



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.
- Ačkoli známe kvantovou teorii téměř 100 let, dodnes ji nerozumíme tak dobře, jak bychom chtěli.



Kvantová teorie

- Na počátku 20. stol. – přibližně ve stejnou dobu jako speciální teorie relativity – se rodí jedna z nejpodivuhodnějších fyzikálních teorií.
- Ačkoli známe kvantovou teorii téměř 100 let, dodnes ji nerozumíme tak dobře, jak bychom chtěli.
- Kvantová teorie – nejpřesněji experimentálně ověřená teorie.
- Kvantová teorie má mnoho praktických aplikací (polovodičové součástky, lasery, jaderná energie, nové materiály, složité molekuly, ...).

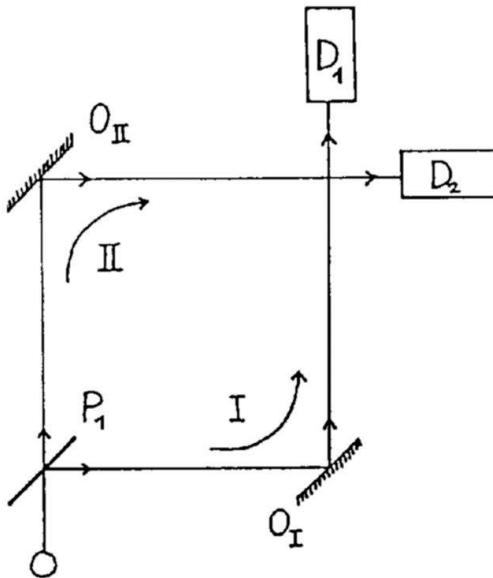


Byly časy, kdy noviny psaly, že pouze dvanáct lidí rozumí teorii relativity. Nevěřím, že tomu tak kdy bylo. Možná bylo období, kdy jí rozuměl pouze jeden člověk, protože byl tím jediným, kdo ji měl v hlavě dřív, než napsal svůj článek. Ale potom si lidé článek přečetli a mnoho z nich teorii relativity 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.

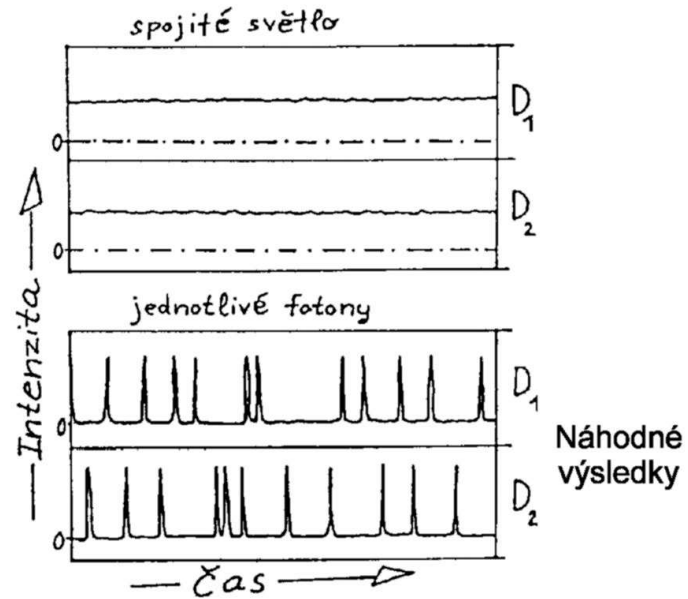
Richard P. Feynman

Foton v interferometru

A: Schéma



B: Záznamy detektorů





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 přesně.
- 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 $|\vec{r}_2\rangle$

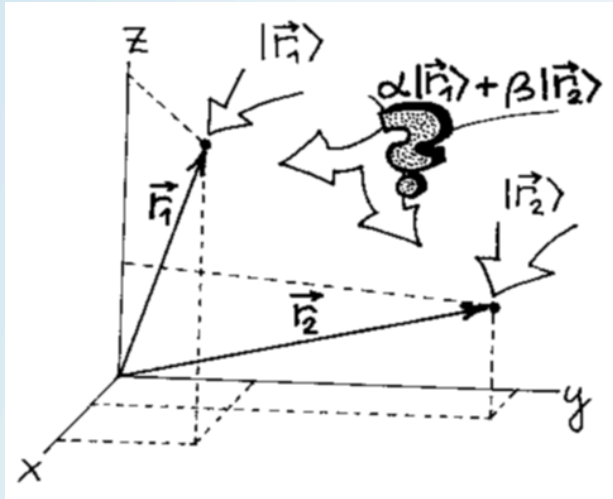
(stav popisujeme vektorem v lineárním prostoru)



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 $\alpha |\vec{r}_1\rangle + \beta |\vec{r}_2\rangle$ také popisuje možný stav elektronu.



p superpozice:

nístě \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 $\alpha |\vec{r}_1\rangle + \beta |\vec{r}_2\rangle$ 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 .
- $\alpha, \beta \dots$ 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.)



