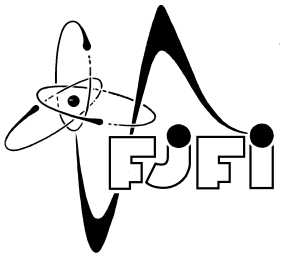
České vysoké učení technické v Praze

Fakulta jaderná a fyzikálně inženýrská

Katedra fyziky



Kvantová komunikace s koherentními stavy

BAKALÁŘSKÁ PRÁCE

Autor: Jiří Maryška

Školitel: prof. Ing. Igor Jex, DrSc.

Akademický rok: 2010/2011

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím uvedené literatury.

Nemám závažný důvod proti použití tohoto školního díla ve smyslu § 60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne Jiří Maryška

. . . .

Poděkování

Rád bych na tomto místě poděkoval svému školiteli, panu prof. Ing. Igoru Jexovi DrSc. za veškerou pomoc kterou mi při vzniku této práce poskytl, zvláště za podnětné konzultace a cenné připomínky. Rád bych také poděkoval panu prof. Nobuyuki Imotovi za ochotu zkonzultovat mé výsledky. Dále bych rád poděkoval všem, kteří přispěli ke konečné podobě této práce ať už jejím pečlivým přečtením, či pomocí s vizuální stránkou.

Název práce: **Kvantová komunikace s koherentními stavy**

Autor: Jiří Maryška

Advisor: prof. Ing. Igor Jex, DrSc.

Abstrakt:

V této práci se budeme věnovat možnému využití kvantové mechaniky pro potřebu bezpečné komunikace. Hlavní náplň je věnována detailnímu popisu několika kryptografických protokolů, které využívají vlastností koherentních stavů. Zvláštní pozornost je věnována kvantitativnímu odhadu bezpečnosti uvedených protokolů vůči několika metodám odposlouchávání.

Klíčová slova: Kvantová optika, teorie informace, kryptografie, kvantová kryptografie, koherentní stavy

Title: **Quantum comunication with coherent states**

Author: Jiří Maryška

Abstract:

In this work, we will examine the possible applications of quantum mechanics for needs of the secret communication. The main part is dedicated to the detailed description of several cryptographic protocols which are using coherent states. Special attention is devoted to the quantitative estimation of security of stated protocols in relation to the several eavesdropping strategies.

Keywords: Quantum optics, theory of information, cryptography, quantum cryptography, coherent states

Obsah

Kapitola 1

Úvod

Potřeba bezpečné komunikace je stará jako písmo samo. Od doby prvního zařízení používaného k bezpečné komunikaci SCYTALE (viz. [1]) byla vyvinuta spousta kryptografických systémů a protokolů, o většině z nich však není dokázáno, že jsou bezpečné vůči libovolným typům odposlouchávání. Cílem této práce je seznámit čtenáře se základy kryptografie a možnostmi, které na toto pole přináší kvantová mechanika.

První kapitola je stručným úvodem do světa kvantové mechaniky. Zavedeme zde formalismus používaný v dalších kapitolách a upozorníme, které vlastnosti kvantové mechaniky budou pro další text zásadní.

V druhé kapitole definujeme koherentní stavy elektromagnetického pole. Ukážeme, že nabývají rovnosti v Heisenbergových relacích neurčitosti a prozkoumáme některé jejich další vlastnosti. Dále zde zmíníme stlačené koherentní stavy, které jsou zobecněním koherentních stavů.

V třetí kapitole je stručně popsán úvod do teorie informace. Budeme se zde věnovat jak klasické teorii informace, tak i kvantové teorii informace. V obou případech zavedeme pojem entropie, který v teorii informace hraje zásadní roli. Dále probereme základní typ kanálu - binární symetrický kanál, který bude důležitý v dalších kapitolách.

Čtvrtá kapitola je úvodem do bezpečné komunikace - kryptografie. Uvedeme zde hlavní typy protokolů a na příkladu ukážeme, čím může kvantová mechanika přispět k bezpečné komunikaci.

V páté kapitole detailně popíšeme několik kryptografických protokolů, které využívají vlastností koherentních stavů, nebo stlačených koherentních stavů. Dále zmíníme několik

možných metod odposlouchávání a zdůvodníme, proč jsou proti nim dané protokoly odolné.

1.1 Postuláty kvantové mechaniky

Kvantová mechanika je založena na tzv. postulátech [2], které jsou obdobou axiomů z matematických teorií. Zde uvedeme jednotlivé postuláty a základní důsledky, které mají.

1.1.1 Postulát o vlnové funkci

Každému fyzikálnímu systému (částici) je přiřazen komplexní Hilbertův prostor $\mathscr{H}$(viz. např. [3]), tzv. stavový prostor. Jednotlivé stavy systému jsou popsány komlexními funkcemi $\psi(x,t) \in \mathscr{H}$, nazývaných vlnovými funkcemi, které tvoří vektory daného stavového prostoru. Jsou-li ψ_1 a ψ_2 možné stavy fyzikálního systému, potom vektor ψ daný vztahem

$$\psi = c_1\psi_1 + c_2\psi_2,$$

kde $c_1, c_2 \in \mathbb{C}$ je také možný stav daného systému. Je-li systém tvořen více částicemi, z nichž každé je přiřazen stavový prostor $\mathscr{H}_i$, potom stavový prostor celého systému má tvar $\mathscr{H} = \Pi_i^{\otimes}\mathscr{H}_i$.

Bornova interpretace vlnové funkce je, že veličina $|\psi(x,t)|^2$ je úměrná hustotě pravděpodobnosti nalezení částice v intervalu $(x, x+dx)$ v čase t.

Na stavovém prostoru je zaveden skalární součin funkcí $\psi(x,t)$ a $\phi(x,t)$ jako

$$(\psi, \phi) = \int_{\mathbb{R}} \psi^*(x,t)\phi(x,t)dx.$$

Stav systému je dán jednoznačně až na tzv. globální fázi. Je totiž zřejmé, že pro $\Psi(x,t) = e^{i\omega}\psi(x,t)$ a $\Phi(x,t) = e^{i\omega}\phi(x,t)$ platí $(\Psi, \Phi) = (\psi, \phi)$. Dále pro $c \in \mathbb{C}$ platí, že funkce $\psi(x,t)$ a $\phi(x,t) = c\psi(x,t)$ popisují stejný stav daného fyzikálního systému. Aby vlnová funkce mohla mít plně pravděpodobnostní interpretaci, volí se většinou tzv. normalizované stavy, tj. je-li stav systému popsán vektorem ψ, potom za stavový vektor volíme

$$\Psi(x,t) = \frac{1}{(\psi,\psi)}\psi(x,t).$$

1.1.2 Postulát o operátorech

Každé fyzikální veličině, která je měřitelná (tzv. pozorovatelná) je přiřazen lineární hermitovský operátor $\hat{A} : \mathscr{H} \to \mathscr{H}$. Tvar těchto operátorů je potom až na výjimky odvozen z principu korespondence.

Nejzákladnější operátory v kvantové mechanice jsou operátor polohy $\hat{x}$ a operátor hybnosti $\hat{p}$. Máme-li dán stav ψ, potom tyto operátory působí následovně:

$$\hat{x}\psi(x,t) = x\psi(x,t),$$
$$\hat{p}\psi(x,t) = -i\hbar\frac{\partial}{\partial x}\psi(x,t).$$

Je zřejmé, že při používání operátorů záleží na pořadí, tj. jsou-li $\hat{A}$ a $\hat{B}$ dva operátory na prostoru $\mathscr{H}$, potom nemusí platit $\hat{A}\hat{B} = \hat{B}\hat{A}$. Důležitým operátorem je proto tzv. komutátor, definovaný vztahem

$$[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}.$$

V kvantové mechanice se občas vyskytují veličiny, které nemají klasický protějšek. V takovém případě je nutné zavést příslušný operátor nezávisle na klasické fyzice, ale například z experimentálního uspořádání.

1.1.3 Postulát o kvantování

Jediné hodnoty, které může měřitelná fyzikální veličina A při jednotlivých měřeních nabývat, jsou vlastní čísla A_n příslušného operátoru $\hat{A}$. Množinu všech těchto vlastních čísel nazýváme spektrem operátoru $\hat{A}$ a značíme $\sigma(\hat{A})$. Dále je-li systém popsán v okamžiku měření vlnovou funkcí ψ, pak střední hodnota veličiny A je dána vztahem

$$\langle A \rangle = \frac{(\psi, \hat{A}\psi)}{(\psi, \psi)}.$$

V kvantové mechanice předpokládáme, že každému lineárnímu hermitovskému operátoru $\hat{A}$ se spektrem $\sigma(\hat{A}) = \{A_n\}$ existuje ortonormální báze $\mathscr{H}$ taková, že pro každé $A_n \in \sigma(\hat{A})$ platí

$$\hat{A}\psi_n = A_n\psi_n.$$

Na tomto místě se ještě zmíníme o Heisenbergových relacích neurčitosti. Pro každé dva operátory $\hat{A}$, $\hat{B}$ platí následující vztah (předpokládáme normalizovanou funkci ψ)

$$(\psi, (\triangle\hat{A})^2\psi)(\psi, (\triangle\hat{B})^2\psi) \geq \frac{(\psi, [\hat{A}, \hat{B}]\psi)^2}{4}.$$

Tento vztah, nazývaný Heisenbergova relace neurčitosti se většinou zapisuje ve tvaru

$$\triangle\hat{A}\triangle\hat{B} \geq \frac{1}{2}|\langle[\hat{A},\hat{B}]\rangle|.$$

Základní relací neurčitosti je vztah mezi variancí polohy a hybnosti

$$\triangle\hat{x}\triangle\hat{p} \geq \frac{\hbar}{2}.$$

Tento vztah nám říká, že pokud zvyšujeme přesnost měření polohy, tím menší je dosažitelná přesnost při současném měření hybnosti a naopak.

1.1.4 Postulát o redukci vlnové funkce

Měření fyzikální veličiny A s výsledkem měření A_n, kde A_n je vlastní hodnota odpovídajícího operátoru $\hat{A}$ převádí měřený systém do stavu popsaného funkcí ψ_n, která je vlastní funkcí operátoru $\hat{A}$ s vlastním číslem A_n.

Ať už byl stav systému před měřením jakýkoliv, řekněme ψ, bezprostředně po měření vlnová funkce "kolabuje"na vektor ψ_n. Z předchozího postulátu víme, že lze psát

$$\psi = \sum_n c_n\psi_n,$$

kde ψ_n jsou vlastní vektory operátoru $\hat{A}$. Pravděpodobnost, že při měření pozorovatelné A přejde do stavu ψ_n je potom úměrná $|c_n|^2$.

Tento postulát nám dále říká, že pokud jsme před měřením neměli o stavu systému žádnou informaci, pak jedním měřením nemůžeme stav systému určit. Abychom znali stav systému, museli bychom znát koeficienty c_n. V principu to není možné zjistit ani mnoha měřeními. Ty nám v limitě sice poskytnou znalosti veličin $|c_n|^2$, vzhledem k tomu, že c_n jsou komplexní čísla je však tato informace nedostačující. Nemáme-li tedy před měřením o systému žádnou informaci, nemůžeme vytvořit systém, který by byl přesnou kopií původního systému. V dalších kapitolách budeme často v situaci, kdy budeme mít o systému částečnou informaci - budeme vědět, z které množiny stavů daný stav pochází. V závislosti na zvoleném měření potom budeme v některých případech schopni určit vlnovou funkci.

1.1.5 Postulát o časové Schrödingerově rovnici

Je-li v čase $t = t_0$ systém ve stavu popsaném vlnovou funkcí $\psi(x, t_0)$, pak je jeho následný vývoj dán časovou Schrodingerovou rovnicí

$$ih\frac{\partial}{\partial t}\psi(x,t) = \hat{H}\psi(x,t). \tag{1.1}$$

Zde $\hat{H}$ je tzv. Hamiltonův operátor, který odpovídá energii daného systému. Je-li systém tvořen jednou částicí v poli s potenciálem $V(\hat{x}, t)$, potom

$$\hat{H} = \frac{1}{2M}\hat{p}^2 + V(\hat{x}, t).$$

Pokud systém tvoří více částic s hamiltoniány $\hat{H}_i$, potom hamiltonián systému je definován jako

$$\hat{H} = \hat{H}_1 \otimes \hat{1} \otimes \cdots \otimes \hat{1} \oplus \cdots \oplus \hat{1} \otimes \cdots \otimes \hat{H}_i \otimes \cdots \otimes \hat{1} \oplus \cdots \oplus \hat{1} \otimes \cdots \otimes \hat{H}_n.$$

Rovnici (1.1) lze ekvivalentně přepsat pomocí tzv. operátoru časového vývoje. Operátor časového vývoje $\hat{U}(t, t_0)$ je unitární operátor, který splňuje následující. Pro libovolné časy t_0, t_1, t_2 platí

$$\hat{U}(t_2, t_0) = \hat{U}(t_2, t_1)\hat{U}(t_1, t_0),$$

$$\hat{U}^\dagger(t_1, t_0) = \hat{U}(t_0, t_1).$$

Pomocí operátoru $\hat{U}(t, t_0)$ lze časový vývoj popsat následovně. Je-li stav v čase t_0 popsán funkcí $\psi(x, t_0)$, potom stav v čase t je dán rovnicí

$$\psi(x,t) = \hat{U}(t, t_0)\psi(x, t_0).$$

Platí-li pro systém $\hat{H} \neq \hat{H}(t)$, potom $\hat{U}(t, t_0) = \hat{U}(t - t_0)$, kde

$$\hat{U}(t - t_0) = \exp\left[-\frac{i}{h}\hat{H}(t - t_0)\right].$$

1.2 Diracův formalismus

Diracův formalismus [4], také někdy bra-ketový formalismus je způsob, jakým zapisovat kvantověmechanické stavy bez uvedení konkrétních souřadnic. Základem Diracova formalismu jsou tzv. ket-vektory $|\psi\rangle$, které jsou pouze jiným zápisem vlnových funkcí ψ. Ekvivalentním způsobem, jak popsat stav systému je tzv. bra-vektor $\langle\psi|$, což je prvek

prostoru $\mathscr{H}^*$. Mezi ket-vektory a bra-vektory je následující souvislost. Je-li systém ve stavu $|\psi\rangle$, který je superpozicí stavů $|\psi_1\rangle$ a $|\psi_2\rangle$:

$$|\psi\rangle = c_1 |\psi_1\rangle + c_2|\psi_2\rangle,$$

potom odpovídající bra-vektor má tvar

$$\langle\psi| = c_1^* \langle\psi_1| + c_2^*\langle\psi_2|.$$

Skalární součin dvou ket-vektorů se zapisuje následovně:

$$(|\psi\rangle, |\phi\rangle) = \langle\psi|\phi\rangle .$$

Střední hodnota pozorovatelné A pak lze psát jako

$$\langle\hat{A}\rangle = \frac{\langle\psi|\hat{A}|\psi\rangle}{\langle\psi|\psi\rangle}.$$

Výrazy typu $|\psi_1\rangle \langle\psi_2|$ potom představují lineární operátory. To lze vidět, aplikujeme-li uvedený výraz na ket-vektor $|\phi\rangle$:

$$|\psi_1\rangle \langle\psi_2| (|\phi\rangle) = |\psi_1\rangle \langle\psi_2|\phi\rangle = \langle\psi_2|\phi\rangle |\psi_1\rangle .$$

Linearita daného operátoru plyne z linearity skalárního součinu, tyto operátory však nejsou obecně hermitovské.

Z postulátu o kvantování plyne, že každý operátor $\hat{A}$ příslušný pozorovatelné A lze psát ve tvaru

$$\hat{A} = \sum_n A_n |\psi_n\rangle \langle\psi_n| , \tag{1.2}$$

kde A_n jsou vlastní čísla operátoru $\hat{A}$ a $|\psi_n\rangle$ jsou příslušné vlastní kety.

1.3 Reprezentace v kvantové mechanice

Reprezentace v kvantové mechanice odpovídá výběru ortonormální báze, ve které daný systém popisujeme [5]. Dvě základní báze se kterými se můžeme setkat jsou tvořeny vlastními kety operátoru polohy, resp. operátoru hybnosti. Začneme popisem reprezentaci v bázi vlastních vektorů operátoru polohy, tedy v tzv. x-reprezentaci.

Pro vlastní kety operátoru polohy $|x\rangle$ platí následující vztahy:

$$\hat{x} |x\rangle = x |x\rangle ,$$

$$\langle x|x'\rangle = \delta(x - x'),$$
$$\int |x\rangle \langle x| \, dx = \hat{1}.$$

První z těchto vztahů nám říká, že $|x\rangle$ jsou vlastní vektory operátoru polohy, další vztahy říkají, že se jedná o ortonormální bázi $\mathscr{H}$. Pomocí těchto vztahů můžeme libovolný ket $|\psi\rangle$ psát jako

$$|\psi\rangle = \int |x\rangle \langle x|\psi\rangle \, dx = \int \psi(x) \, |x\rangle \, dx,$$

kde jsme formálně zavedli $\langle x|\psi\rangle = \psi(x)$. Analogickým postupem najdeme pro operátor $\hat{A}$ vztah

$$\hat{A} = \int \int \langle x|\hat{A}|x'\rangle \, |x\rangle \, \langle x'| \, dxdx'.$$

Čísla $\langle x|\hat{A}|x'\rangle$ se nazývají maticovými elementy operátoru $\hat{A}$ v x-reprezentaci.

