Quantum Digital Signature protokol

Jiří Maryška

Department of Physics
Faculty of Nuclear Sciences and Physical Engineering
Czech Technical University in Prague

13. května 2013

Obsah prezentace

- Úvod do kvantové mechaniky
- Koherentní stavy EM pole
- Porovnávání koherentních stavů
- QDS protokol

Popis stavu kvantověmechanického systému

- Stavový prostor: Hilbertův prostor $\mathscr{H}$ s ortonormální bází $\{|i\rangle\}$ a skalárním součinem $\langle\varphi|\psi\rangle$
- Stav systému: Jednorozměrný podprostor $\{\alpha\,|\psi\rangle\,|\alpha \in \mathbb{C}\}$
  Matice hustoty $\rho = \sum_i p_i\,|\psi_i\rangle\,\langle\psi_i|$, $\rho = \rho^\dagger$, $\mathrm{Tr}[\rho] = 1$, $\rho \geq 0$
- Princip superpozice: Jsou-li $|\varphi\rangle$ a $|\psi\rangle$ dva stavy stejného systému pak $\alpha\,|\varphi\rangle + \beta\,|\psi\rangle$ s $|\alpha|^2 + |\beta^2| \neq 0$ je také stav systému
- Je-li $\langle\varphi|\psi\rangle \neq 0$ pak stavy $|\varphi\rangle$ a $|\psi\rangle$ nejsou rozlišitelné

Pozorovatelné na kvantověmechanickém systému

- Pozorovatelná A: $\hat{A} \in \mathscr{L}(\mathscr{H})$, $\hat{A} = \hat{A}^\dagger$
- Střední hodnota pozorovatelné A: $\langle \mathrm{A} \rangle_\psi = \langle \psi | \hat{A} | \psi \rangle$
- Variance pozorovatelné A: $(\Delta \mathrm{A})_\psi = \langle \mathrm{A}^2 \rangle_\psi - \langle A \rangle_\psi^2$
- Komutátor: $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$
- Heisenbergovy relace neurčitosti: $(\Delta \mathrm{A})_\psi (\Delta \mathrm{B})_\psi \geq \frac{1}{2} | \langle [A, B] \rangle_\psi |$

Hamiltonián

- Operátor $\hat{H}$ příslušící pozorovatelné energii
- Časový vývoj stavu $|\psi\rangle$ splňuje rovnici $ih\frac{d}{dt}|\psi\rangle = \hat{H}|\psi\rangle$

Měření na kvantověmechanickém systému

- Hodnoty pozorovatelné A které lze naměřit jsou shodné se spektrem operátoru $\hat{A}$: $\sigma(\hat{A}) = \{\lambda_i\}$
- Vlastní vektory operátoru $\hat{A}$ $\{|\psi_i\rangle\}$ tvoří ONB $\mathscr{H}$, $\hat{A}\,|\psi_i\rangle = \lambda_i\,|\psi_i\rangle$
- Pro obecný stav $|\psi\rangle = \sum_i \alpha_i\,|\psi_i\rangle$, $\sum_i |\alpha_i|^2 = 1$ je pravděpodobnost naměření hodnoty λ_i rovna $p(\hat{A} = \lambda_i) = |\,\langle\psi_i|\psi\rangle\,|^2 = |\alpha_i|^2$
- Měření mění stav systému - stav systému okamžitě po měření je dán vektorem $|\psi_i\rangle$

Kvantový harmonický oscilátor

- Hamiltonián kvantového harmonického oscilátoru má tvar $\hat{H} = \frac{1}{2}(\hat{P}^2 + \hat{Q}^2)$
- Zavedeme nehermitovský operátor $\hat{a} = \frac{1}{\sqrt{2}}(\hat{Q} + i\hat{P})$. Pomocí tohoto operátoru lze psát $\hat{H} = \hat{a}^\dagger \hat{a} + \frac{1}{2}\hat{I}$
- Pro spektrum $\hat{H}$ platí $\sigma(\hat{H}) = \{n + \frac{1}{2} | n \in \mathbb{N}_0\}$
- Vlastní stavy $|n\rangle$, $n \in \mathbb{N}_0$ splňují $\hat{H}\,|n\rangle = (n + \frac{1}{2})\,|n\rangle$, jsou interpretovány jako stavy s n fotony

