Sdílení kvantového tajemství ve spojitých proměnných

Tomáš Tyc

Ústav teoretické fyziky a astrofyziky, PřF MU Brno

Ve spolupráci s: Barry C. Sanders, David J. Rowe
na Department of Physics, Macquarie University, Sydney, Austrálie

- sdílení tajemství
- prahové schéma $(2, 3)$
- experimentální realizace
- obecné prahové schéma
- minimalizace počtu stlačovačů
- konečné zdroje stlačení

Sdílení tajemství

- České korunovační klenoty – trezor se sedmi zámky, klíče má prezident, předseda vlády, parlamentu, ...
- ti všichni musí **spolupracovat**, aby trezor otevřeli
- sdílení tajemství (secret sharing) – způsob, jak rozdělit tajemství (informaci) mezi n osob (hráčů) tak, aby předem dané skupiny mohly pomocí spolupráce tajemství získat
- **autorizované skupiny** – mohou získat tajemství dokonale
- ostatní skupiny neautorizované – nedozví se o tajemství zhola nic
- příklad – 2 hráči, binární tajemství $a \in \{0, 1\}$
- jednomu hráči dáme a, druhému součet $a + b \bmod 2$, kde $b \in \{0, 1\}$ je náhodné číslo
- **přístupová struktura** – definuje, které skupiny mohou tajemství získat
- prahové schéma (k, n) (threshold scheme) – tajemství získá libovolných k hráčů
- sdílení klasického tajemství existuje pro libovolnou přístupovou strukturu

Sdílení kvantového tajemství

- tajemstvím je kvantová informace, tedy kvantový stav $|\psi\rangle$ z daného Hilbertova prostoru
- **distributor** (dealer) zakóduje tajemství a jeho části rozdělí **hráčům**
- části tajemství jsou rovněž kvantové stavy
- cílem spolupracující skupiny je získat (rekonstruovat) tento stav $|\psi\rangle$
- **rekonstrukce** (extrakce) se provádí pomocí aplikace unitárních operací na stavy spolupracujících hráčů
- je-li tajmeství provázáno (entangled) s jiným stavem, toto provázání se po rekonstrukci obnoví
- pro některé přístupové struktury neexistuje sdílení kvantového tajemství kvůli nemožnosti klonování
- naše práce – nalézt a optimalizovat sdílení tajemství ve spojitých proměnných a navrhnout jeho experimentální realizaci

Prahové schéma (2,3)

- tajemství ve spojité bázi

$$|\psi\rangle = \int_{\mathbb{R}} \psi(x)|x\rangle \,\mathrm{d}x$$

- zakódujeme do provázaného stavu 3 módů

$$|\Phi\rangle = \int_{\mathbb{R}^2} \psi(x_1) \left|\frac{x_2 + x_1}{\sqrt{2}}\right\rangle_1 \left|\frac{x_2 - x_1}{\sqrt{2}}\right\rangle_2 |x_2\rangle_3 \,\mathrm{d}x_1 \,\mathrm{d}x_2$$

jak získáme tajemství z módů 1 a 2?

- hráči 1 a 2 aplikují takový unitární operátor $\hat{U}$, aby

$$\hat{U}_{12}|X\rangle_1|Y\rangle_2 = \left|\frac{X - Y}{\sqrt{2}}\right\rangle_1 \left|\frac{X + Y}{\sqrt{2}}\right\rangle_2$$

- po aplikaci $\hat{U}_{12}$ na módy 1 a 2 bude celkový stav

$$\hat{U}_{12}|\Phi\rangle = \int_{\mathbb{R}^2} \psi(x_1)|x_1\rangle_1|x_2\rangle_2|x_2\rangle_3 \,\mathrm{d}x_1 \,\mathrm{d}x_2 = |\psi\rangle_1 \,|\mathrm{EPR}\rangle_{23}$$

