Kvantová fyzika a náš svět

Miloslav Dušek

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

Motto:

> Mě velmi těší, že se musíme uchýlit k tak podivným pravidlům a bizarnímu způsobu uvažování, abychom pochopili Přírodu, a baví mě o tom lidem vykládat.
>
> *Richard P. Feynman*

Kvantová teorie

- Na počátku 20. stol. – přibližně ve stejnou dobu jako speciální teorie relativity – se rodí jedna z nejpodivuhodnějších fyzikálních teorií.
- Nejpřesněji experimentálně ověřená teorie.
- Má mnoho praktických aplikací: polovodičové součástky, lasery, jaderná energie, nové materiály, . . .

Kvantová teorie

- Na počátku 20. stol. – přibližně ve stejnou dobu jako speciální teorie relativity – se rodí jedna z nejpodivuhodnějších fyzikálních teorií.
- Nejpřesněji experimentálně ověřená teorie.
- Má mnoho praktických aplikací: polovodičové součástky, lasery, jaderná energie, nové materiály, ...
- Zcela změnila paradigma ve fyzice.
- Ačkoli známe kvantovou teorii přibližně 100 let, dodnes ji nerozumíme tak dobře, jak bychom chtěli.

Byly časy, kdy noviny psaly, že pouze dvanáct lidí rozumí teorii relativity. Nevěřím, že tomu tak kdy bylo. Možná bylo období, kdy jí rozuměl pouze jeden člověk, protože byl tím jediným, kdo ji měl v hlavě dřív, než napsal svůj článek. Ale potom si lidé článek přečetli a mnoho z nich teorii relativity tak či onak porozumělo, rozhodně jich bylo víc než dvanáct. Naproti tomu si myslím, že mohu bezpečně prohlásit, že není nikdo, kdo by rozuměl kvantové mechanice.

Richard P. Feynman

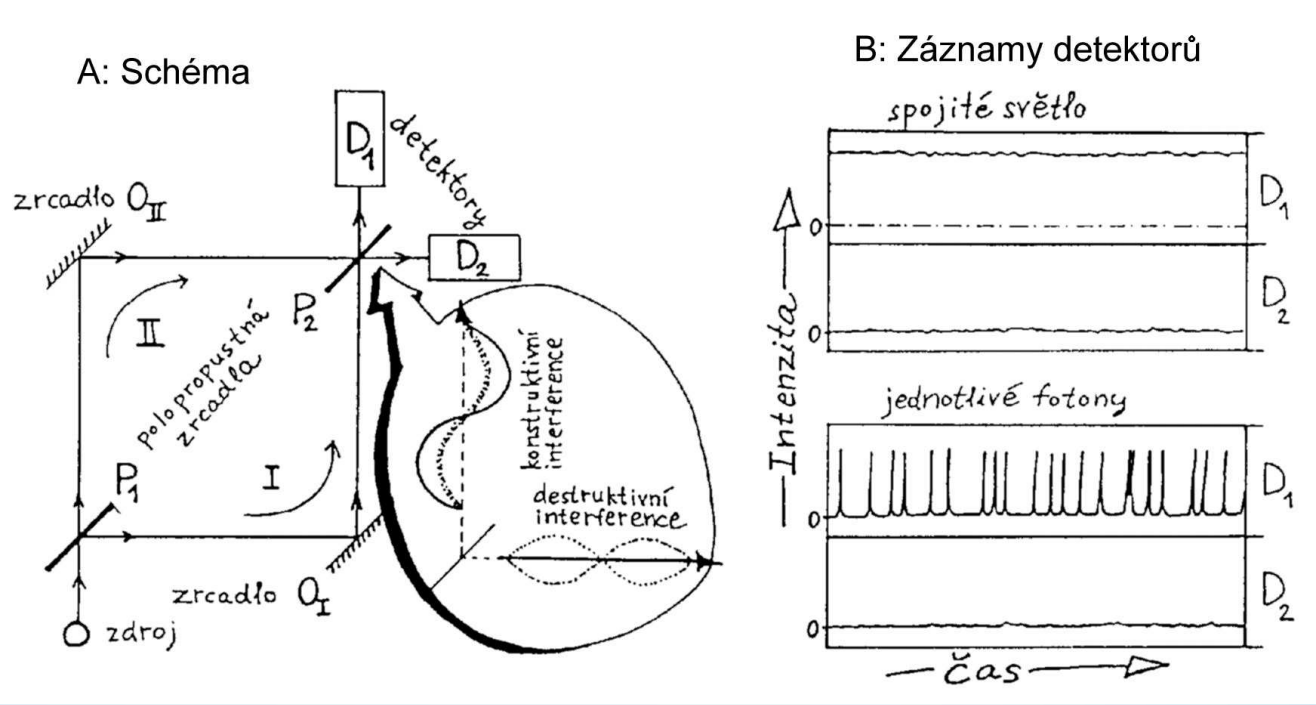
Kvantová teorie

- Při popisu přírody se bez kvantové teorie neobejdeme.
- Kvantová fyzika má ale mnoho kontraintuitivních vlastností:

