第 58 卷 第 10 期 2009 年 10 月
1000-3290/2009/58(10)/6779-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.58,No.10,October,2009

多输入多输出量子密钥分发信道容量研究*

肖海林[1)†] 欧阳缮[1)] 聂在平[2)]

1)(桂林电子科技大学信息与通信学院,桂林 541004)

2)(电子科技大学电子工程学院,成都 610054)

(2008 年 9 月 17 日收到;2008 年 12 月 11 日收到修改稿)

量子安全通信是一个量子密钥分发过程,目前采用的通信技术严重制约了量子密钥分发的比特率.将多输入多输出(MIMO)技术应用于量子密钥分发系统,可提高量子密钥分发的比特率,促进量子安全通信向高速大容量发展.文中首先构造出 MIMO 量子密钥分发信道中多光子纠缠态 Wigner 算符矩阵.并在此基础上,推导出多光子双模压缩纠缠态 Wigner 算符矩阵和 MIMO 量子密钥分发信道容量.为开发稳健的 MIMO 量子安全通信空时处理算法和优化设计高性能 MIMO 量子密钥分发系统提供理论支撑和技术基础.

关键词:多输入多输出,双模压缩态,多光子纠缠态,信道容量

PACC:0365,4230,4250

1. 引 言

量子安全通信是通信技术的又一次划时代革命,与目前采用的通信技术相比,量子安全通信在保密性、通信容量、通信距离等方面都具有十分明显的优势,是未来通信发展的方向.虽然量子安全通信有着广阔的应用前景,但在单元技术和理论方面还有许多需要解决的问题[1].

量子安全通信传送的是密钥而非密文本身,是一个量子密钥分发过程.然而,目前量子密钥分发技术严重制约了通信中传输的比特率,诸如 BB84[2],ERP[3],B92[4] 以及其他协议[5—7] 的量子密钥分发方案,但是这些方案中量子密钥分发效率和粒子的利用率还达不到 50%[7—9].为了实现很高的量子密钥分发的比特率,可利用多输入多输出(MIMO)系统的传输技术[10,11],该系统将多径信道、发端通道与收端通道视为一个整体进行优化处理,这是一种近于最优的空域与时域联合的分集和干扰对消处理.借助多径传播建立空间并行传输通道,采用各种空时编码方案实现发射分集与接收分集,获得相对常规无线通信系统明显的复用增益与分集增益.

在通信系统中,通常采用信道容量来衡量信息传输速率.在 2000 年 Nielsen 等[12] 借助经典香农熵信息理论,提出 von Neumann 熵来描述量子状态,以密度算子来代替密度分布得到具有两个光子纠缠态 von Neumann 熵.然而,这种纯态密度算子的 von Neumann 熵对于 MIMO 量子密钥分发信道中多光子纠缠态是不适用的.2001 年 Andreas[13] 在 Allahverdyan 和 Saakian[14] 基础上利用块编码通过无记忆的离散信道获得离散无记忆信道的信息熵 Holevo 界,但此方法要求密度算子必须是固定的.关于量子安全通信的信道容量,近年来开始有学者进行研究[15—17],但都普遍假设量子之间是独立和去相关的,这种假设与实际量子态并不相符合,研究也仅局限于两光子纠缠态信道,还缺乏理论公式推导.本文首先构造出 MIMO 量子密钥分发信道中多光子纠缠态 Wigner 算符.并在此基础上,推导出多光子双模压缩纠缠态 Wigner 算符矩阵和 MIMO 量子密钥分发信道容量.

2. MIMO 量子密钥分发信道容量研究

2.1. 量子信息论

根据信息论,$H(X)$ 代表接收到输出符号以前

* 国家重点基础研究发展计划(批准号:2008CB317109)、广西自然科学基金(批准号:桂科自 0991241)和国家自然科学基金(批准号:60972084)资助的课题.

† E-mail:xhl_xiaohailin@163.com

关于输入变量 X 的平均不确定性，$H(X|Y)$代表接收到输出符号后关于输入变量 X 的平均不确定性.通过信道传输消除了一些不确定性，获得了一定的信息.所以定义

$$I(X;Y) = H(X) - H(X|Y), \tag{1}$$

其中 $I(X;Y)$被称为 X 和 Y 之间的平均互信息.它代表接收到输出符号后平均每个符号获得的关于 X 的信息量.通常定义最大的信息传输率为信道容量 C，即

$$C = \max\{I(X;Y)\}. \tag{2}$$

在经典信息论中，香农熵测试信号的不确定性是通过信号的概率分布来实现的.量子安全通信也有类似的形式，只不过是采用密度算子来代替概率分布[12].在量子信息论中，von Neumann 熵定义为[12,14,18]

$$H(\boldsymbol{\rho}) = -\mathrm{Tr}[\boldsymbol{\rho}\log\boldsymbol{\rho}], \tag{3}$$

