第 56 卷 第 11 期 2007 年 11 月
1000-3290/2007/56(11)/6427-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.11,November,2007

基于双模压缩态的量子密钥分发方案*

何广强† 易 智 朱 俊 曾贵华

(上海交通大学电子工程系区域光纤通信网与新型光通信系统国家重点实验室,上海 200240)

(2006 年 12 月 20 日收到;2007 年 3 月 18 日收到修改稿)

提出了一种基于双模压缩态的量子密钥分发方案,采用 Shannon 信息论分析了该协议抵抗光束分离攻击的能力,得到秘密信息速率与压缩因子、信道参数之间的解析表达式,双模压缩态的模间关联性保证了该方案的安全性.

关键词:量子密钥分发,双模压缩态,光束分离攻击

PACC:4250,4230Q,0365

1. 引 言

信息安全在信息社会扮演着越来越重要的作用,密码学是保障信息安全的重要工具,目前广泛使用的密码体制依赖于没有严格证明的数学难题.然而,随着经典计算机计算能力的提高和量子计算机取得的重大突破,依赖于数学难题的某些密码算法如 RSA 算法等将面临着严峻的挑战.幸运的是,以经典密码学和量子物理学为基础的量子密码[1—5]作为一种新型密码体制,其安全性由量子力学的基本规律保证.量子测不准原理和量子不可克隆定理保证了量子密码的安全性[6—8]和对窃听的可检测性,使得量子密码具有良好的性能和前景.

连续变量量子密码采用高斯态(相干态和压缩态)作为信号载波,采用光场的正则振幅和正则相位作为信号载波的可观测物理量,通过振幅和相位调制把信号加载到量子载波上,采用散粒噪声限制的零差接收机检测量子信号[9—27].相对于基于单光子发生与检测技术的离散变量量子密钥分发,连续变量量子密钥分发实验实现相对简单,单信号所能传输的信息量较高,即信道容量高,连续变量的量子密码[9]引起了各国学者的极大关注.

连续变量量子密钥分发的安全性与纠缠息息相关[28],因此研究基于纠缠的量子密钥分发具有重要的理论意义,由于双模压缩态是一种连续变量纠缠态,因此研究基于双模压缩态的量子密钥分发具有较好的理论意义.本文研究纠缠对基于双模压缩态的量子密钥分发方案安全性的影响,并给出了合法通信双方之间的秘密信息速率与纠缠之间的解析表达式,定量地讨论纠缠对方案安全性的影响.

本文介绍了基于双模压缩态的量子密钥分发协议的工作过程;介绍了光束分离攻击的物理模型;采用 Shannon 信息论分析了合法通信双方之间的互信息量;计算出窃听者所能窃取的信息量;给出了合法双方之间的秘密信息速率.

2. 基于双模压缩态的 QKD 协议

基于双模压缩态的量子密钥分发方案如图 1 所示.

第一步 Alice 根据随机比特串 n_1 通过双模压缩算符 $\hat{S}(\pm r)$ 作用于光学模 $\hat{a}_1$ 和 $\hat{a}_2$,产生纠缠光学模 $\hat{a}_3$ 和 $\hat{a}_4$.根据比特串 n_1 第 i 位比特 n_1^i 的值,决定执行具体的压缩操作.当 $n_1^i=0$,应用 $\hat{S}(r)$;当 $n_1^i=1$,应用 $\hat{S}(-r)$.

利用双模压缩效应制备纠缠态的过程如下,双模压缩算符为

$$S(\pm r)=\exp[r(\hat{a}_1^{\dagger}\hat{a}_2^{\dagger}-\hat{a}_1\hat{a}_2)]. \qquad (1)$$

* 上海交通大学青年教师校内科研启动基金(批准号:A2831B),上海交通大学 PRP 项目(批准号:T03011030)和国家自然科学基金(批准号:60472018)资助的课题.