Měření

- **Kvantová fyzika:**

- Kvantové měření obecně stav systému podstatně **změní!**

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

Měření

- Kvantová fyzika:

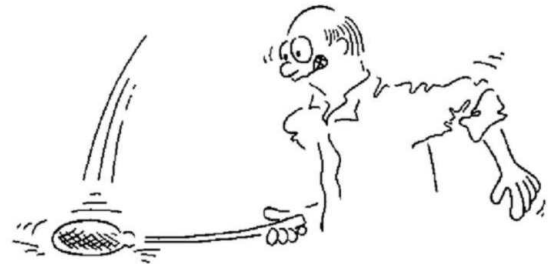
- Kvantové měření obecně stav systému podstatně **změní!**

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



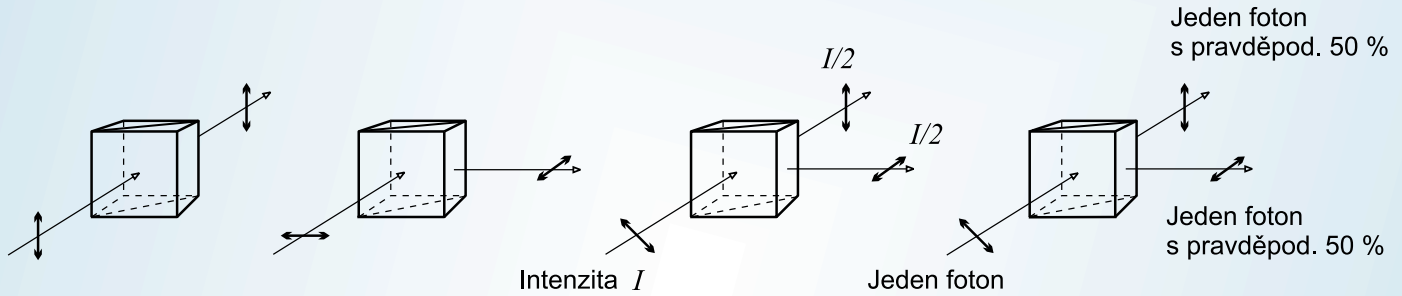
© ŠPIŤA '98

ŽIVA' MOUCHA ZAPLNŮJE CELÝ PROSTOR

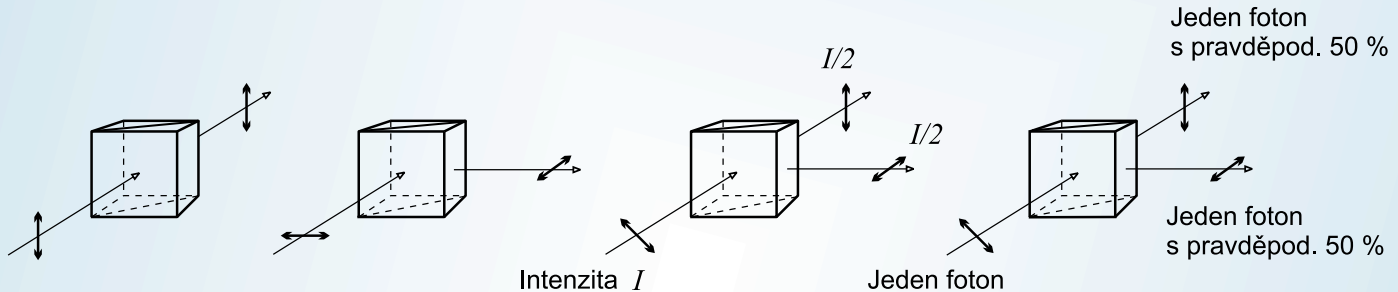


ROZPLÁČNEME - LI MOUCHU, JE LOKALIZOVÁNA.
BOHUŽEL VŠAK SE TÍM ZNIČÍ!