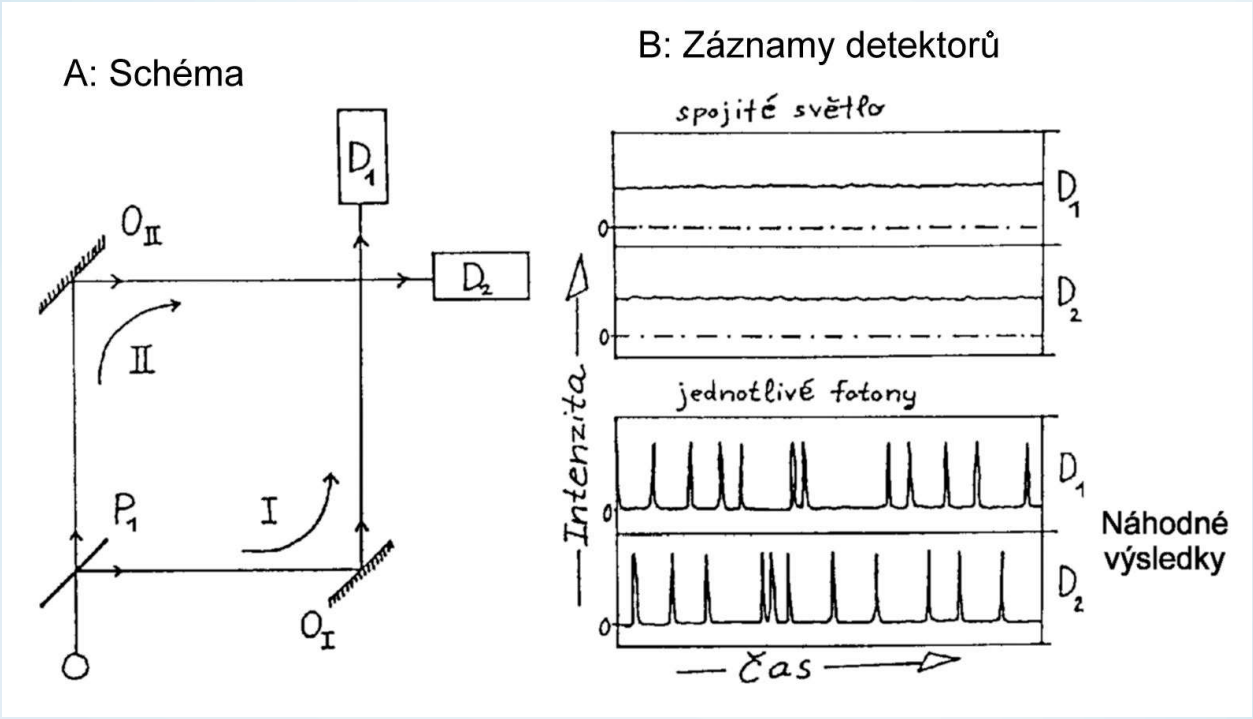
Kvantová teorie

- Při popisu přírody se bez kvantové teorie neobejdeme.
- Kvantová fyzika má ale mnoho kontraintuitivních vlastností:
  - Nevyhnutelná náhodnost výsledků měření.
  - Měření obecně změní stav systému.
  - Existence „nelokálních“ vlastností.

Foton v interferometru



Foton v interferometru



Popis stavu systému

Stavy systému popisujeme jako prvky nějakého prostoru.

Popis stavu systému

Stavy systému popisujeme jako prvky nějakého prostoru.

Klasická fyzika:

- Bezstrukturní částice: poloha $\vec{r}$ a hybnost $\vec{p}$.
- Determinismus (predikce, retrodikce).

Popis stavu systému

Stavy systému popisujeme jako prvky nějakého prostoru.

Klasická fyzika:

- Bezstrukturní částice: poloha $\vec{r}$ a hybnost $\vec{p}$.
- Determinismus (predikce, retrodikce).

Kvantová fyzika:

- Relace neurčitosti: $\vec{r}$ a $\vec{p}$ nelze současně připsat přesné hodnoty. Nelze je měřit zároveň neomezeně presně.
- Měřitelné veličiny jako poloha a hybnost nejsou přímými „charakteristikami systému“.

Popis stavu systému

Kvantová fyzika – princip superpozice:

- Mějme např. elektron v místě $\vec{r}_1$ – stavový vektor $|\vec{r}_1\rangle$
  nebo $\vec{r}_2$ – stavový vektor $|\vec{r}_2\rangle$

  (stav popisujeme vektorem v lineárním prostoru)

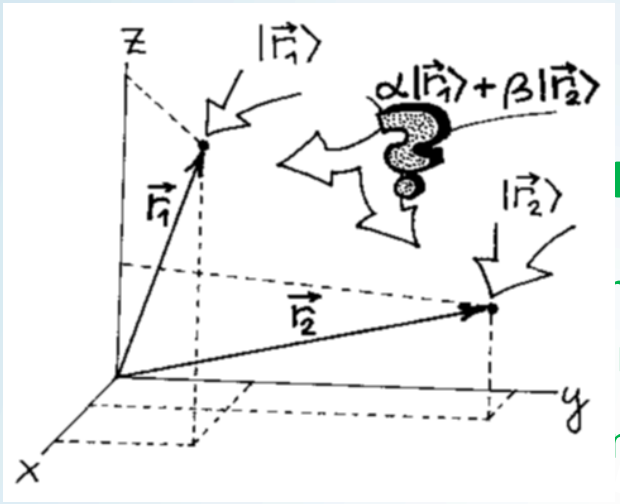
Popis stavu systému

Kvantová fyzika – princip superpozice:

- Mějme např. elektron v místě $\vec{r}_1$ – stavový vektor $|\vec{r}_1\rangle$
  nebo $\vec{r}_2$ – stavový vektor $|\vec{r}_2\rangle$

  (stav popisujeme vektorem v lineárním prostoru)

- Lineární superpozice $\boxed{\alpha\,|\vec{r}_1\rangle + \beta\,|\vec{r}_2\rangle}$ také popisuje možný stav elektronu.



p superpozice:

místě $\vec{r}_1$ – stavový vektor $|\vec{r}_1\rangle$
nebo $\vec{r}_2$ – stavový vektor $|\vec{r}_2\rangle$

m v lineárním prostoru)

- Lineární superpozice $\boxed{\alpha\,|\vec{r}_1\rangle + \beta\,|\vec{r}_2\rangle}$ také popisuje možný stav elektronu.

  Elektron v tomto stavu nemá žádnou konkrétní polohu!

$$\alpha\,|\vec{r}_1\rangle + \beta\,|\vec{r}_2\rangle \;\neq\; |\vec{r}_1\rangle\,,\; |\vec{r}_2\rangle\,,\; |\alpha\,\vec{r}_1 + \beta\,\vec{r}_2\rangle$$

Popis stavu systému

- Když je částice ve stavu $\alpha\,|\vec{r}_1\rangle + \beta\,|\vec{r}_2\rangle$, nemá smysl mluvit o její konkrétní poloze. Měření polohy ale vždy vede k výsledku $\vec{r}_1$ nebo $\vec{r}_2$.
- α, β . . . komplexní čísla
  - $|\alpha|^2, |\beta|^2$ jsou úměrné pravděpodobnostem nalezení částice v místě $\vec{r}_1$ resp. $\vec{r}_2$
  - Fáze nemají klasickou interpretaci. Interference.

Popis stavu systému

- Když je částice ve stavu $\alpha\,|\vec{r}_1\rangle + \beta\,|\vec{r}_2\rangle$, nemá smysl mluvit o její konkrétní poloze. Měření polohy ale vždy vede k výsledku $\vec{r}_1$ nebo $\vec{r}_2$.
- α, β . . . komplexní čísla
  - $|\alpha|^2, |\beta|^2$ jsou úměrné pravděpodobnostem nalezení částice v místě $\vec{r}_1$ resp. $\vec{r}_2$
  - Fáze nemají klasickou interpretaci. Interference.
- Lineární superpozice **neznamená**, že částice je s určitou pravděpodobností na některém konkrétním místě a my pouze nevíme na kterém. Dokud neprovedeme měření, nemůžeme mluvit o tom, že částice někde je.

