Kvantová kryptografie

aneb

ŠIFROVÁNÍ POMOCÍ FOTONŮ

Miloslav Dušek

Kvantová kryptografie je metoda pro bezpečný (utajený) přenos informací. Její bezpečnost je garantována fundamentálními zákony kvantové fyziky.

Vlastně jsem začal s kvantovou mechanikou,
ale někde cestou jsem odbočil špatným směrem

Kvantová fyzika a zpracování informace

Kvantová fyzika a zpracování informace

- Donedávna se o informaci uvažovalo jen v pojmech klasické fyziky. Kvantová mechanika hrála jen podpůrnou roli.

Kvantová fyzika a zpracování informace

- Donedávna se o informaci uvažovalo jen v pojmech klasické fyziky. Kvantová mechanika hrála jen podpůrnou roli.
- Informace je fyzikální (její zpracování je závislé na fyzikálním systému, v němž je zakódována).

Kvantová fyzika a zpracování informace

- Donedávna se o informaci uvažovalo jen v pojmech klasické fyziky. Kvantová mechanika hrála jen podpůrnou roli.
- Informace je fyzikální (její zpracování je závislé na fyzikálním systému, v němž je zakódována).
- Kvantové systémy se chovají jinak než klasické (podivuhodněji).
- Využití kvantových jevů nabízí řešení některých problémů neřešitelných v rámci klasické teorie informace.

Kvantová teorie informace

Kvantová teorie informace

- Spojuje kvantovou fyziku a klasickou teorii informace.
- „Kvantová teorie informace rozšiřuje klasickou teorii informace podobně jako komplexní čísla doplňují čísla reálná.“

Kvantová teorie informace

- Spojuje kvantovou fyziku a klasickou teorii informace.
- „Kvantová teorie informace rozšiřuje klasickou teorii informace podobně jako komplexní čísla doplňují čísla reálná.“

- Aplikace: **kvantové počítače**,
  kvantová kryptografie.


TEN POČÍTAČ JE ÚPLNĚ KVANTOVEJ.
JEN SE NA NĚJ PODÍVÁŠ, ZKOLABUJE.

Kryptografie

Kryptografie

- „Psaní tajným písmem“
- Informace musí být srozumitelná pouze tomu, komu je určena.

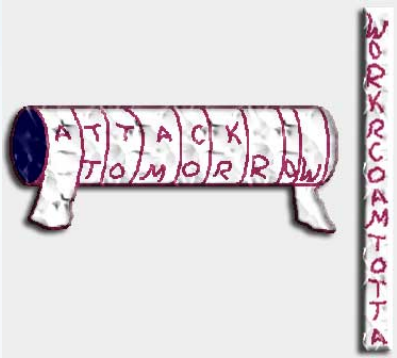
Kryptografie

- „Psaní tajným písmem“
- Informace musí být srozumitelná pouze tomu, komu je určena.
- Kryptologie { kryptografie (šifrování); kryptoanalýza (luštění)

Kryptografie – historie

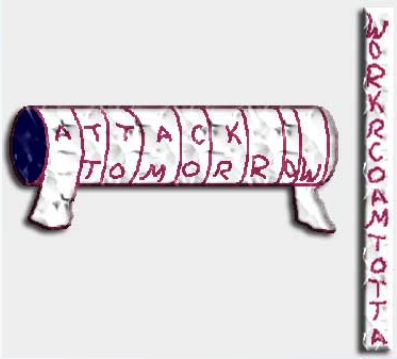
Kryptografie – historie

- Sparťanští velitelé šifrovali své zprávy na bojiště.



Kryptografie – historie

- Sparťanští velitelé šifrovali své zprávy na bojiště.



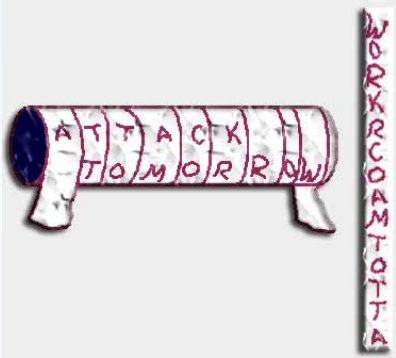
- Julius Caesar také šifroval zprávy do provincií:

$$A \to D, \quad B \to E, \quad C \to F, \quad D \to G, \quad \ldots$$

(podobná šifra je popsána i v Kámasútře).

Kryptografie – historie

- Sparťanští velitelé šifrovali své zprávy na bojiště.



- Julius Caesar také šifroval zprávy do provincií:

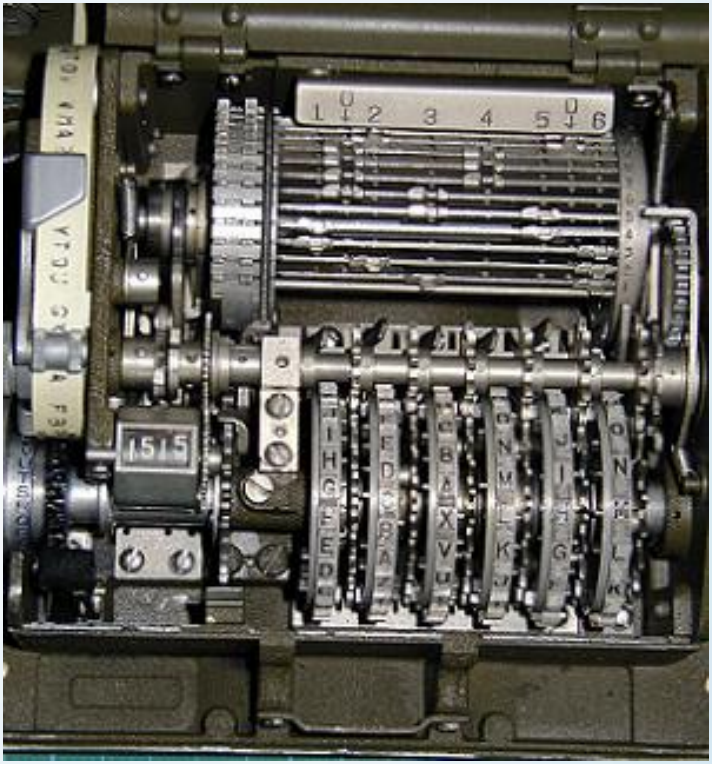
$$A \to D, \quad B \to E, \quad C \to F, \quad D \to G, \quad \ldots$$

(podobná šifra je popsána i v Kámasútře).

- Od r. 1920 automatizace šifrování (ENIGMA).

Kryptografie – historie

Kryptografie – historie



Kryptografie – současnost

- Složitější matematické algoritmy.

Kryptografie – současnost

- Složitější matematické algoritmy.
- **Symetrická kryptografie**
  (odesilatel i příjemce mají stejné klíče):
  - Proudové šifry
  - Blokové šifry

Kryptografie – současnost

- Složitější matematické algoritmy.
- **Symetrická kryptografie**
  (odesilatel i příjemce mají stejné klíče):

Proudové šifry:
Postupně se pozmění každý znak zprávy – obvykle pomocí nějaké pseudonáhodné posloupnosti.

Kryptografie – současnost

- Složitější matematické algoritmy.
- **Symetrická kryptografie**
  (odesilatel i příjemce mají stejné klíče):
  - Proudové šifry
  - Blokové šifry

Kryptografie – současnost

- Složitější matematické algoritmy.
- **Symetrická kryptografie**
  (odesilatel i příjemce mají stejné klíče):
  - Proudové šifry

Blokové šifry:
Zprávu šifrujeme po blocích. V ideálním případě závisí každý bit zašifrovaného bloku na všech bitech klíče a na všech bitech bloku zprávy.

Příklady: DES, AES.

Kryptografie – současnost

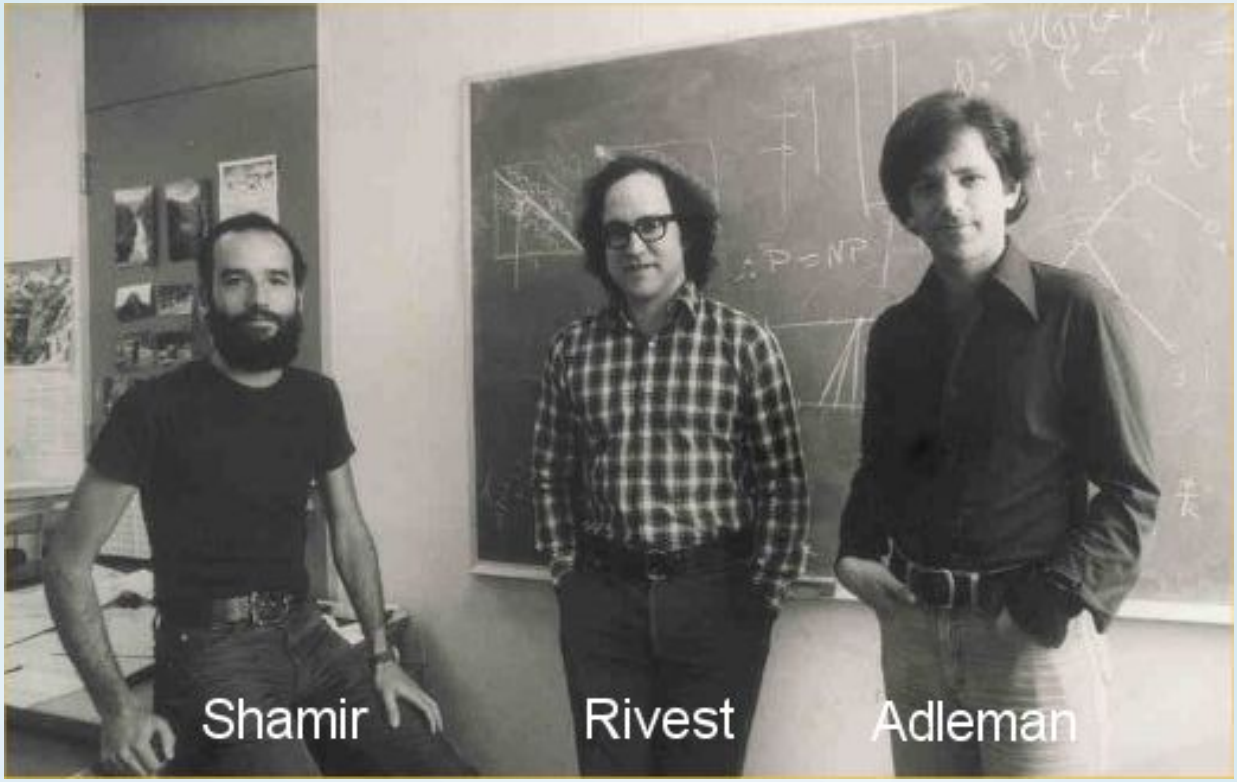
- Složitější matematické algoritmy.
- **Symetrická kryptografie**
  (odesilatel i příjemce mají stejné klíče):
  - Proudové šifry
  - Blokové šifry