- první mód se nachází ve stavu $|\psi\rangle$
- módy 2 a 3 jsou v maximálně provázaném stavu, kdy $x^{(2)} - x^{(3)} = 0$, $p^{(2)} + p^{(3)} = 0$ (tzv. EPR stav)
- hráči 1 a 3 postupují obdobně:

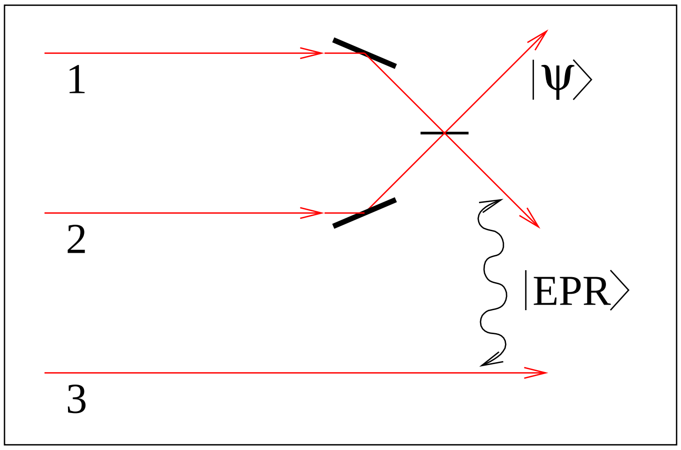
$$\hat{U}_{13}|X\rangle_1|Y\rangle_3 = |\sqrt{2}\,X - Y\rangle_1|\sqrt{2}\,Y - X\rangle_3$$

- po aplikaci $\hat{U}_{13}$ na módy 1 a 3 bude celkový stav

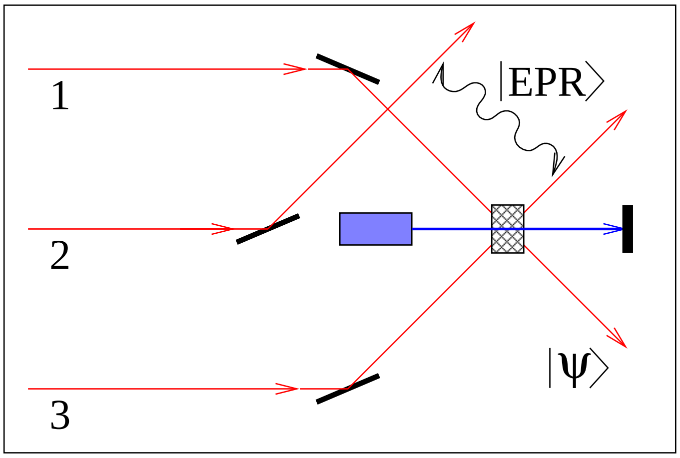
$$\begin{aligned}\hat{U}_{13}|\Phi\rangle &= \int_{\mathbb{R}^2} \psi(x_1)|x_1\rangle_1 \left|\frac{x_2 - x_1}{\sqrt{2}}\right\rangle_2 \left|\frac{x_2 - x_1}{\sqrt{2}}\right\rangle_3 \,\mathrm{d}x_1 \,\mathrm{d}x_2 \\ &= \int_{\mathbb{R}^2} \psi(x_1)|x_1\rangle_1|y\rangle_2|y\rangle_3 \,\mathrm{d}x_1 \,\mathrm{d}y = |\psi\rangle_1 \,|\mathrm{EPR}\rangle_{23}\end{aligned}$$

Experimentální provedení

- $|\Phi\rangle$ – stav tří módů světla
- x_i – kvadratury módů
- su(2) transformace $\hat{U}_{12}$ – 50/50 dělič svazků