Žádný elementární jev není jevem, dokud není registrovaným (pozorovaným) jevem [...] dokud není doveden do konce nevratným aktem zesílení, jakým je zčernání zrna bromidu stříbra ve fotografické emulzi nebo spuštění impulzu fotodetektoru.

John Archibald Wheeler

Měření

- **Klasická fyzika:**
  - Kteroukoli veličinu lze přesně měřit.
  - Vliv měření lze libovolně zmenšit.

Měření

- **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. Umíme předpovědět jen jejich pravděpodobnosti. (Přesto se zdá, že stavový vektor reprezentuje veškerou dostupnou informaci o stavu systému a že tato náhodnost je přírodě vlastní a nelze ji obejít.)

Měření

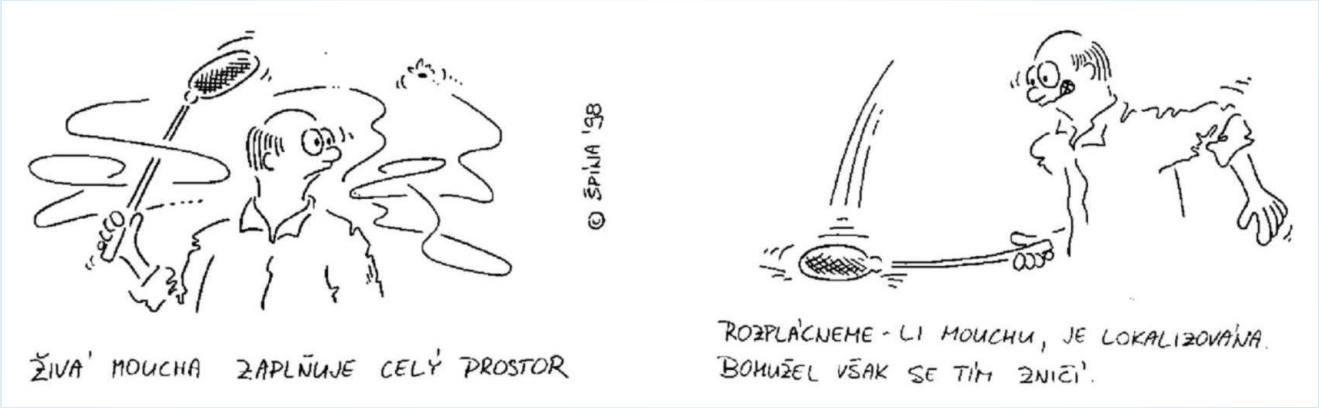
- **Kvantová fyzika:**
  - Kvantové měření obecně stav systému podstatně změní !

$$\alpha \left|\vec{r}_1\right\rangle + \beta \left|\vec{r}_2\right\rangle \quad \Rightarrow \quad \begin{cases} \left|\vec{r}_1\right\rangle, & \text{pravděpod. } |\alpha|^2 \\ \left|\vec{r}_2\right\rangle, & \text{pravděpod. } |\beta|^2 \end{cases}$$

Měření

- **Kvantová fyzika:**
  - Kvantové měření obecně stav systému podstatně změní !

$$\alpha\,|\vec{r}_1\rangle + \beta\,|\vec{r}_2\rangle \;\Rightarrow\; \begin{cases} |\vec{r}_1\rangle, & \text{pravděpod. } |\alpha|^2 \\ |\vec{r}_2\rangle, & \text{pravděpod. } |\beta|^2 \end{cases}$$



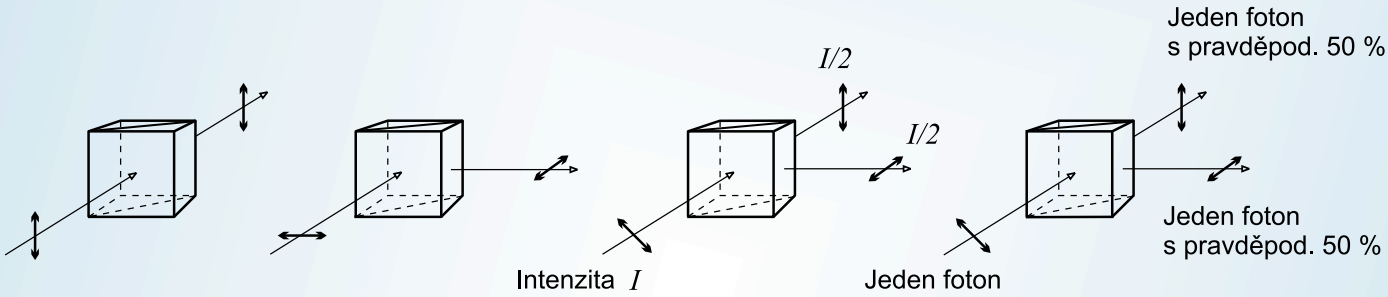
Měření

- **Kvantová fyzika:**
  - Kvantové měření obecně stav systému podstatně změní!

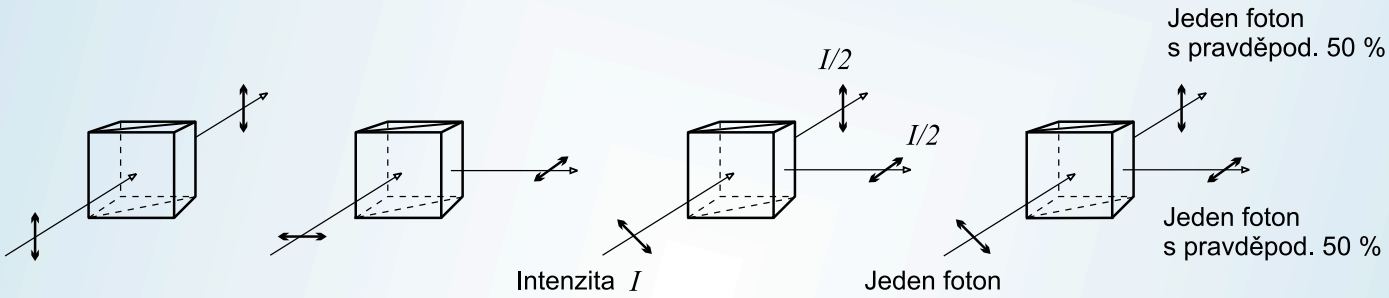
$$\alpha\,|\vec{r}_1\rangle + \beta\,|\vec{r}_2\rangle \;\Longrightarrow\; \begin{cases} |\vec{r}_1\rangle, & \text{pravděpod. } |\alpha|^2 \\ |\vec{r}_2\rangle, & \text{pravděpod. } |\beta|^2 \end{cases}$$

  - Mění se role pozorovatele – už nemůže být „mimo“.