† E-mail:gqhe@sjtu.edu.cn

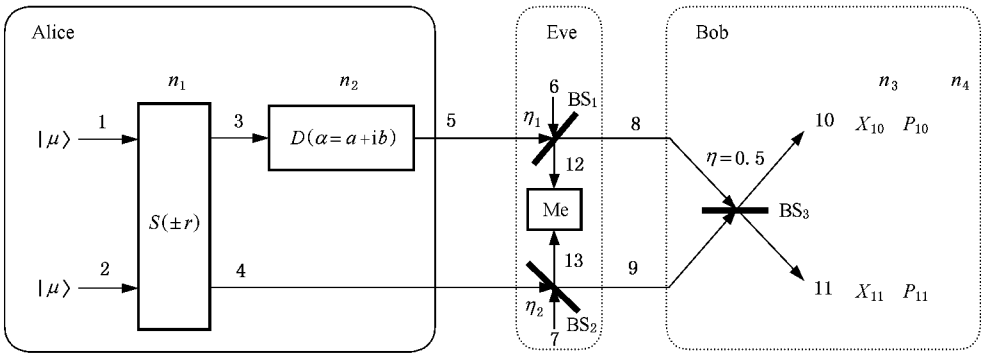

图 1 基于双模压缩态的量子密钥分发方案 $\hat{S}(\pm r)$为双模压缩算符;$\hat{D}(\alpha)$为平移算符;BS 为光束分离器;Me 为测量装置

双模压缩变换为

$$\begin{aligned}\hat{a}_3 &= \hat{S}^{\dagger}(\pm r)\hat{a}_1\hat{S}(\pm r)\\ &= \hat{a}_1\cosh(r) \pm \hat{a}_2^{\dagger}\sinh(r),\\ \hat{a}_4 &= \hat{S}^{\dagger}(\pm r)\hat{a}_2\hat{S}(\pm r)\\ &= \hat{a}_2\cosh(r) \pm \hat{a}_1^{\dagger}\sinh(r).\end{aligned} \tag{2}$$

分别定义正则振幅和正则相位为 $X=\frac{1}{2}(\hat{a}+\hat{a}^{\dagger})$，$P=\frac{1}{2\mathrm{i}}(\hat{a}-\hat{a}^{\dagger})$，则二者满足测不准关系，$\Delta X\Delta P \geqslant \frac{1}{4}$，根据(2)式，则可得如下关系：

$$\begin{aligned}X_3 &= X_1\cosh(r) \pm X_2\sinh(r),\\ P_3 &= P_1\cosh(r) \mp P_2\sinh(r),\\ X_4 &= X_2\cosh(r) \pm X_1\sinh(r),\\ P_4 &= P_2\cosh(r) \mp P_1\sinh(r),\end{aligned} \tag{3}$$

显然 $\lim\limits_{r\to\infty}(X_3 \mp X_4)=0$，$\lim\limits_{r\to\infty}(P_3 \pm P_4)=0$，即应用 $\hat{S}(r)$时，X_3 与 X_4 正相关，P_3 与 P_4 负相关；应用 $\hat{S}(-r)$时，X_3 与 X_4 负相关，P_3 与 P_4 正相关.

第二步 Alice 应用平移算符 $\hat{D}(\alpha=a+\mathrm{i}b)$ 作用于模 $\hat{a}_3$，产生模 $\hat{a}_5$，把服从高斯概率分布的信息 $M=A+\mathrm{i}B$ 加载到载波 $\hat{a}_3$ 上，设 $A\sim N(0,\Sigma_1^2)$，$B\sim N(0,\Sigma_2^2)$，多次传输的信息 M 构成了信息序列 n_2，为便于讨论，本文采用对称调制，即 $A,B\sim N(0,\Sigma^2)$. 本文中用 $\Gamma\sim N(\mu,\Sigma^2)$ 表示随机变量 Γ 服从以 μ 为均值以 Σ^2 为方差的高斯概率分布. 平移算符 $\hat{D}(\alpha)=\exp(\alpha\hat{a}_3^{\dagger}-\alpha^{*}\hat{a}_3)$ 作用于模 $\hat{a}_3$ 产生变换 $\hat{a}_5=\hat{D}^{\dagger}(\alpha)\hat{a}_3\hat{D}(\alpha)=\hat{a}_3+M$，则

$$X_5 = X_3 + \mathrm{Re}(M) = X_3 + A,$$

$$P_5 = P_3 + \mathrm{Im}(M) = P_3 + B. \tag{4}$$

第三步 Alice 通过量子信道把光学模 $\hat{a}_4$ 和 $\hat{a}_5$ 发送到 Bob.

第四步 Bob 通过光束分离器把 BS_3 合成光学模 $\hat{a}_8$ 和 $\hat{a}_9$(如不存在窃听者，则 $\hat{a}_8=\hat{a}_5$，$\hat{a}_9=\hat{a}_4$)，产生光学模 $\hat{a}_{10}$和 $\hat{a}_{11}$.

第五步 Bob 根据随机比特串 n_3 选择测量基 (X_{11},P_{10})或者(X_{10},P_{11})，得到信息序列 n_4. 具体选择规则如下：

若比特串 n_3 第 i 位比特 $n_3^i=0$ 时，选择测量基 (X_{11},P_{10}) 若 $n_3^i=1$，选择测量基(X_{10},P_{11}).

