KVANTOVÁ KRYPTOGRAFIA

Erika Buffová, 3Alb

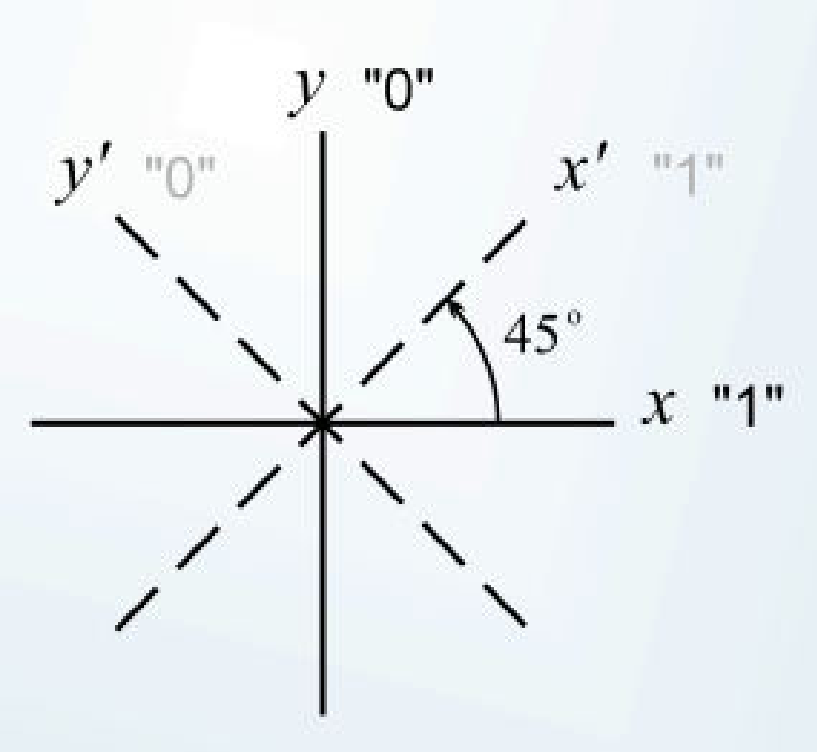
Čo je to ?

- obor využívajúci **kvantovú mechaniku**
- rieši problém **bezpečnej distribúcie kľúča** medzi **odosielateľom** a **príjemcom** + umožňuje spoľahlivú **detekciu odposluchu**
- **1. kvantový** kryptografický **protokol** - 1984 (Bennett & Brassard) - **BB84**