Měření polarizace světla



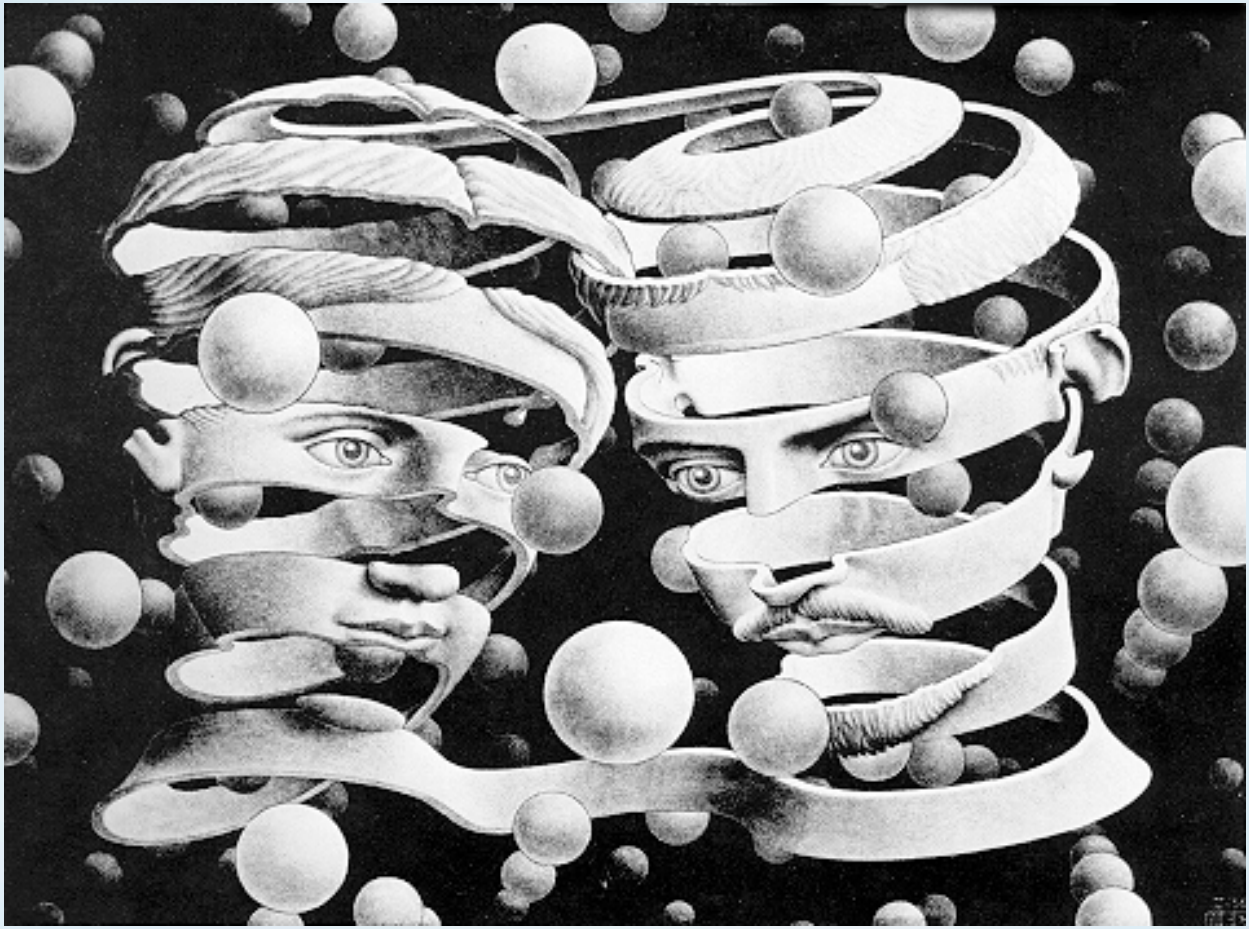
Měření polarizace světla



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**. $|\uparrow V\rangle + |\rightarrow H\rangle$

Entanglement

- Entanglovaný stav = „propletený“ stav více částic. Nelze ho zapsat jako jeden direktní součin stavů jednotlivých částic.
- Jednotlivé části systému nacházejícího se v entanglovaném stavu nelze popsat pomocí tzv. čistých stavů.
- Nejlepší možná znalost celku není totéž, co nejlepší možná znalost jeho částí.



Entanglement

- Entanglovaný stav = „propletený“ stav více částic.
- Entanglement nemá klasickou analogii.
- Kvantové měření na jedné z částic z entanglovaného systému změní celkový stavový vektor všech částic. (To nicméně nelze využít k okamžitému přenosu informace.)

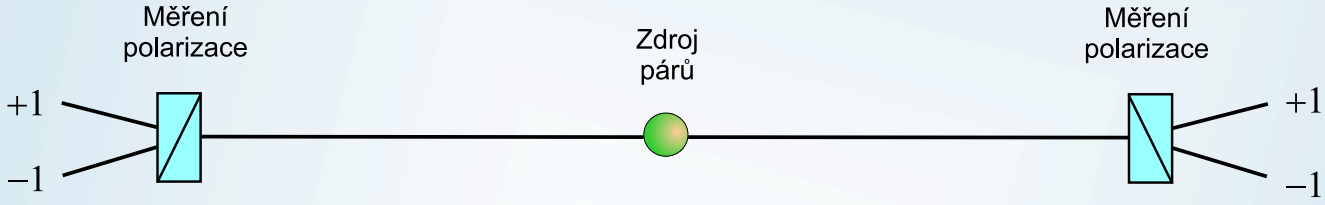
Entanglement

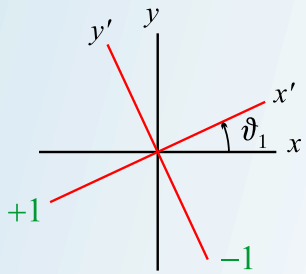
- Entanglovaný stav = „propletený“ stav více částic.
- Entanglement nemá klasickou analogii.
- Kvantové měření na jedné z částic z entanglovaného systému změní celkový stavový vektor všech částic. (To nicméně nelze využít k okamžitému přenosu informace.)
- „Trik, který kvantoví mágové používají k předvádění jevů, které klasičtí mágové nedokáží napodobit.“ *Asher Peres*

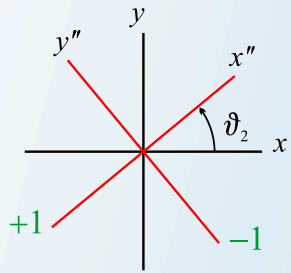
Entanglement

- Entanglovaný stav = „propletený“ stav více částic.
- Entanglement nemá klasickou analogii.
- Kvantové měření na jedné z částic z entanglovaného systému změní celkový stavový vektor všech částic. (To nicméně nelze využít k okamžitému přenosu informace.)
- „Trik, který kvantoví mágové používají k předvádění jevů, které klasičtí mágové nedokáží napodobit.“ *Asher Peres*
- Entanglement hraje klíčovou roli např. v kvantových počítačích nebo při kvantové teleportaci.