第六步 Alice 和 Bob 通过经典信道通信，若 $n_1^i=n_3^i$，保留 n_2^i,n_4^i；$n_1^i\neq n_2^i$，则丢弃 n_2^i,n_4^i，从本文的理论计算中，可以清楚地了解这样选择的原因，通过比较测量基，可得到两个高度相关的信息序列，通过连续变量的协商过程，可得到两串比特串，然后通过纠错和保密增强过程可以得到安全的秘密密钥.

3. 安全性分析

对任何量子密码方案，安全性分析都是衡量其优越性的重要方面. 要分析任何量子密码协议的安全性，原则上要假定窃听者 Eve 可以制造出物理规律所允许的任何窃听装置，而并不受技术的限制. 如果要证明所设计的密码方案的无条件安全性，必须建立全面的数学模型，从信息论的角度证明其安全性，这是一个虽然重要但是相当复杂的问题，而要证明量子密码方案的有条件安全性，必须首先确定 Eve 所采用的特定攻击方式，才可以在此基础上建立对应于该攻击策略的物理模型，针对该物理模型

分析方案的安全性.

3.1. 光束分离攻击策略物理模型

本文分析最直观的光束分离攻击策略，如图 1 所示.直观上，Eve 最可能采用与 Bob 相同的测量方式窃听 Alice 所传送的信息，即 Eve 采用光束分离器 BS_1 和 BS_2 分离信号模 $\hat{a}_5$ 和参考模 $\hat{a}_4$，Eve 采用装置 Me 测量光学模 $\hat{a}_{12}$和 $\hat{a}_{13}$，Eve 可能采用光束分离器测量，则测量装置的结构如图 2 所示.从光束分离器输出的光学模式为 $\hat{a}_{14}$和 $\hat{a}_{15}$，Eve 随机选择测量基(X_{15}，P_{14})或者(X_{14}，P_{15})，从本文的理论计算中，可以清楚地了解这样选择的原因.

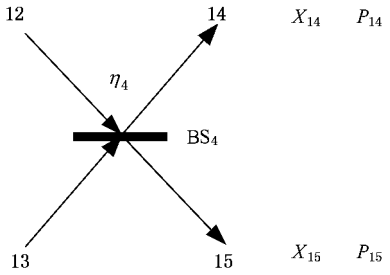

图 2　Eve 的窃听装置

3.2. 合法通信双方之间的互信息量

采用 Shannon 信息论计算各方之间的互信息量并进而计算合法通信双方之间的秘密信息速率之前，首先介绍 Shannon 信息论的基本公式.

Shannon 信息论公式：

若信源 X 为高斯信源，即信源 $X \sim N(0,\Sigma^2)$，并且连接通信双方的信道为加性高斯白噪声(AWGN)信道，加性高斯白噪声 $N \sim N(0,\sigma^2)$，则通信双方之间的信道容量为

$$I(X,Y) = \frac{1}{2}\log_2(1+S), \tag{5}$$

其中 $S = \Sigma^2/\sigma^2$ 为信噪比.

从 Shannon 信息论公式可见，为计算各方之间的互信息量，首先需要计算各方之间的信噪比.本文在海森伯表象中首先计算各个光学器件(即各个算符)对光学模式的变换，然后根据初始光学模服从的概率分布计算各光学模式中的正则算符所服从的概率分布，然后根据各方之间的信噪比，进而计算出通信各方之间的互信息量.

首先计算各个光学模式所对应的正则算符所服从的概率分布. 光束分离器 BS_1 作用于光学模 $\hat{a}_5$ 和 $\hat{a}_6$，输出光学模 $\hat{a}_8$ 和 $\hat{a}_{12}$，根据光束分离器的变换性质，可得

$$\begin{aligned}
X_8 &= \sqrt{\eta_1}X_5 + \sqrt{1-\eta_1}X_6,\\
P_8 &= \sqrt{\eta_1}P_5 + \sqrt{1-\eta_1}P_6,\\
X_{12} &= \sqrt{\eta_1}X_6 - \sqrt{1-\eta_1}X_5,\\
P_{12} &= \sqrt{\eta_1}P_6 - \sqrt{1-\eta_1}P_5,
\end{aligned} \tag{6}$$