其中 $\boldsymbol{\rho}$ 是密度算子，$\mathrm{Tr}[\cdot]$表示求迹.量子纯态(某一组力学量完全集的共同本征态)的密度算子表示为

$$\boldsymbol{\rho} = |\psi\rangle\langle\psi|. \tag{4}$$

从量子力学理论上来讲，对于一个多自由度的体系，如只测量与它的部分自由度相关的可观测量，测量就是不完全测量.因此，为了描述 MIMO 系统的量子态，就需要引进约化密度矩阵[19]

$$\boldsymbol{\rho} = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{5}$$

其中$|\psi_i\rangle$表示 MIMO 量子系统的量子态，i 描述量子态的数目，p_i 表示对应量子态的概率.

2.2. MIMO 量子密钥分发信道中多光子纠缠态 Wigner 算符

在量子力学中，单个光子或体系的量子态是不能观测的，即在原则上不能用实验来测定.但对于在同样实验条件下制备出来的光子(或体系)所构成的系宗而言，量子态的测量则是有意义的.现今进行的测量量子态的实验工作，是测量与波函数或密度矩阵等价的 Wigner 函数[19—21](本文中也称为 Wigner 算符矩阵)，它具有准概率分布函数的性质，并且 Wigner 函数也是能够同时精确地测量某个光子的坐标与动量(也称为双模)和描述量子态$|\psi\rangle$分布的函数，Wigner 算符为[21]

$$\Delta(p,x) = \frac{1}{\pi}:\exp[-(x-X)^2-(p-P)^2]:, \tag{6}$$

其中$:$是正规排序的算符，x 和 p 分别表示光子的坐标和动量.引入

$$x = \frac{1}{\sqrt{2k}}(a - a^+),$$

$$p = \frac{1}{\sqrt{2}}(a + a^+),$$

$$\alpha = \frac{1}{\sqrt{2}}(x + kp), \tag{7}$$

其中 $k^2 = -1$，将(8)式代入(7)式，得到

$$\Delta(p,x) \to \Delta(\alpha) = \frac{1}{\pi}:\exp[-2(a^+ - \alpha^*)(a-\alpha)]:. \tag{8}$$

由(8)式能够得到具有相干态 Wigner 函数

$$\langle z|\Delta(x,p)|z\rangle = \frac{1}{\pi}\exp[-2(z^* - \alpha^*)(z-\alpha)]. \tag{9}$$

上面(8)式又可以写成

$$\Delta(\alpha) = \pi^{-1}D(2\alpha)(-1)^N, N = a^+a,$$
$$D(\alpha) = \exp(\alpha a^+ - \alpha^* a), \tag{10}$$

其中 $D(\cdot)$为平移算符，N 是粒子数算符，a 和 a^+ 分别是玻色湮灭与产生算符，满足对易关系$[a,a^+]=1$，$*$ 表示共轭.

上面讨论了单个光子 Wigner 算符，而在 MIMO 量子密钥分发信道，由于多光子的存在产生多态的纠缠系统，以至于没有一个光子能单独有一个态.换言之，处于纠缠态的光子没有独立的态，或者甚至没有独立光子的性质.鉴于此，要用单光子 Wigner 函数反映整个 MIMO 系统所处的态包含的纠缠性质是不恰当的，必须作合理的改进与推广，才能适合于纠缠光子系统.在 MIMO 量子密钥分发信道，多光子中任意两光子相对坐标 $X_i - X_j$ 与总动量 $P_i + P_j$ 的共同本征态是

$$|\boldsymbol{\eta}\rangle = \exp\left(-\frac{\boldsymbol{\eta}^2}{2} + \boldsymbol{\eta}a_i^+ - \boldsymbol{\eta}^* a_j^+ + a_i^+ a_j^+\right)|0,0\rangle, \tag{11}$$

式中 $\boldsymbol{\eta} = \eta_i + k\eta_j (i \neq j)$，它的正规乘积展开为

$$|\boldsymbol{\eta}\rangle\langle\boldsymbol{\eta}| = :\exp[-(\boldsymbol{\eta} - a_i + a_j^+) \times (\boldsymbol{\eta}^* - a_i^+ + a_j)]:. \tag{12}$$

另一方面，与$|\boldsymbol{\eta}\rangle$正则共轭的纠缠态$|\xi\rangle$的正规乘积展开为

$$|\xi\rangle\langle\xi| = :\exp[-(\xi - a_j^+ - a_i) \times (\xi^* - a_i^+ - a_j)]:. \tag{13}$$

根据(7)式，可以构造出适合于多光子纠缠态 Wigner 算符矩阵

$$\Delta(\sigma,\gamma) = \frac{1}{\pi^2} :\prod_{i\neq j} \exp[-(\sigma - a_i + a_j^+) \times (\sigma^* - a_i^+ + a_j) - (\gamma - a_j^+ - a_i) \times (\gamma^* - a_i^+ - a_j)] :, \quad (14)$$