Měření polarizace světla



Měření polarizace světla

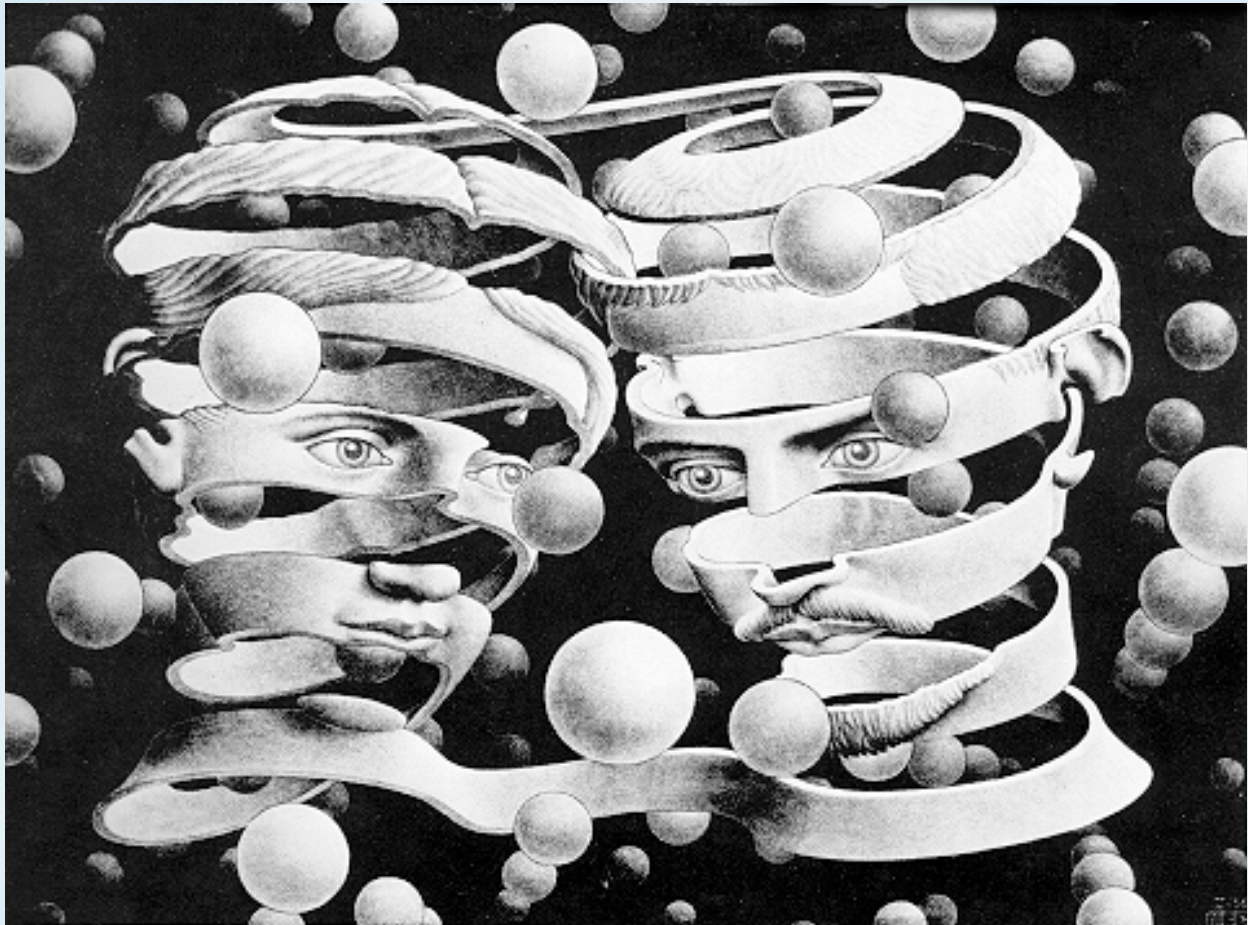


Jeden foton se nemůže rozdělit, je-li polarizován „šikmo“, spatříme ho buď projít nebo se odrazit. Jeho „volba“ je zcela **náhodná**. Po průchodu bude nadále polarizován **svisle**, po odrazu **vodorovně**.



Entanglement

- Entanglovaný stav = „propletený“ stav více částic. Nelze ho zapsat jako jeden 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

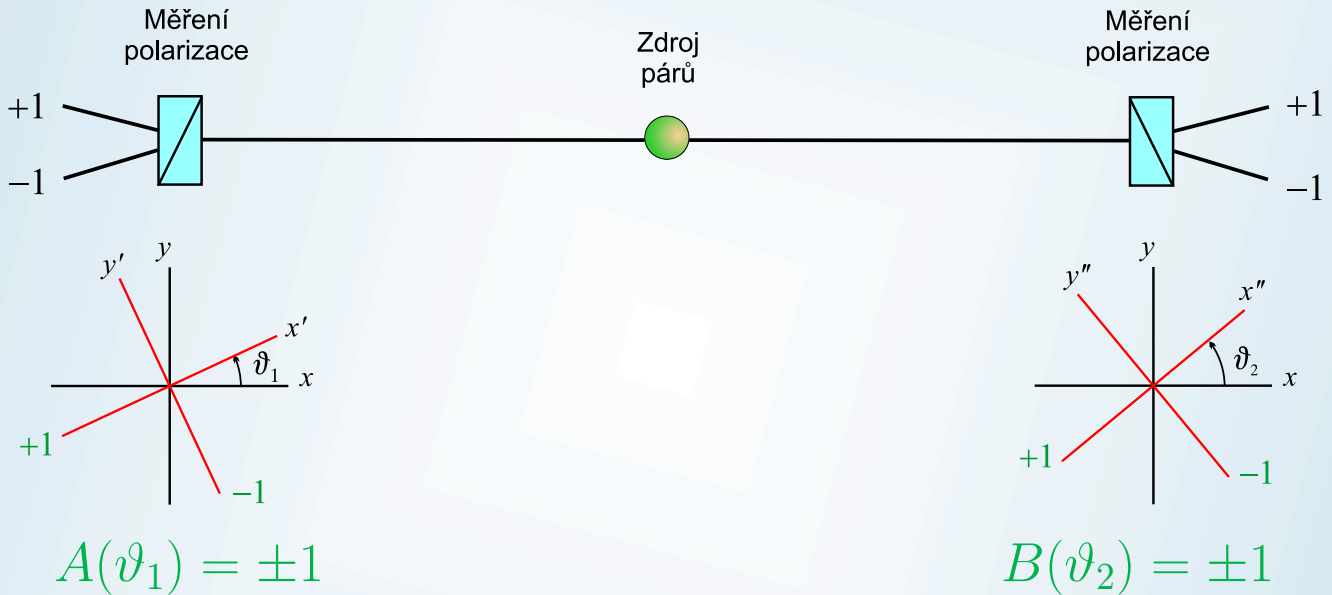
- Entanglovaný stav = „propletený“ stav více částic.
- Nejlepší možná znalost celku není totéž, co nejlepší možná znalost jeho částí.
- Kvantové měření na jedné z částic z entanglovaného systému změní celkový stavový vektor všech částic. (To nicméně nelze využít k okamžitému přenosu informace.)