Podobně v p-reprezentaci je za ortonormální bázi volena báze tvořená vlastními kety $|p\rangle$ operátoru hybnosti $\hat{p}$. Opět platí

$$\hat{p} \, |p\rangle = p \, |p\rangle \, ,$$

$$\langle p|p'\rangle = \delta(p - p'),$$
$$\int |p\rangle \langle p| \, dp = \hat{1}.$$

Pro obecný ket $|\psi\rangle$ a operátor $\hat{A}$ najdeme jako v předchozím případu

$$|\psi\rangle = \int |p\rangle \langle p|\psi\rangle \, dp = \int \psi(p) \, |p\rangle \, dp,$$

$$\hat{A} = \int \int \langle p|\hat{A}|p'\rangle \, |p\rangle \, \langle p'| \, dpdp'.$$

Kde opět $\langle p|\hat{A}|p'\rangle$ jsou maticové elementy operátoru $\hat{A}$ v p-reprezentaci. Přechod mezi x-reprezentací a p-reprezentací je umožněn díky vztahu

$$\langle p|x\rangle = \frac{1}{\sqrt{2\pi\hbar}} \exp\left[-\frac{i}{\hbar} px\right].$$

Z hlediska dalšího výkladu pro nás bude důležitá tzv. energetická reprezentace v případě, kdy operátor $\hat{H}$ má diskrétní spektrum.Volíme zde bázi tvořenou vlastními vektory $|n\rangle$ operátoru $\hat{H}$. Tyto kety splňují vztahy

$$\hat{H} \, |n\rangle = E_n \, |n\rangle \, ,$$

$$\langle m|n\rangle = \delta_{mn},$$

$$\sum_{m,n} |m\rangle \langle n| = \hat{1}.$$

Pro obecný ket $|\psi\rangle$ a operátor $\hat{A}$ najdeme vztahy

$$|\psi\rangle = \sum_n \langle n|\psi\rangle |n\rangle ,$$

$$\hat{A} = \sum_{m,n} \langle m|\hat{A}|n\rangle |m\rangle \langle n| .$$

Čísla $\langle m|\hat{A}|n\rangle$ se nazývají maticové elementy operátoru $\hat{A}$ v energetické reprezentaci. Přechod mezi energetickou reprezentací a x-reprezentací, resp. p-reprezentací je závislý na operátoru $\hat{H}$ a řeší se zavedením kreačních a anihilačních operátorů (viz. kapitola 2).

1.4 Matice hustoty

Existují situace, ve kterých systému nelze přiřadit stavový vektor. Naše znalost systému může být například omezena na znalost pravděpodobností, že systém bude v jednom ze stavů $|\psi_i\rangle$. V tomto případě říkáme, že systém je ve smíšeném stavu. Místo stavového vektoru systému přiřazujeme tvz. operátor hustoty $\hat{\rho}$ (viz. např. [6]). Tento operátor je definován vztahem

$$\hat{\rho} = \sum_n p_n \frac{|\psi_n\rangle \langle \psi_n|}{\langle \psi_n|\psi_n\rangle}.$$

Zde $|\psi_n\rangle$ jsou stavy, ve kterých se systém může nalézat a p_n jsou pravděpodobnosti nalezení systému ve stavu $|\psi_n\rangle$. V dalším budeme předpokládat, že stavy $|\psi_n\rangle$ jsou normalizované.

Pojem operátoru hustoty je zobecnění pojmu stavový vektor. Lze-li systému přiřadit určitý stavový vektor $|\psi\rangle$, tj. je-li v tzv. čistém stavu, je operátor hustoty jednoduše

$$\hat{\rho} = |\psi\rangle \langle \psi| .$$

Je-li systém popsán hamiltoniánem $\hat{H}$, potom časový vývoj operátoru hustoty je dán vztahem

$$\hat{\rho}(t) = \hat{U}(t, t_0)\hat{\rho}(t_0)\hat{U}^\dagger(t, t_0).$$

Operátor hustoty má v energetické reprezentaci tvar

$$\hat{\rho} = \sum_{m,n=0}^{\infty} \rho_{mn} |m\rangle \langle n| .$$

kde $\rho_{mn} = \langle m| \hat{\rho} |n\rangle$. Koeficienty ρ_{mn} představují maticovou reprezentaci operátoru $\hat{\rho}$ v energetické bázi. Maticová reprezentace operátoru hustoty se nazývá matice hustoty. Diagonální prvky této matice představují pravděpodobnosti, že při měření bude systém nalezen ve stavu $|n\rangle$ a nazývají se populace. Mimodiagonální prvky této matice určují, nakolik je daný stav smíšený a nazývají se koherence.

Z energetické reprezentace matice hustoty dostáváme

$$Tr\left[\hat{\rho}\right] = \sum_n \langle n| \hat{\rho} |n\rangle = \sum_n \rho_{nn} = 1.$$

Mějme dále matici hustoty

$$\hat{\rho} = \sum_n p_n |\psi_n\rangle \langle\psi_n| ,$$

kde platí $\langle\psi_n|\psi_m\rangle = \delta_{mn}$. Pro střední hodnotu pozorovatelné $\hat{A}$ ve stavu popsaném maticí hustoty $\hat{\rho}$ platí díky relaci úplnosti vztah

$$\langle\hat{A}\rangle = \sum_m p_m \langle\psi_m| \hat{A} |\psi_m\rangle = \sum_n \langle n| \sum_m p_m |\psi_m\rangle \langle\psi_m| \hat{A}|n\rangle = Tr\left[\hat{\rho}\hat{A}\right].$$

Volíme-li za pozorovatelnou $\hat{\rho}$, dostáváme

$$\langle\hat{\rho}\rangle = Tr\left[\hat{\rho}^2\right] = \sum_{l,m,n} p_m p_n \langle\psi_l|\psi_m\rangle \langle\psi_m|\psi_n\rangle \langle\psi_n|\psi_l\rangle = \sum_n p_n^2.$$

Protože $\sum_n p_n = 1$, platí $Tr\left[\hat{\rho}^2\right] \leq Tr\left[\hat{\rho}\right]$ a tedy $\langle\hat{\rho}\rangle \leq 1$. Rovnost zřejmě nastává, pokud pro nějaké n platí $p_n = 1$, tj. pro čistý stav. Pro libovolný stav $|\psi\rangle$ platí

$$\langle\psi| \hat{\rho} - \hat{\rho}^2 |\psi\rangle = \sum_n (p_n - p_n^2) |\langle\psi|n\rangle|^2 \geq 0,$$

a tedy $\hat{\rho} \geq \hat{\rho}^2$.

Pro danou matici hustoty může existovat více smíšených stavů, kterým daná matice přísluší. Jako příklad uvažujme dvouhladinový systém, který je ve smíšeném stavu

$$\hat{\rho} = \frac{1}{2}(|+\rangle \langle+| + |-\rangle \langle-|),$$

kde $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ a $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Daná matice hustoty je

$$\hat{\rho} = \frac{1}{2}\hat{1}.$$

Stejná matice hustoty však přísluší smíšenému stavu

$$\hat{\rho} = \frac{1}{2}(|0\rangle \langle 0| + |1\rangle \langle 1|).$$

Protože střední hodnoty jakékoliv pozorovatenlé měřené na takových stavech jsou stejné, říkáme, že smíšené stavy, kterým přísluší stejná matice hustoty jsou statisticky nerozlišitelné.

1.5 Zobecněné měření

Měření může být v kvantové mechanice popsáno pomocí úplné sady projektorů $\{\hat{P}_j\}$ [7, 8]. Tyto operátory splňují následují vztahy:

(i) $\sum_n \hat{P}_j = \hat{1}$,

(ii) $Tr[\hat{\rho}\hat{P}_j] \geq 0$,

(iii) $\hat{P}_j = \hat{P}_j^\dagger$,

(iv) $\hat{P}_i\hat{P}_j = \delta_{ij}\hat{P}_i$.

Každý operátor z této sady odpovídá jednomu z možných výsledků měření. Je-li stav systému před měřením popsán maticí hustoty $\hat{\rho}$, potom pravděpodobnosti jednotlivých výsledků jsou dány vztahem

$$p_j = Tr[\hat{\rho}\hat{P}_j].$$

Takovémuto měření se říká projektivní měření. Požadavky (i)-(iii) jsou přirozené. Požadavek (i) zajišťuje, že součet všech pravděpodobností p_j je roven jedné, požadavek (ii) zajišťuje nezápornost pravděpodobností p_j a požadavek (iii) říká, že projektory odpovídají pozorovatelným veličinám. Požadavek (iv) má odlišnou interpretaci - říká, že dané měření je ideální, neboli bez šumu. Máme-li tedy systém ve stavu $|\psi_j\rangle$, který je jedním z možných výsledků měření odpovídajících projektoru $\hat{P}_j$, potom platí $p_j = 1$. Mějme například pozorovatelnou $\hat{A}$ ve tvaru (1.2). Projektory $\hat{P}_j$ potom lze definovat vztahy

$$\hat{P}_j = |\psi_j\rangle \langle\psi_j| .$$

Je-li A_j vícenásobné vlastní číslo, potom

$$\hat{P}_j = \sum_i |\psi_j^{(i)}\rangle \langle\psi_j^{(i)}| ,$$

kde pro každé i jsou $|\psi_j^{(i)}\rangle$ vlastní vektory operátoru $\hat{A}$ příslušné číslu A_j.

Zobecněné měření dostaneme z projektivního měření vynecháním požadavku (iv). Je tedy popsáno úplnou množinou operátorů $\{\hat{\pi}_j\}$, které nemusí být ortogonální. Nemusí se ani jednat o projektory, neboť není zaručena platnost vztahu $\hat{\pi}_j^2 = \hat{\pi}_j$. Důvod k zavedení zobecněného měření je, že reálné měření není téměř nikdy ideální a tedy nemůže být popsáno pomocí projektivního měření. Uvažujme předchozí příklad, kde pro jednoduchost předpokládejme $\dim \mathscr{H} = 2$. Díky šumu neobdržíme vždy správný výsledek. Měření je potom popsáno projektory $\hat{\pi}_1 = p\hat{P}_1 + (1-p)\hat{P}_2$ a $\hat{\pi}_2 = (1-q)\hat{P}_1 + q\hat{P}_2$, kde $p \geq 0, q \geq 0$. Čísla p a q jsou zde pravděpodobnsti obdržení správných výsledků. Snadno se přesvědčíme, že operátory $\hat{\pi}_1$ a $\hat{\pi}_2$ splňují vztahy (i)-(iii) a nesplňují vztah (iv).

Dalším příkladem takovéto množiny je množina $\{|z\rangle\langle z|\}$, kde $|z\rangle$ je koherentní stav (viz. kapitola 2) pro libovolné $z \in \mathbb{C}$. Zobecněné měření bude použito v kapitole 5.

1.6 Wignerova funkce

Jednou z možností vizualizace matice hustoty je tzv. Wignerova funkce [9]. Wignerova funkce pro systém ve stavu popsaném maticí hustoty $\hat{\rho}$ je definována vztahem

$$W(x,p) = \frac{1}{2\pi\hbar}\int_{\mathbb{R}} d\xi e^{-\frac{i}{\hbar}p\xi}\left\langle x + \frac{1}{2}\xi|\hat{\rho}|x - \frac{1}{2}\xi\right\rangle.$$

Wignerova funkce patří mezi kvazidistribuce. Má některé, ale ne všechny vlastnosti distribučních funkcí. Je normalizovaná:

$$\int_{\mathbb{R}} dx \int_{\mathbb{R}} dp\ W(x,p) = 1,$$

a pokud provedeme integraci přes jednu proměnnou, dostaneme skutečnou distribuční funkci pro polohu, nebo hybnost

$$\int_{\mathbb{R}} dp\ W(x,p) = \langle x|\hat{\rho}|x\rangle,$$

$$\int_{\mathbb{R}} dx\ W(x,p) = \langle p|\hat{\rho}|p\rangle.$$

Pro libovolné dvě matice hustoty $\hat{\rho}_1$ a $\hat{\rho}_2$ platí vztah

$$Tr(\hat{\rho}_1\hat{\rho}_2) = 2\pi\hbar\int_{\mathbb{R}} dx \int_{\mathbb{R}} dp\ W_{\hat{\rho}_1}(x,p)W_{\hat{\rho}_2}(x,p). \tag{1.3}$$

Z tohoto vztahu plynou dvě důležité vlastnosti Wignerovy funkce. Volíme-li $\hat{\rho}_1 = \hat{\rho}_2 = \hat{\rho}$ a využijeme-li faktu, že pro libovolnou matici hustoty platí $Tr\hat{\rho}^2 \leq 1$, dostáváme vztah

$$2\pi\hbar \leq \frac{1}{\int_{\mathbb{R}} dx \int_{\mathbb{R}} dp\ W^2_{\hat{\rho}}(x,p)}.$$

Mějme dvě matice hustoty $\hat{\rho}_1$ a $\hat{\rho}_2$ takové, že platí $Tr(\hat{\rho}_1\hat{\rho}_2) = 0$. Potom z (1.3) dostáváme

$$0 = 2\pi\hbar \int_{\mathbb{R}} dx \int_{\mathbb{R}} dp\ W_{\hat{\rho}_1}(x,p) W_{\hat{\rho}_2}(x,p).$$

To ale znamená, že alespoň jedna z funkcí $W_{\hat{\rho}_1}, W_{\hat{\rho}_2}$ nabývá záporných hodnot.

Ukážeme dále, že Wignerova funkce pro čistý stav $|\psi\rangle$ je omezená. Matice hustoty má jednoduchý tvar $\hat{\rho} = |\psi\rangle \langle\psi|$ a tedy

$$W(x,p) = \frac{1}{2\pi\hbar} \int_{\mathbb{R}} d\xi e^{-\frac{i}{\hbar}p\xi} \psi(x + \frac{1}{2}\xi)\psi^*(x - \frac{1}{2}\xi).$$

Definujeme $\phi_1(\xi) = \frac{1}{\sqrt{2}} e^{\frac{i}{\hbar}p\xi}\psi(x - \frac{1}{2}\xi)$ a $\phi_2(\xi) = \frac{1}{\sqrt{2}}\psi(x + \frac{1}{2}\xi)$. Obě tyto funkce jsou normalizované. Dostáváme tedy

$$|W(x,p)| = \frac{1}{\pi\hbar} |\langle \phi_1 | \phi_2 \rangle|^2 \leq \frac{1}{\pi\hbar}.$$

Pomocí Wignerovy funkce jsme se z daného Hilbertova prostoru přesunuli do fázového prostoru - náš stav, dříve popisovaný maticí hustoty $\hat{\rho}$ je nyní popsán funkcí $W(x,p)$. Nicméně naše pozorovatelné jsou pořád charakterizovány operátory definovanými na Hilbertově prostoru. Kvůli relacím neurčitosti nelze vždy definovat pro operátor $\hat{A}(\hat{x},\hat{p})$ funkci $A(x,p)$ vztahem $\hat{A}(\hat{x},\hat{p}) = A(x,p)$. Místo toho definujeme reprezentaci operátoru $\hat{A}(\hat{x},\hat{p})$ pomocí tzv. Weyl-Wignerova řazení jako

$$A(x,p) = \int_{\mathbb{R}} d\xi e^{-\frac{i}{\hbar}p\xi} \langle x + \frac{1}{2}\xi | \hat{A}(\hat{x},\hat{p}) | x - \frac{1}{2}\xi \rangle .$$

Pro takto definovanou reprezentaci operátoru $\hat{A}$ pak bude platit podle (1.3)

$$\langle \hat{A} \rangle = \int_{\mathbb{R}} dx \int_{\mathbb{R}} dp\ A(x,p) W(x,p).$$

Kapitola 2

Koherentní stavy elektromagnetického pole

Koherentní stavy byly poprvé zmíňeny E. Schrödingerem v roce 1926 jako stavy kvantového harmonického oscilátoru, pro které platí rovnost v Heisenbergových relacích neurčitosti. Až do počátku 60. let však v kvantové fyzice nenašly příliš velké uplatnění. V tomto čase R.J. Glauber spolu s J.R. Klauderem a E.C.G. Sudharsanem ukázali, že jsou vhodné pro popis elektromagnetického pole generovaného koherentními zdroji jako je laser [10]. Proto se koherentním stavům občas říká Glauberovy stavy.

Protože elektromagnetické pole lze popsat soustavou harmonických oscilátorů s různými frekvencemi a vektory polarizace [5], je harmonický oscilátor důležitým nástrojem pro popis jevů kvantové optiky. Na začátku této kapitoly najdeme posunovací operátory pro hamiltonián harmonického oscilátoru (viz. dodatek B), které budou pro definici koherentních stavů klíčové. Poté přistoupíme k definici koherentních stavů. Ukážeme, že koherentní stavy lze definovat několika ne zcela ekvivalentními způsoby. V dalších částech této kapitoly se budeme věnovat některým vlastnostem koherentních stavů.

2.1 Kreační a anihilační operátory

Jak už bylo řečeno, pro definici koherentních stavů jsou klíčové posunovací operátory hamiltoniánu harmonického operátoru. Hamiltonián harmonického oscilátoru má tvar

$$\hat{H} = \frac{1}{2M}\hat{p}^2 + \frac{M\omega^2}{2}\hat{x}^2.$$

Protože hamiltonián harmonického oscilátoru je hermitovský, stačí nám nalézt jeden posunovací operátor $\hat{a}$. Při jeho hledání (viz. [5]) nejdříve určíme komutátory operátorů polohy a hybnosti s hamiltoniánem harmonického oscilátoru:

$$\left[\hat{H}, \hat{x}\right] = -\frac{i\hbar}{M}\hat{p},$$
$$\left[\hat{H}, \hat{p}\right] = i\hbar M\omega^2\hat{x}.$$

Odtud je vidět, že posunovací operátor k hamiltoniánu harmonického oscilátoru bude mít tvar $\hat{a} = \alpha\hat{x} + \beta\hat{p}$.

$$\left[\hat{H}, \alpha\hat{x} + \beta\hat{p}\right] = -\alpha\hbar\omega\left(-iM\omega\frac{\beta}{\alpha}\hat{x} + \frac{i}{M\omega}\hat{p}\right).$$

Položíme-li $\beta = \frac{i}{M\omega}\alpha$, dostaneme

$$\left[\hat{H}, \alpha\left(\hat{x} + \frac{i}{M\omega}\hat{p}\right)\right] = -\hbar\omega\alpha\left(\hat{x} + \frac{i}{M\omega}\hat{p}\right).$$

Konstantu α je vhodné zvolit tak, aby platilo

$$\left[\hat{a}, \hat{a}^\dagger\right] = \hat{1}.$$

Tato podmínka vede na výsledek $\alpha = \sqrt{\frac{M\omega}{2\hbar}}$.