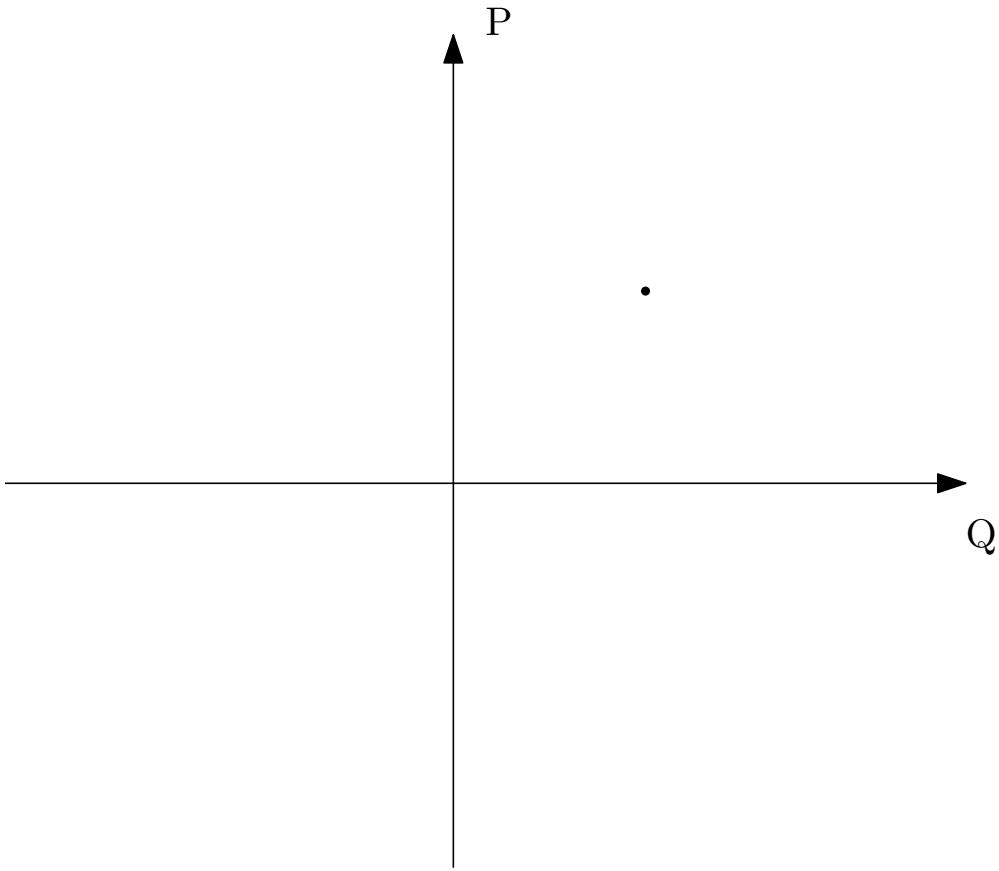
Koherentní stavy

- Formální definice koherentního stavu

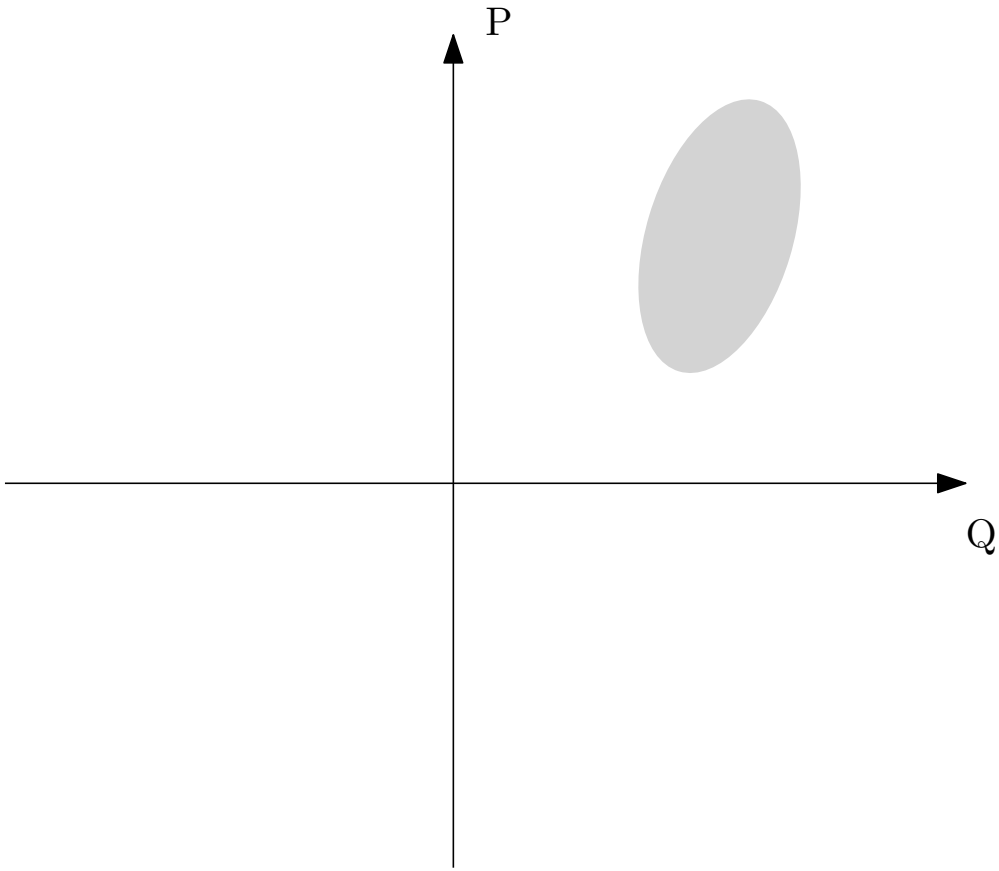
  $\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle,\ \alpha \in \mathbb{C}$

- Řešením předchozí rovnice je stav $|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle$
- Pro relace neurčitosti platí $(\Delta Q)_\alpha (\Delta P)_\alpha = \frac{1}{2},\ (\Delta Q)_\alpha = (\Delta P)_\alpha$
- Pro skalární součin platí $|\,\langle \alpha' | \alpha \rangle\,|^2 = e^{-|\alpha - \alpha'|^2} \neq 0$