其中

$$\sigma_{i\neq j} = \frac{1}{\sqrt{2}}[(x_i - x_j) + k(p_i + p_j)],$$

$$\gamma_{i\neq j} = \frac{1}{\sqrt{2}}[(x_i + x_j) + k(p_i - p_j)]. \quad (15)$$

在$|\eta\rangle$表象中多光子纠缠态 Wigner 算符矩阵

$$\Delta(\sigma,\gamma) = \int \frac{\mathrm{d}^2\eta}{\pi^3} |\sigma - \eta\rangle\langle\sigma + \eta| \times \exp(\eta\gamma^* - \eta^*\gamma). \quad (16)$$

依次类推，也能够得到在$|\xi\rangle$表象中多光子纠缠态 Wigner 算符矩阵

$$\Delta(\sigma,\gamma) = \int \frac{\mathrm{d}^2\xi}{\pi^3} |-\xi + \gamma\rangle\langle\xi + \gamma| \times \exp(\xi^*\sigma - \xi\sigma^*). \quad (17)$$

2.3. 多光子双模压缩纠缠态 Wigner 算符矩阵和 MIMO 量子密钥分发信道容量

在 MIMO 量子密钥分发信道，假设多光量子密钥之间是去相关的（量子密钥的不可克隆定理）.作为信息载体的光量子，受到量子噪声的影响，限制着信息的传输和提取.相干态具有标准的量子极限噪声，因此可采用相干态 Wigner 算符矩阵来描述信道互信息的条件熵.根据两光子双模压缩（坐标本征态与动量本征态）纠缠态[22]构造出多光子双模压缩纠缠态算符矩阵表象为

$$S = \exp[\lambda(a_i^+ a_j^+ - a_i a_j)] \quad (i \neq j), \quad (18)$$

其中 λ 为光子的波长，纠缠态表象$|\eta\rangle$下多光子双模压缩态算符矩阵满足

$$S|\eta\rangle = \frac{1}{\mu}\left|\frac{\eta}{\mu}\right\rangle, \quad (19)$$

其中 μ 称为压缩态算符.将(18)式结合纠缠态的正交性[19]，可知(14)式 Wigner 算符矩阵的压缩变换为

$$S^+(\mu)\Delta(\sigma,\gamma)S(\mu) = \mu^2\int \frac{\mathrm{d}^2\eta}{\pi^3} |\mu(\sigma - \eta)\rangle \times \langle\mu(\sigma + \eta)|\exp(\eta\gamma^* - \eta^*\gamma). \quad (20)$$

根据(14)和(20)式得到多光子双模压缩纠缠态 Wigner 算符矩阵

$$W_\rho(\sigma,\gamma) = \int \frac{\mathrm{d}^2\eta}{\pi}\langle\sigma + \eta|\rho|\sigma - \eta\rangle \times \exp(\eta\gamma^* - \eta^*\gamma), \quad (21)$$

其中 ρ 为(5)式的约化密度矩阵.将(5)式代入(21)式得到

$$W_\rho(\sigma,\gamma) = \int \frac{\mathrm{d}^2\eta}{\pi}\langle\sigma + \eta|\sum_i p_i|\psi_i\rangle \times \langle\psi_i\|\sigma - \eta\rangle\exp(\eta\gamma^* - \eta^*\gamma), \quad (22)$$

特别地，多光子双模压缩纠缠真空态 Wigner 算符矩阵

$$\begin{aligned}&\langle 0,0|S^+(\mu)\Delta(\sigma,\gamma)S(\mu)|0,0\rangle| \\ &= \pi^{-2}\prod_{i\neq j}\exp(-r^2|\sigma|^2 - \frac{|\gamma|^2}{r^2}) \\ &= \pi^{-2}\prod_{i\neq j}\exp\Big\{-\frac{1}{4}\mu^2[(x_i - x_j)^2 + (p_i + p_j)^2] \\ &\quad - \frac{1}{4}\mu^2[(x_i + x_j)^2 + (p_i - p_j)^2]\Big\}. \end{aligned} \quad (23)$$

MIMO 量子密钥分发信道中由于量子噪声的影响多光子处于相干-纠缠态的情况下进行信息传输.由(9)式和(22)式，利用有序算符内的积分技术[23](IWOP)可以得到多光子双模压缩相干-纠缠态 Wigner 算符矩阵

$$\begin{aligned}W'_\rho(\sigma,\gamma) &= \langle\xi|W_\rho(\sigma,\gamma)|\xi\rangle \\ &= \int \frac{\mathrm{d}^2\eta}{\pi}\langle\xi|\sigma + \eta|\sum_i p_i|\psi_i\rangle \\ &\quad \times \langle\psi_i\|\sigma - \eta|\xi\rangle\exp(\eta\gamma^* - \eta^*\gamma) \\ &= (2\pi)^{-1}\rho\prod_{i\neq j}\delta[\sqrt{2}\xi - (x_i - x_j)] \\ &\quad \times \delta[\sqrt{2}\xi - (p_i + p_j)], \end{aligned} \quad (24)$$