Tvar posunovacího operátoru $\hat{a}$ příslušejícího operátru $\hat{H}$ s posunutím $-\hbar\omega$ je tedy

$$\hat{a} = \sqrt{\frac{M\omega}{2\hbar}}\left(\hat{x} + \frac{i}{M\omega}\hat{p}\right).$$

Operátor $\hat{a}^\dagger$ je posunovacím operátorem k operátoru $\hat{H}$ s posunutím $\hbar\omega$:

$$\hat{a}^\dagger = \sqrt{\frac{M\omega}{2\hbar}}\left(\hat{x} - \frac{i}{M\omega}\hat{p}\right).$$

Lze snadno nahlédnout, že operátory $\hat{x}$ a $\hat{p}$ jsou násobky reálné a imaginární části operátoru $\hat{a}$

$$\hat{x} = \sqrt{\frac{\hbar}{2M\omega}}\left(\hat{a} + \hat{a}^\dagger\right) = \sqrt{\frac{\hbar}{2M\omega}}\mathfrak{Re}\hat{a},$$

$$\hat{p} = \frac{1}{i}\sqrt{\frac{M\omega\hbar}{2}}\left(\hat{a} - \hat{a}^\dagger\right) = \sqrt{\frac{M\omega\hbar}{2}}\mathfrak{Im}\hat{a}.$$

Hamiltonián harmonického operátoru lze pomocí kreačního a anihilačního operátoru zapsat v kompaktním tvaru jako

$$\hat{H} = h\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right).$$

Z definice operátorů $\hat{a}$ a $\hat{a}^\dagger$ je zřejmé, že operátor $\hat{N} = \hat{a}^\dagger\hat{a}$ působí na vlastní kety harmonického operátoru následovně:

$$\hat{N}\left|n\right\rangle = n\left|n\right\rangle.$$

Operátor $\hat{N}$, který se nazývá operátorem počtu kvant je narozdíl od kreačního a anihilačního operátoru hermitovský. Z uvedeného je zřejmé, že pro vlastní ket $|n\rangle$ operátoru $\hat{H}$ platí

$$\hat{a}\left|n\right\rangle = \alpha_n^-\left|n-1\right\rangle,$$

$$\hat{a}^\dagger\left|n\right\rangle = \alpha_n^+\left|n+1\right\rangle.$$

K určení koeficientů α_n^- a α_n^+ použijeme operátor $\hat{N}$:

$$|\alpha_n^-|^2 = \langle n|\hat{a}^\dagger\hat{a}|n\rangle = \langle n|\hat{N}|n\rangle = n,$$

$$|\alpha_n^+|^2 = \langle n|\hat{a}\hat{a}^\dagger|n\rangle = \langle n|\hat{N} + \hat{1}|n\rangle = n + 1.$$

Je výhodné dané koeficienty volit kladné a reálné a proto položíme $\alpha_n^- = \alpha_{n-1}^+ = \sqrt{n}$. Celkem tedy dostáváme

$$\hat{a}\left|n\right\rangle = \sqrt{n}\left|n-1\right\rangle,$$

$$\hat{a}^\dagger\left|n\right\rangle = \sqrt{n+1}\left|n+1\right\rangle.$$

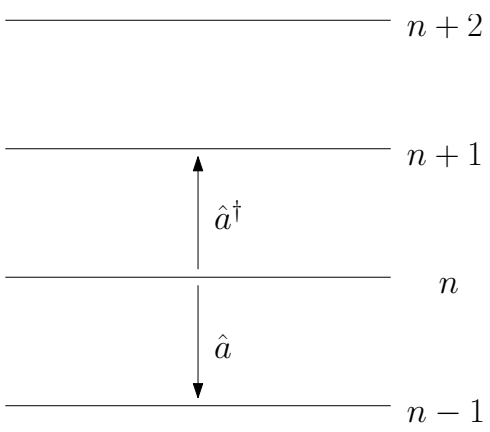
Pomocí těchto výsledků můžeme zapsat energetickou reprezentaci operátorů $\hat{a}$ a $\hat{a}^\dagger$. Pro jejich maticové elementy platí

$$\left\langle m\right|\hat{a}\left|n\right\rangle = \sqrt{n}\ \delta_{m,n-1},$$

$$\left\langle m\right|\hat{a}^\dagger\left|n\right\rangle = \sqrt{n+1}\ \delta_{m,n+1}.$$

a tedy

$$\hat{a} = \sum_{n=1}^{\infty}\sqrt{n}\left|n-1\right\rangle\left\langle n\right|,$$



Obrázek 2.1: Energetické hladiny kvantového harmonického oscilátoru a akce kreačního a anihilačního operátoru.

$$\hat{a}^\dagger = \sum_{n=0}^{\infty} \sqrt{n+1}\,|n+1\rangle\langle n|\,.$$

Nakonec každý Fockův stav $|n\rangle$ lze vyjádřit pomocí operátoru $\hat{a}^\dagger$ a vlastního ketu $|0\rangle$ jako

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}\,|0\rangle\,. \tag{2.1}$$

2.2 Definice koherentních stavů

V této části definujeme koherentní stav pomocí anihilačního operátoru a z této definice odvodíme tvar koherentního stavu ve Fockově bázi. Také zde uvedeme několik základích vlastností koherentních stavů přímo vyplývajících z tvaru tohoto rozvoje.

Koherentní stav je definován jako vlastní ket anihilačního operátoru [6]:

$$\hat{a}\,|z\rangle = z\,|z\rangle\,.$$

Protože Fockovy stavy $|n\rangle$ tvoří ortonormální bázi Hilbertova prostoru $\mathscr{H}$, můžeme psát

$$|z\rangle = \sum_{n=0}^{\infty} c_n\,|n\rangle\,.$$

Po dosazení do předchozí rovnice dostáváme

$$\hat{a}\,|z\rangle = \sum_{n=0}^{\infty} c_n\hat{a}\,|n\rangle = \sum_{n=1}^{\infty} c_n\sqrt{n}\,|n-1\rangle = \sum_{n=0}^{\infty} c_{n+1}\sqrt{n+1}\,|n\rangle = z\sum_{n=0}^{\infty} c_n\,|n\rangle\,.$$

Porovnáme-li koeficienty u stejných členů sumy, dostáváme

$$c_{n+1} = \frac{z}{\sqrt{n+1}} c_n.$$

Opakovanou aplikací nalezneme vztah

$$c_n = \frac{z^n}{\sqrt{n!}} c_0,$$

a tedy

$$|z\rangle = c_0 \sum_{n=0}^{\infty} \frac{z^n}{\sqrt{n!}} |n\rangle .$$

Konstanta c_0 může být použita k normalizaci ketu $|z\rangle$:

$$\langle z|z\rangle = |c_0|^2 e^{|z|^2}.$$

Volba

$$|c_0| = e^{-\frac{|z|^2}{2}}$$

nám zaručí normalizaci stavu $|z\rangle$. Za standartní volbu c_0 budeme považovat

$$c_0 = e^{-\frac{|z|^2}{2}}.$$

Koherentní stav má tedy tvar

$$|z\rangle = e^{-\frac{|z|^2}{2}} \sum_{n=0}^{\infty} \frac{z^n}{\sqrt{n!}} |n\rangle .$$

Je definován pro jakékoliv $z \in \mathbb{C}$, což je důsledek nehermitovosti operátoru $\hat{a}$. Pro $z = 0$ dostáváme Fockův stav $|0\rangle$. Platí

$$\langle n|z\rangle = e^{-\frac{|z|^2}{2}} \frac{z^n}{\sqrt{n!}},$$

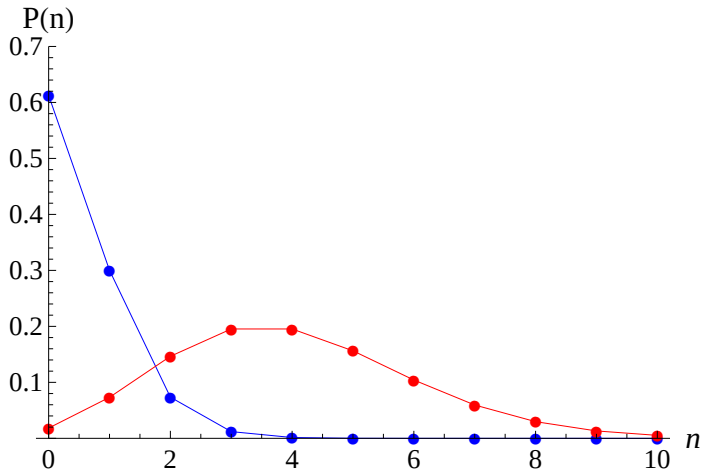
z čehož je vidět, že koherentní stav $|z\rangle$ má pro $z \neq 0$ nenulovou projekci na jakýkoliv Fockův stav $|n\rangle$. Pravděpodobnost, že harmonický oscilátor v koherentním stavu bude nalezen v n-té excitaci je

$$p(n) = |\langle n|z\rangle|^2 = e^{-|z|^2} \frac{|z|^{2n}}{n!},$$

což je Poissonovo rozdělení s parametrem $\lambda = |z|^2$. Střední počet excitací tedy je

$$\langle \hat{N} \rangle = |z|^2.$$

Dané rozdělení je zobrazeno na obr. 2.2. Je vidět, že pro $z < 1$ pravděpodobnost naměření více excitací rychle klesá k nule. Tento fakt bude důležitý v kapitole 5.



Obrázek 2.2: Rozdělení pravděpodobností naměření n excitací pro systém v koherentním stavu. Modře je zobrazeno rozdělení pro $z = 0,7$, červeně je zobrazeno rozdělení pro $z = 2$.

2.3 Operátor posunutí koherentního stavu

Zde ukážeme, že koherentní stav $|z\rangle$ lze získat působením jistého unitárního operátoru $\hat{D}(z)$ na vakuový stav [11]. Také zde odvodíme některé zajímavé vlastnosti tohoto operátoru.

Dosadíme-li ze vztahu (2.1) do rozvoje ve Fockově bázi, dostaneme

$$|z\rangle = e^{-\frac{|z|^2}{2}} \sum_{n=0}^{\infty} \frac{(z\hat{a}^\dagger)^n}{n!} |0\rangle = e^{-\frac{|z|^2}{2}} \exp(z\hat{a}^\dagger) |0\rangle .$$

Uvědomíme-li si, že operátor $\exp(-z^*\hat{a})$ na stav $|0\rangle$ působí jako identický operátor, protože

$$\exp(-z^*\hat{a}) |0\rangle = \sum_{n=0}^{\infty} (-1)^n \frac{(z^*\hat{a})^n}{n!} |0\rangle = |0\rangle ,$$

můžeme psát koherentní stav jako

$$|z\rangle = e^{-\frac{|z|^2}{2}} \exp(z\hat{a}^\dagger) \exp(-z^*\hat{a}) |0\rangle .$$

Užijeme-li nyní CBH identity (viz. dodatek C), dostáváme

$$|z\rangle = \hat{D}(z) |0\rangle ,$$

kde

$$\hat{D}(z) = \exp(z\hat{a}^\dagger - z^*\hat{a})$$

je tzv. operátor posunutí koherentního stavu. Zde je však nutné podotknout, že definice

$$\hat{a}\,|z\rangle = z\,|z\rangle$$

a

$$|z\rangle = \hat{D}(z)\,|0\rangle$$

nejsou zcela ekvivalentní - první z nich je obecnější. Důvodem je volba normalizační konstanty. V prvním případě je obecný tvar konstanty $c_0 = e^{i\phi}e^{-\frac{|z|^2}{2}}$, druhá definice je speciální případ první pro $\phi = 0$.

Operátor posunutí koherentního stavu je zřejmě unitární, platí tedy

$$\hat{D}^\dagger(z) = \hat{D}(-z),$$

$$\hat{D}(z)\hat{D}^\dagger(z) = \hat{1} = \hat{D}^\dagger(z)\hat{D}(z).$$

Složením dvou operátorů posunutí dostaneme až na fázový faktor další operátor posunutí

$$\hat{D}(z)\hat{D}(z') = e^{\frac{zz'^* - z^*z'}{2}}\hat{D}(z+z'), \tag{2.2}$$

kde platí $\mathfrak{Re}(zz'^* - z^*z') = 0$. Tento vztah je opět důsledkem CBH identity. Ze vztahu (2.2) je zřejmé, že operátor posunutí může z libovolného koherentního stavu vytvořit jiný koherentní stav

$$\hat{D}(z)\,|z'\rangle = \hat{D}(z)\hat{D}(z')\,|0\rangle = e^{\frac{zz'^* - z^*z'}{2}}\,|z+z'\rangle\,.$$

Provedeme-li unitární transformaci operátorů $\hat{a}$ a $\hat{a}^\dagger$ pomocí operátoru posunutí, dostaneme [11]

$$\hat{D}^\dagger(z)\hat{a}\hat{D}(z) = \hat{a} + z,$$

$$\hat{D}^\dagger(z)\hat{a}^\dagger\hat{D}(z) = \hat{a} + z^*.$$

Tato rovnost plyne z věty o rozvoji operátoru do řady (viz. dodatek C) a díky rovnostem

$$[-z\hat{a}^\dagger + z^*\hat{a}, \hat{a}] = z,$$

$$[-z\hat{a}^\dagger + z^*\hat{a}, \hat{a}^\dagger] = z^*.$$

Členy řady totiž od druhé mocniny výš vymizí, poněvadž komutátor se redukoval na násobek identického operátoru, který s každým operátorem komutuje. Dostáváme tedy

$$\hat{D}^\dagger(z)\hat{a}\hat{D}(z) = \exp\left[-z\hat{a}^\dagger + z^*\hat{a}\right]\hat{a}\exp\left[z\hat{a}^\dagger - z^*\hat{a}\right] = \hat{a} + z,$$

a podobně pro kreační operátor. Tento výsledek lze však zobecnit. Pro jakoukoliv funkci $f(\hat{a}, \hat{a}^\dagger)$, která lze rozložit do řady platí

$$\hat{D}^\dagger(z) f(\hat{a}, \hat{a}^\dagger) \hat{D}(z) = f(\hat{a} + z, \hat{a}^\dagger + z^*).$$

Rozložíme-li totiž funkci $f(\hat{a}, \hat{a}^\dagger)$ do řady, můžeme vložit mezi každý sousední pár jednotkový operátor $\hat{D}(z)\hat{D}^\dagger(z)$, čímž problém převedeme na předchozí případ.

2.4 Časový vývoj koherentních stavů, relace neurčitosti

Protože až na případ $z = 0$ není koherentní stav $|z\rangle$ vlastním stavem operátoru $\hat{H}$, má netriviální časový vývoj. Časový vývoj probíhá podle rovnice

$$|\psi(t)\rangle = \exp\left[-\frac{i}{\hbar}\hat{H}t\right]|\psi(0)\rangle\,.$$

Je-li tedy $|\psi(0)\rangle = |z\rangle$, dostáváme pomocí rozkladu do Fockových stavů

$$|z(t)\rangle = e^{-\frac{i\omega t}{2}}\,|e^{-i\omega t}z\rangle\,.$$

Koherentní stavy se tedy až na fázový faktor vyvíjejí do jiných koherentních stavů.
Spočítáme střední hodnoty anihilačního a kreačního operátoru v koherentním stavu. Dostaneme

$$\langle z(t)|\,\hat{a}\,|z(t)\rangle = e^{-i\omega t}z,$$

$$\langle z(t)|\,\hat{a}^\dagger\,|z(t)\rangle = e^{i\omega t}z^*.$$

Těchto výsledků můžeme použít k výpočtu středních hodnot polohy a hybnosti v koherentním stavu

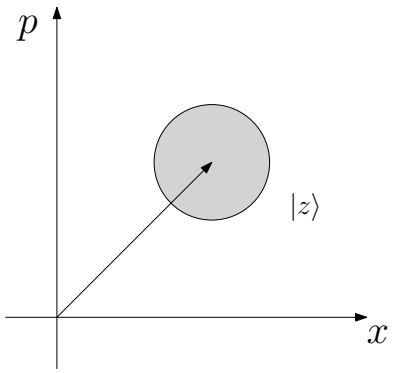
$$\langle z(t)|\,\hat{x}\,|z(t)\rangle = \sqrt{\frac{2\hbar}{M\omega}}|z|\cos(\omega t - arg(z)),$$

$$\langle z(t)|\,\hat{p}\,|z(t)\rangle = -\sqrt{2M\omega\hbar}|z|\sin(\omega t - arg(z)).$$

Střední hodnoty polohy a hybnosti v koherentním stavu jsou tedy analogiemi k polohám a hybnostem klasického harmonického oscilátoru.
Pro určení střední hodnoty variance pohohy a hybnosti spočítáme

$$\langle z(t)|\,\hat{x}^2\,|z(t)\rangle = \frac{\hbar}{2M\omega}(e^{-2i\omega t}z^2 + e^{2i\omega t}(z^*)^2 + 2|z|^2 + 1),$$

$$\langle z(t)|\,\hat{p}^2\,|z(t)\rangle = -\frac{M\omega\hbar}{2}(e^{-2i\omega t}z^2 + e^{2i\omega t}(z^*)^2 - 2|z^2| + 1).$$



Obrázek 2.3: Koherentní stav $|z\rangle$ znázorněný ve fázovém prostoru.

Pro střední hodnotu variance polohy a hybnosti dostaneme

$$\langle z(t)|\,(\triangle\hat{x})^2\,|z(t)\rangle = \langle z(t)|\,\hat{x}^2\,|z(t)\rangle - \langle z(t)|\,\hat{x}\,|z(t)\rangle^2 = \frac{\hbar}{2M\omega},$$

$$\langle z(t)|\,(\triangle\hat{p})^2\,|z(t)\rangle = \langle z(t)|\,\hat{p}^2\,|z(t)\rangle - \langle z(t)|\,\hat{p}\,|z(t)\rangle^2 = \frac{M\omega\hbar}{2}.$$

Celkem máme

$$\langle z(t)|\,(\triangle\hat{x})^2\,|z(t)\rangle^{\frac{1}{2}}\,\langle z(t)|\,(\triangle\hat{p})^2\,|z(t)\rangle^{\frac{1}{2}} = \frac{\hbar}{2}.$$

Pro koherentní stavy tedy nastává v Heisenbergových relacích neurčitosti rovnost. Vidíme také, že "míra rozmazání"v poloze a hybnosti nezávisí na amplitudě koherentního stavu z.