其中 η_1 为光束分离器 BS_1 的透射系数.BS_2 通过作用于光学模式 $\hat{a}_4$ 和 $\hat{a}_7$ 产生了光学模式 $\hat{a}_9$ 和 $\hat{a}_{13}$，利用光束分离器的变换性质，可得

$$\begin{aligned}
X_9 &= \sqrt{\eta_2}X_4 + \sqrt{1-\eta_2}X_7,\\
P_9 &= \sqrt{\eta_2}P_4 + \sqrt{1-\eta_2}P_7,\\
X_{13} &= \sqrt{\eta_2}X_7 - \sqrt{1-\eta_2}X_4,\\
P_{13} &= \sqrt{\eta_2}P_7 - \sqrt{1-\eta_2}P_4.
\end{aligned} \tag{7}$$

光束分离器 BS_3 对光学模式 $\hat{a}_8$ 和 $\hat{a}_9$ 之间的变换为

$$\begin{aligned}
X_{10} &= \sqrt{\eta_3}X_9 + \sqrt{1-\eta_3}X_8,\\
P_{10} &= \sqrt{\eta_3}P_9 + \sqrt{1-\eta_3}P_8,\\
X_{11} &= \sqrt{\eta_3}X_8 - \sqrt{1-\eta_3}X_9,\\
P_{11} &= \sqrt{\eta_3}P_8 - \sqrt{1-\eta_3}P_9.
\end{aligned} \tag{8}$$

光束分离器 BS_3 的透视系数 $\eta_3 = 0.5$，把(3)，(4)，(5)，(6)和(7)式代入(8)式并化简，当采用 $S(r)$ 制备纠缠对时，可得到如下关系式：

$$\begin{aligned}
P_{10} = \frac{\sqrt{2}}{2}\Big[&\left(\sqrt{\eta_1}P_1 + \sqrt{\eta_2}P_2\right)\cosh(r)\\
&-\left(\sqrt{\eta_1}P_2 + \sqrt{\eta_2}P_1\right)\sinh(r)\\
&+\sqrt{1-\eta_1}P_6 + \sqrt{1-\eta_2}P_7 + \sqrt{\eta_1}B\Big],
\end{aligned}$$

$$\begin{aligned}
X_{11} = \frac{\sqrt{2}}{2}\Big[&\left(\sqrt{\eta_1}X_1 - \sqrt{\eta_2}X_2\right)\cosh(r)\\
&+\left(\sqrt{\eta_1}X_2 - \sqrt{\eta_2}X_1\right)\sinh(r)\\
&+\sqrt{1-\eta_1}X_6 - \sqrt{1-\eta_2}P_7 + \sqrt{\eta_1}A\Big].
\end{aligned} \tag{9}$$

当不存在窃听者且具有理想纠缠时，即 $\eta_1 = \eta_2 = 1$，$r \to +\infty$ 时，(9)式简化为 $P_{10} = \frac{\sqrt{2}}{2}B$，$X_{11} = \frac{\sqrt{2}}{2}A$，即通过测量 X_{11}，P_{10} 可以测量 Alice 发送的信息 $M = A + iB$，而当 Bob 选择另外两个正则算符 X_{10}，P_{11} 进行测量时，则将有很大的噪声，很难精确获得信息 $M = A + iB$.当采用 $S(-r)$ 制备纠缠时，采用类似的分析方法，通过测量 X_{10}，P_{11} 可以测量发送的信息 $M = A + iB$.这就是当 Alice 采用 $S(r)$ 时，Bob 选择测量基

(P_{10}, X_{11})，当 Alice 采用 $S(-r)$，Bob 选择测量基 (X_{10}, P_{11}) 进行测量的原因. 当窃听者存在时，即 η_1，η_2 至少有一个小于 1. 在这种情况下，由于纠缠态的制备方式和测量基的选择都是随机的，所以就有 50% 的传输将被丢弃，但是 Alice 和 Bob 通过经典信道完成编码基与测量基比较后，余下的随机变量串 R 所对应的编码基与测量基是完全符合的. 下面首先计算 Alice 和 Bob 之间的互信息量，因初始相干态为高斯态，则

$$X_i, P_i \sim N\left(\mu, \frac{1}{4}\right), i = 1,2,$$
$$X_j, P_j \sim N\left(0, \frac{1}{4}\right), j = 6,7. \tag{10}$$

当测量 P_{10}，只有 $\sqrt{\eta_1}\,B$ 为信号，其余项均为噪声；当测量 P_{11}，只有 $\sqrt{\eta_1}\,A$ 为信号，其余均为噪声. 利用(9)和(10)式，可以得到信噪比

$$S_{\mathrm{P}} = S_{\mathrm{X}} = \frac{4\eta_1\Sigma^2}{(\eta_1+\eta_2)[\cosh(2r)-1] - 2\sqrt{\eta_1\eta_2}\sinh(2r)+2}. \tag{11}$$

