
  - Príjemca vykoná meranie jednej z dvoch určitých veličín
  - Opakuje sa kým nebude dostatok hodnôt

Postup

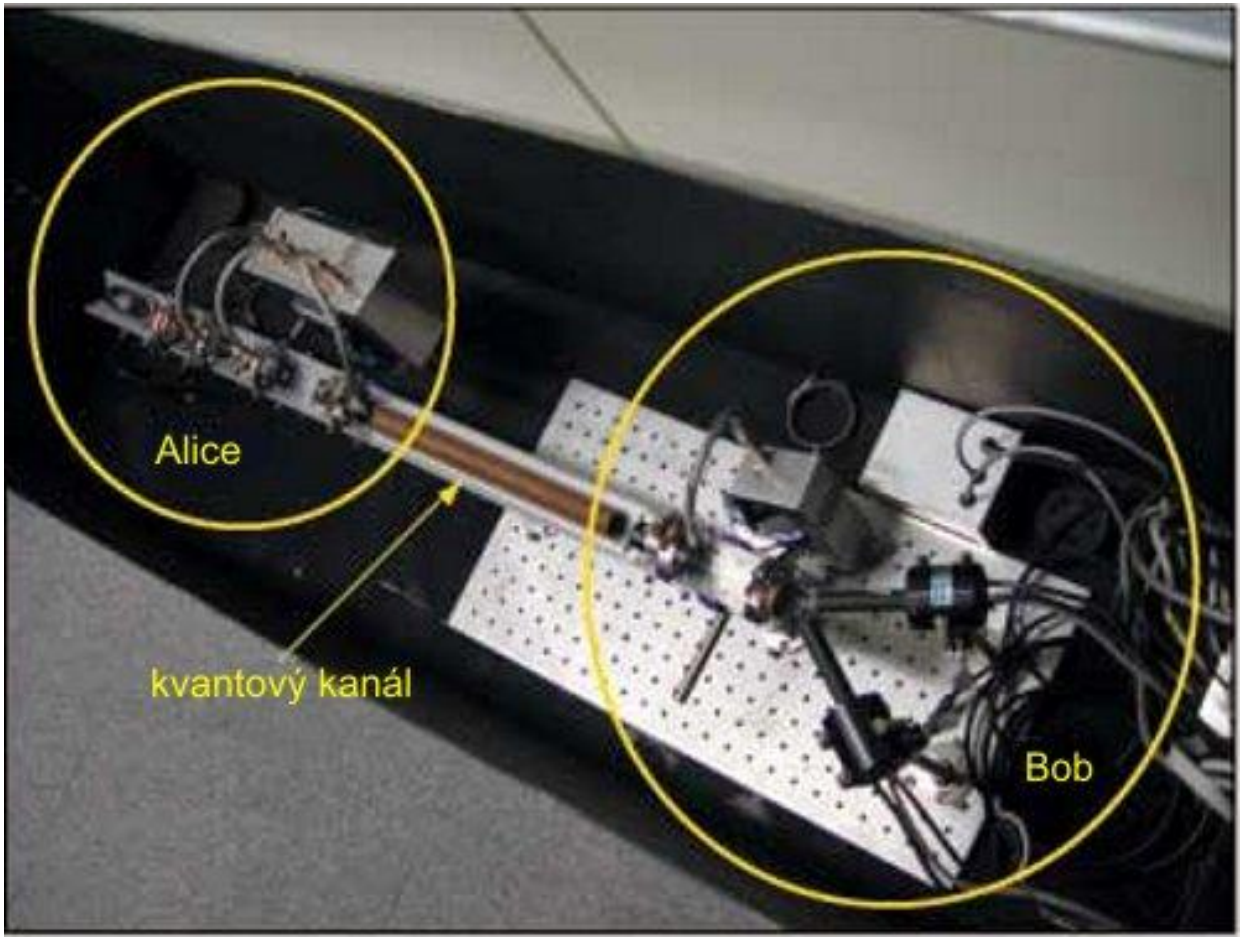
- Referenčná rovina
- Dve polarizačné bázy
  - množiny rovín, v ktorých fotóny kmitajú
    - vertikálne-horizontálna, odklonená od referenčnej roviny o 0° alebo 90°.
    - diagonálne-antidiagonálna, fotóny oscilujú v otočených rovinách o 45° alebo 135°.