Bellovy nerovnosti







$A(\vartheta_1) = \pm 1$

$B(\vartheta_2) = \pm 1$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle_1 |y\rangle_2 - |y\rangle_1 |x\rangle_2\right)$$

Bellovy nerovnosti

- Výsledky měření $A(\vartheta_1)$ a $B(\vartheta_2)$ jsou náhodné.
- Předpokládejme, že jsou určny nějakými skrytými parametry λ, které neznáme.
- Realismus, lokalita.
- Budeme se zajímat o korelační funkce

$$C(\vartheta_1, \vartheta_2) = \left\langle A(\vartheta_1) B(\vartheta_2) \right\rangle_\Lambda$$

$$= \int_{\lambda \in \Lambda} A(\vartheta_1, \lambda)\, B(\vartheta_2, \lambda)\, \mathrm{d}\rho(\lambda).$$

Bellovy nerovnosti

Náhodné proměnné: $\alpha, \beta, \alpha', \beta' = \pm 1$

$$\gamma = \alpha\beta + \alpha\beta' + \alpha'\beta - \alpha'\beta'$$

Bellovy nerovnosti

Náhodné proměnné: $\alpha, \beta, \alpha', \beta' = \pm 1$

$$\gamma = \alpha\beta + \alpha\beta' + \alpha'\beta - \alpha'\beta'$$

α	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	-1	-1	-1	-1	-1	-1	-1	-1
β	$+1$	$+1$	$+1$	$+1$	-1	-1	-1	-1	$+1$	$+1$	$+1$	$+1$	-1	-1	-1	-1
α'	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1	$+1$	$+1$	-1	-1
β'	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1	$+1$	-1
γ	$+2$	$+2$	$+2$	-2	-2	-2	$+2$	-2	-2	$+2$	-2	-2	-2	$+2$	$+2$	$+2$

Střední hodnota γ bude vždy mezi -2 a $+2$:

$$-2 \leq \langle\gamma\rangle \leq +2$$

$$\boldsymbol{-2 \leq \langle\alpha\beta\rangle + \langle\alpha\beta'\rangle + \langle\alpha'\beta\rangle - \langle\alpha'\beta'\rangle \leq +2}$$

Bellovy nerovnosti

$$\alpha = A(\vartheta_1), \qquad \alpha' = A(\vartheta_1'),$$
$$\beta = B(\vartheta_2), \qquad \beta' = B(\vartheta_2').$$

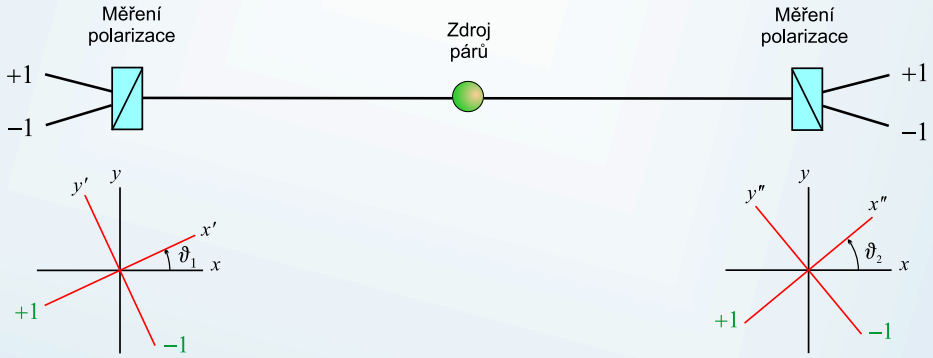
Každá lokálně realistická teorie musí splňovat nerovnost:

$$\left| C(\vartheta_1, \vartheta_2) + C(\vartheta_1', \vartheta_2) + C(\vartheta_1, \vartheta_2') - C(\vartheta_1', \vartheta_2') \right| \leq 2$$

Bellovy nerovnosti

Předpověď kvantové mechaniky:

$$
\begin{aligned}
|\Psi\rangle &= \frac{1}{\sqrt{2}}\Big(|x\rangle_1 |y\rangle_2 - |y\rangle_1 |x\rangle_2\Big) \\
&= \frac{1}{\sqrt{2}}\Big[\sin(\vartheta_2-\vartheta_1)\,|x'\rangle_1 |x''\rangle_2 + \cos(\vartheta_2-\vartheta_1)\,|x'\rangle_1 |y''\rangle_2 \\
&\quad - \cos(\vartheta_2-\vartheta_1)\,|y'\rangle_1 |x''\rangle_2 + \sin(\vartheta_2-\vartheta_1)\,|y'\rangle_1 |y''\rangle_2\Big]
\end{aligned}
$$



Bellovy nerovnosti

Předpověď kvantové mechaniky – pravděpodobnosti výsledků:

$$P_{++} = P_{--} = \frac{1}{2}\left[\sin(\vartheta_2 - \vartheta_1)\right]^2$$

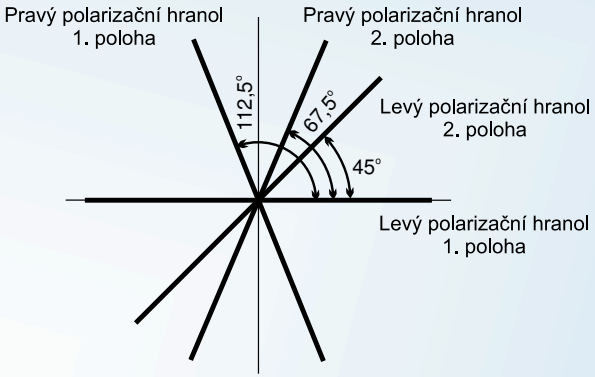
$$P_{+-} = P_{-+} = \frac{1}{2}\left[\cos(\vartheta_2 - \vartheta_1)\right]^2$$

$$\begin{aligned}\left\langle A(\vartheta_1)B(\vartheta_2)\right\rangle &= P_{++} + P_{--} - P_{+-} - P_{-+} \\ &= \left[\sin(\vartheta_2 - \vartheta_1)\right]^2 - \left[\cos(\vartheta_2 - \vartheta_1)\right]^2 \\ &= -\cos\left[2\,(\vartheta_2 - \vartheta_1)\right]\end{aligned}$$

Bellovy nerovnosti

Zvolme např.