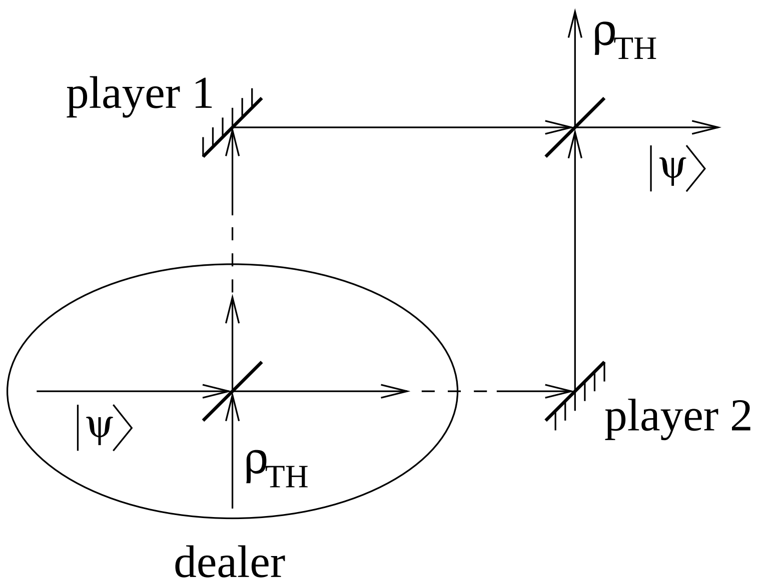


- su(1,1) transformace $\hat{U}_{13}$ – dvojmódový stlačovač



- kódování distributora – inverzní interferometr k interferometru pro hráče 1,2 a jeden EPR stav

- překvapivě jednoduché (2,2) schéma vnikne zničením třetí části tajemství



Prahové schéma $(k, 2k-1)$

- jiná schémata lze získat z tohoto tak, že zničíme některé části tajemství
- n-módový zakódovaný stav

$$|\Phi\rangle = \int \psi(x_1)\,|L_1(\{x_i\})\rangle_1|L_2(\{x_i\})\rangle_2\cdots|L_{2k-1}(\{x_i\})\rangle_{2k-1} \times \, \mathrm{d}x_1\,\mathrm{d}x_2\cdots\,\mathrm{d}x_k,$$

- $L_1, \ldots, L_{2k-1}$ jsou lineární kombinace $x_1, \ldots, x_k$
- všechny k–prvkové podmnožiny množiny $\{x_1, L_1, \ldots, L_{2k-1}\}$ musí být lineárně nezávislé
- Uvažujme, že hráči $1, 2, \ldots, k$ chtějí rekonstruovat tajemství
- Podobně jako předtím – chceme získat tajemství a nějaké EPOR páry
- Hráči naleznou čtvercovou matici T, aby platilo

$$T: \quad \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_k \end{pmatrix} \quad \longrightarrow \quad \begin{pmatrix} x_1 \\ L_{k+1} \\ \vdots \\ L_{2k-1} \end{pmatrix}$$

- aplikací T na $|\Phi\rangle$ dostaneme celkový stav

$$|\Phi\rangle \to \int \psi(x_1)\,|x_1\rangle_1 \times |L_{k+1}\rangle_2\cdots|L_{2k-1}\rangle_k|L_{k+1}\rangle_{k+1}\cdots|L_{2k-1}\rangle_{2k-1}\,\mathrm{d}x_1\,\mathrm{d}L_{k+1}\cdots\,\mathrm{d}L_{2k-1}$$

$$= |\psi\rangle_1\,|\mathrm{EPR}\rangle_{2,k+1}|\mathrm{EPR}\rangle_{3,k+2}\cdots|\mathrm{EPR}\rangle_{k,2k-1}$$

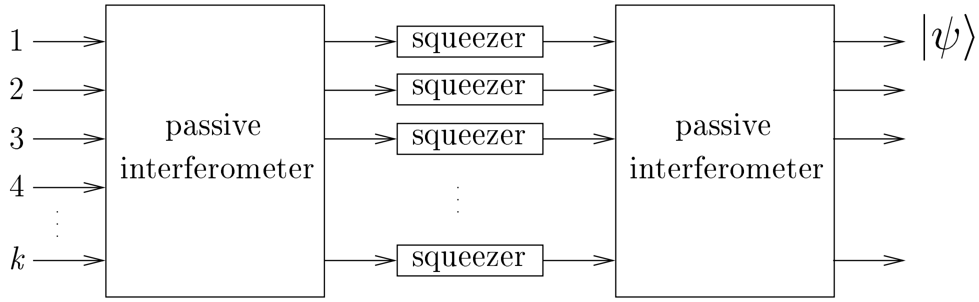
- pro každou autorizovanou skupinu hráčů existuje interferometr, který rekonstruuje tajemství z jejich dílů