2.5 Stlačené koherentní stavy

Stlačené koherentní stavy jsou zobecněním koherentních stavů [11]. Jedná se o stavy, které jak uvidíme splňují stejné relace neurčitosti. Pro $s \in \mathbb{C}$ definujeme tzv. operátor stlačení vztahem

$$\hat{S}(s) = \exp\left[\frac{s}{2}\left(\hat{a}^2 - (\hat{a}^\dagger)^2\right)\right].$$

Stlačený koherentní stav $|z, s\rangle$ je pak definován vztahem

$$|z, s\rangle = \hat{S}(s)\,|z\rangle\,.$$

Koherentní stavy tedy odpovídají případu $s = 0$. Operátor stlačení má následující vlastnosti: Z CBH identity plyne

$$\hat{S}(s)\hat{S}^\dagger(s) = \hat{1}. \tag{2.3}$$

Z věty o rozvoji operátoru do řady dostáváme

$$\hat{S}^{\dagger}(s)\hat{a}\hat{S}(s) = \hat{a}\cosh s - \hat{a}^{\dagger}\sinh s,$$

$$\hat{S}^{\dagger}(s)\hat{a}^{\dagger}\hat{S}(s) = \hat{a}^{\dagger}\cosh s - \hat{a}\sinh s.$$

Pomocí těchto vztahů lze určit

$$\langle z,s|\hat{x}|z,s\rangle = e^{-s}\langle z|\hat{x}|z\rangle,$$

$$\langle z,s|\hat{p}|z,s\rangle = e^{s}\langle z|\hat{p}|z\rangle.$$

Ze vztahu (2.3) potom najdeme

$$\langle z,s|\hat{x}^2|z,s\rangle = e^{-2s}\langle z|\hat{x}^2|z\rangle,$$

$$\langle z,s|\hat{p}^2|z,s\rangle = e^{2s}\langle z|\hat{p}^2|z\rangle.$$

Celkem dostáváme

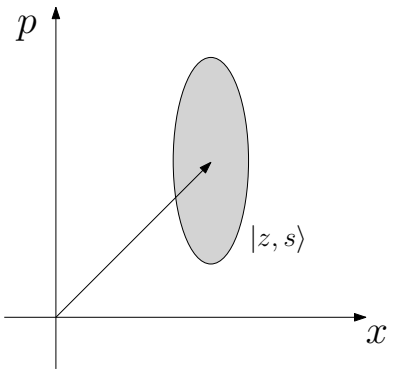
$$\langle z,s|(\triangle\hat{x})^2|z,s\rangle = e^{-2s}\langle z|(\triangle\hat{x})^2|z\rangle,$$

$$\langle z,s|(\triangle\hat{p})^2|z,s\rangle = e^{2s}\langle z|(\triangle\hat{p})^2|z\rangle,$$

a tedy

$$\langle z,s|(\triangle\hat{x})^2|z,s\rangle\,\langle z,s|(\triangle\hat{p})^2|z,s\rangle = \frac{\hbar}{2}.$$

Stlačené koherentní stavy jsou tedy také stavy splňující rovnost v Heisenbergových relacích neurčitosti, "míra rozmazání"v daném směru však není nezávislá na stavu. Na obr. 2.4 je stlačený koherentní stav $|z,s\rangle$ znázorněný ve fázovém prostoru. Směr a míra stlačení jsou závislé na stlačovacím parametru s. Ke stlačeným koherentním stavům se vrátíme v kapitole 5.



Obrázek 2.4: Stlačený koherentní stav $|z, s\rangle$ znázorněný ve fázovém prostoru.

2.6 Neortogonalita a přeúplnost koherentních stavů

V této části ukážeme, že žádné dva koherentní stavy nejsou ortogonální a zmíníme některé netriviální důsledky tohoto faktu.

Pro skalární produkt dvou koherentních stavů dostaneme

$$\langle z'|z\rangle = e^{-\frac{|z|^2+|z'|^2-2z'^*z}{2}},$$

$$|\langle z'|z\rangle|^2 = e^{-|z-z'|^2}.$$

Vidíme tedy, že pro jakékovliv $z \neq z'$ je $\langle z'|z\rangle \neq 0$, tedy žádné dva koherentní stavy nemohou být ortogonální. Z průběhu funkce $e^{-|z-z'|^2}$ je však zřejmé, že už pro celkem blízké hodnoty z a z' jsou tyto stavy přibližně ortogonální.

Koherentní stavy splňují relaci úplnosti ve tvaru (viz. [11])

$$\frac{1}{\pi}\int |z\rangle\langle z|\, d^2z = \hat{1}.$$

Zde integrace probíhá přes celou komplexní rovinu a d^2z je zkrácený zápis pro $d(\mathfrak{Re}z)d(\mathfrak{Im}z)$. Každý stav $|\psi\rangle$ lze tedy vyjádřit pomocí koherentních stavů jako

$$|\psi\rangle = \frac{1}{\pi}\int \langle z|\psi\rangle\, |z\rangle\, d^2z.$$

Toto má závažné důsledky. Máme-li koherentní stav $|z'\rangle$, můžeme ho psát ve tvaru

$$|z'\rangle = \frac{1}{\pi}\int e^{-\frac{|z|^2+|z'|^2-2z'z^*}{2}}\, |z\rangle\, d^2z.$$

Tento vztah lze přepsat do tvaru

$$\int \left(\frac{1}{\pi}e^{-\frac{|z|^2+|z'|^2-2z'z}{2}} - \delta^2(z-z')\right)|z\rangle\, d^2z = 0, \tag{2.4}$$

který vyjadřuje, že koherentní stavy nejsou lineárně nezávislé.

Z těchto vlastností plyne, že koherentní stavy tvoří tzv. překompletní soubor stavů v prostoru $\mathscr{H}$. Každý stav $|\psi\rangle$ lze vyjádřit pomocí koherentních stavů jako

$$|\psi\rangle = \frac{1}{\pi}\int \langle z|\psi\rangle\,|z\rangle\,d^2z.$$

Stejně tak každý operátor $\hat{A}$ na $\mathscr{H}$ lze vyjádřit jako

$$\hat{A} = \frac{1}{\pi^2}\int\int \langle z'|\,\hat{A}\,|z\rangle\,|z'\rangle\,\langle z|\,d^2z d^2z'.$$

Nicméně tyto reprezentace stavů a operátorů nejsou jednoznačné. Například libovolný stav $|\psi\rangle$ můžeme díky vztahu (2.4) rozložit pomocí libovolného koherentního stavu $|z'\rangle$ jako

$$|\psi\rangle = \int \left[\frac{1}{\pi}\left(\langle z|\psi\rangle + e^{-\frac{|z|^2+|z'|^2-2z^*z'}{2}}\right) - \delta^2(z-z')\right]|z\rangle\,d^2z.$$

2.7 Wignerova funkce koherentního stavu

Pro nalezení Wignerovy funkce koherentního stavu nejdříve nalezneme souřadnicovou reprezentaci koherentního stavu. Po dosazení za anihilační operátor dostáváme diferenciální rovnici prvního řádu

$$\sqrt{\frac{M\omega}{2\hbar}}\left(x + \frac{\hbar}{M\omega}\frac{d}{dx}\right)\psi_z(x) = z\psi_z(x).$$

Tato rovnice má řešení (včetně normalizace)

$$\psi_z(x) = e^{(\mathfrak{Im}z)^2}\left(\frac{M\omega}{2\pi\hbar}\right)^{\frac{1}{4}}\exp\left[-\frac{M\omega}{2\hbar}\left(x - \sqrt{\frac{2\hbar}{M\omega}}z\right)^2\right].$$

Dosadíme-li tento výsledek do definice Wignerovy funkce, dostaneme

$$W(x,p) = \frac{1}{\pi\hbar}\exp\left[-\frac{M\omega}{\hbar}\left(x - \sqrt{\frac{2\hbar}{M\omega}}z\right)^2 - \frac{1}{M\omega\hbar}p^2\right].$$

Jako příklad použití Wignerovy funkce spočítáme střední hodnotu energie koherentního stavu. Protože v Hamiltoniánu $\hat{H} = \frac{1}{2M}\hat{p}^2 + \frac{M\omega^2}{2}\hat{x}^2$ jsou nekomutující prvky pouze v součtu, bude platit

$$H(x,p) = \frac{1}{2M}p^2 + \frac{M\omega^2}{2}x^2.$$

Po dosazení dostáváme

$$\langle \hat{H} \rangle = \int_{\mathbb{R}} dx \int_{\mathbb{R}} dp \; H(x,p) W(x,p) = \hbar\omega \left(|z|^2 + \frac{1}{2} \right).$$

Stejný výsledek bychom dostali jednodušeji přímo z definice střední hodnoty. Vidíme, že velikost komplexního čísla z hraje roli amplitudy koherentního stavu.

Kapitola 3

Úvod do teorie informace

Informace je schopnost bezpečně rozlišovat mezi různými možnými alternativami. Jako taková musí být přenášena reálnými fyzikálními objekty, například fotony. V kvantové fyzice hraje pojem informace zásadní roli. Ve svém slavném dvojštěrbinovém experimentu Thomas Young ukázal, že světlo má vlnovou povahu. Nemáme-li žádnou informaci o tom, kterou štěrbinou foton prošel, na stínítku se vytváří interferenční obrazec. Jakmile však do jedné ze štěrbin vložíme detektor, interferenční obrazec je zničen. Důvod je ten, že pokud je kvantový systém informačně izolován, může vykazovat interferenční vlastnosti [6]. Jakákoliv získaná informace o systému tuto interferenci zničí. Vložením detektoru jsme získali informaci o cestě fotonu, ale zničili jsme interferenční obrazec.

V této kapitole podáme stručný úvod do teorie informace [6, 7]. V úvodu definujeme klasickou entropii [12], veličinu, pomocí které lze měřit informaci přenášenou klasickými objekty. Poté se podíváme, jak probíhá klasická komunikace mezi dvěma systémy a prozkoumáme velice důležitý binární symetrický kanál. Dále popíšeme přenost informace pomocí kvantových objektů, tj. zadefinujeme entropii, která bude vhodná pro popis míry informace přenášenou těmito objekty a najdeme vztah mezi klasickou a kvantovou entropií. Nakonec popíšeme pojem qubit, analog klasického bitu, který je přirozeným nositelem informací v kvantové teorii informace.

3.1 Klasická komunikace, entropie

Proces předávání informace mezi dvěma systémy A a B probíhá následovně. Každý ze systémů má k dispozici předem danou množinu symbolů $\{a_1, \ldots, a_m\}$, resp.$\{b_1, \ldots, b_n\}$. Těmto množinám symbolů se říká abeceda. Systémy A a B jsou propojeny tzv. kanálem. Systém A pošle kanálem symbol a_i a systém B přijme symbol b_j.

Mějme daný systém A s abecedou $\{a_1, \ldots, a_m\}$. Nechť pravděpodobnost odeslání symbolu a_i v dostatečně dlouhé zprávě je rovna p_i. Chceme definovat kvantitu, která by udávala množství informace, které takováto zpráva přenáší. Tato kvantita H by měla splňovat následující požadavky [12]:

(i) H by měla být spojitou funkcí proměnných $p_1, \ldots, p_m$.

(ii) Pro rovnoměrné rozdělení $p_i = \frac{1}{m}$ by H měla být rostoucí s m.

(iii) H by měla splňovat vztah

$$H(p_1, \ldots, p_m) = H(N, 1-N) + N \times H\left(\frac{p_1}{N}, \ldots, \frac{p_r}{N}\right) + (1-N) \times H\left(\frac{p_{r+1}}{1-N}, \ldots, \frac{p_m}{1-N}\right),$$

kde

$$N = \sum_{i=1}^{r} p_i.$$

Vztah (iii) nám říká, že rozdělíme-li systém na dva podsystémy, entropie celého systému je dána entropií mezi podsystémy a entropií jednotlivých podsystémů s příslušnými vahami.

Lze ukázat, že jediná funkce vyhovující těmto podmínkám má tvar

$$H(p_1, \ldots, p_m) = -K \sum_{i=1}^{m} p_i \log p_i.$$

Většinou se pokládá $K = 1$ a $\log \equiv \log_2$. Jednotka takto definované funkce se nazývá bit. Funkce H pro obecný základ logaritmu se nazývá Shannonova entropie.

3.2 Klasický kanál, společná informace

Mějme dané systémy A a B s abecedami definovanými jako v kapitole 3.1. Chtějí-li spolu tyto systémy komunikovat, musí být spojeny nějakým kanálem [7]. Vlastnosti

tohoto kanálu jsou plně určeny tzv. přenosovou funkcí, která je definována vztahem

$$Q(a_i, b_j) = P(a_i|b_j),$$

tj. jedná se o pravděpodobnost, že pokud systém B obdrží symbol b_j, tak byl systémem A vyslán symbol a_i. Platí-li

$$Q(a_i, b_j) = \delta_{ij},$$

potom je kanál věrohodný a tzv. jednoznačně dekódovatelný. Máme-li dány příslušné pravděpodobnostní rozdělelní, můžeme definovat dané entropie

$$H(A) = -\sum_{i=1}^{m} p_i \log p_i,$$

$$H(B) = -\sum_{j=1}^{n} q_j \log q_j.$$

Obdrží-li systém B symbol b_j, potom entropie systému A bude

$$H(A|b_j) = -\sum_{i=1}^{n} Q(a_i, b_j) \log Q(a_j, b_j).$$

Po přečtení informací získaných systémem B zbývající informace nesená systémem A je rovna

$$H(A|B) = -\sum_{i,j} q_j Q(a_i, b_j) \log Q(a_i, b_j).$$

Je-li kanál věrohodný, platí

$$H(A|B) = 0,$$

a tedy informace získaná systémem B je stejná jako informace odeslaná systémem A. Buď $P(a_i, b_j)$ pravděpodobnost odeslání symbolu a_i a přijetí symbolu b_j. Potom celková entropie systému AB je

$$H(AB) = -\sum_{i,j} P(a_i, b_j) \log P(a_i, b_j).$$

Mezi pravděpodobnostmi $P(a_i, b_j)$ a $Q(a_i, b_j)$ platí vztah $P(a_i, b_j) = q_j Q(a_i, b_j)$. Pomocí tohoto vztahu lze lehce ukázat, že platí

$$H(AB) = H(B) + H(A|B), \tag{3.1}$$

tj. že celková informace obsažená ve složeném systému AB se skládá z informace obsažené v systému B a informace obsažené v systému A, kterou nelze získat přečtením systému B.

Důležitou veličinou je společná informace systémů A a B. Ta je definována vztahem

$$I_{AB} = H(A) - H(A|B).$$

Od informace nesené systémem A tedy odečteme informaci, kterou nemůžeme získat znalostí systému B. Společná informace je tedy mírou pro korelaci systémů A a B. Z rovnice (3.1) lze tento vztah zapsat symetricky jako

$$I_{AB} = H(A) + H(B) - H(AB).$$

Lze ukázat, že platí $I_{AB} \geq 0$. Pomocí společné informace lze definovat kapacitu kanálu jako

$$C_{AB} = \max_{A} I_{AB}.$$

3.3 Binární symetrický kanál

Binární symetrický kanál [7] je velice důležitý příklad klasického kanálu, který později využijeme v kapitole 5. Jedná se o kanál, který není věrohodný a míra zkreslení výsledků nezáleží na jednotlivých znacích abecedy.

Mějme systémy A a B se stejnými abecedami $\{0, 1\}$. Systémy A a B jsou tedy charakterizovány abecedami $\{0, 1\}$ s pravděpodobnostními rozděleními $\{p, 1-p\}$, resp. $\{q, 1-q\}$. Buď P pravděpodobnost věrohodného přenosu, tj. pravděpodobnost, že při odeslání symbolu i systémem A přijme systém B signál i. Pravděpodobnost nevěrohodného přenosu je $1-P$. Kanálu s takovýmito vlastnostmi se říká binární symetrický kanál. Pravděpodobnosti p a q jsou spolu svázány maticovým vztahem

$$\begin{pmatrix} q \\ 1-q \end{pmatrix} = \begin{pmatrix} P & 1-P \\ 1-P & P \end{pmatrix} \begin{pmatrix} p \\ 1-p \end{pmatrix}.$$

Pomocí Bayesovy věty [13] určíme přenosovou funkci jako

$$Q(0,0) = \frac{pP}{pP + (1-p)(1-P)},$$

$$Q(1,1) = \frac{(1-p)P}{p(1-P) + (1-p)P},$$

$$Q(0,1) = \frac{p(1-P)}{p(1-P)+(1-p)P},$$
$$Q(1,0) = \frac{(1-p)(1-P)}{pP+(1-p)(1-P)}.$$

Po zjištění informace uložené v systému B je zbývající informace systému A rovna

$$H(A|B) = H(p,1-p) + H(P,1-P) - H(q,1-q).$$

Z tohoto můžeme určit společnou informaci:

$$I_{AB} = H(p,1-p) - H(P,1-P).$$

První člen je maximální pro $p = \frac{1}{2}$ a kapacita binárního symetrického kanálu v bitech je tedy rovna

$$C_{AB} = 1 - H_2(P,1-P).$$

3.4 Kvantová komunikace

Při kvantové komunikaci mezi systémy A a B jsou abecedy nahrazeny množinami stavů $\{|a_1\rangle, \ldots, |a_m\rangle\}$ a $\{|b_1\rangle, \ldots, |b_n\rangle\}$. Systém A pošle kvantovým kanálem stav $|a_i\rangle$ a systém B naměří stav $|b_j\rangle$. Rozdíl mezi klasickou a kvantovou komunikací je, že na rozdíl od znaků abecedy v klasické komunikaci nemusí být znaky abecedy v kvantové komunikaci dokonale rozlišitelné. V průběhu této kapitoly se setkáme s důležitými důsledky tohoto faktu.

Jsou-li pravděpodobnosti výskytu stavů $|a_i\rangle$, v dostatečně dlouhé zprávě rovny p_i, potom systém A je charakterizován maticí hustoty

$$\hat{\rho}_A = \sum_{i=1}^{m} p_i |a_i\rangle \langle a_i| .$$

Systém B je s podobně definovanými pravděpodobnostmi q_j popsán maticí hustoty

$$\hat{\rho}_B = \sum_{j=1}^{n} q_j |b_j\rangle \langle b_j| .$$

Shannonova entropie je v kvantové komunikaci nahrazena tzv. von Neumannovou entropií [7]. Je-li systém popsán maticí hustoty $\hat{\rho}$, kde

$$\hat{\rho} = \sum_{m,n} c_{mn} |\psi_m\rangle \langle \psi_n| ,$$

potom von Neumannova entropie systému je definována vztahem

$$S(\hat{\rho}) = -Tr(\hat{\rho}\log\hat{\rho}).$$

Z této definice je zřejmé, že čisté stavy mají nulovou entropii a tedy nejsou schopné přenášet informaci. Shannonova entropie však může být stále definována jako

$$H(\hat{\rho}) = -\sum_n c_{nn}\log c_{nn}.$$

Takto definovaná entropie však záleží na zvolené reprezentaci. Pokud je matice hustoty $\hat{\rho}$ v diagonalizovaném tvaru, potom platí $H(\hat{\rho}) = S(\hat{\rho})$, tedy jinými slovy von Neumannova entropie systému popsaného maticí hustoty $\hat{\rho}$ je Shannonova entropie, do které dosadíme vlastní hodnoty matice hustoty $\hat{\rho}$.

