Studium fyziky v podání kvantového experimentátora

Bc. Jiří Fadrný

Univerzita Palackého Olomouc, Přírodovědecká fakulta, Katedra optiky

27. ledna 2019

Outline

Úvod do kryptografie

1. Kryptografie je věda zabývající se bezpečným přenášením informací. (zprávy, fotky, hudba,...)
2. Zpráva se šifruje tak, aby byla čitelná jen tomu, komu je určena.
3. Využívá se ve vojenství, bankovnictvý,...

Příklad jednoduché šifry — binární reprezentace

Počítače používají binární kodování — povídají si pomocí jedniček a nul.

A	h	o	j
01000001	01101000	01101111	01101010

Příklad jednoduché šifry

$\Longrightarrow$ Ukažme si princip Vernamovi šifry.

1. Matematicky dokázaná bezpečnost
2. Závislá na schopnosti bezpečně přenést náhodný klíč

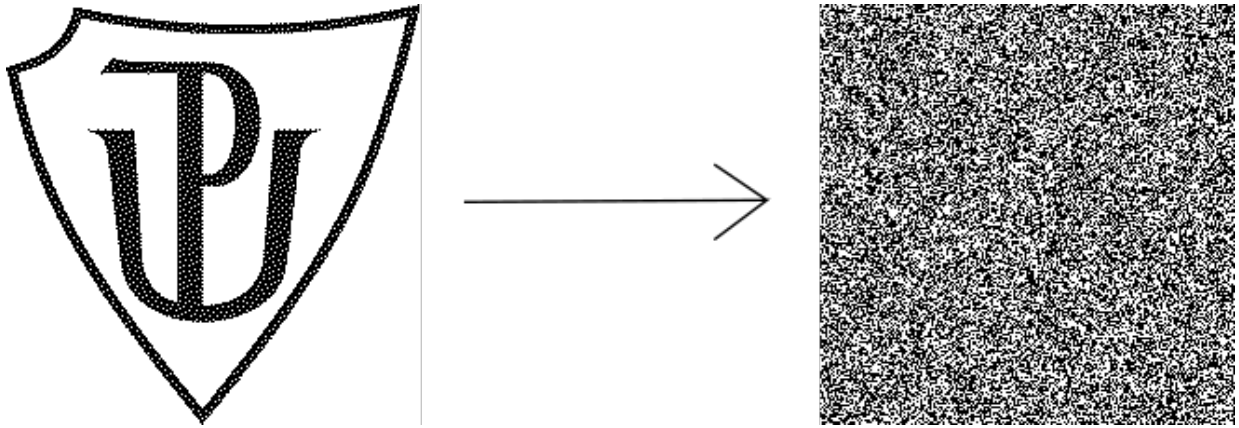
Zpráva	1	1	0	0
Klíč	1	0	1	0
Šifrovaná zpráva	0	1	1	0

Příklad jednoduché šifry

$\Longrightarrow$ Ukažme si princip Vernamovi šifry.