式中正确地反映测量$|\xi\rangle$在相空间$(x_i - x_j, p_i + p_j)$中的值.由(3)式和(23)式，得到 MIMO 量子密钥分发信道中 Von Neumann 熵

$$H(\rho) = -\mathrm{Tr}\Big[\pi^{-2}\prod_{i\neq j}\exp\Big(-r^2|\sigma|^2 - \frac{|\gamma|^2}{r^2}\Big) \times \log\pi^{-2}\prod_{i\neq j}\exp(-r^2|\sigma|^2 - \frac{|\gamma|^2}{r^2})\Big]. \quad (25)$$

类似地，由(3)式和(24)式可以得到，MIMO 量子密钥分发信道中多光子的条件熵为

$$\begin{aligned}H'(\rho) = -\mathrm{Tr}\Big[&(2\pi)^{-1}\rho\prod_{i\neq j}\delta[\sqrt{2}\xi - (x_i - x_j)] \\ &\times \delta[\sqrt{2}\xi - (p_i + p_j)] \\ &\log(2\pi)^{-1}\rho\prod_{i\neq j}\delta[\sqrt{2}\xi - (x_i - x_j)] \\ &\times \delta[\sqrt{2}\xi - (p_i + p_j)]\Big]. \end{aligned} \quad (26)$$

将(25)和(26)式代入(1)和(2)式中，可以得到多光子双模压缩纠缠态 MIMO 量子密钥分发信道容量为

$$C = \max\{H(\boldsymbol{\rho}) - H'(\boldsymbol{\rho})\}$$

$$= \max\left\{-\mathrm{Tr}\left[\log\frac{\left\{\pi^{-2}\prod_{i\neq j}\exp\left(-\boldsymbol{\mu}^2|\boldsymbol{\sigma}|^2-\frac{|\boldsymbol{\gamma}|^2}{\boldsymbol{\mu}^2}\right)\right\}^{\pi^{-2}\prod_{i\neq j}\exp\left(-\boldsymbol{\mu}^2|\boldsymbol{\sigma}|^2-\frac{|\boldsymbol{\gamma}|^2}{\boldsymbol{\mu}^2}\right)}}{\left\{(2\pi)^{-1}\boldsymbol{\rho}\prod_{i\neq j}\delta[\sqrt{2}\xi-(x_i-x_j)]\,\delta[\sqrt{2}\xi-(p_i+p_j)]\right\}^{(2\pi)^{-1}\boldsymbol{\rho}\prod_{i\neq j}\delta[\sqrt{2}\xi-(x_i-x_j)]\,\delta[\sqrt{2}\xi-(p_i+p_j)]}}\right]\right\}. \quad (27)$$

下面我们以具体的信道来分析 MIMO 量子信道容量与影响信道容量参数(ξ,μ,σ,γ)变化关系,并得到 MIMO 量子信道容量的量化关系式.

3. MIMO 量子高斯信道下的信道容量

对于多光子纠缠态 Wigner 算符矩阵应满足海森堡正则变换关系,将(15)式写成下面的形式

$$[\sigma_i,\gamma_k] = i\delta_{ik}\hbar I,[\sigma_j,\sigma_k] = 0,[\gamma_j,\gamma_k] = 0. \quad (28)$$

定义列向量 $\boldsymbol{R} = [\sigma_1,\cdots,\sigma_T;\gamma_1,\cdots,\gamma_T]^{\mathrm{T}}$ 和 $\boldsymbol{Z} = [x_1,\cdots,x_T;y_1,\cdots,y_T]^{\mathrm{T}}$,在 Hilbert 空间的进行 U 变换有[24,25]

$$\boldsymbol{V}(t) = \exp\left[\mathrm{i}\sum_{j=1}^{T}(x_j\sigma_j + y_j\gamma_j)\right] = \exp(\mathrm{i}R^{\mathrm{T}}Z). \quad (29)$$

将(14)式乘以(29)式求迹有

$$\mathrm{Tr}[\boldsymbol{\Delta}(\boldsymbol{\sigma},\boldsymbol{\gamma})\boldsymbol{V}(t)] = \exp(\mathrm{i}\boldsymbol{M}^{\mathrm{T}}\boldsymbol{Z} - \frac{1}{2}\boldsymbol{Z}^{\mathrm{T}}\boldsymbol{\alpha}\boldsymbol{Z}), \quad (30)$$