Pro libovolné dvě matice hustoty platí Kleinova nerovnost [7]

$$\hat{\rho}_A\left(\log\hat{\rho}_A - \log\hat{\rho}_B\right) \leq \hat{\rho}_A - \hat{\rho_B}.$$

Mějme libovolnou matici hustoty $\hat{\rho}$. Definujeme si matici hustoty $\hat{\rho}_D$ jako diagonální část matice $\hat{\rho}$ v ortonormální bázi $|\psi_i\rangle$, tj.:

$$\hat{\rho} = \sum_{i,j}\rho_{ij}\left|\psi_i\right\rangle\left\langle\psi_j\right|,$$

$$\hat{\rho}_D = \sum_i \rho_{ii}\left|\psi_i\right\rangle\left\langle\psi_i\right|.$$

Aplikací Kleinovy nerovnosti potom dostáváme

$$S(\hat{\rho}) \leq H(\hat{\rho}).$$

Kvantové systémy tedy podle očekávání nemohou přenášet více informace než klasické systémy, je to důsledek možné neortogonality stavů reprezentující znaky abecedy.

Společná informace systémů A a B je dána vztahem

$$S_{AB} = S(\hat{\rho}_A) + S(\hat{\rho}_B) - S(\hat{\rho}_{AB}).$$

Zapíšeme-li matici hustoty $\hat{\rho}_A$ ve tvaru

$$\hat{\rho}_A = \sum_i p_i\hat{\rho}^{(i)},$$

kde $\hat{\rho}^{(i)}$ může být matice jak čistého tak smíšeného stavu, potom existuje tzv. Holevova mez [7], dána vztahem

$$I_{AB} \leq S(\hat{\rho}_A) - \sum_i p_i S(\hat{\rho}^{(i)}) \leq H(A).$$

Tato mez určuje maximální klasickou informaci, kterou lze získat z kvantového systému. Za povšimnutí stojí, že tato mez není závislá na výběru systému B. Nakonec kapacita kanálu je definována stejně jako v případě klasické komunikace jako

$$C_{AB} = \max_A S_{AB}.$$

3.5 Qubit

Analogem klasického bitu v kvantové komunikaci je tzv. qubit [1, 6, 7]. Jedná se o systém s 2D Hilbertovým prostorem s bází $\{|0\rangle, |1\rangle\}$. Narozdíl od klasického bitu, qubit je obecně v superponovaném stavu

$$|Q\rangle = \alpha |0\rangle + \beta |1\rangle,$$

kde $|\alpha|^2 + |\beta|^2 = 1$. S konkrétními realizacemi qubitu se setkáme v následujících kapitolách.

Kapitola 4

Kvantová kryptografie

Pojem kryptografie vzešel z potřeby bezpečné komunikace. Chce-li Alice poslat zprávu Bobovi, aniž by si Eva mohla přečíst obsah zprávy, je nutné zprávu zašifrovat pomocí klíče. Zašifrovaná zpráva by neměla být korelovaná s původní zprávou. Má-li Bob přístup ke klíči, může ho použít k rozšifrování zprávy. Protože je velmi obtížné navrhnout protokol, který by byl absolutně bezpečný, při navrhování protokolů se klade důraz na následující. Alice a Bob by měli mít možnost dosáhnout libovolně vysokého stupně bezpečnosti jejich komunikace, který by byl nezávislý na dostupných technologiích, známých algoritmech a podobných faktorech. Protože veškerá dnešní komunikace probíhá za pomocí přístrojů pracujících ve dvojkové soustavě, budeme zde uváděné protokoly používat ve spojitosti s binárními kanály.

Principy kvantové mechaniky přinesly na pole kryptografie nové, dosud nepoznané možnosti. Z postulátu o redukci vlnové funkce plyne, že za jistých podmínek bude jakýkoliv pokus o odposlouchávání do systému vnášet detekovatelnou chybu. Jak uvidíme, tohoto faktu lze využít k tvorbě bezpečného klíče.

4.1 Typy kryptografických protokolů

4.1.1 Vernamova šifra

Jediná známá metoda, jak zcela bezpečně komunikovat skrze klasický kanál je tzv. Vernamova šifra (také jednorázová tabulková šifra). Je založena na velice jednoduchém principu - každý znak zprávy se posune o náhodný počet míst v abecedě dál. Klíč je tvořen řetězem číslic nesoucích informaci, o kolik míst se daný znak posunul. Má-li Bob klíč, stačí každý znak posunout o daný počet míst opačným směrem. Vernamova šifra je tedy založena na následujících principech:

(i) Klíč je stejně dlouhý jako přenášená zpráva.

(ii) Klíč je absolutně náhodný.

(iii) Klíč se použije právě jednou.

Problém tohoto protokolu tkví v distribuci klíče. Chce-li Alice bezpečně komunikovat skrz veřejný kanál s Bobem, musí mít k dispozici ještě jeden, soukromý kanál. Skrz soukromý kanál Alice pošle Bobovi klíč, který je jediným nástrojem k dešifrování její zprávy. Jak dále uvidíme, díky principům kvantové mechaniky je tento problém možné eliminovat v kvantové kryptografii.

4.1.2 Asymetrická kryptografie

Na rozdíl od Vernamovy šifry, v asymetrické kryptografii nemusí mezi Alicí a Bobem proběhnout výměna klíče. Alice vlastní dva druhy klíčů - veřejný a soukromý. Veřejný klíč může Bob použít k zašifrování zprávy pro Alici, která danou zprávu rozšifruje pomocí soukromého klíče. Přitom se využívá tzv. jednocestných funkcí Jednocestné funkce jsou založený na následujícím principu. Vyčíslení jednocestné funkce f v jednom směru vyžaduje polynomialní čas vzhledem k délce vstupu a pro libovolný algoritmus A s polynomiální časovou složitostí, libovolný pozitivní polynom p a dostatečně vysoké n platí

$$P(f(A(f(x))) = f(x)) \leq \frac{1}{p(n)}.$$

Jednocestná funkce je tedy snadno vyčíslitelná v jednom směru, ale nesmírně obtížně vyčíslitelná ve směru druhém. Zatímco v roce 1941 bylo dokázáno, že Vernamova šifra

je bezpečná, protokoly založené na asymetrické kryptografii lze prolomit. Klasické protokoly založené na asymetrické kryptografii spoléhají na nedostatečnou výpočetní sílu dnešních počítačů, z toho důvodu jsou do budoucna nespolehlivé.

Dnes nejrozšířenější protokol založený na principech asymetrické kryptografie je RSA protokol, který spoléhá na vysokou obtížnost faktorizace součinu dvou velkých prvočísel. Dnešní algoritmy pro takový úkol potřebují čas exponencialně se zvyšující s velikostí prvočísel na jejich rozšifrování. Dodnes však není podán důkaz jeho bezpečnosti a pokud bude úspěšně sestrojen tzv. kvantový počítač, bude RSA mnohem snáze napadnutelnější, poněvadž díky Shorovu algoritmu je potřeba k splnění takového úkolu čas zvyšující se polynomiálně s velikostí prvočísel.

Kvantová kryptografie je úzce svázána s kvantovou optikou. Jako nositelů informace se zde využívá fotonů. Jak uvidíme dále, informace může být ve fotonech uložena různými způsoby například pomocí polarizace polarizace, nebo posunu fáze vůči referenčnímu fotonu. Jako příklad zde uvedeme nejstarší protokol kvantové kryptografie BB84, který byl představen roku 1984 C. H. Bennettem a G. Brassardem.

4.2 BB84

V této části popíšeme princip protokolu BB84 který byl představen roce 1984 C. H. Bennettem a G. Brassardem. [14] Je zde uveden jako příklad použití zákonů kvantové fyziky pro potřeby kryptografie.

Pomocí protokolu BB84 může Alice bezpečně poslat Bobovi klíč, který pak bude využit při šifrování zprávy Vernamovou šifrou. K tomuto účelu vlastní Alice a Bob kvantový kanál. Přes tento kanál může Alice posílat Bobovi polarizované fotony. Alice má k dispozici dvě sady fotonů. První sada $\oplus$ obsahuje vertikálně a horizontálně polarizované stavy fotonů $|0\rangle$ a $|1\rangle$, druhá sada $\otimes$ obsahuje fotony polarizované pod úhlem 45° a 135° označované $|+\rangle$ a $|-\rangle$. Mezi těmito stavy je vztah

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$

$$|-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right).$$

Právě v tomto vztahu tkví síla protokolu BB84. Alice přiřadí qubitům z jednotlivých sad jejich bitové protějšky. Bez újmy na obecnosti nechť stavy $|0\rangle$ a $|+\rangle$ reprezentují bit 0 a

Alice	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
	1	0	1	1	1	0	0	1	0	1	0	0	0
Bob	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
	1	0	0	1	1	0	1	0	0	1	0	0	1
Klíč	1	×	×	1	1	×	×	×	0	1	×	0	×

Tabulka 4.1: Příklad vytváření bezpečného klíče bez přítomnosti Evy.

stavy $|1\rangle$ a $|-\rangle$ reprezentují bit 1. Předpokládejme, že Alice má k dispozici zcela náhodnou posloupnost bitů a taktéž zcela náhodou posloupnost volby sad $\oplus$, $\otimes$ stejné délky. Bob má k dispozici zařízení, pomocí něhož může měřit polarizaci přicházejících fotonů buď v bázi $\oplus$ nebo $\otimes$ a zpětně jim přiřazovat jejich bitové hodnoty. Měří-li přilétající foton ve stejné bázi v které byl připraven, jeho bit je perfektně korelován s bitem Alice, měři-li ho v odlišné bázi, dostane naprosto náhodný výsledek. Po provedení měření na všech fotonech vlastní Alice a Bob klíče, které však nemusí být stejné, poněvadž Bob v průměru v polovině měření použil špatnou bázi. Oba se přes veřejný kanál domluví a přestanou uvažovat všechny bity, u kterých Bob použil bázi odlišnou od báze Alice, tedy v průměru polovinu bitů. Tabulka 4.1 slouží jako příklad, jak takováto komunikace probíhá.

Eva se však může pokusit provést vlastní měření a podle výsledku připravit foton v daném stavu, který přepošle Bobovi. Nicméně ani ona nemá žádnou informaci o tom, jakou bázi Alice použila a tím pádem v polovině případů bude měřit ve špatné bázi. Evou připravený foton je tedy z jiné sady, než foton připravený Alicí. Měří-li nyní Bob ve správné bázi, s pravděpodobností $\frac{1}{2}$ se jeho bit bude lišit od bitu Alice, přestože oba použili stejnou bázi. Příklad z tabulky 4.1 by potom mohl mít tvar, který je zobrazen na tabulce 4.2.

Porovnáním částí svých klíčů se Alice a Bob mohou ujistit, že jejich kvantový kanál není odposloucháván. K tomuto účelu obětují část bitů, při kterých použili stejnou bázi a přes veřejný kanál si sdělí jejich hodnoty. Pokud se na těchto bitech shodnou, můžou usoudit že distribuce klíče proběhla bez odposlouchávání, bity které použili k ověření však musí zahodit. Liší-li se v některých bitech, znamená to přítomnost Evy a musí tedy začít klíč znovu vytvářet. Čím více bitů obětují k tomuto účelu, tím větší

Alice	⊗	⊗	⊕	⊗	⊕	⊕	⊕	⊗	⊕	⊗	⊕	⊕	⊗
	1	0	1	1	1	0	0	1	0	1	0	0	0
Eva	⊗	⊕	⊕	⊕	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊗	⊕
	1	0	1	0	0	0	1	0	0	1	0	1	1
Bob	⊗	⊕	⊗	⊗	⊕	⊗	⊗	⊕	⊕	⊗	⊗	⊕	⊕
	1	0	0	0	1	0	1	0	1	1	0	0	1
Klíč-Alice	1	×	×	1	1	×	×	×	0	1	×	0	×
Klíč-Bob	1	×	×	0	1	×	×	×	1	1	×	0	×

Tabulka 4.2: Příklad vytváření klíče za přítomnosti Evy. Výsledné řetězce Alice a Boba se liší a přítomnost Evy je tedy detekovatelná.

pravděpodobnost mají k odhalení Evy.

Kvůli obtížím s generací jednofotonových stavů se v praxi využívají slabé koherentní pulzy. Proto se k protokolu BB84 vrátíme v další kapitole.

4.3 Kvantová kryptografie s provázanými stavy

V této části zmíníme další typ kryptografického protokolu [1], který nemá v klasické kryptografii obdobu. Předpokládejme, že máme nějaký zdroj, který produkuje provázané [1, 6, 7] páry fotonů. Informace je v těchto fotonech zakódována pomocí jejich polarizace. Tyto páry jsou distribuované Alici a Bobovi tak, že každý z nich vždy dostane jeden foton z každého páru. Ti na nich stejně jako v protokolu BB84 provádějí měření. Protože provázané páry jsou dokonale korelované, pokud Alice a Bob měří ve stejné bázi, jejich výsledky jsou shodné. Pokud měří v různé bázi, jejich výsledky nemají žádnou korelaci. Problém kterému Eva čelí je, že svým měřením ničí korelaci fotonových párů, což můžou Alice s Bobem detekovat.

Bezpečnost tohoto protokolu byla dokázána, nicméně jsou obtíže s generací provázaných fotonů. Tento protokol je však důležitý z pohledu důkazu bezpečnosti ostatních kryptografických protokolů. Bezpečnost kryptografického protokolu A lze dokázat následovně. Najdeme-li protokol ekvivalentní protokolu s provázanými stavy, který by v sobě jako svou část obsahoval protokol A, potom protokol A je bezpečný.

Kapitola 5

Koherentní stavy v kvantové kryptografii

Koherentní stavy našly v kvantové kryptografii díky svým vlastnostem široké využití. Jsou snadno generovatelné a transformovatelné pomocí pasivních optických zařízení jako je dělič paprsků (viz. Dodatek A). Navíc jsou neortogonální, díky čemuž bude při odposlouchávání vnášena detekovatelná chyba. V této kapitole se zaměříme na detailní popis několika protokolů využívajících koherentní stavy. Zvláštní pozornost bude věnována určení bezpečnosti těchto protokolů.

5.1 BB84 s koherentními stavy

Jak už bylo řečeno, při praktické implementaci protokolu BB84 se většinou využívá slabých pulzů koherentního světla [15]. Stavy používané pro komunikaci označíme kety $|z,0\rangle$, $|z,1\rangle$, $|z,+\rangle$, $|z,-\rangle$. Amplituda koherentního stavu z by měla být znatelně menší než 1. To zajišťuje, že pravděpodobnost detekce dvou a více fotonů zůstává dostatečně nízká. Jak uvidíme dále, detekce více fotonů je pro bezpečnost komunikace katastrofální.

Přenosová rychlost je v průměru rovna pravděpodobnosti přenosu. Protože polarizace a fotonové číslo jsou nezávislé veličiny, dostaneme pro přenosovou rychlost vztah

$$t_{(BB84)} = \frac{1}{2}\left(1 - e^{-|z|^2}\right),$$

což je polovina pravděpodobnosti, že v koherentním stavu s amplitudou z bude měřením nalezen nenulový počet fotonů. Faktor $\frac{1}{2}$ pochází z faktu, že Bob v průměru v polovině měření použije špatnou měřící bázi a tyto výsledky budou zahozeny.

Určíme nyní společnou informaci Alice a Evy jako funkci chyby, kterou Eva svým odposloucháváním vnese do schématu. Představme si, že Eva měří celkem N fotonů. Použije-li stejnou měřící bázi jako Alice, nevnáší do systému žádnou chybu, zatímco při použití odlišné báze vnese do systému chybu $\frac{1}{2}$. Celková vnesená chyba je tedy pro velká N rovna

$$Q = \frac{N}{4}.$$

Pokud Eva měří ve stejné bázi jako Alice, získává o bitu celou informaci, měří-li v odlišné bázi, nezískává žádnou informaci. Společná informace Alice a Evy je tedy

$$I^{AE}_{BB84}(N) = \frac{N}{2},$$

odkud je zřejmý vztah mezi získanou informací a vnesenou chybou:

$$I^{AE}_{BB84}(Q) = 2Q.$$

Protokol je z tohoto pohledu symetrický, tedy společná informace Alice a Evy je stejná jako společná informace Evy a Boba:

$$I^{AE}_{BB84} = I^{EB}_{BB84}.$$

Předvedeme nyní, jaké riziko představuje špatná volba amplitudy koherentního stavu. Pravděpodobnost naměření více než jednoho fotonu v koherentním stavu je rovna

$$p(n{>}1) = 1 - \left(1 + |z|^2\right) e^{-|z|^2}.$$

Je-li amplituda koherentního stavu dostatešně vysoká, $z \sim 1$ potom Eva může koherentní stav rozdělit pomocí děliče paprsků. Prošlý koherentní stav přepošle Bobovi a odražený si nechá. Poté počká až Alice řekne Bobovi přes veřejný kanál které báze byly správné a poté může provést vlastní měření ve správných bázích. Rozdělení se projeví v přenosové rychlosti, nicméně pouze pro malé amplitudy z.

5.2 B92

V roce 1992 C. H. Bennett ukázal, že pro potřeby kvantové kryptografie jsou postačující jakékoliv dva neortogonální stavy [16]. Poněvadž jakékoliv dva koherentní stavy jsou neortogonální, lze je v principu využít pro bezpečnou tvorbu klíče.

Kvůli neortogonalitě koherentních stavů nejsme schopni pokaždé deterministicky určit příchozí stav jedním měřením. Pomocí zobecněného měření jsme však schopni provést test který nám dá buď správnou odpověď, nebo žádnou odpověd [15]. Jedná se tedy o měření se třemi různými výsledky. Bezpečnost tohoto protokolu potom spoléhá na fakt, že Eva taktéž nemůže získat deterministickou odpověď.

V dalším textu popíšeme dané měření a probereme některé z možných způsobů odposlouchávání, ke kterým se může uchýlit a ukážeme, že při použití těchto metod nutně vnese do systému detekovatelnou chybu.