Kryptografie – současnost

- Složitější matematické algoritmy.
- **Symetrická kryptografie**
  (odesilatel i příjemce mají stejné klíče):
  - Proudové šifry
  - Blokové šifry
- **Asymetrická kryptografie, s veřejným klíčem**
  (jeden klíč pro šifrování, jiný, tajný klíč pro dešifrování):
  - Např. algoritmus RSA

Algoritmus RSA (Rivest, Shamir, Adleman)

Algoritmus RSA (Rivest, Shamir, Adleman)



Algoritmus RSA (Rivest, Shamir, Adleman)

- Dvě velká prvočísla p a q — tajná.
- Jejich součin pq — veřejný.
- Dvě velká přirozená čísla d a e taková, že $(de-1)$ je dělitelné $(p-1)(q-1)$:

  e představuje veřejný klíč,
  d představuje tajný privátní klíč.

- P – zpráva, která má být zašifrována (ve formě čísla $P < pq$).
- C – výsledná šifra.
- Šifrování: $C = P^e \bmod pq$.
- Dešifrování: $P = C^d \bmod pq$.
- K přečtení zprávy bez znalosti privátního klíče d je třeba faktorizovat (rozložit na prvočinitele) číslo pq.

Luštění šifer

Luštění šifer

- Jednoduché šifry:
  - Zjišťování četnosti výskytu jednotlivých znaků (různá písmena se v přirozeném jazyku vyskytují různě často) nebo jejich dvojic a podobně.
  - Hledání očekávaných frází.
  - „Hrubá síla“ – vyzkoušení všech možných klíčů.

Luštění šifer

- Jednoduché šifry:
  - Zjišťování četnosti výskytu jednotlivých znaků (různá písmena se v přirozeném jazyku vyskytují různě často) nebo jejich dvojic a podobně.
  - Hledání očekávaných frází.
  - „Hrubá síla“ – vyzkoušení všech možných klíčů.
- Ale i rafinované matematické algoritmy lze v principu rozluštit.

Luštění šifer

- **Podstata asymetrických šifer:**
  Některé matematické operace jsou v jednom směru snadné, ale v opačném velmi nesnadné (tj. počet nutných operací roste prudce – exponenciálně – s délkou vstupu).

Luštění šifer

- **Podstata asymetrických šifer:**
  Některé matematické operace jsou v jednom směru snadné, ale v opačném velmi nesnadné (tj. počet nutných operací roste prudce – exponenciálně – s délkou vstupu).
- V případě **RSA** je tou „těžkou“ operací rozklad velkých čísel na prvočinitele

$$\mathbf{131} \times \mathbf{593} = \mathbf{77683}$$

$$\mathbf{77683} = ? \times ?$$

Luštění šifer

- Musí rozklad čísla o 129 cifrách trvat tisíce let?

Luštění šifer

- Musí rozklad čísla o 129 cifrách trvat tisíce let? NE!
  V r. 1994 bylo faktorizováno za 8 měsíců. V r. 1999 bylo dokonce rozlomeno RSA se součinem dlouhým 155 cifer.

Luštění šifer

- Musí rozklad čísla o 129 cifrách trvat tisíce let? NE!
  V r. 1994 bylo faktorizováno za 8 měsíců. V r. 1999 bylo dokonce rozlomeno RSA se součinem dlouhým 155 cifer.
- Výkon počítačů roste – obrana: prodlužování klíčů.

Luštění šifer

- Musí rozklad čísla o 129 cifrách trvat tisíce let? NE!
  V r. 1994 bylo faktorizováno za 8 měsíců. V r. 1999 bylo dokonce rozlomeno RSA se součinem dlouhým 155 cifer.
- Výkon počítačů roste – obrana: prodlužování klíčů.
- Není ovšem dokázáno, že neexistuje efektivní (tj. polynomiální) algoritmus pro faktorizaci.

Luštění šifer

- Musí rozklad čísla o 129 cifrách trvat tisíce let? NE!
  V r. 1994 bylo faktorizováno za 8 měsíců. V r. 1999 bylo dokonce rozlomeno RSA se součinem dlouhým 155 cifer.
- Výkon počítačů roste – obrana: prodlužování klíčů.
- Není ovšem dokázáno, že neexistuje efektivní (tj. polynomiální) algoritmus pro faktorizaci.
- Kvantové počítače by uměly faktorizovat mnohem rychleji než počítače klasické – hrozba nejen pro RSA !

Luštění šifer

- Musí rozklad čísla o 129 cifrách trvat tisíce let? NE!
  V r. 1994 bylo faktorizováno za 8 měsíců. V r. 1999 bylo dokonce rozlomeno RSA se součinem dlouhým 155 cifer.
- Výkon počítačů roste – obrana: prodlužování klíčů.
- Není ovšem dokázáno, že neexistuje efektivní (tj. polynomiální) algoritmus pro faktorizaci.
- Kvantové počítače by uměly faktorizovat mnohem rychleji než počítače klasické – hrozba nejen pro RSA !
- Ani bezpečnost ostatních klasických šifer není „absolutní“. Až na jednu výjimku.

Vernamova šifra (one-time pad)

- Gilbert S. Vernam, 1918.
- Bezpečnost této šifry lze matematicky dokázat.

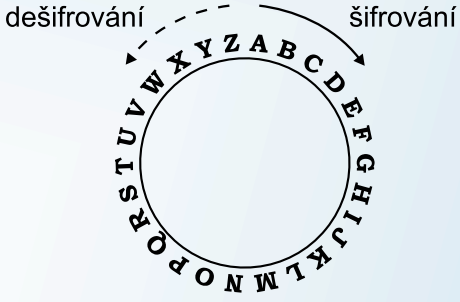
Vernamova šifra (one-time pad)

- Gilbert S. Vernam, 1918.
- Bezpečnost této šifry lze matematicky dokázat.
- Zpráva se „sečte“ se stejně dlouhou zcela náhodnou posloupností (ta představuje **klíč**). Výsledkem je náhodný sled znaků.
- „Neodečte-li“ se stejný klíč, je šifra zcela nečitelná.
- Každý klíč smí být použit jen jednou.
- Použití v diplomacii a špionáži (Bílý dům – Kreml, „atomový špión“ Klaus Fuchs, . . .)

Vernamova šifra (one-time pad)

Abeceda s 26 písmeny:

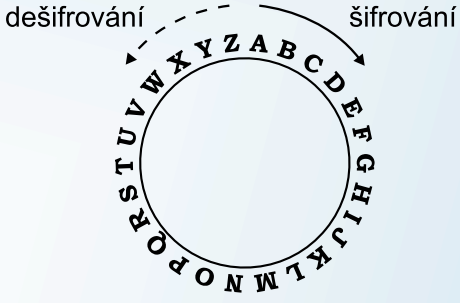
Zpráva:	V	E	R	N	A	M
Klíč:	7	23	11	5	0	16
Šifra:	C	B	C	S	A	C



Vernamova šifra (one-time pad)

Abeceda s 26 písmeny:

Zpráva:	V	E	R	N	A	M
Klíč:	7	23	11	5	0	16
Šifra:	C	B	C	S	A	C



Binární sekvence:

Zpráva:	1	1	1	1	0	0	0	0	↓
Klíč:	1	0	1	0	0	1	1	0	↓ ↑
Šifra:	0	1	0	1	0	1	1	0	↑

šifrování a dešifrování (XOR):

$$11 \rightarrow 0$$
$$10 \rightarrow 1$$
$$01 \rightarrow 1$$
$$00 \rightarrow 0$$

Problém distribuce klíče

Problém distribuce klíče

- Bezpečný přenos zprávy je podmíněn bezpečným přenosem klíče stejné délky (kryptografická Hlava XXII ?).
- Jak bezpečně přenést klíč ? (důvěryhodný kurýr? fyzická ochrana kanálu?)

Problém distribuce klíče

- Bezpečný přenos zprávy je podmíněn bezpečným přenosem klíče stejné délky (kryptografická Hlava XXII ?).
- Jak bezpečně přenést klíč ? (důvěryhodný kurýr? fyzická ochrana kanálu?)

- **Řešení: kvantová fyzika**.

Kvantová distribuce klíče

- Abeceda, do níž se kóduje = kvantové stavy jedné částice (např. fotonu, částice světla).

Kvantová distribuce klíče

- Abeceda, do níž se kóduje = kvantové stavy jedné částice (např. fotonu, částice světla).
- Odposlech se pozná – ovlivní stav částice.