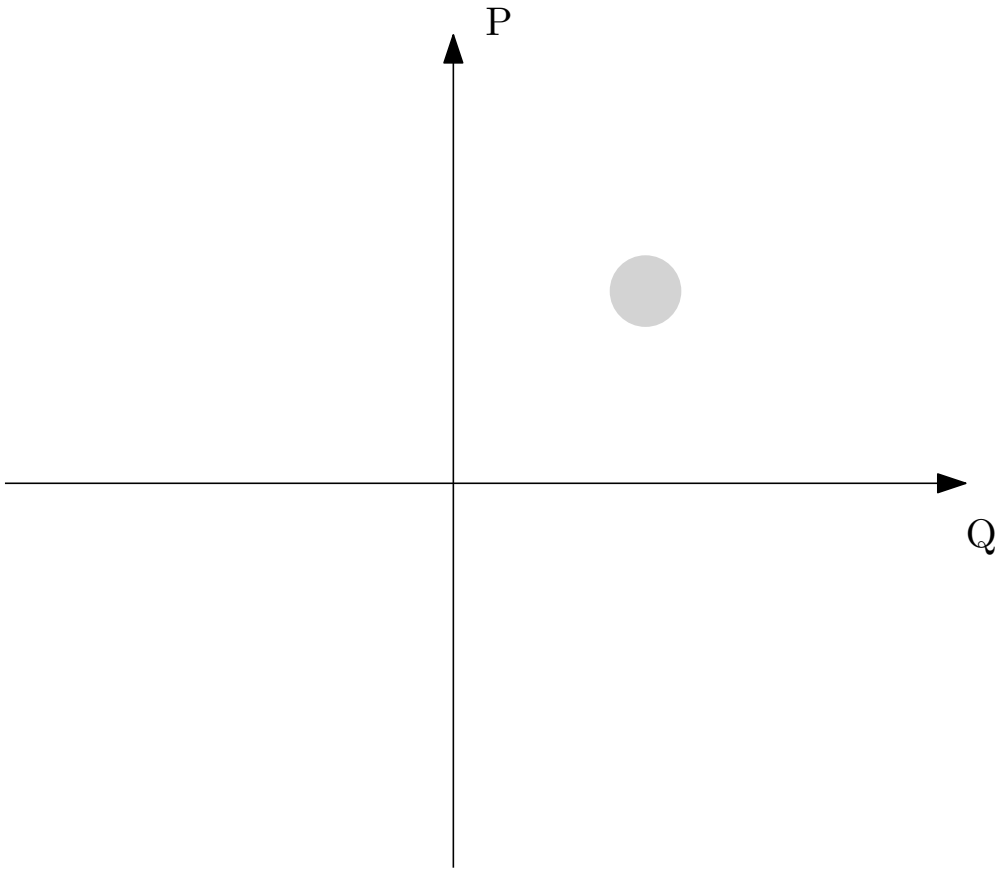
Fázový prostor



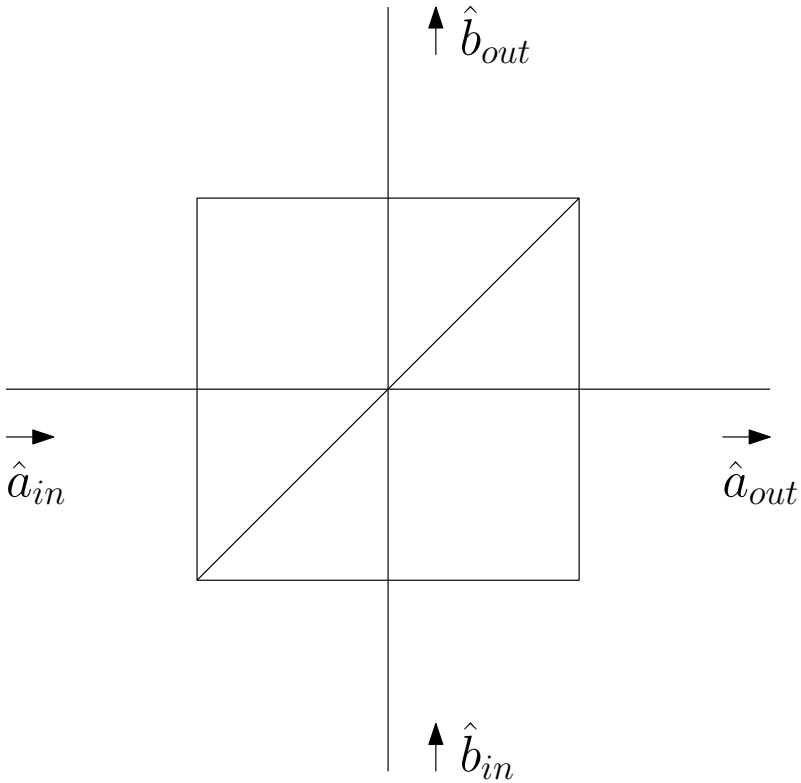
Fázový prostor



Fázový prostor



Dělič paprsků



Porovnávání koherentních stavů

- $\hat{a}_{out} = \frac{1}{\sqrt{2}}(\hat{a}_{in} + \hat{b}_{in})$
  $\hat{b}_{out} = \frac{1}{\sqrt{2}}(\hat{a}_{in} - \hat{b}_{in})$
- $|\alpha\rangle_{in} \otimes |\beta\rangle_{in} \rightarrow |\frac{\alpha+\beta}{\sqrt{2}}\rangle_{out} \otimes |\frac{\alpha-\beta}{\sqrt{2}}\rangle_{out}$
- Je-li $\alpha = \beta$, pak na výstupu děliče paprsků je stav $|\sqrt{2}\alpha\rangle_{out} \otimes |0\rangle_{out}$
- Dalším použitím děliče paprsků na první stav dostaneme stav $|\alpha\rangle \otimes |\alpha\rangle$, tj. původní vstupní stav
- Toto měření má tzv. nedemoliční charakter, pokud stav $|\alpha\rangle \otimes |\beta\rangle$ úspěšně projde testem lze ho pomocí dalšího děliče paprsků zpětně zrekonstruovat