K distribuci klíče k Bobovi má Alice k dispozici slabé koherentní stavy $|z\rangle$, $|-z\rangle$ a silný koherentní stav $|Z\rangle$, který bude použit jako fázová reference pro slabé koherentní stavy. Bez újmy na obecnosti můžeme uvažovat, že stav $|z\rangle$ reprezentuje bit 0 a stav $|-z\rangle$ reprezentuje bit 1. Tyto stavy jsou posílány společně se silným koherentním stavem $|Z\rangle$, který je opačně polarizován, prochází přes polarizační dělič paprsků, kde se díky rozdílné polarizaci oddělí. Stav $|Z\rangle$ je poté polarizován do stejného směru jako stav $|\pm z\rangle$ a je nasměrován na na dělič paprsků, jehož koeficient odrazu je volen tak, že odražená část je rovna $|z\rangle$. Tato část poté na dalším děliči paprsků (který je balancovaný) interferuje se slabým stavem $|\pm z\rangle$.

Tato interference probíhá následovně. Balancovaný dělič paprsků je popsán maticí

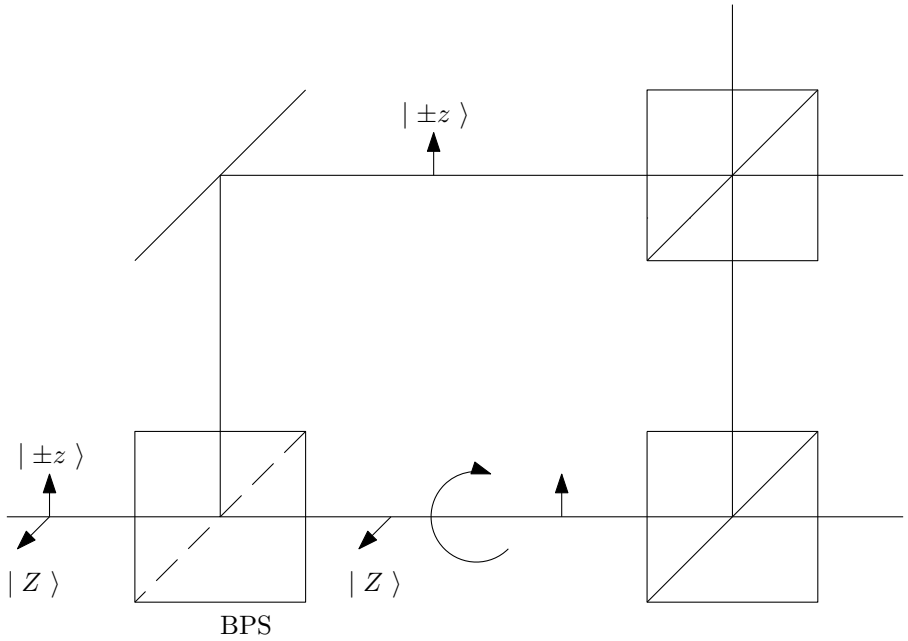
$$\hat{U} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Z transformačních vztahů (viz. apendix A) plyne

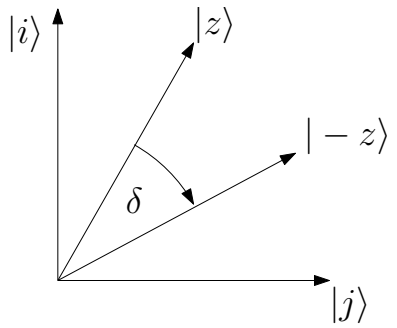
$$|z\rangle_{a,in} |z\rangle_{b,in} = |\sqrt{2}z\rangle_{a,out} |0\rangle_{b,out},$$

$$|-z\rangle_{a,in} |z\rangle_{b,in} = |0\rangle_{a,out} |\sqrt{2}z\rangle_{b,out}.$$

V jednom z výstupů děliče paprsků bude tedy stav $|0\rangle$, v druhém výstupu bude stav $|\sqrt{2}z\rangle$. Poněvadž koherentní stavy mají nenulovou vakuovou složku, detektory na výstupu z tohoto děliče paprsků nemusí zaznamenat žádné fotony - to odpovídá nerozhodnému výsledku. Je-li však detekován foton, máme deterministickou odověď. Po provedení všech měření Bob sdělí Alici přes veřejný kanál, které z jeho měření byly úspěšné. Ostatní bity se dále neuvažují.



Obrázek 5.1: Schéma uspořádání při protokolu B92 s koherentními stavy. PBS je zde zkratka pro polarizační dělič paprsků.



Obrázek 5.2: Metoda projekce na ortogonální stavy.

Pravděpodobnost naměření nulového počtu fotonů je rovna

$$p(0) = e^{-2|z|^2} = \cos\delta.$$

Z tohoto vztahu můžeme určit průměrnou přenosovou rychlost jako

$$t_{B92} = 1 - e^{-2|z|^2} = 1 - \cos\delta.$$

Předpokládáme, že Eva při svém odposlouchávání používá metodu analogickou k metodě v protokolu BB84 - provede tedy měření na stavu vyslaném Alicí a na základě výsledků tohoto měření připraví stav, který přepošle Bobovi. Otázkou však zůstává, kolik informace může Eva svým měřením získat.

Jedním možným způsobem je projektování slabých stavů $|\pm z\rangle$ na ortogonální stavy $|i\rangle$ a $|j\rangle$, vyobrazená na obr. 5.2. Oba stavy $|\pm z\rangle$ mají však nenulové projekce jak na stav $|i\rangle$, tak na stav $|j\rangle$, což bude způsobovat chyby v měření. Je-li úhel mezi stavy $|z\rangle$ a $|-z\rangle$ roven δ, potom pravděpodobnost naměření stavu $|j\rangle$, když původní stav byl ve skutečnosti $|z\rangle$ je rovna

$$p(j|z) = \cos^2\left(\frac{\pi}{4} + \frac{\delta}{2}\right) = \frac{1-\sin\delta}{2}.$$

Správný výsledek je tedy získán s pravděpodobností

$$p(i|z) = 1 - p(j|z) = \frac{1+\sin\delta}{2}.$$

Protože takovéto měření odpovídá svým uspořádáním binárnímu symetrickému kanálu, je společná informace Alice a Evy jako funkce překrytí stavů $|z\rangle$ a $|-z\rangle$ rovna

$$I^{AE}_{B92(1)}(\delta) = 1 + \frac{1-\sin\delta}{2}\log_2\left(\frac{1-\sin\delta}{2}\right) + \frac{1+\sin\delta}{2}\log_2\left(\frac{1+\sin\delta}{2}\right).$$

Potom, co Bob s Alicí odstraní všechny nežádoucí výsledky je společná informace Evy a Boba jednoduše

$$I^{EB}_{B92(1)}(\delta) = 1.$$

Nyní nás zajímá společná informace jako funkce chyby, kterou Eva svým měřením vnáší do systému. Pravděpodobnost že Eva pošle Bobovi jiný stav, než posílala Alice je dána $p(j|z)$. Provádí-li Eva měření na N stavech, vnese do systému chybu

$$Q = N\frac{1-\sin\delta}{2},$$

zatímco získaná informace bude rovna

$$I^{AE(1)}_{B92}(\delta, N) = N\left(1 + \frac{1-\sin\delta}{2}\log_2\left(\frac{1-\sin\delta}{2}\right) + \frac{1+\sin\delta}{2}\log_2\left(\frac{1+\sin\delta}{2}\right)\right).$$

Odtud získáváme společnou informaci Alice, Evy a Evy, Boba jako funkci překrytí mezi stavy $|z\rangle$ a $|-z\rangle$ a chyby, kterou do systému vnesna:

$$I^{AE(1)}_{B92}(\delta, Q) = \frac{2Q}{1-\sin\delta} I^{AE(1)}_{B92}(\delta),$$

$$I^{EB(1)}_{B92}(\delta, Q) = \frac{2Q}{1-\sin\delta}.$$

Další způsob, kterým Eva může získat informaci je použít stejné měření, které provádí Bob. V některých případech tedy dostane deterministickou odpověď, v ostatních případech však musí hádat, který stav Alice poslala.

Použije-li Eva tuto metodu, je společná informace Alice a Evy jako funkce překrytí stavů $|z\rangle$ a $|-z\rangle$ rovna

$$I^{AE(2)}_{B92}(\delta) = 1 - \cos\delta,$$

protože nedostane-li Eva deterministický výsledek, je získaná informace rovna 0, v opačném případě má celou informaci. Schéma je navíc symetrické a tedy

$$I^{AE(2)}_{B92}(\delta) = I^{EB(2)}_{B92}(\delta).$$

S pravděpodobností $p = \cos\delta$ však Eva nezjistí, který stav Alice poslala. Musí tedy hádat, což se jí v polovině případů nepovede. Po N měřeních je tedy chyba vnesená do systému rovna

$$Q(\delta, N) = N\frac{\cos\delta}{2},$$

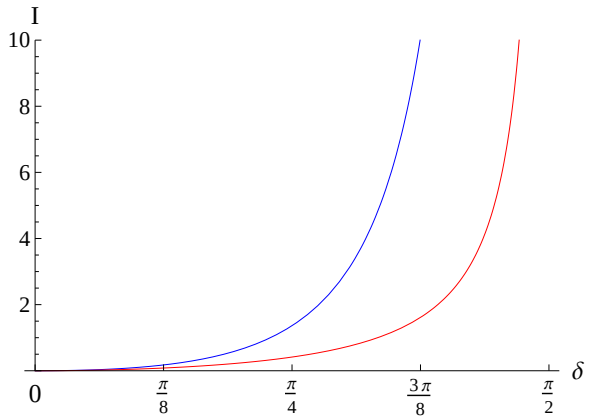
zatímco získaná informace je rovna

$$I_{B92}^{AE(2)}(\delta, N) = N(1 - \cos\delta).$$

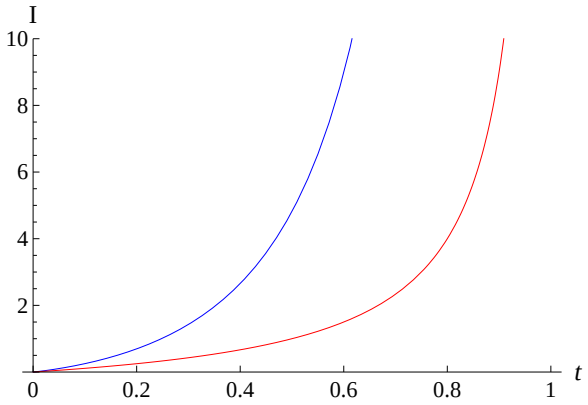
Z tohoto vztahu můžeme určit společnou informaci Alice, Evy a Evy, Boba jako funkci překrytí stavů $|z\rangle$, $|-z\rangle$ a vnesené chyby:

$$I_{B92}^{AE(2)}(\delta, Q) = I_{B92}^{EB(2)}(\delta, Q) = \frac{2Q}{\cos\delta}(1 - \cos\delta).$$

Na obr. 5.3 vidíme porovnání obou metod. Z obrázku je zřejmé, že metoda projekce stavů $|\pm z\rangle$ na ortogonální stavy $|i\rangle$ a $|j\rangle$ dává Evě více informace při jakékoliv volbě parametru překrytí δ. Dále je z grafu zřejmé, že v protokolu má smysl použít pouze stavy s malým překrytím δ. Vhodnou volbou tohoto parametru pak můžeme zajistit, aby informace získaná Evou byla libovolně malá. Zmenšováním parametru δ však snižujeme také přenosovou rychlost. To je potřeba brát v úvahu pro použitelnost protokolu. Vhodné volby parametru jsou více zřejmé z obr. 5.4. Je vidět, že pro přenosovou rychlost $t \gtrsim 0.2$ dává protokol B92 horší výsledky, než protokol BB84, jinak je protokol B92 výhodnější.



Obrázek 5.3: Porovnání dvou představených metod odposlouchávání z hlediska společné informace Alice a Evy v protokolu B92. Modrá křivka odpovídá metodě projektování na ortogonální stavy, červená křivka odpovídá použití stejného měření jako Bob. Graf je normován vzhledem k společné informaci Alice a Evy v protokolu BB84.



Obrázek 5.4: Společná informace Alice a Evy v protokolu B92 jako funkce přenosové rychlosti. Modrá křivka odpovídá metodě projektování na ortogonální stavy, červená křivka odpovídá použití stejného měření jako Bob. Graf je normován vzhledem k společné informaci Alice a Evy v protokolu BB84.

5.3 Protokol 4+2

Vraťme se nyní na chvíli k protokolu BB84. Hlavní síla protokolu BB84 je skryta ve faktu, že volba sad $\oplus$, $\otimes$ je neznámá a je-li měřící báze volena špatně, není žádná korelace mezi vstupním a výstupním bitem. Při implementaci nebylo nutné, aby stavy v jednotlivých sadách byly ortogonální. 4+2 protokol využívá tohoto faktu v kombinaci s protokolem B92 [15].

Sady $\oplus$ a $\otimes$ jsou voleny následovně. Do sady $\oplus$ patří stavy $|\pm z\rangle$, do sady $\otimes$ patří stavy $|\pm iz\rangle$. To odpovídá posuntí fáze o 0, $\frac{\pi}{2}$, π a $\frac{3\pi}{2}$ vzhledem k referenčnímu stavu $|Z\rangle$. Podmínka neznalosti volby sady je však splněna pouze pro $|z| \ll 1$. Platí totiž

$$|z\rangle + |-z\rangle \neq |iz\rangle\,,$$

ale pro $|z| \ll 1$ je

$$|z\rangle + |-z\rangle \sim |iz\rangle\,.$$

Schéma protokolu 4+2 je pak identické schématu protokolu B92. Volba měřících bází je potom provedena pomocí posunovače fáze v jednom rameni interferometru. Chce-li Bob měřit v bázi $\otimes$, vloží do ramene posunovač fáze, chce-li měřit v bázi $\oplus$, potom ho nevloží. Při stejné volbě báze jsou transformační vztahy stejné jako v protokolu B92.

Volí-li Bob odlišnou bázi, potom tranformační vztahy jsou

$$|iz\rangle_{a,in}\,|z\rangle_{b,in} = |\frac{z+iz}{\sqrt{2}}\rangle_{a,out}\,|\frac{z-iz}{\sqrt{2}}\rangle_{b,out},$$

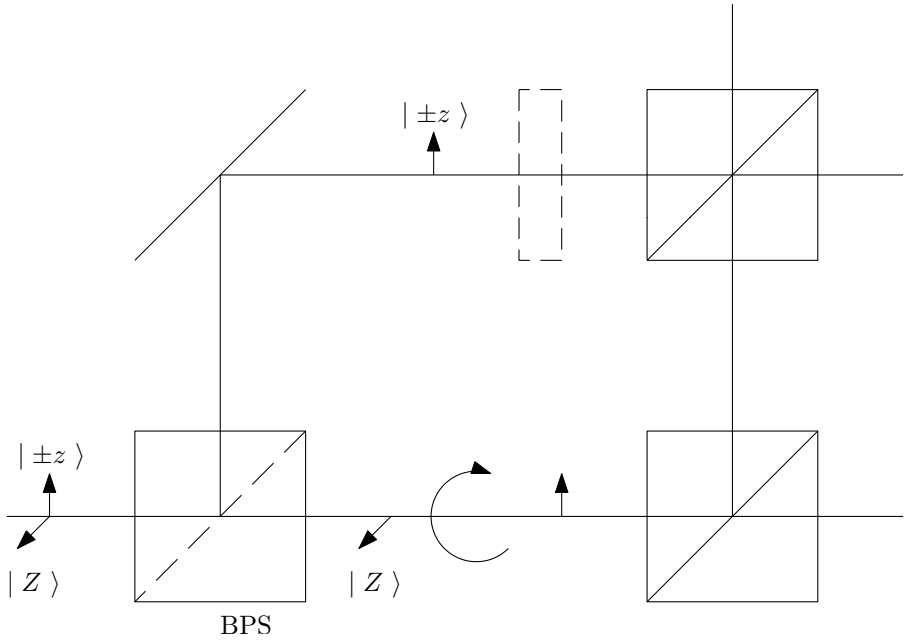
$$|-iz\rangle_{a,in}\,|z\rangle_{b,in} = |\frac{z-iz}{\sqrt{2}}\rangle_{a,out}\,|\frac{z+iz}{\sqrt{2}}\rangle_{b,out}.$$

Pokud tedy Bob zvolí odlišnou měřící bázi, jeho výsledek nemá žádnou korelaci s Alicí, v obou výstupech může detekovat libovolný počet fotonů. Po provedení všech měření se Alice s Bobem opět komunikací přes veřejný kanál zbaví všech neúspěšných měření a měření, při kterých Bob použil odlišnou měřící bázi. Jak uvidíme níže, bezpečnost protokolu může být zvýšena, pokud před tímto procesem porovnají volby svých bází u všech případů, v nichž naměřili nenulový počet fotonů v obou výstupech.

Pravděpodobnost naměření nulového počtu fotonů při použití správné měřící báze zůstává stejná jako v protokolu B92, ale v polovině případů Bob použije odlišnou měřící bázi. Průměrná přenosová rychlost je tedy rovna

$$t_{4+2} = \frac{1}{2}\left(1 - e^{-2|z|^2}\right) = \frac{1}{2}(1 - \cos\delta).$$

Předpokládejme, že Eva volí stejné metody odposlouchávání jako při protokolu B92. Nyní však čelí dalšímu problému - neví, z které sady příchozí stav pochází.



Obrázek 5.5: Schéma pro realizaci protokolu 4+2. Od protokolu B92 se liší možným posunutím fáze o $\frac{\pi}{2}$ v horním rameni, které odpovídá volbě měřící báze.