Kvantová distribuce klíče

- Abeceda, do níž se kóduje = kvantové stavy jedné částice (např. fotonu, částice světla).
- Odposlech se pozná – ovlivní stav částice.
- Zjistí-li se odposlech, klíč se nepoužije – žádná informace neunikne!

Kvantová distribuce klíče

- Abeceda, do níž se kóduje = kvantové stavy jedné částice (např. fotonu, částice světla).
- Odposlech se pozná – ovlivní stav částice.
- Zjistí-li se odposlech, klíč se nepoužije – žádná informace neunikne!
- Kvantová kryptografie sice neumí odposlechu zabránit, ale umí ho odhalit – pro přenos klíče to stačí.

Kvantové měření

- Odposlech = měření na fyzikální entitě nesoucí informaci.

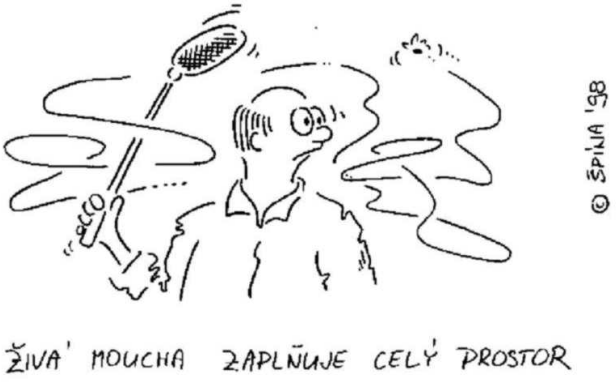
Kvantové měření

- Odposlech = měření na fyzikální entitě nesoucí informaci.
- **Klasická fyzika:**
  - Kteroukoli veličinu lze přesně měřit.
  - Vliv měření lze libovolně zmenšit.

Kvantové měření

- Odposlech = měření na fyzikální entitě nesoucí informaci.
- **Klasická fyzika:**
  - Kteroukoli veličinu lze přesně měřit.
  - Vliv měření lze libovolně zmenšit.
- **Kvantová fyzika:**
  - V určitých stavech některé veličiny nelze přesně změřit; opakování měření na přesných replikách systému vede k různým výsledkům.
  - Kvantové měření obecně stav systému podstatně změní !

Kvantové měření

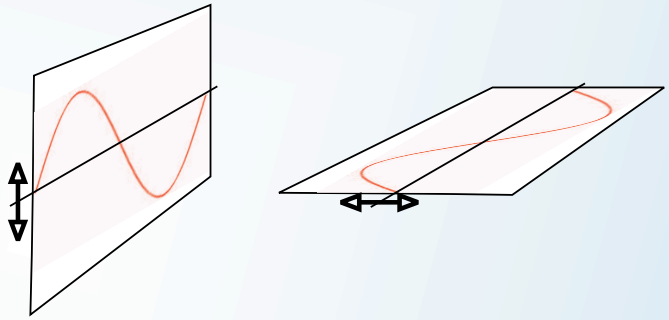


- **Kvantová fyzika:**
  - V určitých stavech některé veličiny nelze přesně změřit; opakování měření na přesných replikách systému vede k různým výsledkům.
  - Kvantové měření obecně stav systému podstatně změní !

Měření polarizace světla

Měření polarizace světla

- Lineární polarizace světla: vektor elektrického pole kmitá ve stále stejném směru:



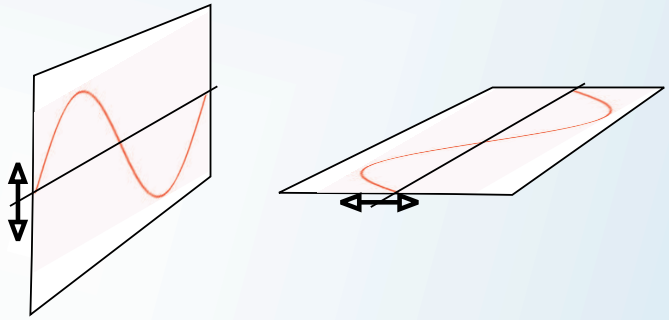
Vertikální polarizace

Horizontální polarizace

- Polarizace má dobrý smysl i v případě jednotlivých fotonů.

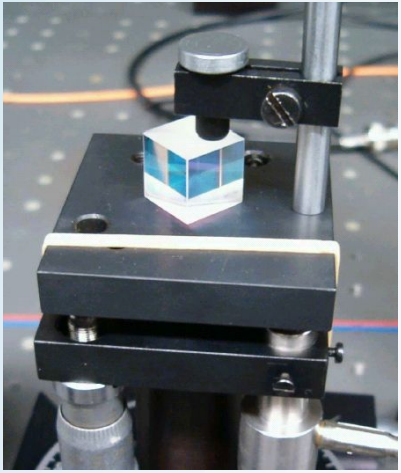
Měření polarizace světla

- Lineární polarizace světla: vektor elektrického pole kmitá ve stále stejném směru:

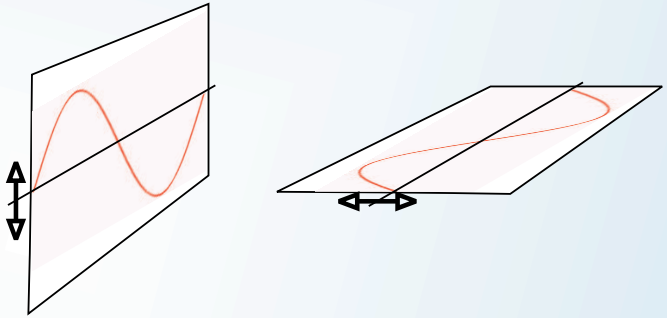


- Polarizace má dobrý smysl i v případě jednotlivých fotonů.
- Např. hranol z islandského vápence umí rozdělit obecnou polarizaci na dvě **kolmé** složky (určené natočením hranolu).

Měření polarizace světla

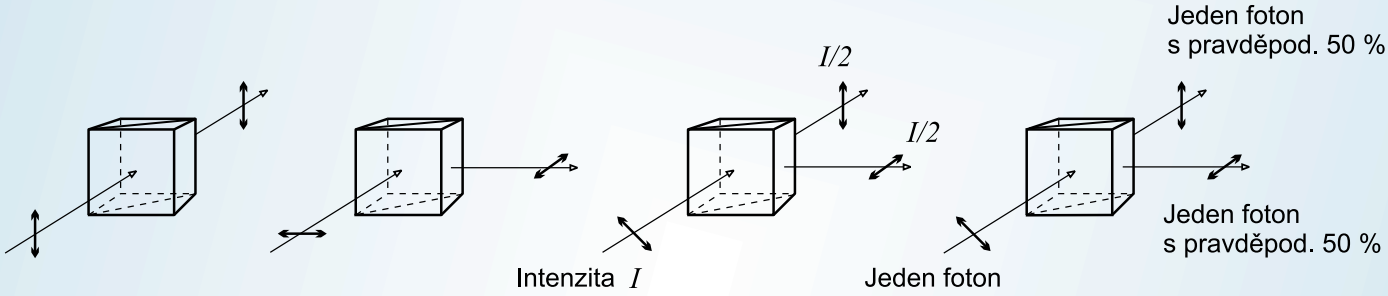


ce světla: vektor elektrického pole kmitá směru:

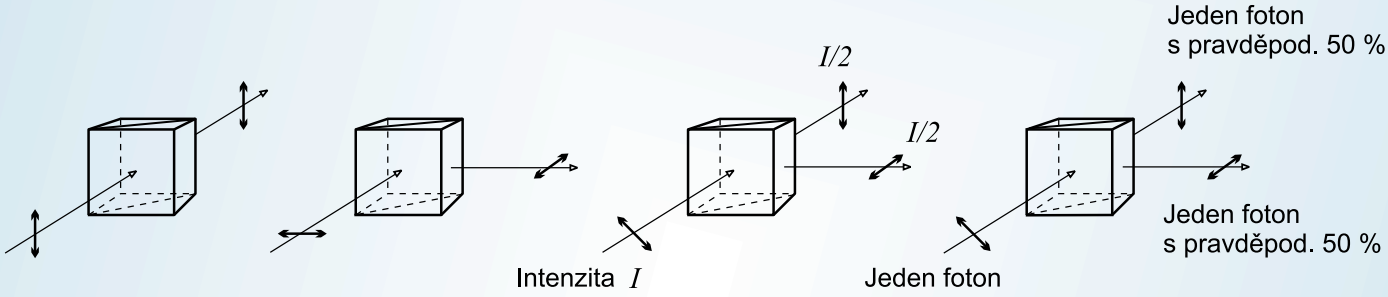


- Polarizace má dobrý smysl i v případě jednotlivých fotonů.
- Např. hranol z islandského vápence umí rozdělit obecnou polarizaci na dvě **kolmé** složky (určené natočením hranolu).

Měření polarizace světla



Měření polarizace světla



Jeden foton se nemůže rozdělit, je-li polarizován „šikmo“, spatříme ho buď projít nebo se odrazit. Jeho „volba“ je zcela **náhodná**. Po průchodu bude nadále polarizován **svisle**, po odrazu **vodorovně**.