- matici T lze rozložit jako

$$T = UT_dV,$$

kde U, V jsou ortogonální a T_d je diagonální

- T lze realizovat dvěma pasivními interferometry (U, V) a k jednomódovými stlačovači (T_d)



Optimalizace schématu

- ve volbě transformace T je jistá volnost:

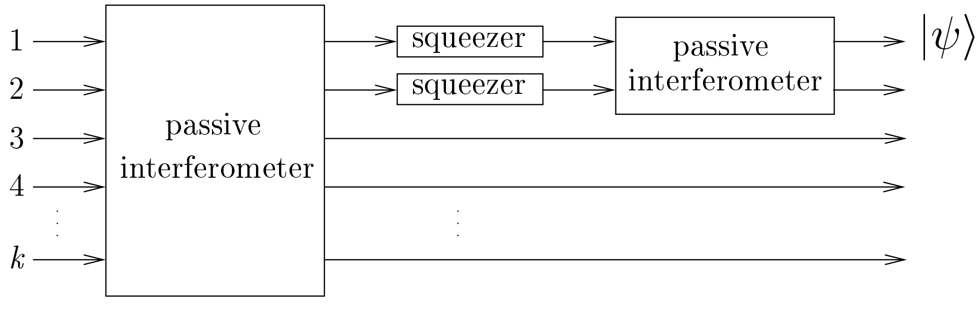
$$T' : \quad \begin{pmatrix} L_1 \\ L_2 \\ \vdots \\ L_k \end{pmatrix} \quad \longrightarrow \quad \begin{pmatrix} x_1 \\ M_2(L_{k+1}, \ldots, L_{2k-1}) \\ \vdots \\ M_k(L_{k+1}, \ldots, L_{2k-1}) \end{pmatrix}$$

- pro minimalizaci potřebného stlačení zkusme zvolit T' „co nejortogonálnější“
- zadefinujeme-li skalární součin tak, aby vektory $L_1, L_2, \ldots, L_k$ tvořily ortonormální systém, snažíme se, aby systém $x_1, M_2, M_3, \ldots, M_k$ byl co nejortogonálnější
- zvolíme $M_2, M_3, \ldots, M_k$ jako ortonormální bázi podprostoru generovaného vektory $L_{k+1}, \ldots, L_{2k-1}$
- pak postačí stlačení v rovině (2D)
- T' lze rozložit jako

$$T' = \left(\begin{array}{cc|ccc} \alpha & \beta & 0 & \ldots & 0 \\ 0 & \gamma & 0 & \ldots & 0 \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & I & \\ 0 & 0 & & & \end{array}\right) O$$

  kde O je ortogonální

- stačí pouze dva stlačovače



Konečné zdroje stlačení pro distributora

- pokud distributor nemá přístup k EPR párům, schéma nebude pracovat ideálně
- Wignerova funkce rekonstruovaného tajemství bude gaussovskou konvolucí původní Wignerovy funkce

Závěr

- nalezli jsme obecný způsob, jak sdílet kvantové tajemství ve spojitých proměnných
- schéma lze realizovat s pouhými dvěma stlačovači (plus vstupní stavy pro distributora)
- náš výsledek lze zobecnit na libovolnou přístupovou strukturu
- stále mnoho praktických problémů – skladování částí tajemství (dekoherence), požadavek vysoce stlačených stavů, nedokonalosti přístrojů atd.
- mnoho zajímavých problémů do budoucna – „spravedlivé“ sdílení tajemství, kritéria experimentálního provedení apod.