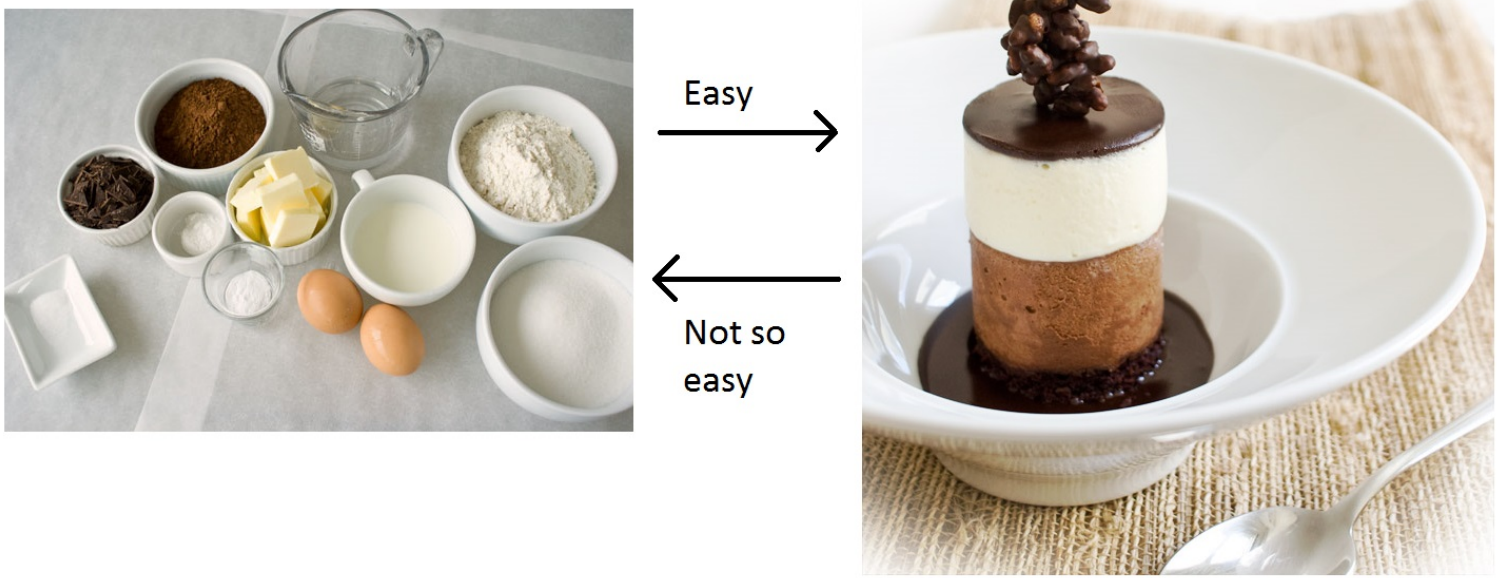
Cíl DS

- Cílem je, aby Alice byla schopna podepsat posílanou zprávu tak, aby si kdokoliv mohl ověřit, že zpráva skutečně pochází od Alice.

Obecný algoritmus

- Předpokládejme že Alice má k dispozici jednocestnou funkci $f : k \to f(k)$
- Alice zvolí k_0 a k_1
- Alice veřejně ohlásí $(0, f(k_0))$ a $(1, f(k_1))$
- K poslání podepsaného bitu b poskytne Alice dvojici (b, k_b). Kdokoliv si může ověřit výpočtem $f(k_b)$ shodu s předchozím oznámením $f(k_0)$ a $f(k_1)$
- Bezpečnost je zaručena obtížností nalézání vzorů $f(k)$

Jednocestné funkce



Kvantové jednocestné funkce

- Mějme množinu koherentních stavů

  $\{|e^{\frac{2i\pi k}{N}}\alpha\rangle = |\alpha_k\rangle \,|k \in \{0,\ldots,N-1\}\}$