式中 $\boldsymbol{M},\boldsymbol{\alpha}$ 分别为量子高斯信道下多光子纠缠态的均值和相关矩阵,$\boldsymbol{M}$ 是一个 $2T$ 列向量,$\boldsymbol{\alpha}$ 是一个实对称的 $2T\times 2T$ 矩阵且满足

$$\boldsymbol{M} = \mathrm{Tr}[\boldsymbol{\Delta}(\boldsymbol{\sigma},\boldsymbol{\gamma})\boldsymbol{R}]$$

$$\boldsymbol{\alpha} - \frac{1}{2}\boldsymbol{\Delta} = \mathrm{Tr}[\boldsymbol{R}\boldsymbol{\Delta}(\boldsymbol{\sigma},\boldsymbol{\gamma})\boldsymbol{R}^{\mathrm{T}}], \quad (31)$$

其中

$$\boldsymbol{\Delta} = \begin{bmatrix} 0 & 0 & 0 & 0 & \hbar & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \hbar & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \hbar \\ -\hbar & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\hbar & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & -\hbar & 0 & 0 & 0 & 0 \end{bmatrix}.$$

根据通用的罗伯逊不确定关系,(31)式可以写为

$$\boldsymbol{\alpha} - \frac{1}{2}\boldsymbol{\Delta} \geqslant 0, \quad (32)$$

化简(32)式得到双模压缩态多光子密度算符为纯态时的变化关系式

$$\alpha_j = \hbar(N_j + \frac{1}{2}), \quad (33)$$

由海森堡测不准关系可得到(32)式的转置 $\boldsymbol{\alpha} + \frac{1}{2}\boldsymbol{\Delta} \geqslant 0$,即有

$$\boldsymbol{\Delta}^{-1}\boldsymbol{\alpha}\boldsymbol{\Delta}^{-1} + \frac{1}{4}\boldsymbol{\alpha}^{-1} \geqslant 0. \quad (34)$$

当 $\boldsymbol{\Delta}(\boldsymbol{\sigma},\boldsymbol{\gamma})$为纯态时,且有

$$(\boldsymbol{\Delta}^{-1}\boldsymbol{\alpha})^2 = -\frac{1}{4}\boldsymbol{I}, \quad (35)$$

式中 $\boldsymbol{\alpha}$ 可表示为

$$\boldsymbol{\alpha} = \begin{bmatrix} \alpha^{\sigma\sigma} & \alpha^{\sigma\gamma} \\ \alpha^{\gamma\sigma} & \alpha^{\gamma\gamma} \end{bmatrix}. \quad (36)$$

化简(18)式得到 MIMO 量子高斯信道下多光子压缩态

$$\langle\boldsymbol{\eta}|\boldsymbol{S} = \exp\left(-\frac{\mu}{2}\right)\langle\boldsymbol{\eta},\mathrm{e}^{-\mu}\boldsymbol{\sigma}|, \quad (37)$$

其中 $\boldsymbol{\mu} = r\mathrm{e}^{\mathrm{i}\theta}$,对于光量子密钥分发的相关矩阵有 $\alpha^{pq} = \alpha^{qp} = 0$,将(36)式代入(35)式,得到

$$\alpha^{pp}\alpha^{qq} = \frac{\hbar^2}{4},\alpha^{pp} = \frac{\hbar}{2w}e^{-2r},$$

$$\alpha^{qq} = \frac{\hbar w}{2}\mathrm{e}^{2r}. \quad (38)$$

设信号 τ 在量子信道中的映像为 $\rho(\tau)$,即 $\tau\rightarrow\rho(\tau)$,$P(d\tau)$为先验输入概率密度分布.根据 von Neumann 熵 $S(\boldsymbol{\rho}) = -\mathrm{Tr}[\boldsymbol{\rho}\ln\boldsymbol{\rho}]$,得到量子密钥分发能量约束条件

$$\mathrm{Tr}[H\int\boldsymbol{\rho}(\tau)P(\mathrm{d}\tau)] \leqslant \hbar\left(N_{\mathrm{t}} + \frac{1}{2}\right), \quad (39)$$

式中 H 为哈密顿量 $H = \hbar(a^+a + \frac{1}{2})$,$N_{\mathrm{t}}$ 为量子密钥分发的光子数目(等于发射单光子源的数目)在 MIMO 量子高斯信道下(24)式可化简为

$$W'_{\rho}(\boldsymbol{\sigma},\boldsymbol{\gamma}) = S(\xi)\mathrm{Tr}[\boldsymbol{\rho}\boldsymbol{\Delta}(\boldsymbol{\sigma},\boldsymbol{\gamma})]S(\xi)^{\mathrm{T}}$$
$$= \int \mathrm{Tr}[\boldsymbol{\rho}(\tau)\boldsymbol{\Delta}(\boldsymbol{\sigma},\boldsymbol{\gamma})]P(\mathrm{d}\tau)$$
$$= \int \mathrm{Tr}[\boldsymbol{\rho}(\tau)\pi^{-2}\vdots\exp[-2(a_i^{+}-\zeta^{*})(a_i-\zeta)$$
$$-2(a_j^{+}-\delta^{*})(a_j-\delta)]\vdots]P(d\tau)$$
$$= \frac{1}{2}\mathrm{Tr}[\boldsymbol{\Delta}(\zeta)] + \frac{1}{2}\mathrm{Tr}[\boldsymbol{\Delta}(\delta)], \quad (40)$$