Nechť Eva používá projekce na ortogonální stavy. Protože platí

$$|\langle iz|z\rangle| = |\langle iz| - z\rangle|,$$

nezíská Eva žádnou informaci, pokud špatně zvolila bázi. Oba stavy budou mít totiž totožné projekce na dané ortogonální stavy $|i\rangle$ a $|j\rangle$. Volí-li Eva správnou bázi, potom získaná informace je stejná jako v protokolu B92. Toto nastane v polovině případů. Společná informace Alice a Evy jako funkce překrytí stavů $|\pm z\rangle$ je tedy rovna

$$I^{AE}_{4+2(1)}(\delta) = \frac{1}{2} I^{AE}_{B92(1)}(\delta),$$

zatímco po vyřazení všech neúspěšných měření je

$$I^{AE}_{4+2(1)}(\delta) = 1.$$

Pokud Eva měří ve správné bázi, vnáší do systému stejnou chybu jako při protokolu B92. Měří-li ve špatné bázi, vnáší chybu $\frac{1}{2}$. Celková vnesená chyba po N měřeních bude tedy

$$Q(\delta, N) = \frac{N}{2}\left(1 - \frac{\sin\delta}{2}\right).$$

Celková informace, kterou má Eva po N měřeních je rovna

$$I^{AE}_{4+2(1)}(\delta, N) = \frac{N}{2} I^{AE}_{B92(1)}(\delta).$$

Odtud dostáváme společnou informaci Alice, Evy a Evy, Boba jako funkci překrytí stavů $|\pm z\rangle$ a vnesené chyby jako

$$I^{AE}_{4+2(1)}(\delta, Q) = \frac{Q}{1 - \frac{\sin\delta}{2}} I^{AE}_{4+2(1)}(\delta),$$

$$I^{EB}_{4+2(1)}(\delta, Q) = \frac{Q}{1 - \frac{\sin\delta}{2}}.$$

Pokud Eva použije stejné měření jako Bob, je situace znatelně složitější. Použije-li Eva stejnou bázi jako Alice a dostane-li deterministický výsledek, získává celou informaci. Pokud však použje odlišnou bázi, může v některých případech získat alespoň částečnou informaci. Při měření ve bázi shodné s bází Alice totiž nikdy nemůžeme naměřit nenulový počet fotonů na obou výstupech, což je v odlišné bázi možné. Naměří-li tedy Eva nenulový počet fotonů v obou výstupech, ví že použila odlišnou bázi. Neví který stav Alice poslala, nicméně ví, do kterého setu správný stav patří.

Pro společnou informaci Alice a Evy z těchto úvah dostáváme

$$I_{4+2}^{AE}(\delta) = \frac{1}{4}\left(3 - \cos\delta - 2\sqrt{\cos\delta}\right).$$

Je více způsobů, kterými může Eva vnést do systému detekovatelnou chybu. Ty jsou následující:

(i) Nedostane deterministický výsledek nezávisle na své volbě báze. Bobovi přeposílá náhodně zvolený stav

(ii) Dostane deterministický výsledek, přičemž zvolila špatnou bázi. Stav, který Bobovi přeposílá je s jistotou špatný.

(iii) Při použití špatné měřící báze naměří nenulový počet fotonů v výstupech. Posílá Bobovi stav ze správného setu.

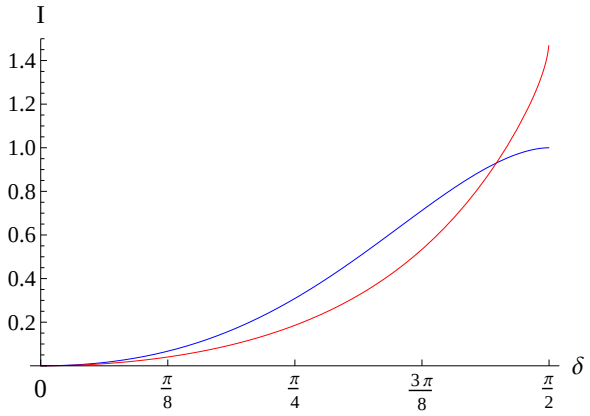
Celková chyba, kterou Eva vnese svými měřeními do systému je

$$Q(\delta, N) = \frac{N}{4}\left(1 + 2\frac{(\cos\delta)^{\frac{3}{2}} - \cos^2\delta}{1 - \cos\delta}\right).$$

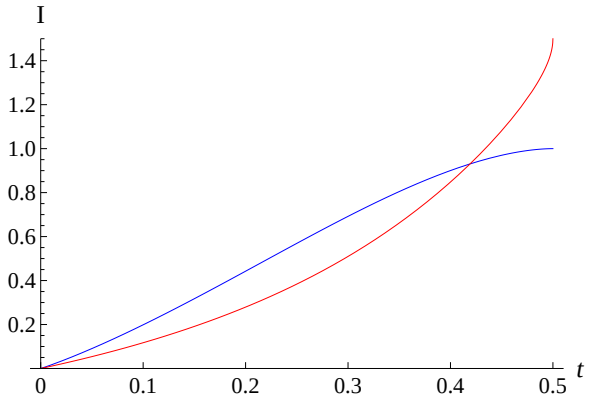
Společná informace Alice a Evy jako funkce překrytí stavů $|\pm z\rangle$ a vnesené chyby je tedy

$$I(\delta, Q) = \frac{Q}{1 + 2\frac{(\cos\delta)^{\frac{3}{2}} - \cos^2\delta}{1-\cos\delta}}\left(3 - \cos\delta - 2\sqrt{\cos\delta}\right).$$

Na obr. 5.6 vidíme, že v tomto případě není metoda projektování na ortogonální bázi vždy lepší metodou pro odposlouchávání. To je důsledkem faktu, že zatímco při použití stejného měření jako Bob může Eva získat částečnou informaci o bázi, projekce na ortogonální stavy podobné výhody nemá. Vzhledem k tomu, že nás však zajímají malé hodnoty parametru δ, lze říci, že metoda projekce na ortogonální stavy je pro Evu výhodnější. Vhodnou volbou parametru δ můžeme opět zajistit, že společná informace Alice a Evy je libovolně malá, opět je však důležité ho zvolit tak, aby přenosová rychlost byla dostatečně vysoká.

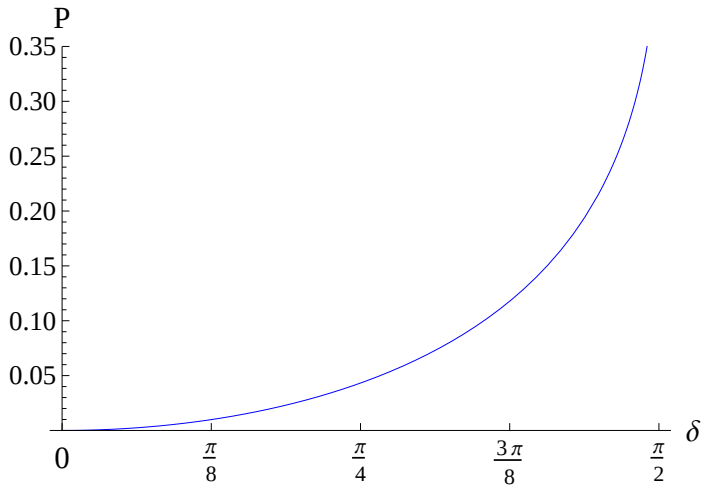


Obrázek 5.6: Porovnání dvou představených metod odposlouchávání z hlediska společné informace Alice a Evy v 4+2 protokolu. Modrá křivka odpovídá metodě projektování na ortogonální stavy, červená křivka odpovídá použití stejného měření jako Bob. Graf je normován vzhledem k společné informaci Alice a Evy v protokolu BB84.



Obrázek 5.7: Společná informace Alice a Evy v 4+2 protokolu jako funkce přenosové rychlosti. Modrá křivka odpovídá metodě projektování na ortogonální stavy, červená křivka odpovídá použití stejného měření jako Bob. Graf je normován vzhledem k společné informaci Alice a Evy v protokolu BB84.

Nakonec ukážeme, jak lze vylepšit bezpečnost protokolu 4+2. Pokud Bob naměří v obou výstupech nenulový počet fotonů, ví, že poslaný koherentní stav byl ze druhého setu. Poslala-li ho Alice, budou se jejich volby bází lišit. Pokud však stav poslala Eva, mohou být jejich volby bází stejné. Porovnáním svých bází ve všech případech, kdy Bob naměřil nenulový počet fotonů na obou výstupech mohou tedy přítomnost Evy odhalit. Aby toto mohlo být znatelným vylepšením bezpečnosti, musí daný případ nastávat s



Obrázek 5.8: Pravděpodobnost naměření nenulového počtu fotonů v obou výstupech.

nezanedbatelnou pravděpodobností. Pro tuto pravděpodobnost dostaneme

$$p(n, m > 0) = \frac{1}{2} \frac{(1 - \sqrt{\cos \delta})^2}{1 - \cos \delta}.$$

Na obr. 5.8 vidíme, že pro hodnoty parametru δ blízké $\frac{\pi}{4}$, které jsou vhodné i z hlediska společné informace Alice a Evy a přenosové rychlosti lze tímto nezanedbatelně zlepšit bezpečnost protokolu.

5.4 Kvantová kryptografie se stlačenými stavy

Jak už bylo řečeno, stlačené koherentní stavy splňují stejně jako koherentní stavy rovnost v Heisenbergových relacích neurčitosti. Máme-li stlačený koherentní stav, vždy existuje význačný směr ve fázovém prostoru, ve kterém je neurčitost malá a směr, který je k němu kolmý, ve kterém je neurčitost velká. Právě tohoto faktu využívá protokol, které v této části popíšeme [17]. Při jeho popisu nebudeme uvažovat faktor $\hbar$, který je irelevantní. Uvažujme koherentní stavy stlačené jedním ze dvou způsobů - buď ve směru reálné části amplitudy, nebo ve směru imaginární části amplitudy. Reálné, resp. imaginární části amplitudy přísluší operátor

$$\hat{X}_1 = \frac{1}{2}\left(\hat{a}^\dagger + \hat{a}\right),$$

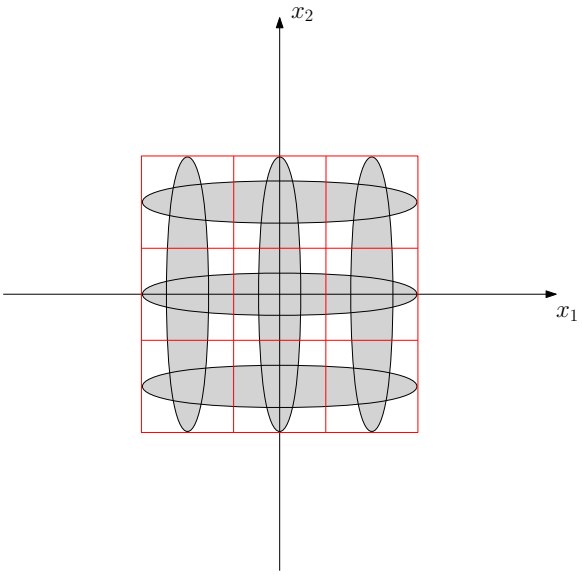
resp.

$$\hat{X}_2 = \frac{i}{2}\left(\hat{a}^\dagger - \hat{a}\right).$$

Tyto operátory jsou pouze násobky operátorů polohy resp. hybnosti. Platí pro ně relace neurčitostií

$$\Delta\hat{X}_1 \Delta\hat{X}_2 \geq \frac{1}{4}. \tag{5.1}$$

Obě složky amplitudy tedy nelze současně měřit s přesností větší než $\frac{1}{2}$. Alice a Bob se přes veřejný kanál domluví na parametru $\varepsilon < \frac{1}{2}$. Poté rozdělí určitou část fázového prostoru s osami x_1, x_2 centrovanou kolem středu na čtverce o straně ε. Každý čtverec poté bude odpovídat určitému symbolu předem zvolené abecedy. Alice bude nyní přeposílat Bobovi koherentní stavy stlačené buď ve směru x_1, nebo ve směru x_2. Je-li koherentní stav stlačen ve směru x_i, parametr stlačení s by měl být zvolen tak, aby pro délku vedlejší osy elipsy d představující stav ve fázovém prostoru platilo $d < \frac{\varepsilon}{2}$. Délka hlavní osy elipsy je pak určena relací neurčitosti (5.1). Délkou hlavní elipsy je také určena oblast fázového prostoru, který musíme rozdělit na čtverce. Stavy stlačené ve směru x_1 jsou vycentrované na ose x_i a jejich středy jsou posunuté o ε. Plocha fázového prostoru zaujímaného stavy stlačenými ve směru x_1 je tedy stejná, jako plocha fázového prostoru zaujímaná stavy stlačenými ve směru x_2. Alice si nyní pošle náhodný stav. Bob si vybere, zdali bude měřit $\hat{X}_1$, nebo $\hat{X}_2$. Zvolí-li správné měření, potom vždy dostane správný výsledek, zvolí-li špatné měření, je výsledek náhodný (pravděpodobnostní rozložení výsledků není rovnoměrné, ale pro dostatečný počet stlačených stavů přibližně rovnoměrné). Dále je



Obrázek 5.9: Příklad množiny stlačitelných stavů použitelných pro kvantovou kryptografii se stlačenými stavy zobrazený ve fázovém prostoru. Rozdělení dané části fázového prostoru na čtverce je vyznačeno červeně.

protokol analogický protokolu BB84. Alice Bobovi přes veřejný kanál sdělíi, v jakém směru byly dané stavy stlačeny a Bob Alici sdělí, jaké měření provedl. Výsledky měření, ve kterých zvolil odlišnou bázi se dále neuvažují.

Pokud Bob zvolí správný typ měření, nezíská vždy správný výsledek. Pravděpodobnost získání chybného měření lze však udělat libovolně malou pomocí volby parametru ε. K určení závislosti pravděpodobnosti chybného měření na velikosti stlačení stačí zkoumat stlačený vakuový stav (stačí zkoumat pro stlačení ve směru x_1). Zajímá nás pravděpodobnost, že pokud Bob měří $\hat{X}_1$, pak dostane jiný než vakuový stav. Pravděpodobnostní rozdělení ve směru x_1 je pro stlačený vakuový stav

$$p(x_1) = \sqrt{\frac{s}{\pi}} e^{-sx_1^2}.$$

Pravděpodobnost nalezení v intervalu $\left[-\frac{\varepsilon}{2}, \frac{\varepsilon}{2}\right]$ je rovna

$$p_\varepsilon = 2\sqrt{\frac{s}{\pi}} \int_0^{\frac{\varepsilon}{2}} e^{-sx_1^2} dx_1.$$

Pravděpodobnost chybného měření je tedy

$$P_1(s) = 1 - 2\sqrt{\frac{s}{\pi}} \int_0^{\frac{\varepsilon}{2}} e^{-sx_1^2} dx_1.$$

Tento vztah udává pravděpodobnost chybného výsledku při správně zvoleném měření jako funkci parametru stlačení. Pro $s \to \infty$ je $P_1 \to 0$ a Alice s Bobem tedy můžou docílit libovolně malé chyby měření.

Naproti tomu pravděpodobnost, že bude naměřen správný výsledek při špatně zvoleném měření je

$$P_2(s) = 2\sqrt{\frac{1}{s\pi}} \int_0^{\frac{\varepsilon}{2}} e^{-\frac{x_2^2}{s}} dx_2^2.$$

Pro $s \to \infty$ je $P_2 \to 0$ a tedy pravděpodobnost, že Eva by nebyla potrestána za špatně zvolené měření lze udělat libovolně malou.

Zapíšeme-li $s = |s|e^{i\phi}$, dostáváme z vlastností operátoru stlačení

$$\langle 0, s|\hat{n}|0, s\rangle = \sinh^2 |s|.$$

Z průběhu funkce sinh je zřejmé, že tímto faktem se tento protokol od předchozích odlišuje. Narozdíl od nich se zde nepracuje se slabými pulsy, což ovlivňuje přenosovou rychlost a otevírá nové možnosti pro Evu. Jak později ukážeme, nemůže však tohoto faktu využít pro své dobro.

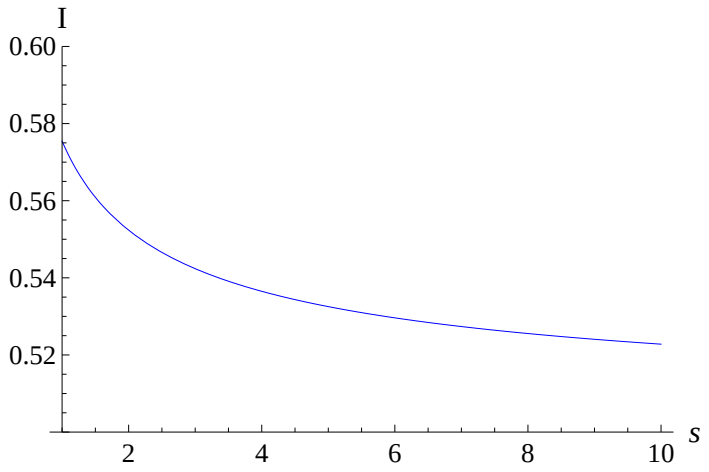
Poněvadž Bob prakticky pokaždé dostane výsledek, je průměrná přenosová rychlost rovna

$$t_{sq} = \frac{1}{2},$$

je tedy nezávislá na volbě parametru ε. Nevýhodou však je, že pro libovolnou volbu paramteru ε vždy existuje nenulová pravděpodobnost, že v přenosu budou chyby, které Alice s Bobem nemůžou detekovat.

Zvolí-li Alice s Bobem $\varepsilon \geq \frac{1}{2}$, potom Eva může obě složky současně změřit s dostatečnou přesností. Dostane-li výsledky z_1 a z_2, přepošle Bobovi koherentní stav centrovaný v bodě $[z_1, z_2]$. Pokud Bob zvolí správné měření, dostane s tímto stavem správný výsledek. Poté, co mu Alice sdělí jaké stavy použila, Eva ví, který ze svých výsledků použít. Musí tedy platit $\varepsilon < \frac{1}{2}$.

Z předchozího textu je zřejmé, že tento protokol se v mnohém podobá protokolu BB84. Podstatný rozdíl zde však tvoří fakt, že chyba, kterou Eva do systému vnáší je pro vhodnou volbu parametru s mnohem lépe detekovatelná. Provede-li Eva správné měření, získává celou informaci o systému. Provede-li však špatné měření, pravděpodobnost, že dostane špatný výsledek roste s parametrem stlačení s.



Obrázek 5.10: Společná informace Alice a Evy pro $\varepsilon = \frac{1}{4}$ jako funkce parametru stlačení. Graf je normalizován vzhledem k společné informaci Alice a Evy v protokolu BB84.

Z předchozích úvah můžeme určit společnou informaci Alice a Evy jako

$$I_{SCS}^{AE}(s) = \frac{N}{2}(1 + P_2(s)).$$

Schéma je opět symetrické a proto

$$I_{SCS}^{EB}(s) = I_{SCS}^{AE}(s).$$

Použije-li Eva správné měření, nevnáší do systému žádnou chybu, použije-li špatné měření, vnáší chybu $1 - P_2(s)$ Celková vnesená chyba je tedy

$$Q(s) = \frac{N}{2}(1 - P_2(s)).$$

Odtud dostáváme společnou informaci Alice a Evy jako funkci parametru stlačení a vnesené chyby:

$$I_{SCS}^{AE}(s, Q) = \frac{Q}{1 - P_2(s)}(1 + P_2(s)).$$

Společná informace Alice a Evy jako funkce parametru stlačení je vyobrazena na obr. 5.10. Opět zde vyniká podobnost mezi tímto protokolem a protokolem BB84.

