Quantum key distribution

Využití kvantové fyziky v kryptografii

Jan Štaffa, Jakub Macíček, Pavel Pazdziora

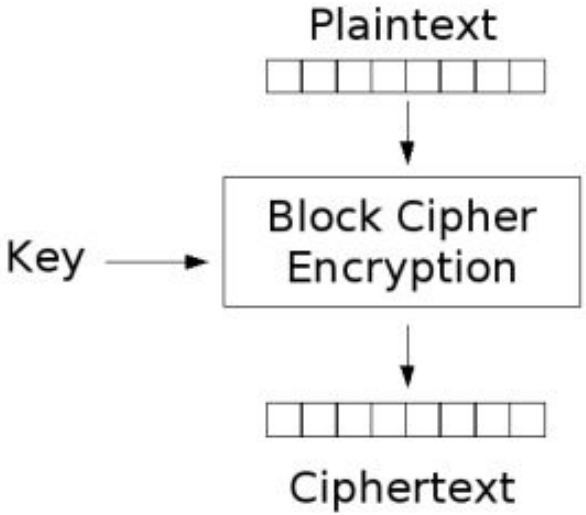
Úvod

- bezpečnost nade vše
- vzestup kvantových počítačů = hrozba
- jak ochránit naše data?

Kryptografie obecně

- **symetrické** x **asymetrické** klíče
- **symetrické** - prakticky neprolomitelné, pokud zůstane klíč tajný
- **asymetrické** - veřejný a osobní klíč, dá se prolomit