式中利用了 $S(\xi)\boldsymbol{\Delta}(\boldsymbol{\sigma},\boldsymbol{\gamma})S(\xi)^{\mathrm{T}} = \boldsymbol{\Delta}(\boldsymbol{\sigma},\boldsymbol{\gamma})$，$\zeta = \frac{1}{\sqrt{2}}(x_i + ip_i)$ 和 $\delta = \frac{1}{\sqrt{2}}(x_j + ip_j)(i \neq j)$，其中 $\boldsymbol{\gamma} = \zeta + \delta^{*}$ 和 $\boldsymbol{\sigma} = \zeta - \delta^{*}$. MIMO 量子高斯信道下多光子压缩相干-纠缠态密度算符矩阵 $W'_{\rho}(\boldsymbol{\sigma},\boldsymbol{\gamma})$，满足 $\mathrm{Tr}[W'_{\rho}(\boldsymbol{\sigma},\boldsymbol{\gamma})] \leqslant 1$，当且仅当密度算符 $W'_{\rho}(\boldsymbol{\sigma},\boldsymbol{\gamma})$ 为纯态时取等号，联立(39)和(40)式，可以得到

$$\frac{1}{2}\mathrm{Tr}[\boldsymbol{\Delta}(\zeta)] + \frac{1}{2}\mathrm{Tr}[\boldsymbol{\Delta}(\delta)] \leqslant \hbar\left(N_{\mathrm{t}} + \frac{1}{2}\right), \quad (41)$$

式中左边第一项 $\frac{1}{2}\mathrm{Tr}[\boldsymbol{\Delta}(\zeta)]$ 描述压缩态能量，它的值小于输入的能量 $\hbar\left(N_{\mathrm{t}} + \frac{1}{2}\right)$. 将(36)式代入(41)式中得到压缩参数 r 满足

$$\frac{1}{2}\ln[2(N_{\mathrm{t}}+1) - \sqrt{4(N_{\mathrm{t}}+1)^2 - 1}] \leqslant r$$
$$\leqslant \frac{1}{2}\ln[2(N_{\mathrm{t}}+1) + \sqrt{4(N_{\mathrm{t}}+1)^2 - 1}]. \quad (42)$$

在 MIMO 量子高斯信道下，接收端采用零差接收，当双模压缩多光子相干-纠缠态的压缩参数满足 $r_0 = \frac{1}{2}\ln[2(N_{\mathrm{t}}+1) + \sqrt{4(N_{\mathrm{t}}+1)^2 - 1}]$，化简(27)式得到双模压缩多光子相干-纠缠态信道容量

$$C = \max W'_{\rho}(\boldsymbol{\sigma},\boldsymbol{\gamma})H(\boldsymbol{\rho})$$
$$= \max_{0 \leqslant j \leqslant N_{\mathrm{r}} \leqslant N_{\mathrm{t}}} g\left(\alpha_j - \frac{1}{2}\right) + g\left(\beta_j - \frac{1}{2}\right)$$
$$- g\left(\alpha_0 - \frac{1}{2}\right) - g\left(\beta_0 - \frac{1}{2}\right), \quad (43)$$

式中 $g(x) = (x+1)\ln(x+1) - x\ln x (x > 0)$，$\beta_j$ 为接收端双模压缩态多光子密度算符矩阵 $\boldsymbol{\beta}$ 为纯态时变化关系式，其中 $\boldsymbol{\beta}$ 也可表示为 $\boldsymbol{\beta} = \begin{bmatrix} \beta^{pp} & \beta^{pq} \\ \beta^{qp} & \beta^{qq} \end{bmatrix}$. 且满足正定条件

$$\beta^{pp}\beta^{qq} - (\beta^{pq})^2 \geqslant 0. \quad (44)$$

简化(44)式得到

$$\frac{\beta^{pp} + \beta^{qq}}{2} + \hbar N_{\mathrm{r}} \leqslant \hbar N_{\mathrm{t}}, \quad (45)$$

式中 N_{r} 为接收光量子密钥的数目(等于接收单光子探测器的数目)，将(33)和(45)式代入(43)式中得到(β_j 的计算方法与 α_j 一样)

$$C_{\max} \approx \ln(1 + N_{\mathrm{t}}\sqrt{(1+N_{\mathrm{t}})(3N_{\mathrm{r}}-1)})$$
$$\geqslant \ln(1 + 2N_{\mathrm{t}}), \quad (46)$$

式中的右侧不等式就是 YUEN-OZAWA 边界[26] 和 Holevo 边界[27,28]. 当且仅当 $N_{\mathrm{r}} = N_{\mathrm{t}} = 1$ 时，(47)式取等式.