Polarizačný stav	Bitová hodnota	Báza
→	0	+
↑	1	+
↗	0	×
↖	1	×

Prax

- Polarizácia - kryštál $CaCO_3$,
  - Horizontálne polarizované fotóny prejdu priamo
  - Vertikálne polarizované odkláňa mimo osi smeru pohybu
- Smer diagonálne polarizovaných fotónov
  - Na 50% sa odklonia od pôvodnej osi (polarizácia sa zmení na vertikálnu)
  - Na 50% prejdú priamo (kmitajú horizontálne)
- Výsledok merania
  - Meranie v diagonálnej báze nič nehovorí o pôvodnom smere kmitania fotónov polarizovaných v horizontálne-vertikálnej báze.
- Meracie bázy sú komplementárne
  - Nemôžnosť bez zmeny stavu merať súčasne v oboch bázach
- Diagoálne-antidiagonálna báza
  - Natočenie mriežky kryštálu o 45°
  - Vyhodnocovanie polarizácií je podobné

Prvý systém kvantovej kryptografie



Charles Bennett, John Smolin (1989), Kvantový kanál je dlhý 30 cm.

Protokol BB84

- Charles Bennett a Gilles Brassard, 1984
- Polarizácia fotónov
- Na prenos informácií - dva kanály:
  - Klasický (internet) - správa
  - Kvantový - kľúč
- Nerieši celú bezpečnosť komunikácie,
  - Iba dohodu a prenos tajného kľúča

Distribúcia kľúča

1. A generuje náhodné bity
2. A náhodne volí bázy
3. A kóduje bity do polarizácie fotónov a odosiela ich B
4. B náhodne volí bázy
5. B v nich meria prijaté fotóny
6. B dekóduje bity
7. A a B sa verejne dohovoria, na ktorých bázach sa zhodli
8. A a B obetujú niektoré bity na detekciu odposluchu
9. Všetky kontrolné bity sa zhodujú - E nepočúva
10. Zvyšné bity tvoria tajný kľúč pre Vernamovu šifru

1	1	0	0	0	1	1
2	×	×	+	×	×	+
3	↖	↗	→	↗	↖	↑
4	+	×	×	×	×	+
5	↑	↗	↖	↗	↖	↑
6	1	0	1	0	1	1
7		OK		OK	OK	OK
8				0	1	
9				OK	OK	
10		0				1

Vlastnosti BB84

- Bez autentizácie verejného kanálu
- Ak Eva vytrvale odpočúva Alica s Bobom sa nedohodnú
- Nemožnosť použiť zosilňovač – efektívne max 50 km
  - Rekordná vzdialenosť 122 km, rýchlosť 2 kbps
- Počet odoslaných fotónov >= 2x počet bitov správy
- Eva môže len odpočúvať, merať
  - Nesprávna báza, Bob nameria náhodný stav
- 50% správny, 25% iný
- Pri 32bitoch 99,99% odhalenia

Záver

- Nepodmienená bezpečnosť
- Platnosť dnes známych prírodných zákonov
  - máločo je na svete tak spoľahlivé ako prírodné zákony
- Absolútne bezpečná

Záver

- Nepodmienená bezpečnosť
- Platnosť dnes známych prírodných zákonov
  - máločo je na svete tak spoľahlivé ako prírodné zákony
- Absolútne bezpečná

Ďakujem za pozornosť

Literatúra

- http://kaleidoskop.upol.cz/old/kal2004/Dusek/Dusek.pdf
- http://www.aldebaran.cz/bulletin/2005_14_kry.php
- http://blackhole.sk/topickvantova-kryptografia-i-uvod-do-sifier
- http://www.krypta.cz/articles.php?ID=130
- http://www.lupa.cz/clanky/kvantova-kryptografie-pro-bezpecnou-distribuci-klicu/
- http://server.gphmi.sk/pages/sifry/kvant.html
- https://www.google.com/