Entanglement

- Entanglovaný stav = „propletený“ stav více částic.
- Nejlepší možná znalost celku není totéž, co nejlepší možná znalost jeho částí.
- 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



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



Bellovy nerovnosti

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

$$\begin{aligned} C(\vartheta_1, \vartheta_2) &= \langle A(\vartheta_1)B(\vartheta_2) \rangle_{\Lambda} \\ &= \int_{\lambda \in \Lambda} A(\vartheta_1, \lambda) B(\vartheta_2, \lambda) d\rho(\lambda). \end{aligned}$$



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 $+2$:

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

$$-2 \leq \langle \alpha\beta \rangle + \langle \alpha\beta' \rangle + \langle \alpha'\beta \rangle - \langle \alpha'\beta' \rangle \leq +2$$



Bellovy nerovnosti

$$\begin{aligned}\alpha &= A(\vartheta_1), & \alpha' &= A(\vartheta'_1), \\ \beta &= B(\vartheta_2), & \beta' &= B(\vartheta'_2).\end{aligned}$$

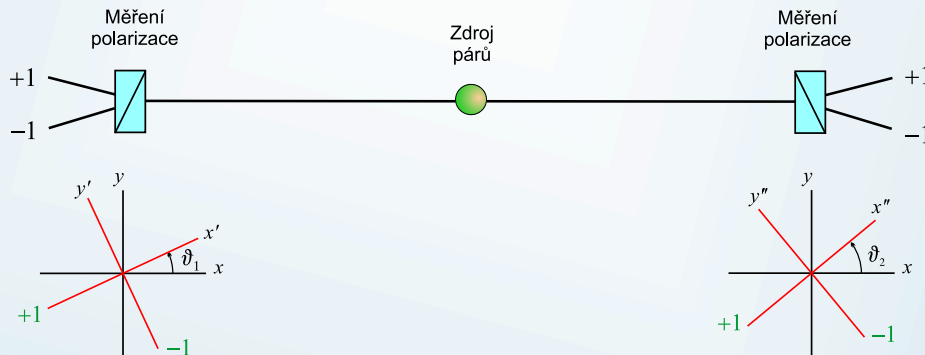
Každá lokálně realistická teorie musí splňovat nerovnost:

$$|C(\vartheta_1, \vartheta_2) + C(\vartheta'_1, \vartheta_2) + C(\vartheta_1, \vartheta'_2) - C(\vartheta'_1, \vartheta'_2)| \leq 2$$

Bellovy nerovnosti

Předpověď kvantové mechaniky:

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





Bellovy nerovnosti

Předpověď kvantové mechaniky – pravděpodobnosti výsledků:

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

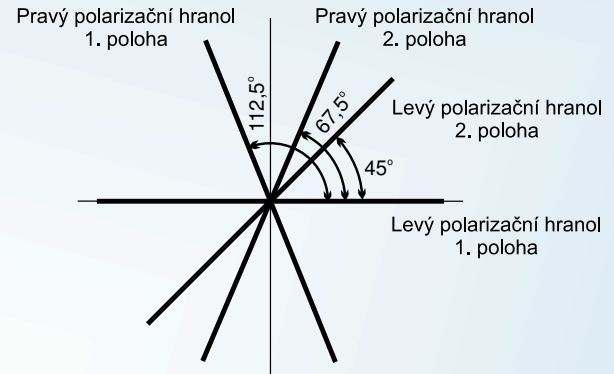
$$P_{+-} = P_{-+} = \frac{1}{2} [\cos(\vartheta_2 - \vartheta_1)]^2$$