将(46)式化简得到

$$C_{\max} \approx \ln(1 + \sqrt{4N_{\mathrm{t}}(1+N_{\mathrm{t}})N_{\mathrm{t}}(3N_{\mathrm{r}}-1)/4}), \quad (47)$$

式中 $4N_{\mathrm{t}}(1+N_{\mathrm{t}})$ 是信噪比[29]，令 $\lambda = 4N_{\mathrm{t}}(1+N_{\mathrm{t}})$，即有

$$C_{\max} \approx \ln(1 + \sqrt{\lambda N_{\mathrm{t}}(3N_{\mathrm{r}}-1)/4}). \quad (48)$$

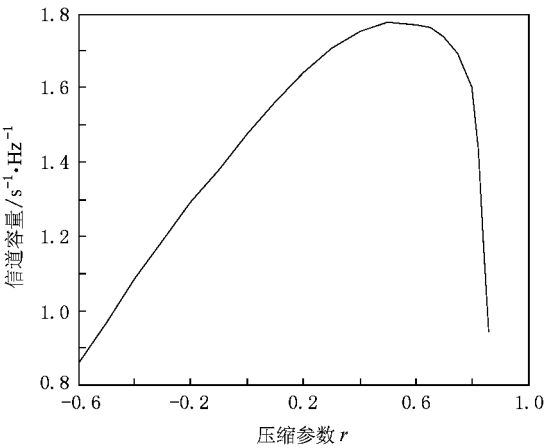

图 1　$N_{\mathrm{t}} = N_{\mathrm{r}} = 2$，压缩参数 r 与信道容量变化关系

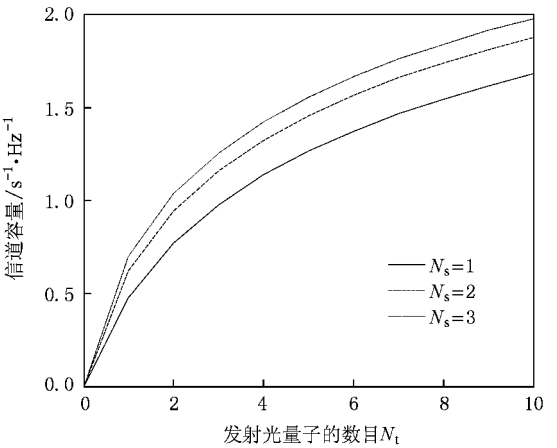

图 2　不同的单光子探测器数目下，发射光量子的数目与信道容量的变化关系

图 1 给出了 $N_{\mathrm{t}} = N_{\mathrm{r}} = 2$，压缩参数 r 与信道容量的变化关系，从图 1 中得到信道容量随着压缩参数 r 增大先增大后减小，而压缩参数的取值由发射

光量子的数目 N_t 决定，增加发射光量子的数目能够增大信道容量，但并非发射光量子的数目越多越好，这是由于量子密钥分发系统也面临着信道噪声和多光量子消相干克服问题. 图 2 描述不同的单光子探测器数目 N_r，发射光量子的数目 N_t 与信道容量的变化关系，从图 2 中可以发现随着单光子探测器数目的增加，信道容量也增加，这是因为采用多个单光子探测器能够消除光量子信号抖动和漂移带来光量子密钥分发的丢失，从而提高信道容量.

4. 结 论

量子安全通信是涉及经典信息论和量子力学的新兴综合学科. 利用量子安全通信可以建立超光速通信和无法破译的密钥系统. 然而，目前采用的通信技术严重制约了量子密钥分发的比特率. 将多输入多输出(MIMO)技术应用于量子安全通信系统，提高量子密钥分发的比特率，促进量子安全通信向高速大容量发展. 本文首先构造出 MIMO 量子密钥分发信道中多光子双模压缩纠缠态 Wigner 算符. 并在此基础上，推导出多光子相干-纠缠态 Wigner 函数和 MIMO 量子密钥分发信道容量. 这些研究将为开发稳健的 MIMO 量子安全通信空时处理算法和优化设计高性能 MIMO 量子密钥分发系统提供理论支撑和技术基础.