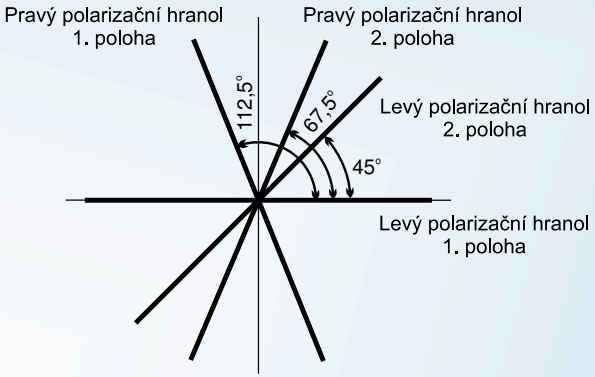
$$\vartheta_1 = 0°, \qquad \vartheta_1' = 45°,$$
$$\vartheta_2 = 112{,}5°, \qquad \vartheta_2' = 67{,}5°.$$



Bellovy nerovnosti

Zvolme např.

$$\vartheta_1 = 0°, \qquad \vartheta_1' = 45°,$$
$$\vartheta_2 = 112{,}5°, \qquad \vartheta_2' = 67{,}5°.$$

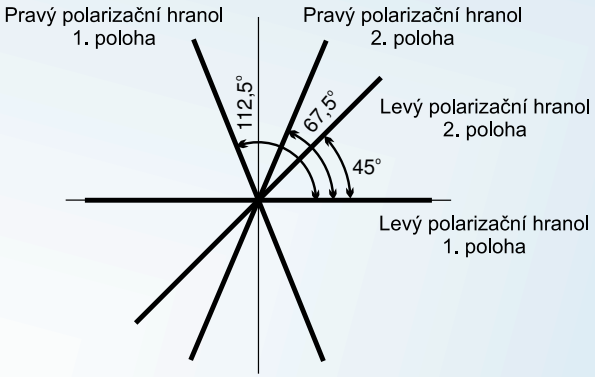


$$\begin{aligned}
&\left|C(\vartheta_1,\vartheta_2) + C(\vartheta_1',\vartheta_2) + C(\vartheta_1,\vartheta_2') - C(\vartheta_1',\vartheta_2')\right| \\
&= \left|-\cos(225°) - \cos(135°) - \cos(135°) + \cos(45°)\right| \\
&= \mathbf{2\sqrt{2} \;>\; 2}
\end{aligned}$$

Bellovy nerovnosti

Zvolme např.

$$\vartheta_1 = 0°, \qquad \vartheta_1' = 45°,$$
$$\vartheta_2 = 112{,}5°, \qquad \vartheta_2' = 67{,}5°.$$



$$\begin{aligned} &\left|C(\vartheta_1,\vartheta_2) + C(\vartheta_1',\vartheta_2) + C(\vartheta_1,\vartheta_2') - C(\vartheta_1',\vartheta_2')\right| \\ &= \left|-\cos(225°) - \cos(135°) - \cos(135°) + \cos(45°)\right| \\ &= \mathbf{2\sqrt{2} \;\; > \;\; 2} \end{aligned}$$

Kvantová teorie porušuje Bellovy nerovnosti !!

Potvrzeno experimentálními testy.

Kvantová fyzika a zpracování informace

- Donedávna se o zpracování informace uvažovalo jen v pojmech klasické fyziky. Kvantová mechanika hrála jen podpůrnou roli.
- Informace je abstraktní pojem, ale to, co můžeme s informací provádět, závisí na fyzikálním systému, který informaci nese.
- Kvantové systémy se chovají jinak než klasické (podivuhodněji).

Kvantová fyzika a zpracování informace

- Využití kvantových systémů při zpracování informace nabízí řešení některých problémů, které jsou v rámci klasické teorie informace neřešitelné nebo jejichž klasické řešení není známé.
- Jedná se např. o bezpečný přenos kryptografického klíče nebo o faktorizaci velkých čísel v polynomiálním výpočetním čase.

Kvantová teorie informace

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

Kvantová teorie informace

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

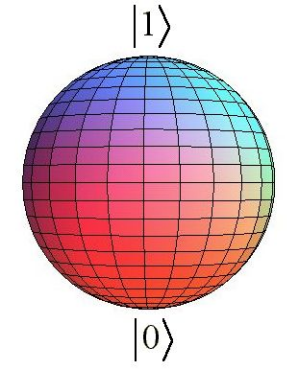
- Aplikace: **kvantové počítače**,
  kvantová kryptografie.

Kvantový bit

- **Klasický bit:** 0, 1 – např. dvě úrovně napětí.

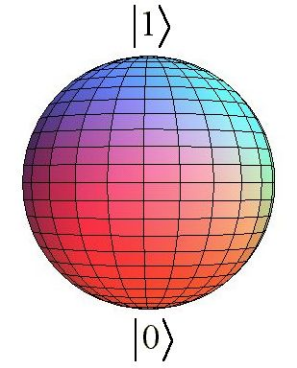
Kvantový bit

- **Klasický bit:** 0, 1 – např. dvě úrovně napětí.
- **Kvantový bit (qubit):** dvouhladinový kvantový objekt.
  - Bázové stavy: $|0\rangle, |1\rangle$
  - Obecný stav – superopozice: $\alpha|0\rangle + \beta|1\rangle$



Kvantový bit

- **Klasický bit:** 0, 1 – např. dvě úrovně napětí.
- **Kvantový bit (qubit):** dvouhladinový kvantový objekt.
  - Bázové stavy: $|0\rangle, |1\rangle$
  - Obecný stav – superopozice: $\alpha|0\rangle + \beta|1\rangle$



- **Kvantový registr:** registr složený z qubitů.
  - Superpozice stavů celého registru (nejen jednotlivých qubitů)!
  - Př. (2 qubity): $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ ← entanglovaný stav.


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

Kvantové počítače

- Výpočet je realizován evolucí kvantového systému.
- Umožňují řešit některé úlohy (např. rozklad čísla na prvočinitele) podstatně efektivněji než počítače klasické.
- Počet operací neroste s délkou vstupu exponenciálně, ale jen jako polynom konečného stupně.
- Pracují v jistém smyslu s mnoha vstupními hodnotami zároveň (superpozice stavů kvantového registru – entanglement). S rostoucím počtem qubitů N roste dimenze prostoru stavů jako 2^N.
- Představují ohrožení pro klasické kryptosystémy.

Kvantová kryptografie

- Metoda pro utajenou komunikaci.
- Její bezpečnost nezávisí na výpočetních nebo technologických možnostech útočníka, ale je garantována zákony kvantové fyziky.
- Konvenční kryptografické algoritmy obvykle spoléhají na to, že rozluštit zprávu bez znalosti klíče je výpočetně náročné.