- **šifry** - Vernamova šifra, AES



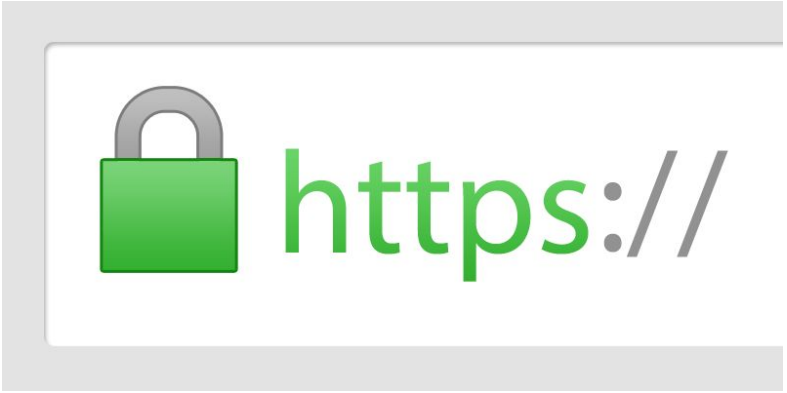
Minulost šifrování

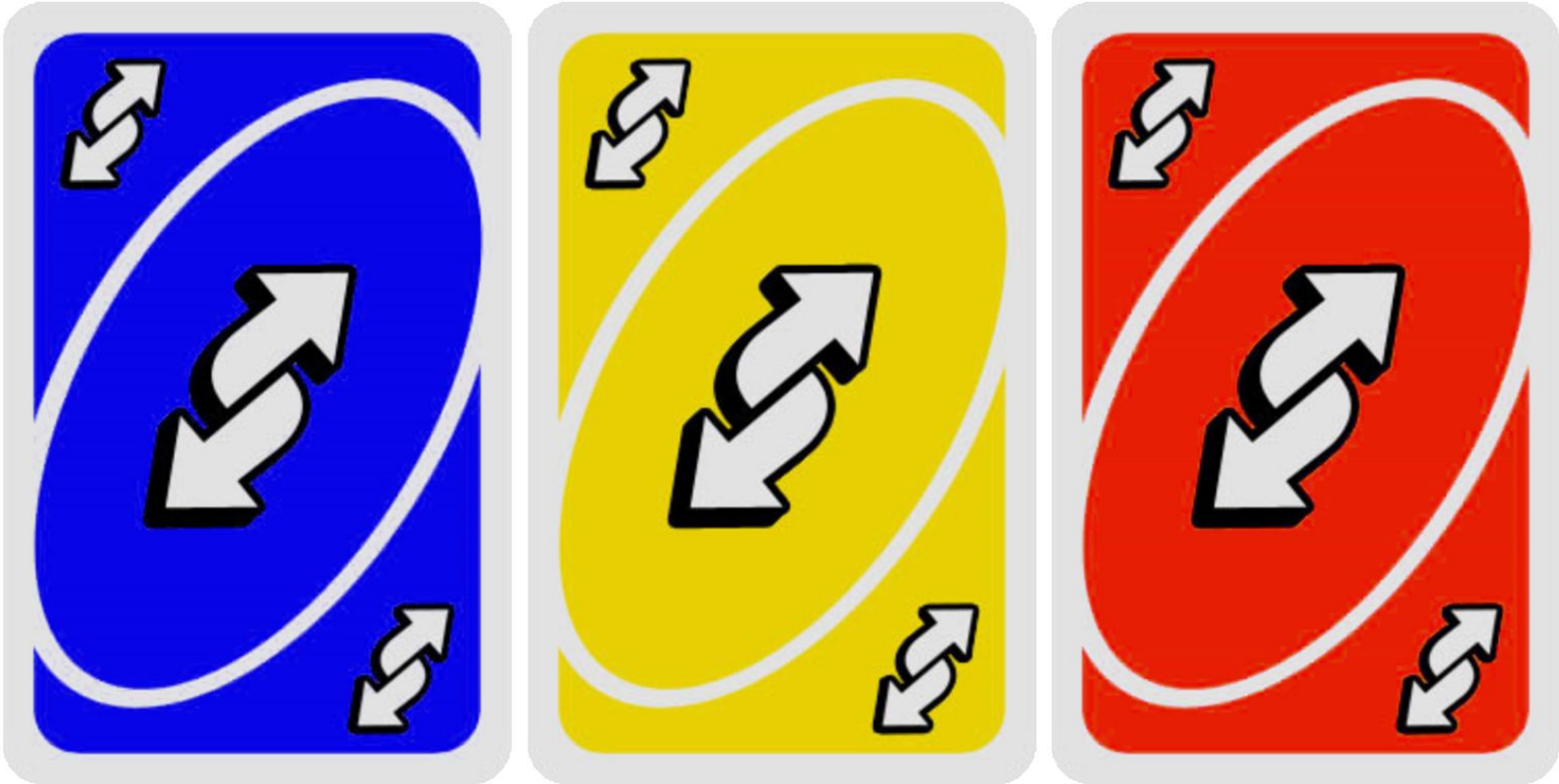
- symetrické klíče
- závislost na lidském faktoru

- Scytale

Současnost šifrování

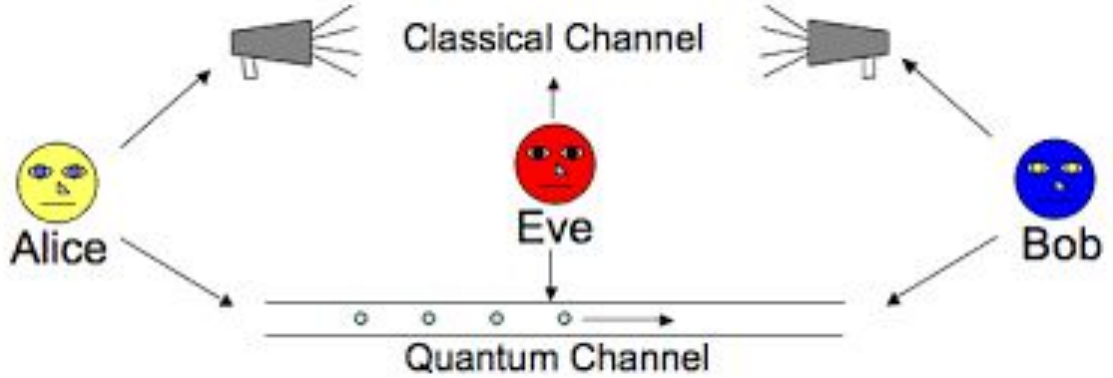
- asymetrické klíče
- HTTPS - RSA
- závisí na složitosti zpětného výpočtu některých matematických problémů
  - faktorizace čísla
- ohroženo kvantovými počítači



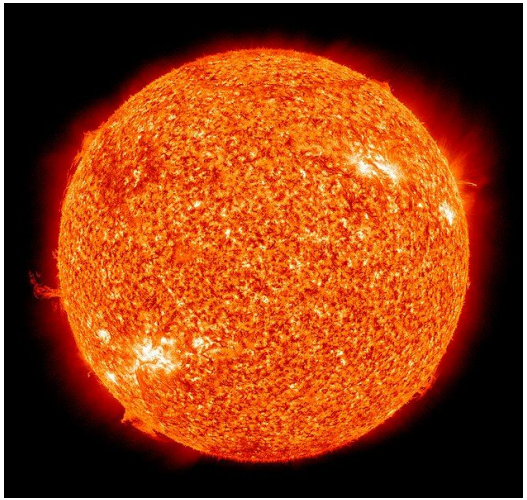


Kvantová mechanika a kryptografii

- využívá stavy fotonu k přenosu symetrického klíče
- znemožňuje osobě uprostřed získat tento klíč
- po získání klíče probíhá komunikace ve veřejném kanále



Jak získáme jeden foton?