Princip kvantové kryptografie
(polarizační kódování)

Princip kvantové kryptografie
(polarizační kódování)

Binární signály 0 a 1 jsou kódovány do dvou navzájem kolmých lineárních polarizací ze dvou polarizačních bází pootočených o $45°$:

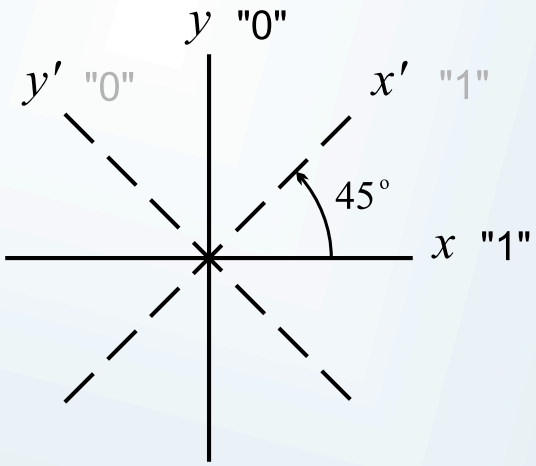
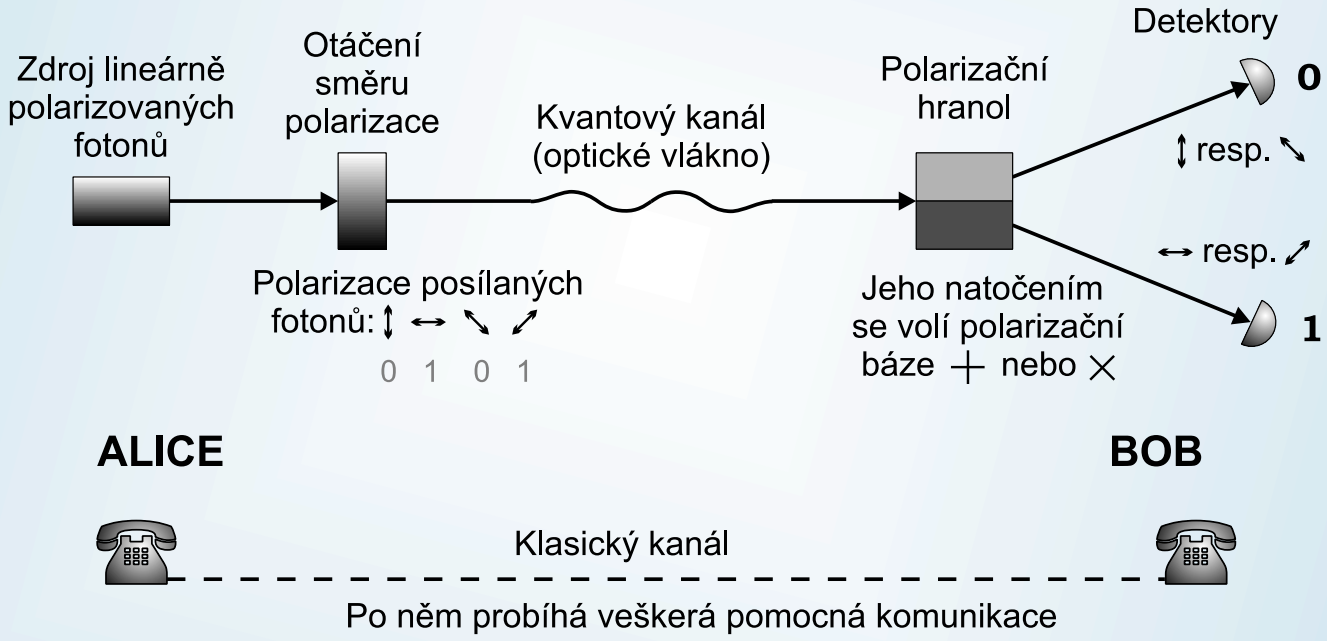


Schéma pro kvantový přenos klíče (polarizační kódování)



Princip kvantové kryptografie

Předpokládejme zatím, že Alice a Bob používají pouze bázi $+$, tj. $[x, y]$:

Princip kvantové kryptografie

Předpokládejme zatím, že Alice a Bob používají pouze bázi $+$, tj. $[x, y]$:

- Alice posílá náhodnou sekvenci nul a jedniček (tedy vertikálně a horizontálně polarizovaných fotonů).
- Protože Bob používá stejnou polarizační bázi jako Alice, je chování fotonů na jeho polarizačním hranolu zcela deterministické a Bob přijímá stejnou sekvenci bitů, jakou Alice poslala.

Princip kvantové kryptografie

Předpokládejme zatím, že Alice a Bob používají pouze bázi $+$, tj. $[x, y]$:

- Alice posílá náhodnou sekvenci nul a jedniček (tedy vertikálně a horizontálně polarizovaných fotonů).
- Protože Bob používá stejnou polarizační bázi jako Alice, je chování fotonů na jeho polarizačním hranolu zcela deterministické a Bob přijímá stejnou sekvenci bitů, jakou Alice poslala.
- **Co se stane pokud někdo odposlouchává ?**

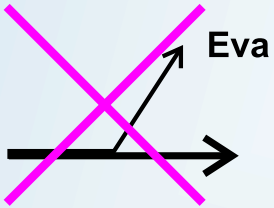
Odposlech

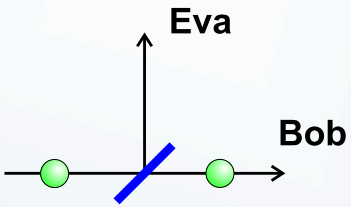
Jak lze odposlouchávat ?

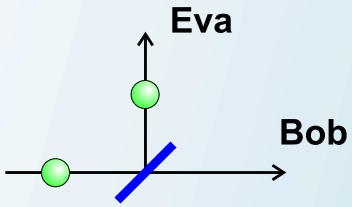
Odposlech

Jak lze odposlouchávat ?

- Pasívní odposlech, kdy se odvede část signálu, nepřichází v úvahu. Foton nelze rozdělit – buď pokračuje k Bobovi (Eva nemá nic), nebo odbočí k Evě, ale pak příslušný bit nebude použit v klíči (jisté ztráty se tolerují).



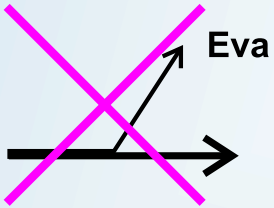


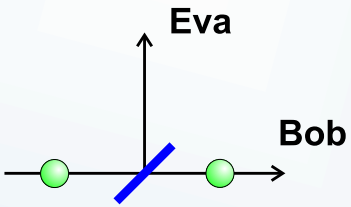


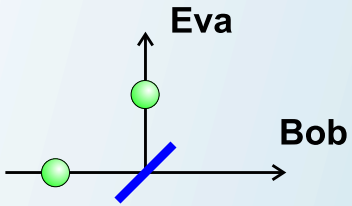
Odposlech

Jak lze odposlouchávat ?

- Pasívní odposlech, kdy se odvede část signálu, nepřichází v úvahu. Foton nelze rozdělit – buď pokračuje k Bobovi (Eva nemá nic), nebo odbočí k Evě, ale pak příslušný bit nebude použit v klíči (jisté ztráty se tolerují).



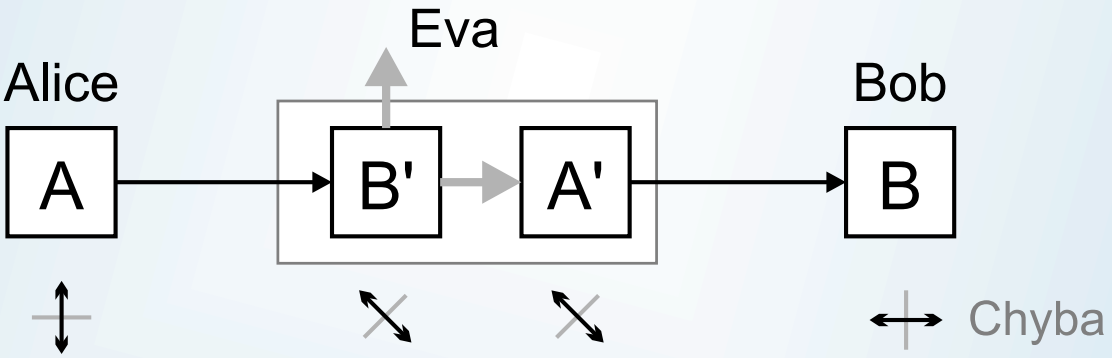




- Nelze vytvořit ani přesnou kopie neznámého stavu kvantové částice (foton nelze klonovat).

Odposlech

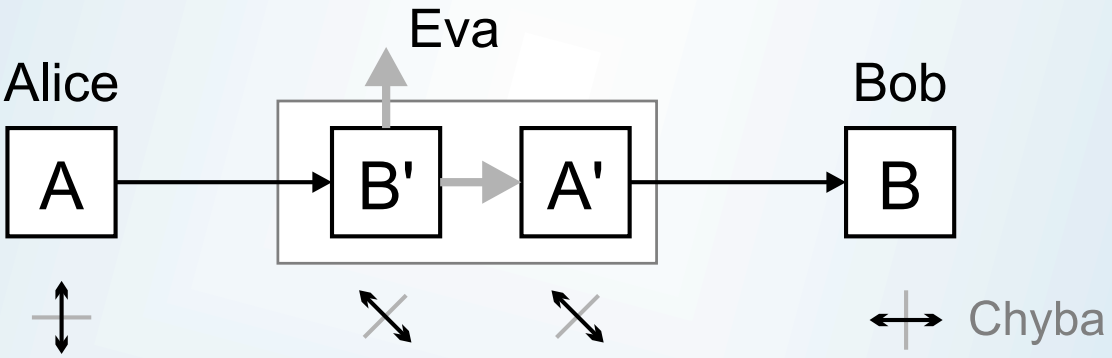
- Rozumná strategie: provést měření polarizace podobným zařízením, jaké má Bob, a každý bit pak znovu poslat podobným zařízením, jaké má Alice:



- Eva **nezná** polarizační bázi, používanou Alicí a Bobem.

Odposlech

- Rozumná strategie: provést měření polarizace podobným zařízením, jaké má Bob, a každý bit pak znovu poslat podobným zařízením, jaké má Alice:



- Eva **nezná** polarizační bázi, používanou Alicí a Bobem.
- Jakákoli jiná interakce s fotonem jeho stav také ovlivní.