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

Bellovy nerovnosti

Zvolme např.

$$\begin{aligned} \vartheta_1 &= 0^\circ, & \vartheta'_1 &= 45^\circ, \\ \vartheta_2 &= 112,5^\circ, & \vartheta'_2 &= 67,5^\circ. \end{aligned}$$

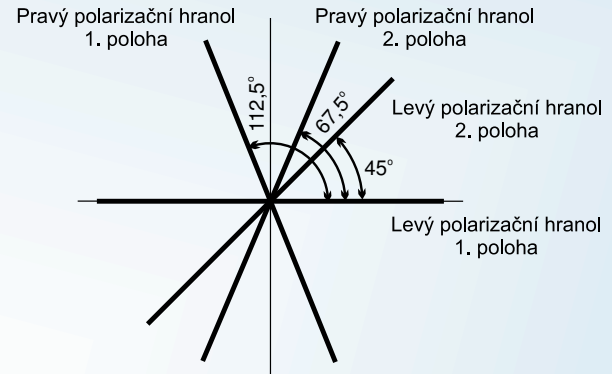


Bellovy nerovnosti

Zvolme např.

$$\vartheta_1 = 0^\circ, \quad \vartheta'_1 = 45^\circ,$$

$$\vartheta_2 = 112,5^\circ, \quad \vartheta'_2 = 67,5^\circ.$$

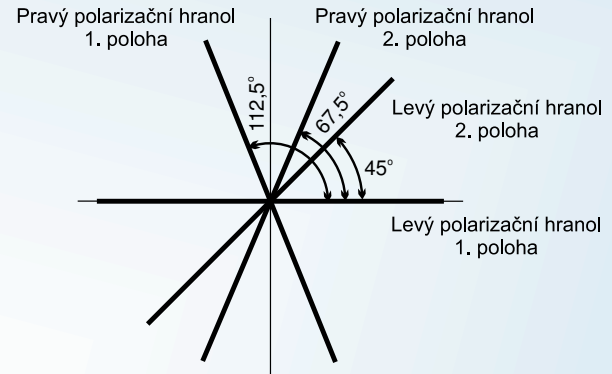


$$\begin{aligned} & |C(\vartheta_1, \vartheta_2) + C(\vartheta'_1, \vartheta_2) + C(\vartheta_1, \vartheta'_2) - C(\vartheta'_1, \vartheta'_2)| \\ &= |-\cos(225^\circ) - \cos(135^\circ) - \cos(135^\circ) + \cos(45^\circ)| \\ &= \mathbf{2\sqrt{2} > 2} \end{aligned}$$

Bellovy nerovnosti

Zvolme např.

$$\begin{aligned} \vartheta_1 &= 0^\circ, & \vartheta'_1 &= 45^\circ, \\ \vartheta_2 &= 112,5^\circ, & \vartheta'_2 &= 67,5^\circ. \end{aligned}$$



$$\begin{aligned} & |C(\vartheta_1, \vartheta_2) + C(\vartheta'_1, \vartheta_2) + C(\vartheta_1, \vartheta'_2) - C(\vartheta'_1, \vartheta'_2)| \\ &= |-\cos(225^\circ) - \cos(135^\circ) - \cos(135^\circ) + \cos(45^\circ)| \\ &= 2\sqrt{2} > 2 \end{aligned}$$

Kvantová teorie porušuje Bellovy nerovnosti !!

Potvrzeno experimentálními testy.



Kvantová fyzika a zpracování informace





Kvantová fyzika a zpracování informace

- Donesávna 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

- Donesávna 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

- 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*
- Oživení zájmu o studium jevů souvisejících se základy kvantové teorie. Informatický pohled na fyziku ukazuje leccos v novém světle.
- Aplikace: **kvantové počítače,**
kvantová kryptografie.



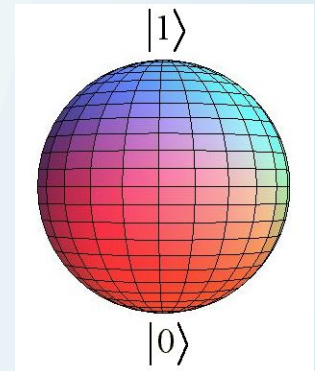
Kvantový bit

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



Kvantový bit

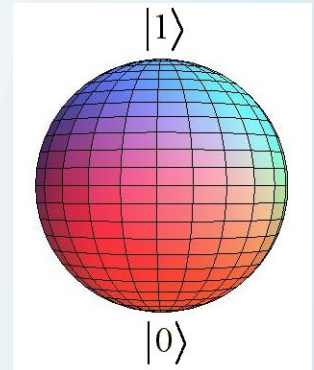
- **Klasický bit:** 0, 1 – např. dvě úrovně napětí.
- **Kvantový bit (qubit):** dvouhladinový kvantový objekt.
 - Bázové stavy: $|0\rangle$, $|1\rangle$
 - Obecný stav – superopozice: $\alpha |0\rangle + \beta |1\rangle$





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)!
 - Příklad (2 qubity): $\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$ ← entanglovaný stav.