Princíp kvantovej kryptografii

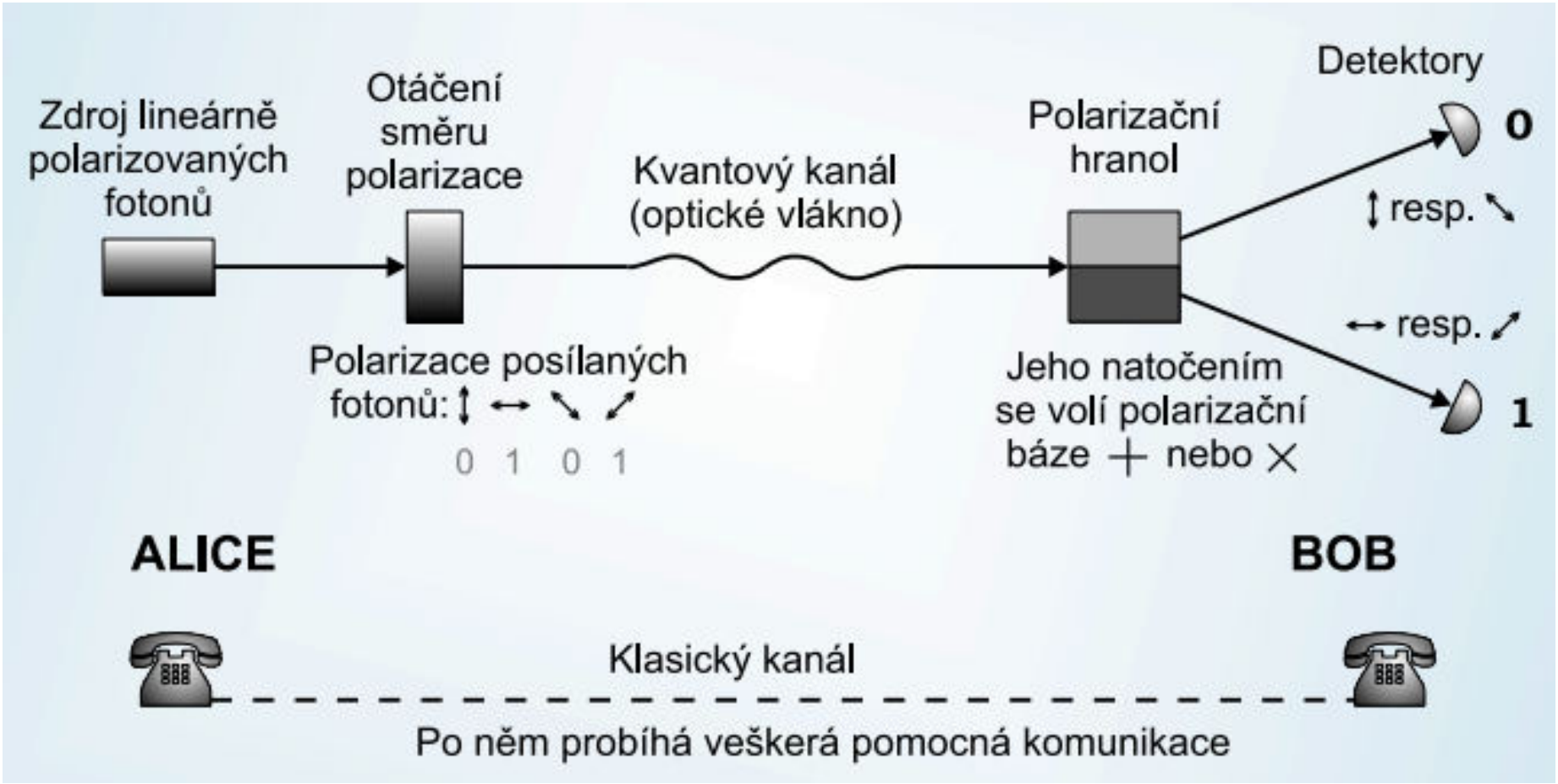
- **polarizačné kódovanie**

- Binárne signály **0** a **1** su kodované do **dvoch** vzájomne kolmých **lineárnych polarizacií** z dvoch polarizačných báz **pootočených o 45 stupňov**.



http://optics.upol.cz/userfiles/file/prezent-krypto.pdf

Schéma pre kvantový prenos kľúča



http://optics.upol.cz/userfiles/file/prezent-krypto.pdf

Princíp kvantovej kryptografii

- Predpokladajme, že Alica a Bob používajú rovnakú bázu **+**, tj. [x, y].

- Alica posiela sekvenciu núl a jednotiek (teda **vertikálne** a **horizontálne** polarizovaných fotónov)

- Bob **prijíma rovnakú sekvenciu bitov**, ktorú Alica poslala, pretože používa rovnakú polarizačnú bázu

A čo odposluch ?

- Fotón **nie je** možné **klonovať** (nevytvoríme kópiu)
- Fotón **nejde** ani **rozdeliť** - **buď** pokračuje k **Bobovi alebo** odbočí k **Eve**, ale potom príslušný bit nebude možné použiť v kľúči (isté straty povolené)

- Rozumná **stratégia** :
  - **merianie** podobným zariadením, aké má Bob a potom **odosielanie** každého bitu podobným zariadením, aké má Alica
  - Eva **nepozná** polarizačnú **bázu** !

A čo odposluch ?

- Eva **nepozná** bázu, takže spôsobí **chyby**
- Avšak je **možné odhalenie** bázy

- Preto Alica a Bob musia **striedať + a x** náhodne a nezávisle

- Po prenose si povedia, ktoré bázy použili a **nechajú** si len **bity**, pre ktoré boli použité **rovnaké bázy**

- Keď **Eva pozná** bázu, tak priemer je **50 %**
- Keď **Eva nepozná** bázu, tak prieme je **50 %**

BB84 - Kvantový prenos

1. Alica **vyberie** náhodné **bity**
2. Alica náhodne **vyberie** vysielajúcu **polarizačnú bázu**
3. Alica **kóduje bity** pre polarizáciu posielaných fotónov
4. Bob náhodne **vyberá** prijímajúcu **polarizačnú bázu**
5. Bob **zaznamenáva** prijaté **bity** (možná strata niektorých fotónov)

BB84 - Verejná diskusia

6. Bob **oznamí bázu**, v ktorej nameral fotóny
7. Alica **oznamuje**, ktoré bázy boli správne **"uhadnuté"**
8. Ak sa Alica a Bob **zhodli v bázach**, prenesené **bity si ponechajú** (Eva neodpočúvala a Bob má presne to, čo Alica poslala)

BB84 - Obetovanie bitov

9. Bob **obetuje** niektoré náhodne vybraté bity kvôli **odhaleniu** Evy
10. Alica **potvrdzuje** tieto **obetované** bity
    (Eva by spôsobila odchýlky)
11. Zvyšné **tajné bity** zdieľané medzi Alicou a Bobom **tvoria kľúč**

- **zásluha** :
  Charles **Bennet** & Gilles **Brassard**

Čo tak dať si príklad ?

Oprava chýb a zosilnenie utajenia

- Chyby spôsobuje nielen Eva ale aj **nepresnosti** a **šum** zariadení.

- **Oprava ?**
  - Nemôžeme si byť istý, že **chyby nepochádzajú z odposluchu** (Eva mohla vymeniť prenosovú linku za lepšiu)

- **Zosielnenie utajenia?**
  - možnosť uhadnutia **maximálnej informácie**, ktorú Eva dosiahla
  - Z pôvodného kľúča sa vyrobí **nový**, **kratší**, o ktorom má Eva **minimálnu** znalosť

Ďakujem za pozornosť