Odposlech

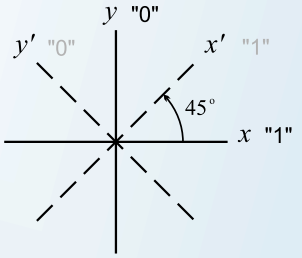
- Nezná-li Eva používanou bázi, způsobí v přenosu chyby.

Odposlech

- Nezná-li Eva používanou bázi, způsobí v přenosu chyby.
- Eva se by se ale mohla nějak dozvědět jakou polarizační bázi Alice a Bob používají – pak by zůstala neodhalena.

Odposlech

- Nezná-li Eva používanou bázi, způsobí v přenosu chyby.
- Eva se by se ale mohla nějak dozvědět jakou polarizační bázi Alice a Bob používají – pak by zůstala neodhalena.
- Proto Alice a Bob musejí **náhodně a nezávisle** střídat báze $+$ a $\times$.
- Po přenosu si Alice a Bob řeknou jaké báze použili a ponechají pouze ty bity, pro které použili stejné báze.



Odposlech

- Nyní, i když Eva zná báze, trefí se do té správné v průměru jen v **50 % případů**.
- Pokud Eva zvolí chybnou bázi způsobí v přenosu průměrně **50 % chyb**.

Odposlech

- Nyní, i když Eva zná báze, trefí se do té správné v průměru jen v **50 % případů**.
- Pokud Eva zvolí chybnou bázi způsobí v přenosu průměrně **50 % chyb**.

Nepřetržitý odposlech tedy způsobí průměrně

25 % chyb

Odposlech

- Nyní, i když Eva zná báze, trefí se do té správné v průměru jen v **50 % případů**.
- Pokud Eva zvolí chybnou bázi způsobí v přenosu průměrně **50 % chyb**.

Nepřetržitý odposlech tedy způsobí průměrně

25 % chyb

- Alice a Bob porovnají část přenesených bitů. Není-li v systému jiný zdroj chyb, indikuje každá neshoda přítomnost odposlechu.

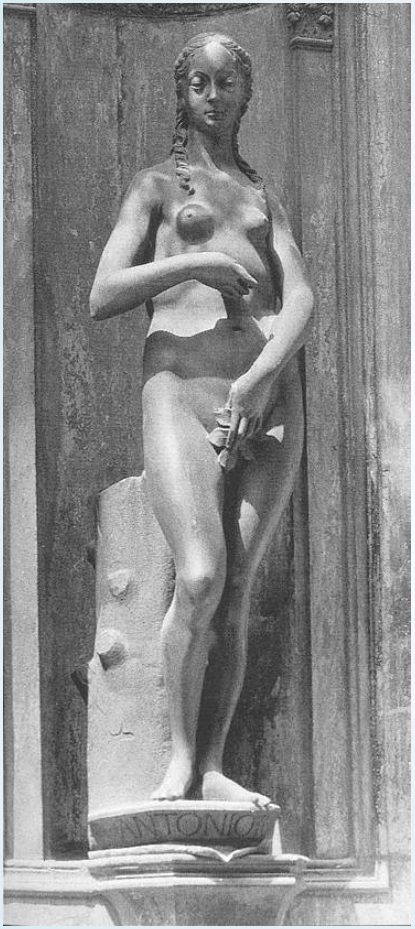
Odposlech

- Nyní, i když Eva zná báze, trefí se do té správné v průměru jen v **50 % případů**.
- Pokud Eva zvolí chybnou bázi způsobí v přenosu průměrně **50 % chyb**.

Nepřetržitý odposlech tedy způsobí průměrně

25 % chyb

- Srovnání **100** bitů $\Rightarrow$ pravděpodobnost, že odposlech **nebude** odhalen $P = (1 - 0{,}25)^{100} \approx \mathbf{3 \cdot 10^{-13}}$.



Hlavní výhodou kvantové kryptografie je, že Eva je nakonec vždy odhalena.

Antonio Rizzo, *Eva*,
2. polovina 15. století,
mramor.

Kvantová distribuce klíče – BB84

Kvantová distribuce klíče – BB84

$$\begin{array}{lcccc} + : & \updownarrow & = 0 & \leftrightarrow & = 1 \\ \times : & \searrow\!\!\nwarrow & = 0 & \swarrow\!\!\nearrow & = 1 \end{array}$$

Kvantová distribuce klíče – BB84

$$+: \quad \updownarrow = 0 \quad \leftrightarrow = 1$$
$$\times: \quad \searrow\!\swarrow = 0 \quad \nearrow\!\swarrow = 1$$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1

Kvantová distribuce klíče – BB84

$$+: \quad \updownarrow = 0 \quad \leftrightarrow = 1$$
$$\times: \quad \searrow = 0 \quad \nearrow = 1$$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
×	+	×	+	+	+	+	+	×	×	+	×	×	×	+

Kvantová distribuce klíče – BB84

$$+: \quad \updownarrow = 0 \quad \leftrightarrow = 1$$
$$\times: \quad \searrow = 0 \quad \nearrow = 1$$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
↘	↔	↗	↕	↔	↔	↕	↕	↗	↘	↔	↗	↘	↘	↔

Kvantová distribuce klíče – BB84

$$+: \quad \updownarrow = 0 \quad \leftrightarrow = 1$$
$$\times: \quad \searrow = 0 \quad \nearrow = 1$$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
↘	↔	↗	↕	↔	↔	↕	↕	↗	↘	↔	↗	↘	↘	↔
+	×	×	+	+	×	×	+	×	+	×	×	×	×	+

Kvantová distribuce klíče – BB84

$$+: \quad \updownarrow = 0 \quad \leftrightarrow = 1$$
$$\times: \quad \searrow = 0 \quad \nearrow = 1$$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
↘	↔	↗	↕	↔	↔	↕	↕	↗	↘	↔	↗	↘	↘	↔
+	×	×	+	+	×	×	+	×	+	×	×	×	×	+
1		1		1	0	0	0		1	1	1		0	1

Kvantová distribuce klíče – BB84

$$+: \quad \updownarrow = 0 \quad \leftrightarrow = 1$$
$$\times: \quad \searrow = 0 \quad \nearrow = 1$$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
↘	↔	↗	↕	↔	↔	↕	↕	↗	↘	↔	↗	↘	↘	↔
+	×	×	+	+	×	×	+	×	+	×	×	×	×	+
1		1		1	0	0	0		1	1	1		0	1

Veřejná diskuse

+		×		+	×	×	+		+	×	×		×	+

Kvantová distribuce klíče – BB84

$+:$	$\updownarrow$	$=0$	$\leftrightarrow$	$=1$
$\times:$	$\searrow$	$=0$	$\nearrow$	$=1$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
$\times$	$+$	$\times$	$+$	$+$	$+$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$\times$	$\times$	$+$
$\searrow$	$\leftrightarrow$	$\nearrow$	$\updownarrow$	$\leftrightarrow$	$\leftrightarrow$	$\updownarrow$	$\updownarrow$	$\nearrow$	$\searrow$	$\leftrightarrow$	$\nearrow$	$\searrow$	$\searrow$	$\leftrightarrow$
$+$	$\times$	$\times$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$+$	$\times$	$\times$	$\times$	$\times$	$+$
1		1		1	0	0	0		1	1	1		0	1

Veřejná diskuse

$+$		$\times$		$+$	$\times$	$\times$	$+$		$+$	$\times$	$\times$		$\times$	$+$
		✓		✓			✓				✓		✓	✓

Kvantová distribuce klíče – BB84

$+:\ \updownarrow = 0 \quad \leftrightarrow = 1$

$\times:\ \searrow = 0 \quad \nearrow = 1$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
↘	↔	↗	↕	↔	↔	↕	↕	↗	↘	↔	↗	↘	↘	↔
+	×	×	+	+	×	×	+	×	+	×	×	×	×	+
1		1		1	0	0	0		1	1	1		0	1

Veřejná diskuse

+		×		+	×	×	+		+	×	×		×	+
		✓		✓			✓				✓		✓	✓
		1		1			0				1		0	1

Kvantová distribuce klíče – BB84

$+:\ \updownarrow = 0 \quad \leftrightarrow = 1$

$\times:\ \searrow = 0 \quad \nearrow = 1$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
↘	↔	↗	↕	↔	↔	↕	↕	↗	↘	↔	↗	↘	↘	↔
+	×	×	+	+	×	×	+	×	+	×	×	×	×	+
1		1		1	0	0	0		1	1	1		0	1

Veřejná diskuse

+		×		+	×	×	+		+	×	×		×	+
		✓		✓			✓				✓		✓	✓
		1		1			0				1		0	1

Obětování bitů

				1									0	

Kvantová distribuce klíče – BB84

$+:$	$\updownarrow$	$=0$	$\leftrightarrow$	$=1$
$\times:$	$\searrow$	$=0$	$\nearrow$	$=1$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
↘	↔	↗	↕	↔	↔	↕	↕	↗	↘	↔	↗	↘	↘	↔
+	×	×	+	+	×	×	+	×	+	×	×	×	×	+
1		1		1	0	0	0		1	1	1		0	1

Veřejná diskuse

+		×		+	×	×	+		+	×	×		×	+
		✓		✓			✓				✓		✓	✓
		1		1			0				1		0	1

Obětování bitů

				1									0	
				✓									✓	

Kvantová distribuce klíče – BB84

$+: \quad \updownarrow = 0 \quad \leftrightarrow = 1$

$\times: \quad \searrow = 0 \quad \nearrow = 1$

Kvantový přenos

0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
↘	↔	↗	↕	↔	↔	↕	↕	↗	↘	↔	↗	↘	↘	↔
+	×	×	+	+	×	×	+	×	+	×	×	×	×	+
1		1		1	0	0	0		1	1	1		0	1

Veřejná diskuse

+		×		+	×	×	+		+	×	×		×	+
		✓		✓			✓				✓		✓	✓
		1		1			0				1		0	1

Obětování bitů

				1									0	
				✓									✓	
		1					0				1			1

Kvantová distribuce klíče – BB84

I. Kvantový přenos

1) *Alice* vybere náhodné bity.
2) *Alice* náhodně vybere vysílací polarizační báze.
3) *Alice* kóduje bity do polarizací posílaných fotonů.
4) *Bob* náhodně vybírá přijímací polarizační báze.
5) *Bob* zaznamenává obdržené bity
   (některé fotony se ovšem ztratí – nejsou zadetegovány).