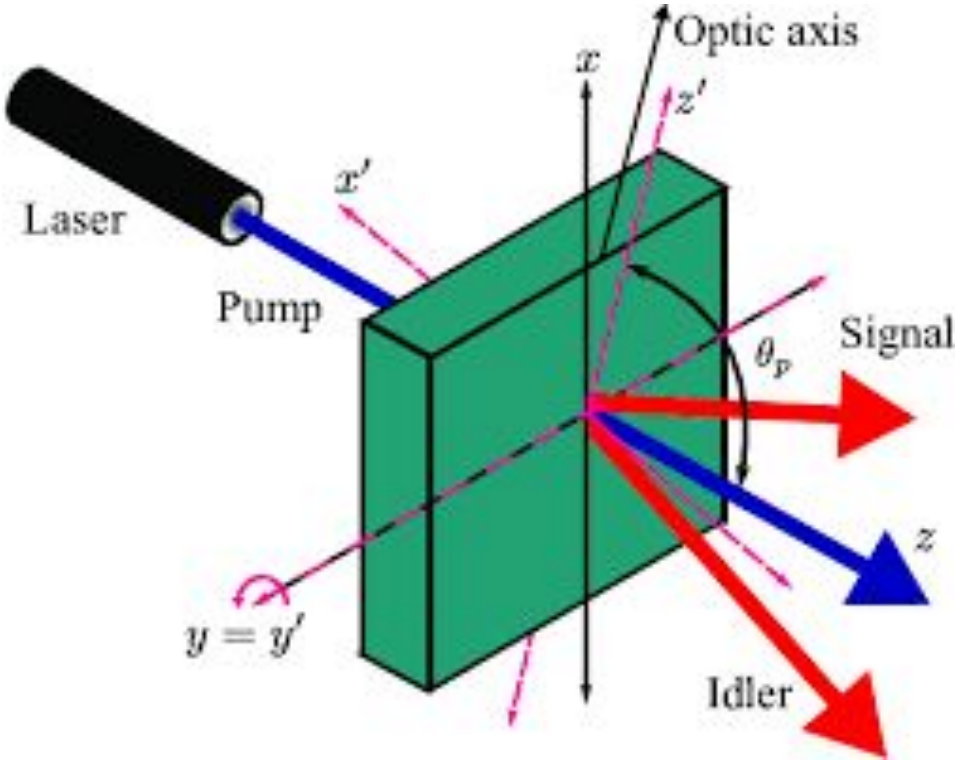
10^{45}

10^{20}

2.5e34

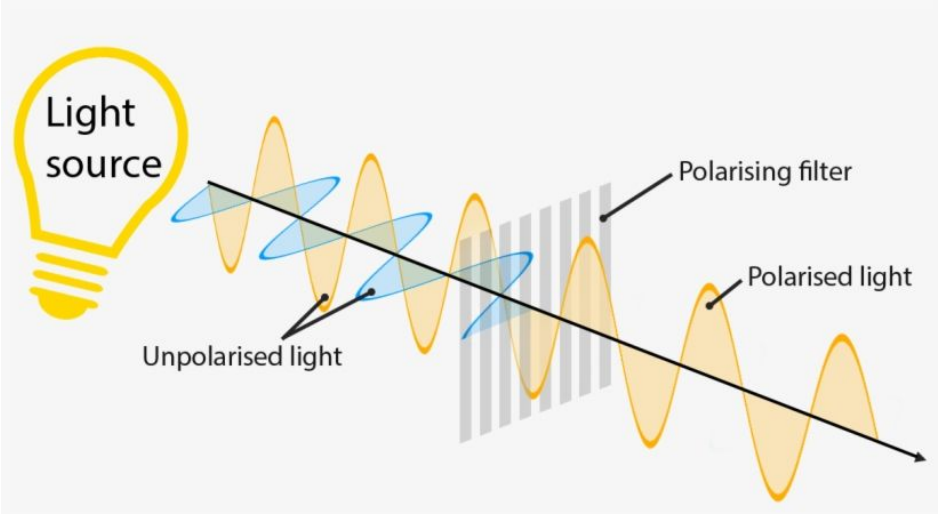
Jak získáme jeden foton?