TEH POČÍTAČ JE ÚPLNĚ KVANTOVĚJ.
JEN SE NA NĚJ PODÍVAŠ, ŽKOLABUJE.



Kvantové počítače

- 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.
- Pracují v jistém smyslu s mnoha vstupními hodnotami zároveň (superpozice stavů kvantového registru – entanglement).



Kvantová kryptografie

- Metoda pro utajenou komunikaci, jejíž bezpečnost je garantována zákony kvantové teorie.
- 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 odposlech, klíč se nepoužije. Žádná informace neunikne.

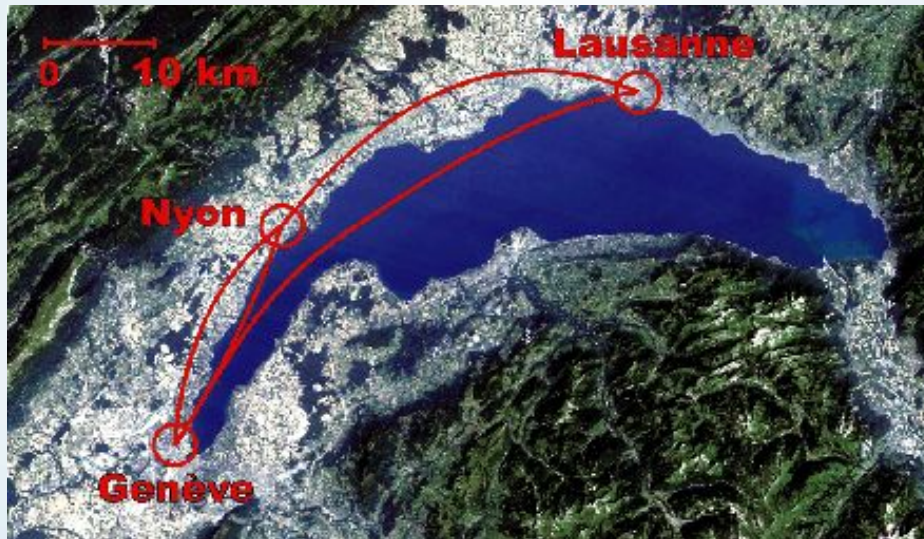


Kvantová kryptografie

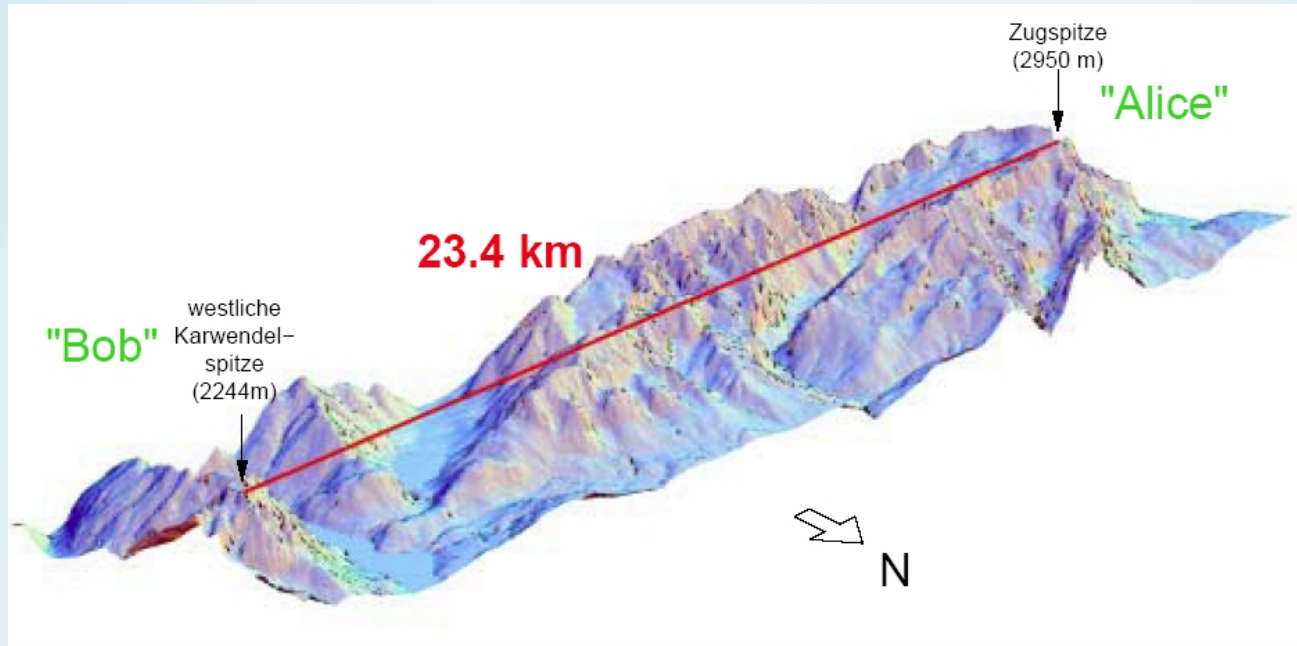
- Kvantová kryptografie sice neumí odposlechu zabránit, ale umí ho odhalit.
- Nepřenáší se zpráva, ale klíč pro Vernamovu šifru. Je-li odhalen odposlech, klíč se nepoužije. Žádná informace neunikne.
- Abeceda, do níž se kóduje = kvantové stavy jedné částice (např. fotonu, částice světla).
- Odposlech = měření na fyzikální entitě nesoucí informaci. Odposlech ovlivní stav částice nesoucí informaci.