II. Veřejná diskuse

6) *Bob* oznamuje báze, ve kterých naměřil fotony.
7) *Alice* oznamuje, které báze byly správně „uhodnuty“.
8) Shodli-li se *Alice* a *Bob* v bázích, přenesený bit si ponechají.
   (nenaslouchala-li *Eva* má *Bob* přesně to, co *Alice* poslala).

III. Obětování bitů

9) *Bob* obětuje některé náhodně vybrané bity k odhalení *Evy*.
10) *Alice* potvrzuje tyto obětované bity (*Eva* by způsobila odchylky).
11) Zbylé tajné bity sdílené *Alicí* a *Bobem* tvoří klíč.

Kvantová distribuce klíče – BB84

Charles Bennett

Gilles Brassard

I. Kvantový přenos

1) *Alice* vybere náhodné bity.
2) *Alice* náhodně vybere vysílací polarizační báze
3) *Alice* kóduje bity do polarizací posílaných foto
4) *Bob* náhodně vybírá přijímací polarizační báze
5) *Bob* zaznamenává obdržené bity
   (některé fotony se ovšem ztratí – nejsou zadet

II. Veřejná diskuse

6) *Bob* oznamuje báze, ve kterých naměřil fotony.
7) *Alice* oznamuje, které báze byly správně „uhodnuty“.
8) Shodli-li se *Alice* a *Bob* v bázích, přenesený bit si ponechají.
   (nenaslouchala-li *Eva* má *Bob* přesně to, co *Alice* poslala).

III. Obětování bitů

9) *Bob* obětuje některé náhodně vybrané bity k odhalení *Evy*.
10) *Alice* potvrzuje tyto obětované bity (*Eva* by způsobila odchylky).
11) Zbylé tajné bity sdílené *Alicí* a *Bobem* tvoří klíč.

Oprava chyb a zesílení utajení

Oprava chyb a zesílení utajení

Chyby způsobuje nejen Eva, ale i nepřesnosti a šum zařízení. Jisté malé procento chyb proto musíme tolerovat.

Oprava chyb a zesílení utajení

Chyby způsobuje nejen Eva, ale i nepřesnosti a šum zařízení. Jisté malé procento chyb proto musíme tolerovat.

- Oprava chyb

Oprava chyb a zesílení utajení

Chyby způsobuje nejen Eva, ale i nepřesnosti a šum zařízení. Jisté malé procento chyb proto musíme tolerovat.

- Oprava chyb

Nemůžeme si ale být jisti, že chyby nepocházejí z odposlechu (Eva mohla např. vyměnit přenosovou linku za lepší).

Oprava chyb a zesílení utajení

Chyby způsobuje nejen Eva, ale i nepřesnosti a šum zařízení. Jisté malé procento chyb proto musíme tolerovat.

- Oprava chyb

Nemůžeme si ale být jisti, že chyby nepocházejí z odposlechu (Eva mohla např. vyměnit přenosovou linku za lepší).

- Zesílení utajení
  - Z počtu chyb v přenosu lze odhadnout maximální informaci, kterou mohla získat Eva.
  - Z původního klíče se vyrobí nový, **kratší**, o němž má Eva minimální znalost (tj. Evina informace se sníží za cenu zkrácení klíče).

Autentizace

- Eva by mohla zasahovat i do komunikace po klasickém kanálu. Např. by mohla přerušit oba kanály a chovat se vůči Alici jako Bob (vyměnit si klíč s Alicí a případně i jiný klíč s Bobem).

Autentizace

- Eva by mohla zasahovat i do komunikace po klasickém kanálu. Např. by mohla přerušit oba kanály a chovat se vůči Alici jako Bob (vyměnit si klíč s Alicí a případně i jiný klíč s Bobem).
- Zprávy posílané pomocným klasickým kanálem je nutno autentizovat.
- Bob musí být schopen ověřit, že zprávu skutečně poslala Alice a že nebyla cestou pozměněna.

Autentizace

- Eva by mohla zasahovat i do komunikace po klasickém kanálu. Např. by mohla přerušit oba kanály a chovat se vůči Alici jako Bob (vyměnit si klíč s Alicí a případně i jiný klíč s Bobem).
- Zprávy posílané pomocným klasickým kanálem je nutno autentizovat.
- Bob musí být schopen ověřit, že zprávu skutečně poslala Alice a že nebyla cestou pozměněna.
- Alice a Bob musejí na počátku sdílet heslo pro autentizaci. To se po každém přenosu nahradí novým z přeneseného klíče.

Omezený dosah

- Omezení vzdálenosti je podmíněno ztrátami ve vlákně a šumem detektorů (detektor občas pošle impuls, i když na něj nedopadne žádný foton).

Omezený dosah

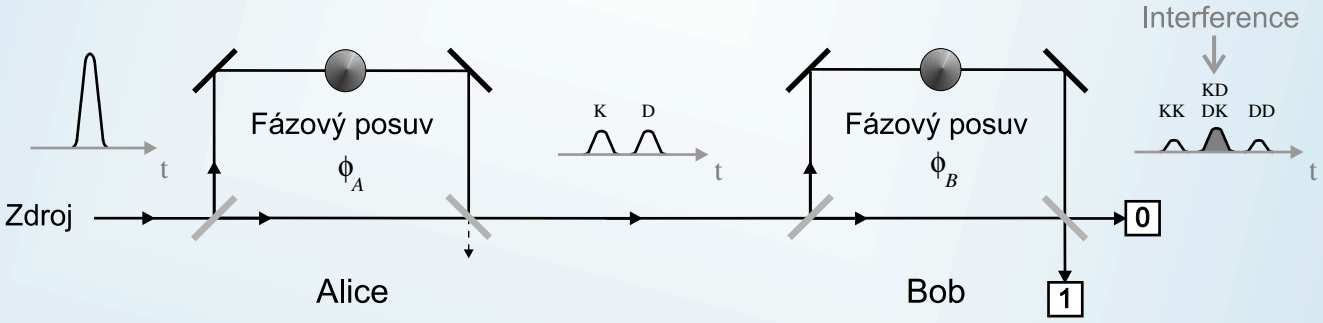
- Omezení vzdálenosti je podmíněno ztrátami ve vlákně a šumem detektorů (detektor občas pošle impuls, i když na něj nedopadne žádný foton).
- Jakmile počet fotonů přicházejících za jednotku času poklesne vlivem ztrát natolik, že je srovnatelný s počtem šumových impulsů detektoru, přestává být zařízení použitelné.
- Zesilovače použít nelze, protože by ovlivňovaly kvantový stav částic podobným způsobem jako odposlech.

Fázové kódování

Fázové kódování

V optických vláknech není polarizační kódování výhodné. Proto se používá tzv. fázové kódování. Na principu přenosu klíče se ale nic nemění.

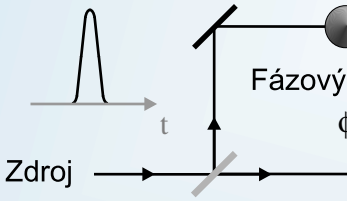
ϕ_A	„+“:	$0°$	$\equiv$	„1“,	$180°$	$\equiv$	„0“	ϕ_B	„+“:	$0°$
	„×“:	$90°$	$\equiv$	„1“,	$270°$	$\equiv$	„0“		„×“:	$90°$



Fázové kódování

V optických vlák oto
se používá tzv. f se
ale nic nemění.