Kvantová kryptografie

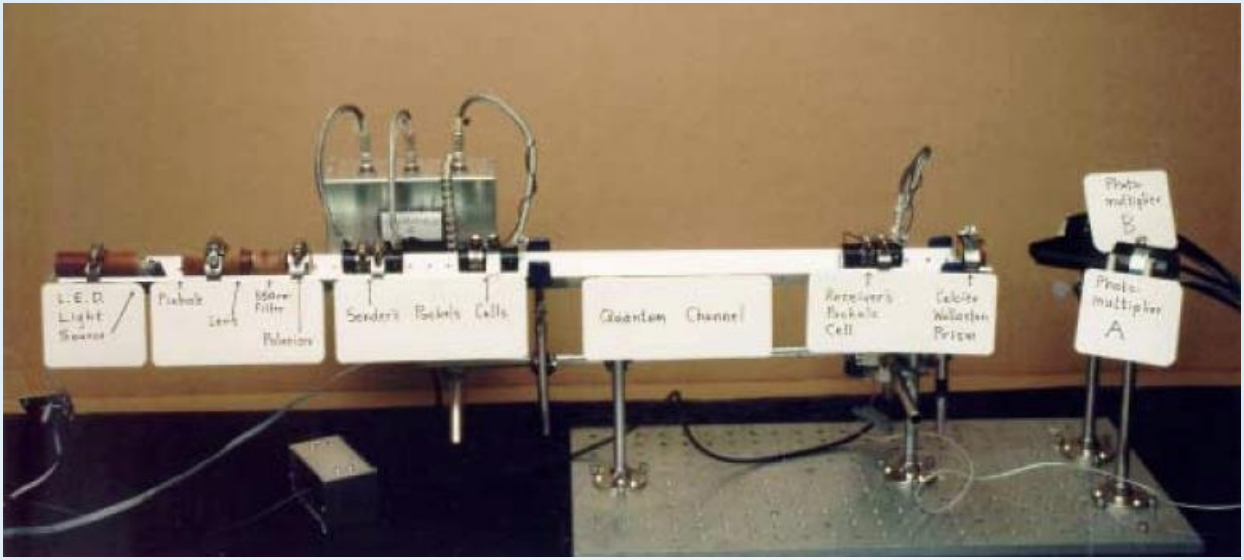
- Kvantová kryptografie sice neumí odposlechu zabránit, ale umí ho odhalit.
- Nepřenáší se zpráva, ale klíč pro Vernamovu šifru. Je-li odhalen odpolsech, klíč se nepoužije. Žádná informace neunikne.
- Kvantová fyzika řeší problém distribuce kryptografického klíče.

Kvantová kryptografie

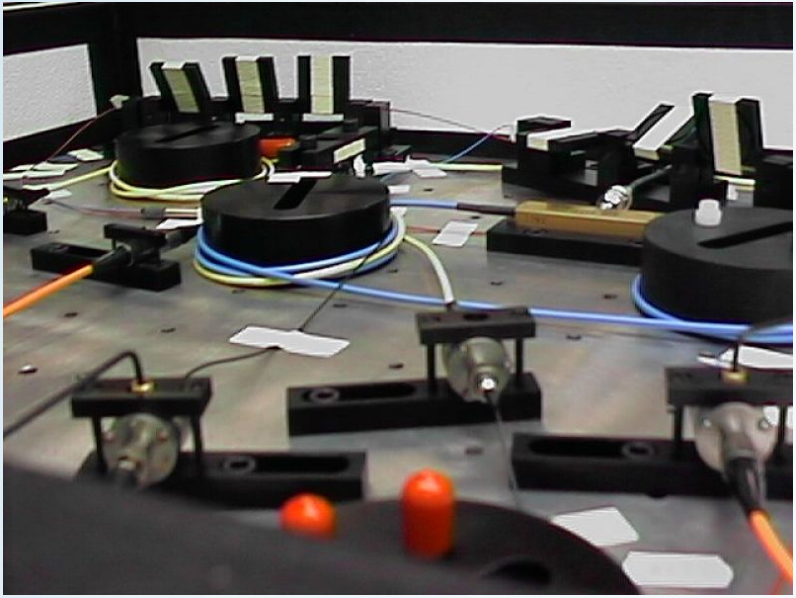
- Informace je kódována do neortogonálních stavů kvantových systémů (např. fotonů).
- Odposlech = interakce s fyzikální entitou nesoucí informaci (např. měření).
- Jakákoli interakce s kvantovým systémem, která může vést k úniku informace, obecně ovlivní stav systému.
- Proto je možné odposlech odhalit.

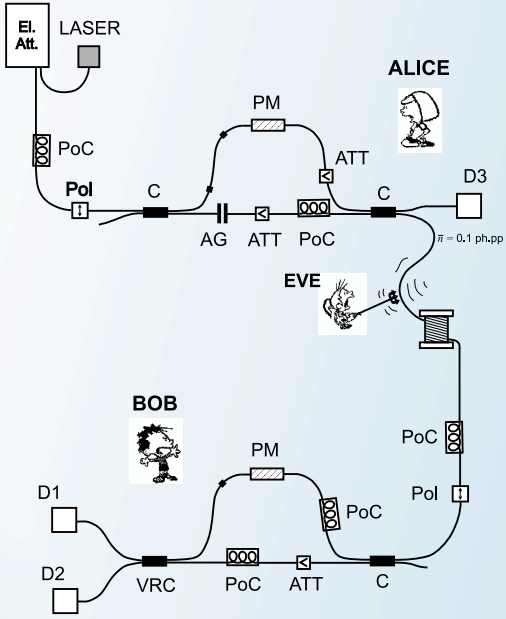
Kvantová kryptografie – první experiment

- Bennett, Bessette, Brassard, Salvail, Smolin, 1989.
  Polarizační kódování, volný prostor (32 cm).