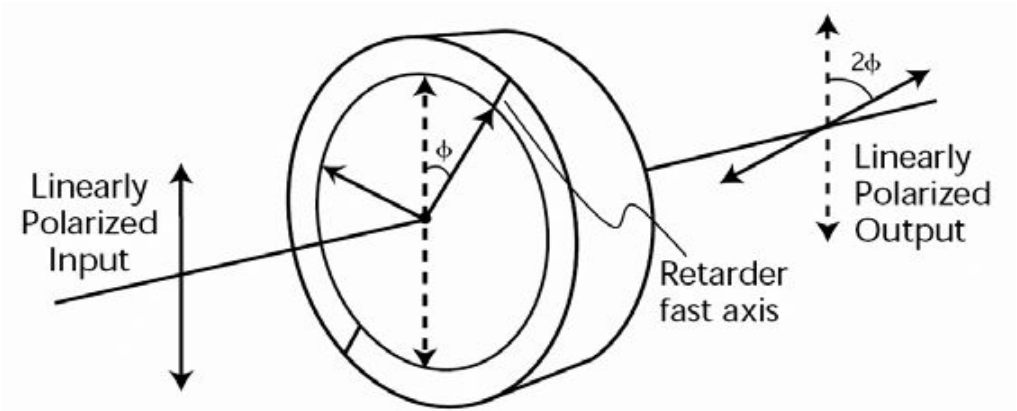
- nezískáme
- fotonové páry
- nonlineární krystaly



Polarizace

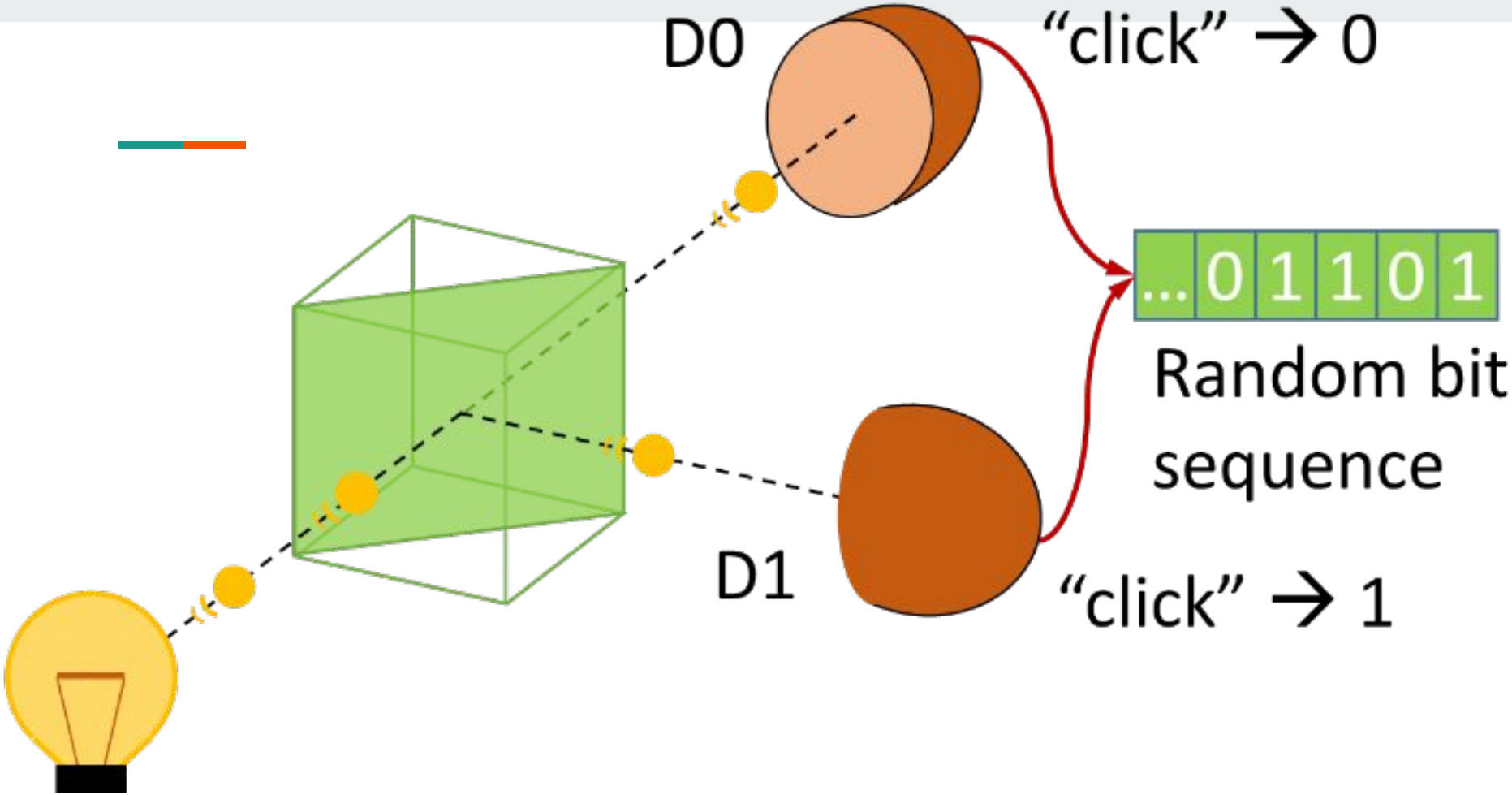
- změna směru vlnění fotonu
- polarizátor
- half-wave plate (vlnová destička)