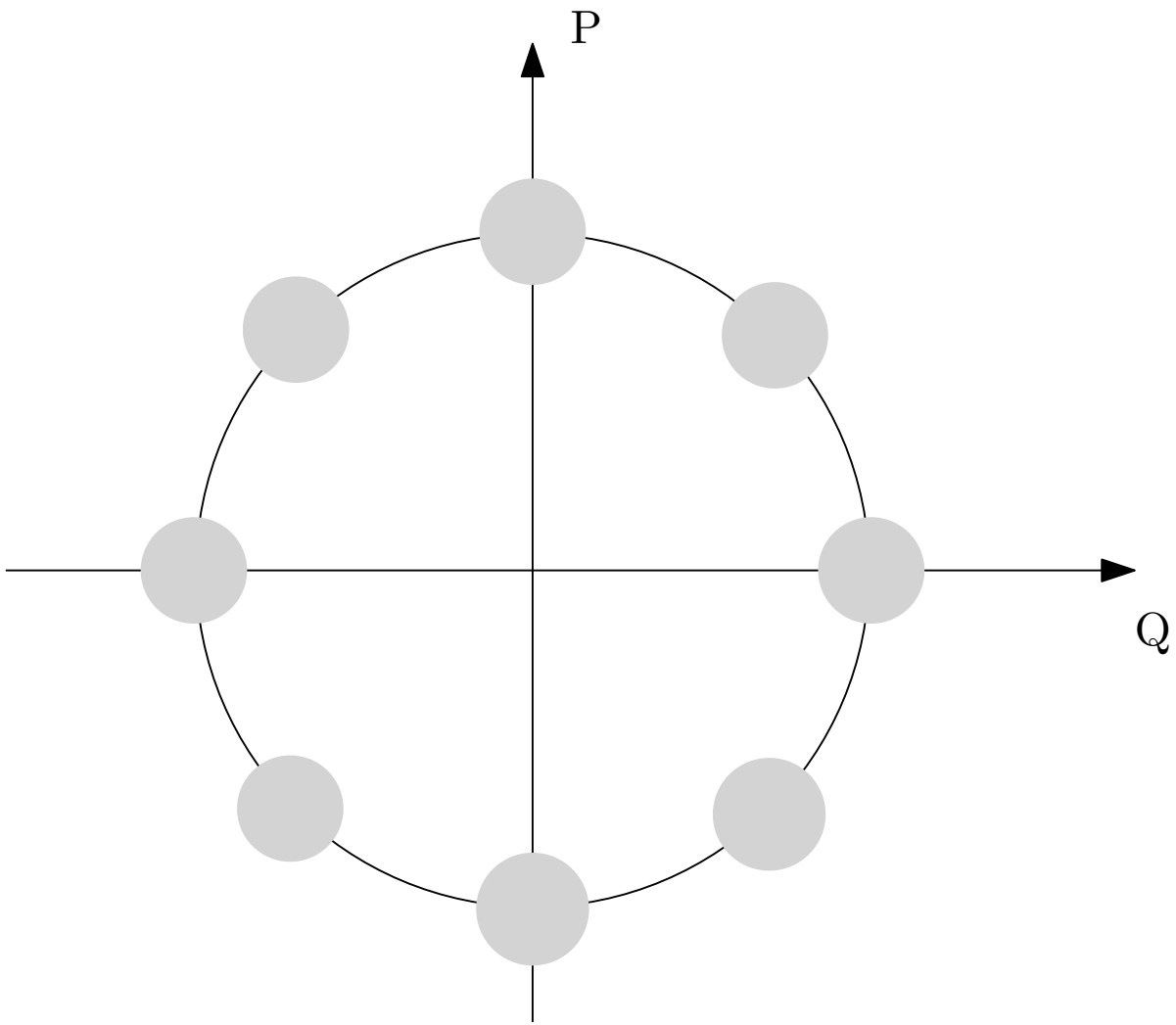
- Při vhodné volbě α a N je funkce $f(k) = |\alpha_k\rangle$ jednocestnou funkcí