[1] Ghonaimy M A R 2006 *Int. Conf. Computers Engineering and Systems* (New York: IEEE) p1

[2] Bennett C H, Brassard G 1984 *Int. Conf. Computers Systems and Signal Processing* (New York: IEEE) p175

[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[4] *Bennett C H* 1992 *Phys. Rev. Lett.* **68** 3124

[5] Yang Y G, Wen Q Y, Zhu F C 2005 *Acta Phys. Sin.* **54** 5544 (in Chinese) [杨宇光、温巧燕、朱甫臣 2005 物理学报 **54** 5544]

[6] Zhao F, Lu Y Q, Wang F Q, Chen X, Li M M, Guo B H, Miao C J, Liu S H 2007 *Acta Phys. Sin.* **56** 2175 (in Chinese) [赵 峰、路轶群、王发强、陈 霞、李明明、郭拜红、廖常俊，刘颂豪 2007 物理学报 **56** 2175]

[7] Zhang Q, Tang C J, Gao F 2002 *Acta Phys. Sin.* **51** 15 (in Chinese) [张 权、唐朝京、高 峰 2002 物理学报 **51** 15]

[8] Zhang J, Wang F Q, Zhao F, Lu Y Q, Liu S H 2008 *Acta Phys. Sin.* **57** 4946 (in Chinese) [张 静、王发强、赵 峰、路轶群、刘颂豪 2008 物理学报 **57** 4946]

[9] Yang Y G, Wen Q Y, Zhu F C 2005 *Acta Phys. Sin.* **54** 5549 (in Chinese) [杨宇光、温巧燕、朱甫臣 2005 物理学报 **54** 5549]

[10] Foschini G J, Gans M J 1998 *Wireless Personal Commun.* **6** 311

[11] Tekatar I E 1999 *European Trans. Telecomm.* **10** 585

[12] Nielsen M A, Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[13] Andreas W 2001 *IEEE Trans. Information Theory* **47** 3059

[14] Allahverdvan A E, Saakian D B 1999 *Quantum Computing and Quantum Communications* (Lecture Notes in Computer Science) (Vol.1509) (Berlin, Germany: Springer Verlag)

[15] Hranilovic S, Frank R, Kschischang F R 2006 *IEEE Journal of Selected Topics in Quantum Electronics* **12** 859

[16] Gabay M, Arnon S 2006 *IEEE Journal of Lightwave Technology* **24** 3114

[17] Schaich F, Speidel J 2007 *IEEE Journal of Selected Topics in Quantum Electronics* **13** 1429

[18] Nielsen M A 2005 *Cluster-State Quantum Computation* **57** 1321

[19] Zeng J Y 2000 *Quantum Mechanics* (3rd ed.) (Beijing: Science Press) (in Chinese) [曾谨言 2000 量子力学 (北京：科学出版社)]

[20] Wigner E 1932 *Phys. Rev.* **40** 749

[21] Fan H Y, Fan Y 1996 *Phys. Rev.* A **54** 958

[22] Fan H Y, Cheng H L 2001 *Commun. Theor. Phys.* **36** 651

[23] Fan H Y, Xu Z H 1994 *Phys. Rev.* A **50** 2921

[24] Sohma M, Hirota O 2007 *Phys. Rev.* A **76** 024303

[25] Holevo A S, Sohma M, Hirota O 1999 *Phys. Rev.* A **59**1821

[26] Yuen H P, Ozawa M 1993 *Phys. Rev.* A **70** 363

[27] Holevo A S 1998 *IEEE Trans. Information Theory* **44** 269

[28] Holevo A S 1998 *IEEE Trans. Information Theory* **21** 533

[29] Yuen H P 1976 *Phys. Lett.* A **56** 105

Capacity of multiple-input-multiple-output quantum key distribution channels *

Xiao Hai-Lin[1)†] Ouyang Shan[1)] Nie Zai-Ping[2)]

1)(*School of Information and Communications*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

2)(*School of Electronic Engineering*, *University of Electronic Science and Technology of China*, *Chengdu* 610054, *China*)

(Received 17 September 2008; revised manuscript received 11 December 2008)

Abstract

Quantum safety communications is a process of quantum key distribution (QKD). Current QKD technology restricts transmission to a low bit rate. To improve the QKD bit rate and develope high rate and large capacity, we propose a multiple-input-multiple-output(MIMO) quantum key distribution system. The Wigner operator of multi-photon entangled states in MIMO quantum key distribution channel is presented. As a result, the Wigner function of multi-photon double-model squeezed entangled sates and MIMO quantum key distribution channel capacity are also obtained, which will provide theoretical support and technical basis for developing robust space-time processing algorithm of MIMO quantum safety communications and designing optimum high performance system of MIMO quantum key distribution.

Keywords: multiple input multiple output (MIMO), double model squeezed state, multi-photon entangled states, channel capacity

PACC: 0365, 4230, 4250

* Project supported by the National Basic Research Program of China (Grant No. 2008CB317109), the Guangxi Natural Science Foundation, China (Grant No. 0991241), and the National Natural Science Foundation of China (Grant No. 60972084).

† E-mail: xhl_xiaohailin@163.com