Generace náhodných čísel

- **pravá** x **pseudo**-náhodná čísla
- **generace ze semena** - vždy stejný výsledek
- **pravé náhodné číslo nelze matematicky vypočítat**
  - vnější vstup
  - kvantová mechanika
- **opravdu náhodný bit** = 50% - 1, 50% - 0


D0
“click” → 0
...01101
Random bit sequence
D1
“click” → 1

BB84 Protocol

+	↑	→
×	↗	↘

Rectilinear Basis

Diagonal Basis

+	+	×	+	×	×	×	+
0	1	1	0	1	0	0	1
↑	→	↘	↑	↘	↗	↗	→

↑	↗	↘	↗	→	↗	→	→
0	0	1	1	0	0	1	1
+	×	×	×	+	×	+	+

Alice
(Sender)

Bob
(Receiver)

Výzkum

- jak je QKD bezpečné a jaká je chybovost?

qutools
CAUTION
CLASS 3B LASER RADIATION
WHEN OPEN.
AVOID EXPOSURE TO BEAM
CLASSIFIED ACCORDING TO IEC 60825-1:2015-07

Výsledky

Alice *a*	Alice *b*	Bob *p*	hodnota (nárazy/s)	pravděpodobnost	∢ P_1 (deg)	∢H_1 (deg)
0	0	0	4900	98%	100˚	5˚
1	0	0	180	4.5%	100˚	50˚
0	1	0	2400	43%	100˚	27.5˚
1	1	0	2400	43%	100˚	-17.5˚

Výsledky II.

rozdíl (deg)	rozmezí hodnot (nárazy/s)	pravděpodobnost
0˚	4700 - 5000	94% - 100%
±45˚	2000 - 2700	40% - 54%
90˚	150 - 200	3% - 3.9%

Děkujeme za pozornost

Zdroje obrázků

https://upload.wikimedia.org/wikipedia/commons/0/0c/Encryption.png

https://i.ytimg.com/vi/44G9UuB2RWI/maxresdefault.jpg

https://www.researchgate.net/profile/Suman-Karan-2/publication/328040517/figure/fig8/AS:902681551978500@1592227461834/The-coordinate-representation-of-the-nonlinear-crystal-in-both-lab-frame-x-y-z-and.png

https://www.researchgate.net/profile/Kristina-Irsch/publication/33429293/figure/fig5/AS:646814864797699@1531224089850/A-half-wave-plate-rotates-the-plane-of-linearly-polarized-light-by-twice-the-angle.png

https://upload.wikimedia.org/wikipedia/commons/thumb/9/94/Wire-grid-polarizer.svg/2560px-Wire-grid-polarizer.svg.png

https://qt.eu//app/uploads/2018/11/QNRG.png

https://media.wired.com/photos/5b1594a444335046642e3e8e/master/pass/WI070118_AP_LavaLamps_LO_01.jpg

https://upload.wikimedia.org/wikipedia/commons/5/51/Skytale.png