Jak je řečeno výše, další způsob, který Eva může použít k získání informace je použít dělič paprsků. Zde je však otázka, jak volit koeficienty odrazu a průchodu. Eva musí docílit dvou věcí. Musí být schopna získat z příchozího signálu dost informace, ale zároveň tento signál nesmí výrazně narušit. V dalším textu ukážeme, že tyto dvě podmínky nelze současně splnit.

Budeme uvažovat pouze děliče paprsků, jejichž příslušná unitární matice je reálná. Dělič je tedy popsán maticí $\hat{U}$:

$$\hat{U} = \begin{pmatrix} t & r \\ -r & t \end{pmatrix}$$

Budeme zkoumat, jak se změní stav stlačený ve směru x_1 vycentrovaný v bodě z po průchodu takovýmto děličem paprsků. Označíme $\hat{X}_{ij}$ operátor $\hat{X}_i$ v j-tém módu. Ze vztahů pro vstupní a výstupní kreační operátory dostáváme

$$\hat{X}_{11,out} = t\hat{X}_{11,in} + r\hat{X}_{12,in},$$

$$\hat{X}_{12,out} = -r\hat{X}_{11,in} + t\hat{X}_{12,in}.$$

Dále platí

$$\hat{U}\left|x_{11}, x_{12}\right\rangle_{out} = \left|tx_{11} + rx_{12}, -rx_{11} + tx_{12}\right\rangle_{in}.$$

V souřadnicové reprezentaci tedy dostáváme

$$\psi_{out}(x_{11}, x_{12}) = \psi_{in}(tx_{11} + rx_{12}, -rx_{11} + tx_{12}).$$

V našem případě máme

$$\psi_{out}(x_{11}, x_{12}) = \left\langle x_{11}, x_{12}|\psi\right\rangle_{out} = \left\langle x_{11}|z, s\right\rangle_{out}\left\langle x_{12}, 0\right\rangle_{out}.$$

Dostáváme

$$\psi_{out}(x_{11}, x_{12}) = N\exp\left[-\frac{s}{2}\left(tx_{11,in} + rx_{12,in} - \frac{z}{\sqrt{s}}\right)^2\right]\exp\left[-\frac{1}{2}(-rx_{11,in} + tx_{12,in})^2\right],$$

kde N je normalizační konstanta. Poté, co Eva provede měření $\hat{X}_{12}$ se vlnová funkce stane produktem vlnové funkce v x_{11} a vlastní funkce operátoru $\hat{X}_{12}$ s vlastní hodnotou, kterou Eva naměřila, řekněme y. Tato funkce je poslána Bobovi. Její explicitní tvar je

$$\phi_{out}(x_{11}) = M\exp\left[-\frac{1}{2}\left(st^2 + r^2\right)\left(x_{11,in} - \frac{st\left(\frac{z}{\sqrt{s}} - ry\right) + rty}{st^2 + r^2}\right)^2\right].$$

Vidíme tedy, že parametry s a z se změnili následujícím způsobem:

$$s \to st^2 + r^2,$$

$$z \to \sqrt{s}\frac{st\left(\frac{z}{\sqrt{s}} - ry\right) + rty}{st^2 + r^2}.$$

Aby obě tyto změny malé, musí zřejmě být $t \sim 1$.

Pro střední hodnoty operátorů $\hat{X}_{11,out}$ a $\hat{X}_{12,out}$ dostáváme

$$\langle \hat{X}_{11,out} \rangle = tz,$$

$$\langle \hat{X}_{12,out} \rangle = -rz.$$

Pro kvadrát variance platí

$$(\triangle\ \hat{X}_{11,out})^2 = \frac{1}{4}\left(r^2 + \frac{t^2}{s}\right),$$

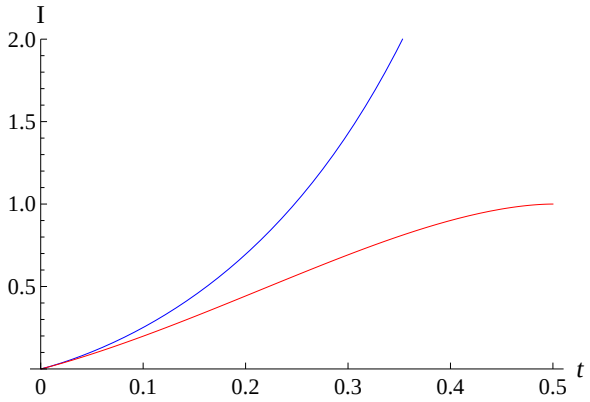
$$(\triangle\ \hat{X}_{12,out})^2 = \frac{1}{4}\left(t^2 + \frac{r^2}{s}\right).$$

Poslední vztah nám určuje, kolik informace může Eva dostat z odraženého paprsku. K získání informace potřebuje, aby platilo $t \ll 1$. To je však ve sporu s podmínkou na nenarušení původního vztahu. Tímto způsobem tedy Eva nemůže získat informace, aniž by do systému vnesla detekovatelnou chybu.

Kapitola 6

Závěr

V této práci jsme čtenáře seznámili se základy teorie informace a úvodem do kvantové kryptografie. V hlavní části jsme detailně popsali několik vybraných kryptografických protokolů, které využívají koherentní stavy. Představili jsme několik možných metod odposlouchávání a zdůvodnili, proč jsou vůči nim dané protokoly odolné, nepodali jsme však obecný důkaz bezpečnosti daných protokolů. Dále jsme navrhli způsob, kterým by mohla být nezanedbatelně zvýšena bezpečnost protokolu 4+2. Protokoly BB84, B92 a 4+2 jsou kvalitativně porovnány na obr. 6.1, kde je vyobrazena společná informace Alice a Evy při použití metody projekce na ortogonální stavy. Vidíme, že protokol 4+2



Obrázek 6.1: Kvantitativní porovnání protokolů BB84, B92 a 4+2. Modrá křivka odpovídá společné informaci Alice a Evy v protokolu B92, červená křivka odpovídá společné informace Alice a Evy v protokolu 4+2. Graf je normován vzhledem k společné informaci Alice a Evy v protokolu BB84.

je pro libovolnou přenosovou rychlost výhodnější než protokoly BB84 a B92. Vzhledem ke značné odlišnosti není možné provést porovnání protokolu využívajícího stlačené koherentní stavy s ostatními protokoly. Je však zřejmé, že zatímco ostatní protokoly se zaměřují na minimalizaci společné informace Alice a Evy, protokol využívající stlačené koherentní stavy se zaměřuje na to, aby chyba vnesená Evou při špatně zvoleném měření byla snáze detekovatelná.

Připomeňme na tomto místě, že všechny zde popisované protokoly jsou používány pouze k vytvoření bezpečného klíče, jedná se tedy o bezpečnou komunikaci při použití Vernamovy šifry. Existují i protokoly založené na asymetrické kryptografii [18, 19], které ve své implementaci používají koherentní stavy.

Příloha A

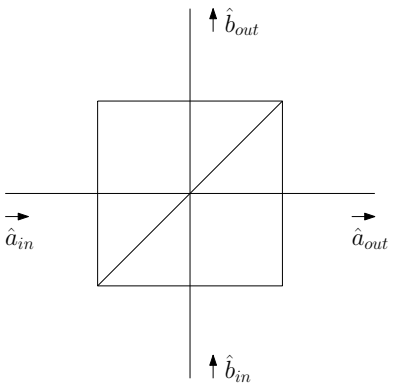
Dělič paprsků

Dělič paprsků je pasivní optické zařízení, které lineárně transformuje dva vstupní stavy ve dva výstupní stavy. Transformace provedená děličem paprsků lze zapsat pomocí kreačních operátorů jako

$$\hat{a}^\dagger_{out} = t_a \hat{a}^\dagger_{in} + r_b \hat{b}^\dagger_{in}$$

$$\hat{b}^\dagger_{out} = r_a \hat{a}^\dagger_{in} + t_b \hat{b}^\dagger_{in}$$

Koeficienty t_a, t_b, r_a, r_b jsou komplexní čísla odpovídající koeficientům průchodu a odrazu. Kreační a anihilační operátory splňují tzv. bosonické komutační relace



Obrázek A.1: Grafické znázornění děliče paprsků.

$$[\hat{a}_{in}, \hat{a}_{in}^\dagger] = [\hat{b}_{in}, \hat{b}_{in}^\dagger] = \hat{1}$$

$$[\hat{a}_{in}, \hat{b}_{in}^\dagger] = 0$$

Daná transformace musí být unitární a proto tyto rovnice musí splňovat i operátory $\hat{a}_{out}$ a $\hat{b}_{out}$. To vede na podmínky kladené na koeficienty průchodu a odrazu:

$$t_a r_a^* + t_b^* r_b = 0$$

$$|t_a|^2 + |r_b|^2 = 1 = |t_b|^2 + |r_a|^2$$

Z těchto podmínek lze odvodit vztahy

$$|r_a| = |r_b|$$

$$|t_a| = |t_b|$$

Tyto vztahy lze přepsat pomocí maticového formalismu. Vztahy mezi vstupními a výstupními kreačními operátory lze psát ve tvaru

$$\begin{pmatrix} \hat{a}_{out}^\dagger \\ \hat{b}_{out}^\dagger \end{pmatrix} = \begin{pmatrix} t_a & r_b \\ r_a & t_b \end{pmatrix} \begin{pmatrix} \hat{a}_{in}^\dagger \\ \hat{b}_{in}^\dagger \end{pmatrix}.$$

Dělič paprsků lze tedy úplně popsat pomocí jedné unitární matice $\hat{U}$:

$$\hat{U} = \begin{pmatrix} t_a & r_b \\ r_a & t_b \end{pmatrix}.$$

Alternativně můžeme dělič paprsků popsat pomocí Hamiltonova formalismu. Hamiltonián děliče paprsků má obecně tvar

$$\hat{H} = \lambda \left(e^{i\phi} \hat{a}_{in}^\dagger \hat{b}_{in} + e^{-i\phi} \hat{a}_{in} \hat{b}_{in}^\dagger \right),$$

kde $\lambda, \phi \in \mathbb{R}$ jsou svázány s koeficienty průchodu a odrazu. Unitární transformace děliče paprsků je pak popsána operátorem

$$\hat{U}(t) = \exp\left[-\frac{i}{\hbar} \hat{H} t \right].$$

Použijeme-li větu o rozvoji operátoru, dostaneme časový vývoj kreačních operátorů

$$\hat{a}^\dagger(t) = \cos\left(\frac{\lambda t}{\hbar}\right) \hat{a}_{in}^\dagger + i e^{-i\phi} \sin\left(\frac{\lambda t}{\hbar}\right) \hat{b}_{in}^\dagger$$

$$\hat{b}^\dagger(t) = ie^{i\phi} \sin\left(\frac{\lambda t}{\hbar}\right) \hat{a}^\dagger_{in} + \cos\left(\frac{\lambda t}{\hbar}\right) \hat{b}^\dagger_{in}$$

Interakce s děličem paprsků probíhá po určitý čas T. Definujeme-li $\theta = \frac{\lambda T}{\hbar}$, dostáváme

$$\hat{a}^\dagger_{out} = \cos\theta\ \hat{a}^\dagger_{in} + ie^{-i\phi} \sin\theta\ \hat{b}^\dagger_{in}$$

$$\hat{b}^\dagger_{out} = ie^{i\phi} \sin\theta\ \hat{a}^\dagger_{in} + \cos\theta\ \hat{b}^\dagger_{in}$$

Nechť mód a obsahuje m fotonů a mód b n fotonů. Vstupní stav je tedy

$$|m\rangle_a |n\rangle_b = \frac{(\hat{a}^\dagger_{in})^m}{\sqrt{m!}} \frac{(\hat{b}^\dagger_{in})^n}{\sqrt{n!}} |0,0\rangle$$

Výstupní stav dostaneme, pokud za operátory $\hat{a}^\dagger_{in}$ a $\hat{b}^\dagger_{in}$ dosadíme operátory $\hat{a}^\dagger_{out}$ a $\hat{b}^\dagger_{out}$. Výsledek je

$$|m\rangle_{a,in} |n\rangle_{b,in} = \sum_{k,l=0}^{m,n} \binom{m}{k} \binom{n}{l} \frac{(\cos\theta)^{m+l-k}}{\sqrt{m!}} \frac{(-i\sin\theta)^{n+k-l}}{\sqrt{n!}} e^{i(n-l-k)\phi} \times$$

$$\times \sqrt{(m+n-k-l)!}\sqrt{(k+l)!}\, |m+n-k-l\rangle_{a,out} |k+l\rangle_{b,out}\,.$$

V případě, že $n = 0$ lze tento výsledek zjednodušit na

$$|m\rangle_{a,in} |0\rangle_{b,in} = \sum_{k=0}^{m} \sqrt{\binom{m}{k}} (\cos\theta)^{m-k} (-ie^{-i\phi} \sin\theta)^k\, |m-k\rangle_{a,out} |k\rangle_{b,out}\,.$$

Pomocí rozložení do Fockovy báze můžeme takto popsat akci děliče na jakýkoliv vstupní stav.

Určíme akci děliče paprsků, pokud jsou ve vstupních módech koherentní stavy. Nechť mód a obsahuje stav $|z\rangle$ a mód b obsahuje stav $|z'\rangle$. Využijeme-li definice koherentního stavu pomocí operátoru posunutí a invertujeme-li vztahy pro $\hat{a}^\dagger_{out}$ a $\hat{b}^\dagger_{out}$, dostaneme

$$|z\rangle_{a,in} |z'\rangle_{b,in} = |\cos\theta\ z - ie^{i\phi} \sin\theta\ z'\rangle_{a,out} |\cos\theta\ z' - ie^{-i\phi} \sin\theta\ z\rangle_{b,out}$$

Koherentní stav je tedy děličem paprsků transformován v jiný koherentní stav.

Příloha B

Posunovací operátory

Posunovací operátory jsou velice užitečným nástrojem ke zkoumání spekter a vlastních fukncí operátorů. Operátor $\hat{A}$ se nazývá posunovacím operátorem k operátoru $\hat{B}$ s posunutím λ, pokud platí:

$$[\hat{B}, \hat{A}] = \lambda \hat{A}.$$

Je-li $|\Lambda\rangle$ vlastní vektor operátoru $\hat{B}$ s vlastní hodnotou Λ, potom platí

$$\hat{B}\hat{A}\,|\Lambda\rangle = (\Lambda + \lambda)\hat{A}\,|\Lambda\rangle\,,$$

tedy platí $\hat{A}\,|\Lambda\rangle = |\Lambda + \lambda\rangle$.

Dále ze vztahu $[\hat{B^\dagger}, \hat{A^\dagger}] = -[\hat{B}, \hat{A}]^\dagger$ dostáváme, že je-li $\hat{A}$ posunovacím operátorem k operátoru $\hat{B}$ s posunutím λ, potom $\hat{A^\dagger}$ je posunovacím operátorem k operátoru $\hat{B^\dagger}$ s posunutím $-\lambda^*$.

Je-li operátor $\hat{B}$ navíc samozdružený, všechny jeho vlastní hodnoty jsou reálné a pokud existuje alespoň jeden vlastní ket $\hat{A}\,|\Lambda\rangle \neq 0$, potom platí $\lambda \in \mathbb{R}$.

Příloha C

Věta o rozvoji operátoru do řady a CBH identita

ěta o rozvoji operátoru do řady je důležitou větou funkcionální analýzy, která je v kvantové mechanice často užitečná, například při odvozování vztahů ve spojistosti s unitárními transformacemi. Buďte $\hat{A}$ a $\hat{B}$ libovolné operátory. Potom platí následující vztah

$$\exp[\hat{A}]\hat{B}\exp[-\hat{A}] = \hat{B} + [\hat{A}, \hat{B}] + \frac{1}{2!}[\hat{A}, [\hat{A}, \hat{B}]] + \dots .$$

Neméně důležitá je tzv. Cambell-Baker-Hausdorffova identita (CBH identita). Mějme dva operátory $\hat{A}$ a $\hat{B}$, které splňují následující vztah

$$[\hat{A}, [\hat{A}, \hat{B}]] = 0 = [\hat{B}, [\hat{A}, \hat{B}]].$$

Potom platí

$$\exp[\hat{A} + \hat{B}] = \exp[\hat{A}]\exp[\hat{B}]\exp\left[-\frac{[\hat{A}, \hat{B}]}{2}\right].$$

Vidíme tedy, že vztah

$$\exp[\hat{A} + \hat{B}] = \exp[\hat{A}]\exp[\hat{B}]$$

platí pouze pro komutující operátory.

Literatura

[1] D. Bouwmeester, A. Ekert, and A. Zeilinger. *The Physics of quantum information.* Springer, 2000.

[2] L. Skála. *Úvod do kvantové mechaniky.* Academia, 2005.

[3] J. Blank, P. Exner, and M. Havlíček. *Lineární operátory v kvantové fyzice.* Universita Karlova, 1993.

[4] P.A.M. Dirac. *The Principles of quantum mechanics.* Oxford University Press, 1958.

[5] L. Hlavatý. Slabikář kvantové mechaniky, 2009.

[6] B. Schumacher and M. Westmoreland. *Quantum Processes Systems, & Information.* Cambridge University Press, 2010.

[7] S. Stenholm and K. Suominen. *Quantum Approach to Informatics.* Wiley Inter-Science, 2005.

[8] S.M. Barnett. *Quantum Informaion.* Oxford University Press, 2009.

[9] W.P. Schleich. *Quantum optics in phase space.* Wiley Inter-Science, 2001.

[10] R.J. Glauber. The quantum theory of optical coherence. *Phys. Rev. Lett.*, 130:2529, 1963.

[11] L. Mandel and E. Wolf. *Optical coherence and quantum optics.* Cambridge University Press, 1995.

[12] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[13] K. Zvára and J. Štěpán. *Pravděpodobnost a matematická statistika.* matfyzpress, 2006.

[14] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and key tossing. 1984.

[15] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev.*, A51:1863, 1995.

[16] C.H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121, 1992.

[17] M. Hillery. Quantum cryptography with squeezed states. *Phys. Rev.*, A61, 2000.

[18] E. Andersson, M. Curty, and I. Jex. Experimentally realizable quantum comparison of coherent states and its applications. *Phys. Rev.*, A 74, 2006.

[19] C. Hamilton, H. Lavička, E. Andersson, J. Jeffers, and I. Jex. Quantum public key distribution with imperfect device components. *Phys. Rev.*, A 79, 2009.