1. Matematicky dokázaná bezpečnost
2. Závislá na schopnosti bezpečně přenést náhodný klíč

Zpráva	1	1	0	0
Klíč	1	0	1	0
Šifrovaná zpráva	0	1	1	0



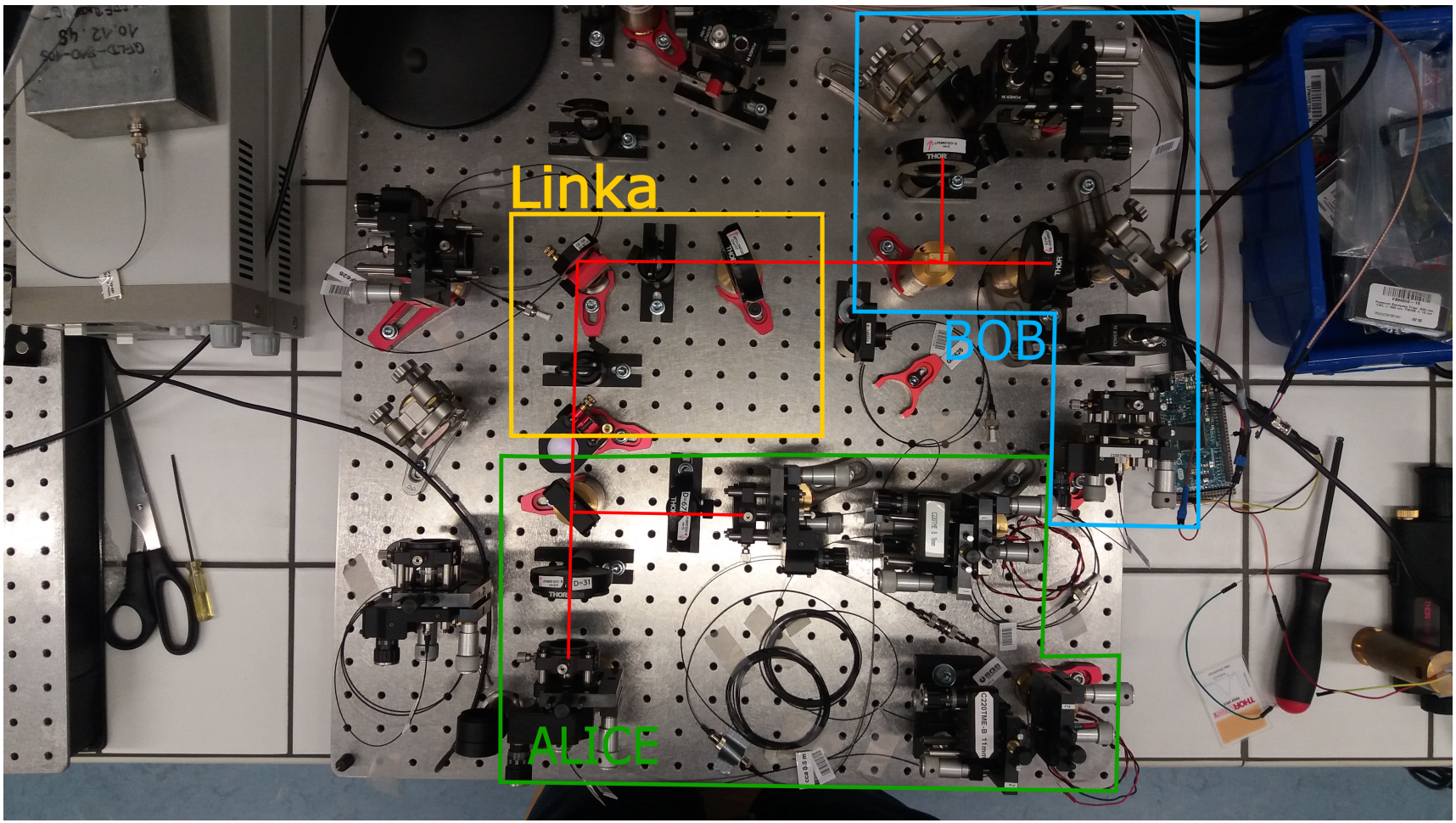
Moje práce — Kvantové sdílení tajného klíče

1. Pro každou zprávu je třeba sdílet nový/unikátní klíč
2. Mojí prací je sdílet takový klíč mezi dvěma místy
3. Hádejte jak to děláme :) Posíláme informaci ve světlu

Kvantové sdílení tajného klíče

1. Pro přenášení klíče používáme světlo
2. Jednotlivá kvanta světla — fotony
3. Bity informace (jedničky a nuly) jsou kódovány do polarizace fotonů
4. Sdílení pomocí komunikační kvantové linky — kvantová fyzika umožňuje odhalit odposlech!

Kvantové sdílení tajného klíče



Studium a práce

1. Práce v laboratoři kvantové optiky je unikátní
2. Možnost vybrat si zajímavé téma
3. Pracuji pod vedením školitele, ale samostatně.
4. Stavět experiment je skoro jako stavět lego :)
5. Zahrnuje i čtení literatury, zpracování dat a programování
6. Standardně se vídám se školitelem a jsem v labu alespoň jednou týdně (podle času méně/více)
7. Za nadstandardní práci v labu nebo její reprezentaci lze získat finanční stipendia

Děkuji za pozornost