ϕ_A	„+“:	$0°$
	„×“:	$90°$



ce

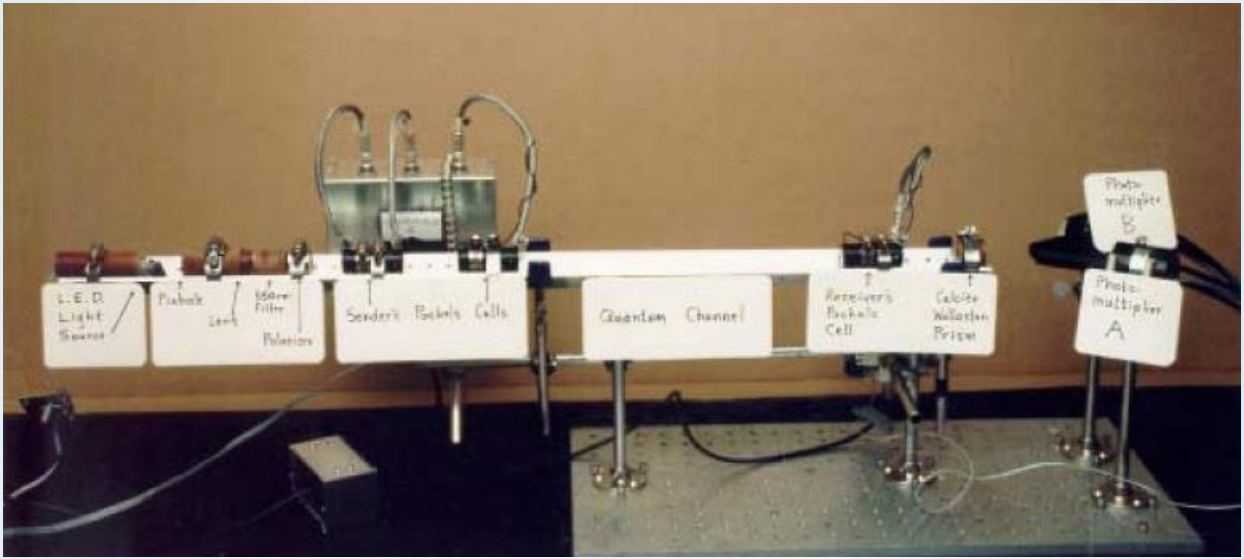
t

Alice Bob

Experimenty

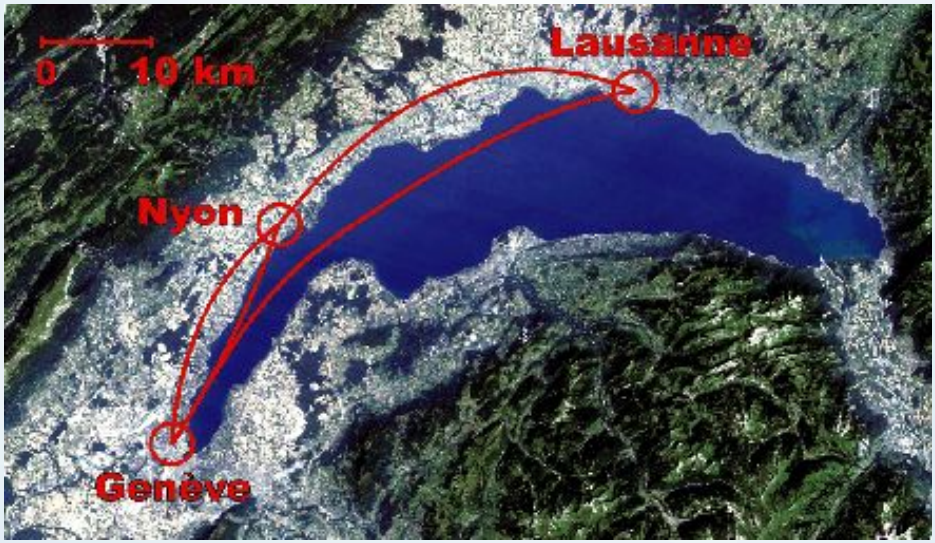
Experimenty

- První experiment r. 1989, polarizační kódování, volný prostor, 32 cm.



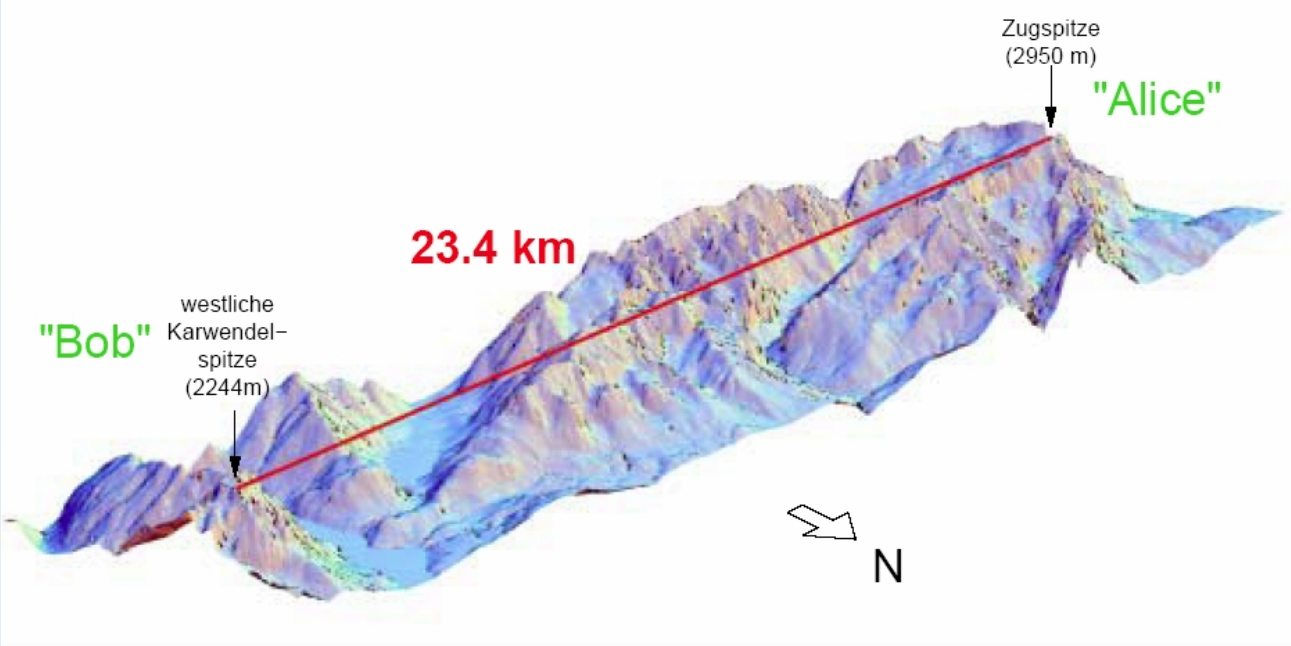
Experimenty

- Dnes už je odzkoušen přenos na desítky kilometrů. Např. na univerzitě v Ženevě testovali přenos běžnými telekomunikačními vlákny až na 67 km.