- Holevova mez: Udává klasickou informaci kterou lze z kvantového systému ve stavu popsaném maticí hustoty $\rho = \sum_k p_k \rho_k$ získat jedním měřením
  $I_{acc} \leq S(\rho) - \sum_k p_k S(\rho_k)$, kde $S(\rho) = -\mathrm{Tr}[\rho \log \rho]$

- Je-li k zvoleno náhodně, pak $\rho = \frac{1}{N}\sum_k |\alpha_k\rangle \langle\alpha_k|$

- Je-li $\log N \gg S(\rho)$ pak $I_{acc} \ll 1$

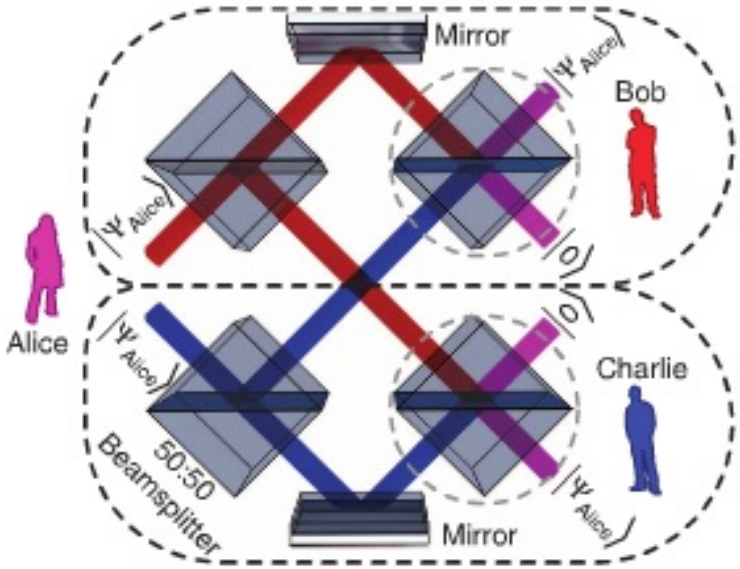
Kvantové jednocestné funkce



QDS

- Předpokládejme, že Alice chce poslat podepsaný bit Bobovi a Charliemu
- Alice vytvoří stavy $|\psi^0\rangle = |\alpha_{j_1^0}\rangle \otimes \cdots \otimes |\alpha_{j_M^0}\rangle$ a $|\psi^1\rangle = |\alpha_{j_1^1}\rangle \otimes \cdots \otimes |\alpha_{j_M^1}\rangle$ kde $|\alpha_{j_k^i}\rangle$ je volen náhodně z množiny $\{|\alpha_k\rangle\}$
- K poslání podepsaného bitu b Bobovi a Charliemu Alice pošle speciálním interferometrem dvojici $(b, |\psi^b\rangle)$ jako Bobovi tak Charliemu

QDS


Mirror
|Ψ Alice⟩
Bob
|Ψ Alice⟩
|0⟩
Alice
|0⟩
|Ψ Alice⟩
Charlie
50:50
Beamsplitter
|Ψ Alice⟩
Mirror

QDS

- Poslala-li Alice Bobovi a Charliemu různé stavy, není na výstupech interferometru stav $|0\rangle$
- Po ověření shodnosti obou stavů Alice sdělí Bobovi a Charliemu posloupnost $(j_1, \ldots, j_M)$. Bob a Charlie potom mohou vytvořit stav $|\psi^b\rangle$ a provést porovnání tohoto koherentního stavu se stavem který zaslala Alice
- Bezpečnost je zaručena Holevovou mezí, je-li T počet kopií $|\psi^b\rangle$ a platí $M \log N \gg T \cdot S(\rho)$ pak $I_{acc} \ll 1$

Reference

- E. Andersson, M. Curty and I. Jex. Experimentally realizable quantum comparison of coherent states and its applications, Physical Review, **A74**, 022304-1, 2006
- P.J. Clarke, R.J. Collins, V. Dunjko, E. Andersson, J. Jeffers and G.S. Buller. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light, Nature Communications **3:1174** doi:10.1038/ncomms2172, 2012