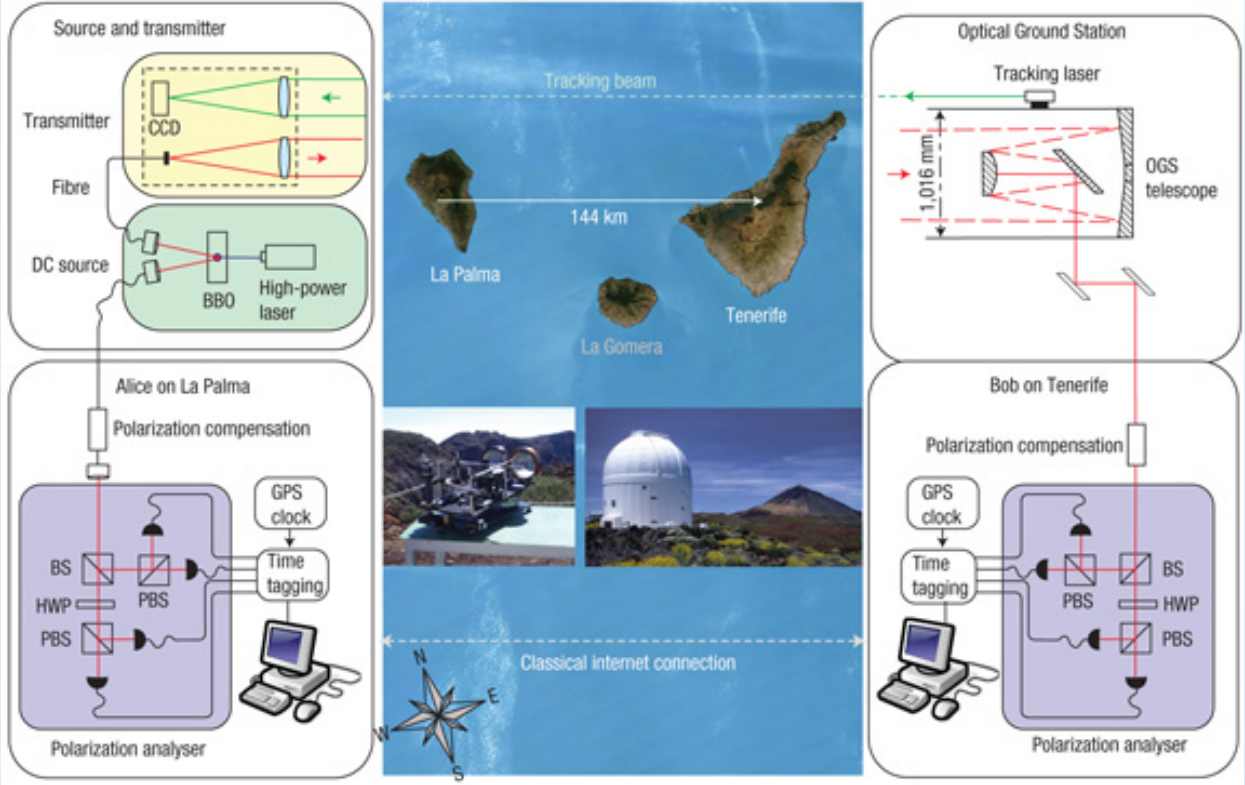


Olomouc 1998

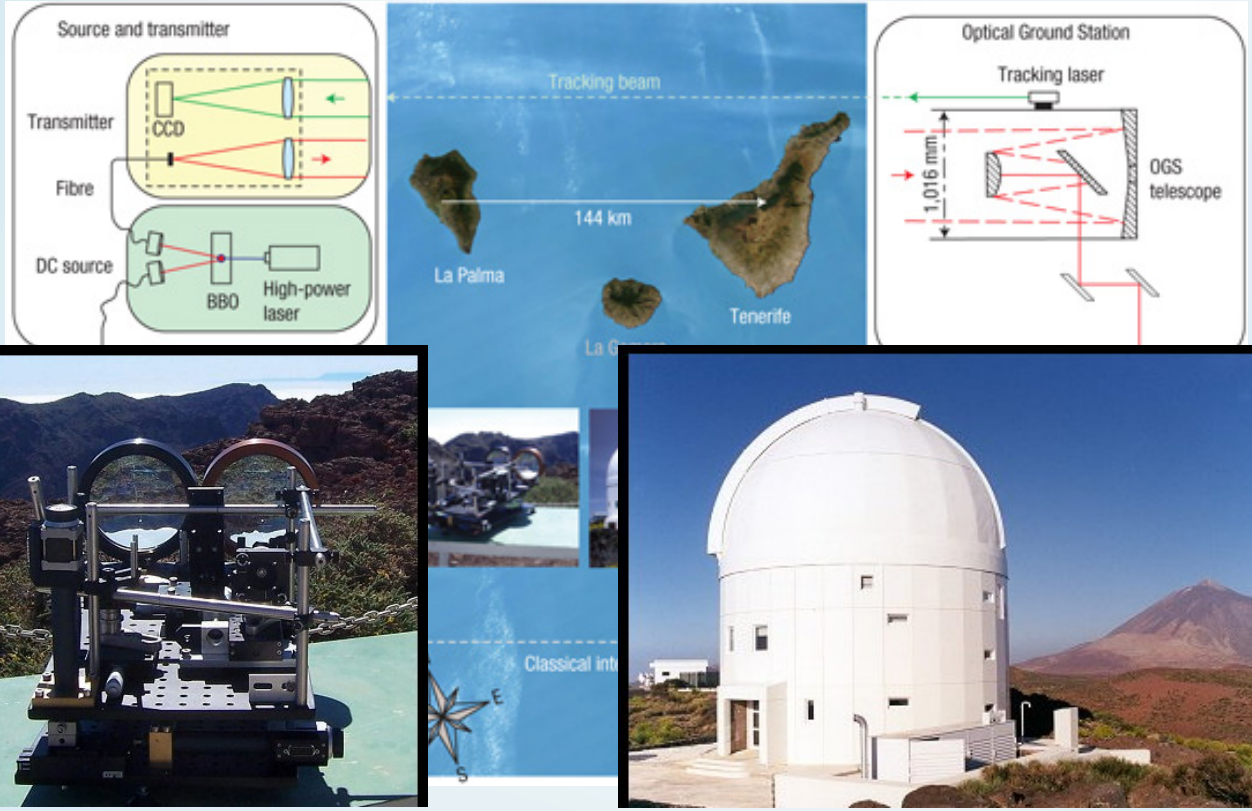




Přenos klíče volným prostorem



Přenos klíče volným prostorem



Kvantová kryptografie v praxi

- id Quantique

- MagiQ

- Toshiba Research Europe, NEC Corporation,...

Setkat se s kvantovým světem je cítit se jako cestovatel z daleké země, který poprvé v životě vidí automobil. Ta věc má zjevně dávat nějaký užitek, a to podstatný, jenže jaký? Člověk může otevřít dveře, stáhnout a vytáhnout okénko, zapnout a vypnout světla a snad i protočit startér, to všechno bez znalosti hlavního smyslu. Svět kvant je ten automobil.

John Archibald Wheeler

KONEC


VAROVÁNÍ MINISTRA ZDRAVOTNICTVÍ
PŘEMÝŠLENÍ NAD KVANTOVOU FYZIKOU VYVOLÁVÁ
NESPAVOST