Kvantová kryptografie – experimenty

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

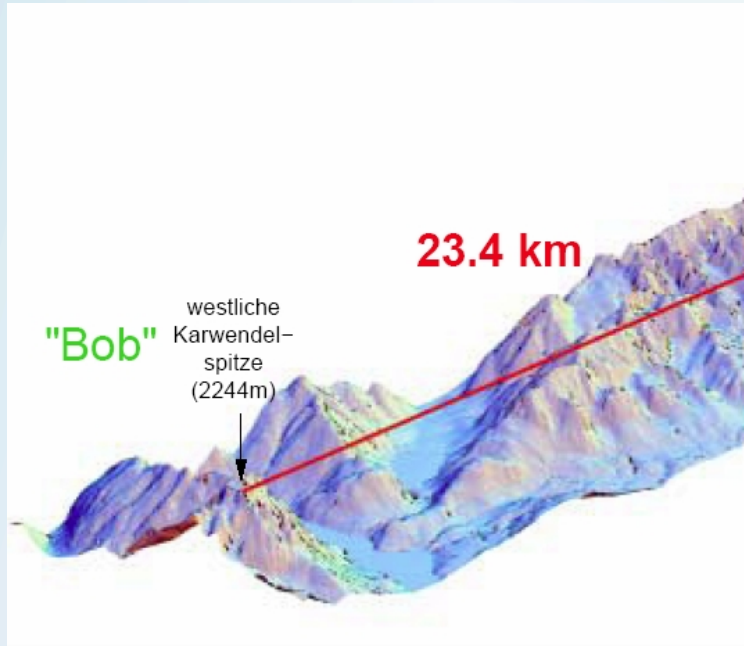


Přenos klíče volným prostorem

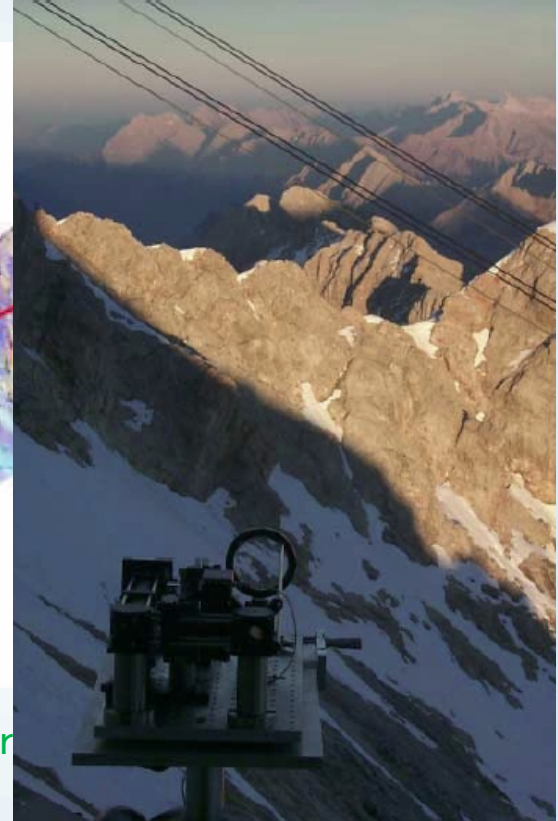


Mnichovská univerzita, prof. Weintfurter, polarizační kódování

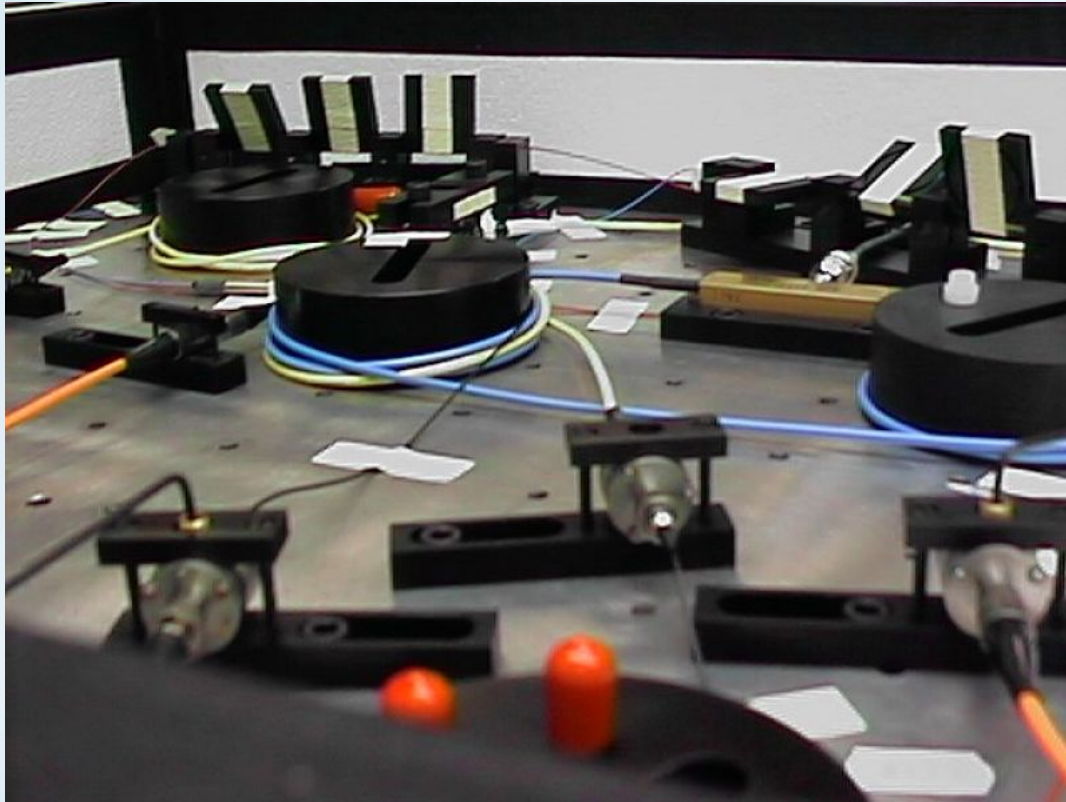
Přenos klíče volným prostorem



Mnichovská univerzita, prof. Weintfurter