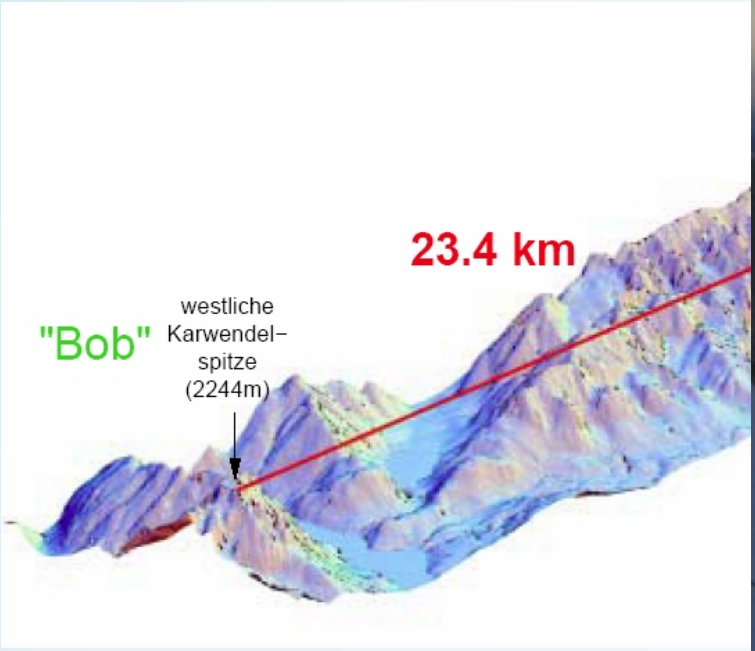
Přenos klíče volným prostorem

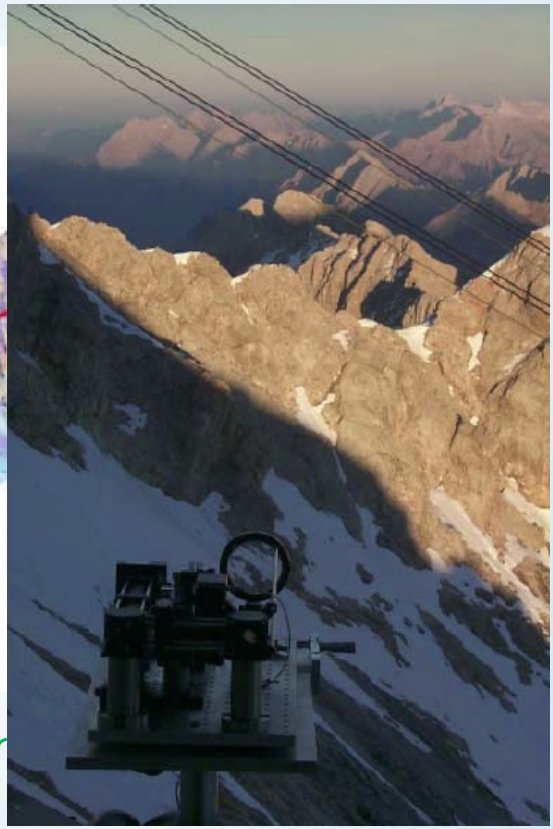
Přenos klíče volným prostorem



Mnichovská univerzita, prof. Weintfurter, polarizační kódování

Přenos klíče volným prostorem

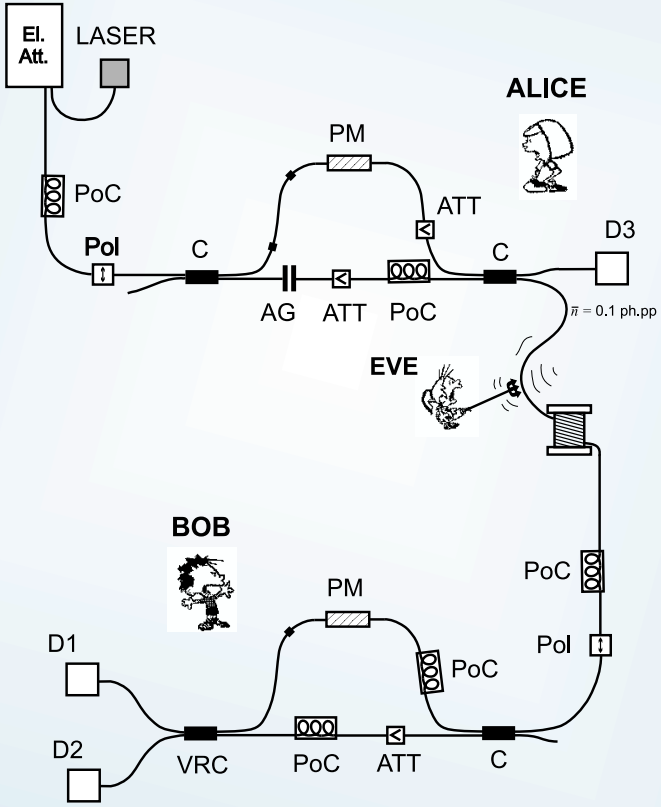




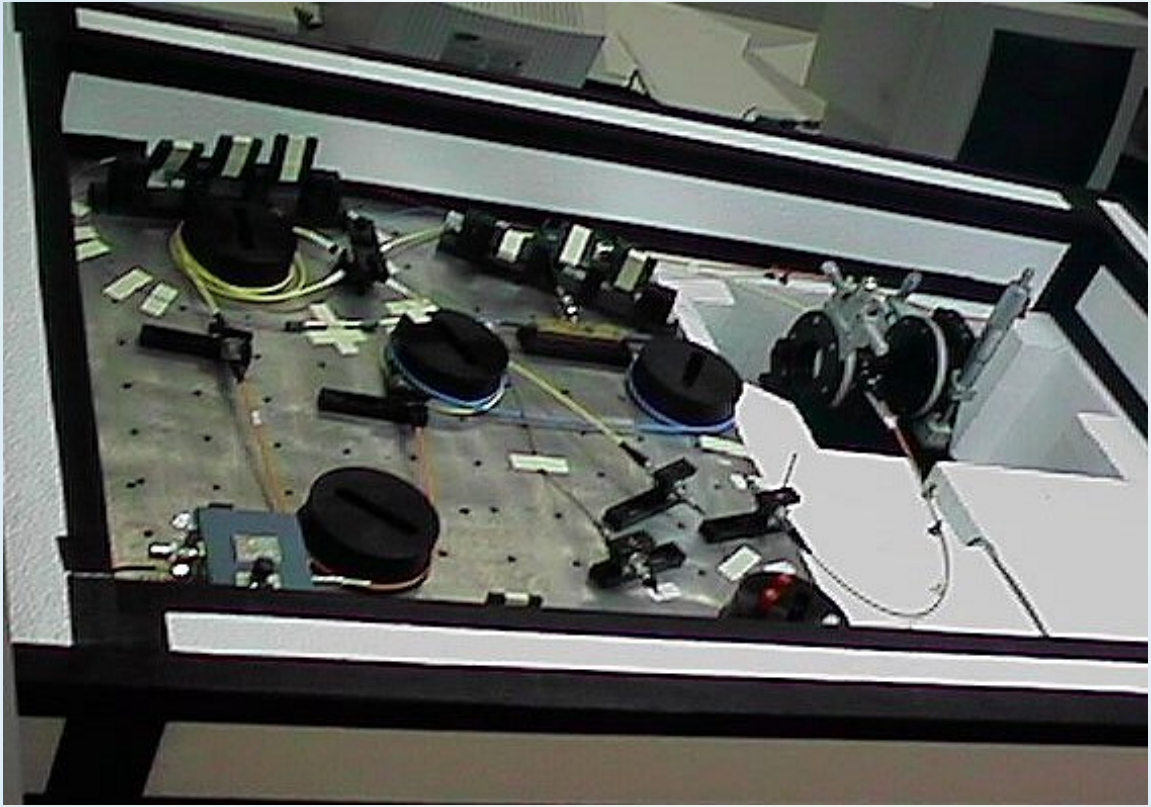
Mnichovská univerzita, prof. Weintfurter

Kvantová kryptografie v Olomouci

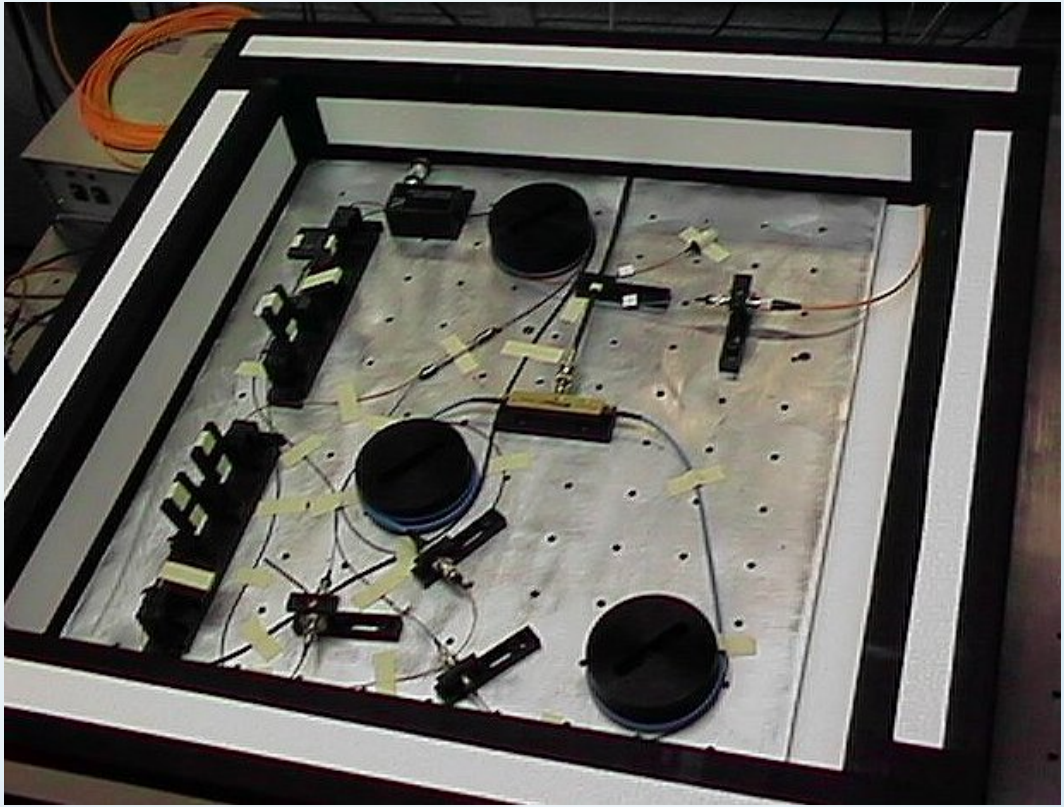
Kvantová kryptografie v Olomouci



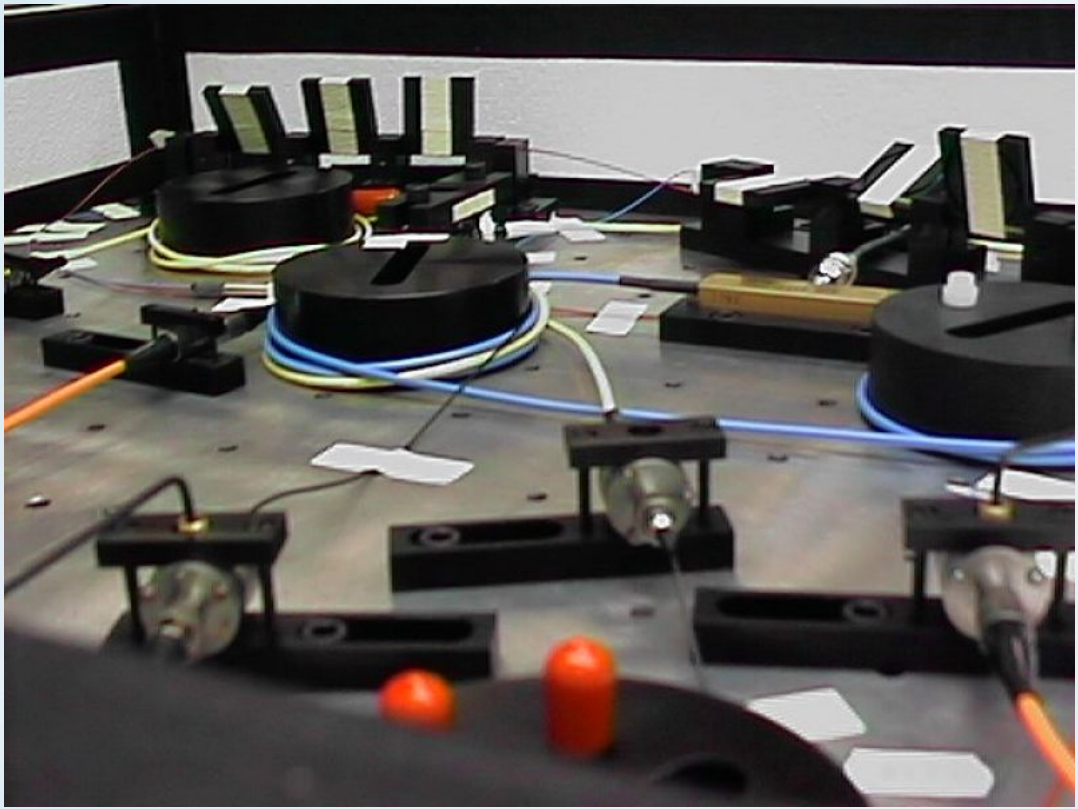
Kvantová kryptografie v Olomouci



Kvantová kryptografie v Olomouci



Kvantová kryptografie v Olomouci



Kvantová kryptografie v Olomouci

Kvantová kryptografie v praxi

Kvantová kryptografie v praxi

- id Quantique

Kvantová kryptografie v praxi

- id Quantique
- MagiQ

KONEC


VAROVÁNÍ MINISTRA ZDRAVOTNICTVÍ
PŘEMÝŠLENÍ NAD KVANTOVOU FYZIKOU VYVOLÁVÁ
NESPAVOST