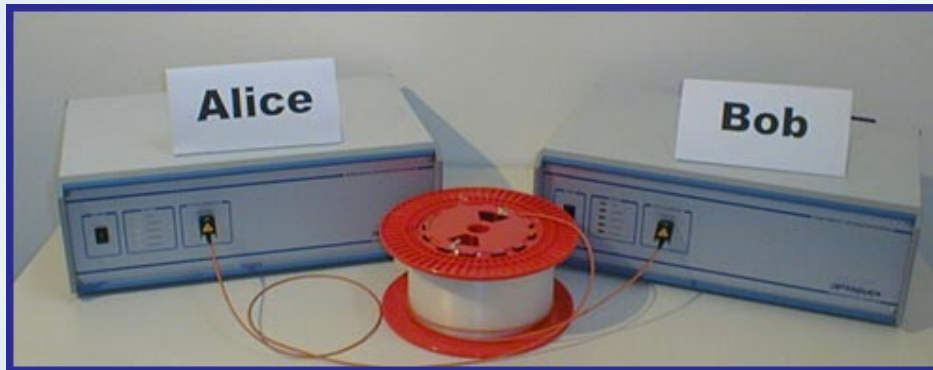


Kvantová kryptografie v Olomouci



Kvantová kryptografie v praxi

- id Quantique



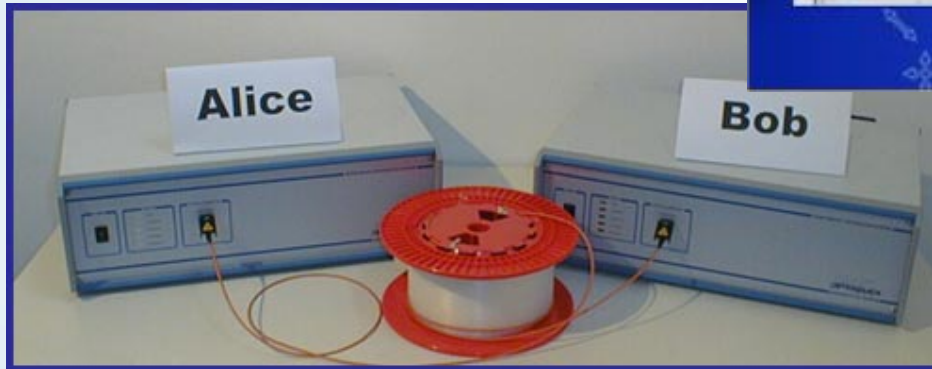
Kvantová kryptografie v praxi

- id Quantique
- MagiQ



Kvantová kryptografie v praxi

- id Quantique
- MagiQ
- SECOQC





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