由于 Bob 同时测量 X_{11} 和 P_{10}，因此 Alice 和 Bob 之间的互信息量为

$$\begin{aligned} I(\alpha,\beta) &= \frac{1}{2}\log_2(1+S_X) + \frac{1}{2}\log_2(1+S_P) \\ &= \log_2\left[1 + \frac{4\eta_1\Sigma^2}{(\eta_1+\eta_2)[\cosh(2r)-1] - 2\sqrt{\eta_1\eta_2}\sinh(2r)+2}\right]. \end{aligned} \tag{12}$$

3.3. 窃听者所能窃取的信息量

本文只讨论在正向协商过程中，即在经典通信过程中，协商信息是 Alice 告诉 Bob 的，也就是以 Alice 的数据作为密钥源，在这情况下窃听者所窃取的信息量为 Eve 与 Alice 之间的互信息量. 根据光束分离攻击策略原理图 2，由(6)和(7)式可得模 $\hat{a}_{14}$ 和 $\hat{a}_{15}$ 的关系式

$$\begin{aligned} X_{14} &= \sqrt{\eta_4}\,X_{13} + \sqrt{1-\eta_4}\,X_{12}, \\ P_{14} &= \sqrt{\eta_4}\,P_{13} + \sqrt{1-\eta_4}\,P_{12}, \\ X_{15} &= \sqrt{\eta_4}\,X_{12} - \sqrt{1-\eta_4}\,X_{13}, \\ P_{15} &= \sqrt{\eta_4}\,P_{12} - \sqrt{1-\eta_4}\,P_{13}. \end{aligned} \tag{13}$$

本文假设窃听者有量子内存，则窃听者可以在 Alice 公布编码基之后采用正确地测量基测量所窃取的量子态，下面讨论方案在这种情况下的安全性. 本文以 Eve 选择测量基 (X_{15}, P_{14}) 为例计算. 由(3)，(4)，(6)，(7)和(13)式，可得

$$\begin{aligned} X_{15} &= \sqrt{(1-\eta_2)(1-\eta_4)}\,[X_1\sinh(r) + X_2\cosh(r)] \\ &\quad - \sqrt{(1-\eta_1)\eta_4}\,[X_1\cosh(r) + X_2\sinh(r)] \\ &\quad + \sqrt{\eta_1\eta_4}\,X_6 - \sqrt{\eta_2(1-\eta_4)}\,X_7 \\ &\quad - \sqrt{(1-\eta_1)\eta_4}\,A, \\ P_{14} &= \sqrt{(1-\eta_2)\eta_4}\,[P_1\sinh(r) - P_2\cosh(r)] \\ &\quad + \sqrt{(1-\eta_1)(1-\eta_4)}\,[P_2\sinh(r) - P_1\cosh(r)] \\ &\quad + \sqrt{\eta_1(1-\eta_4)}\,P_6 + \sqrt{\eta_2\eta_4}\,P_7 \\ &\quad - \sqrt{(1-\eta_1)(1-\eta_4)}\,B. \end{aligned} \tag{14}$$

理论上，窃听者通过调节 η_4 来窃听到最大的信息量，计算出 $I(\alpha,\varepsilon)$ 的解析表达式，然后通过求解 $\frac{\partial I(\alpha,\varepsilon)}{\partial\eta_4} = 0$ 得到 $\eta_4 = f(\Sigma, r, \eta_1, \eta_2)$，代入 $I(\alpha,\varepsilon)$ 得到最大窃听者所能窃听到的最大信息量 $I_{\max}(\alpha,\varepsilon)$. 然而 $I(\alpha,\varepsilon)$ 太复杂，难以得到 $I_{\max}(\alpha,\varepsilon)$ 的表达式. 但是多次数值计算发现 $\eta_4 = 0.5$ 时，$I(\alpha,\varepsilon)$ 达到最大值. $\eta_4 = 0.5$ 表明窃听者采用和 Bob 同样的测量装置，这也完全符合实际情况. 本文在计算 $I(\alpha,\varepsilon)$ 时，设 $\eta_4 = 0.5$. 根据(10)和(14)式可以求得 Eve 与 Alice 之间的信噪比为 $S_{\mathrm{X}}^{\mathrm{Eve}} = S_{\mathrm{P}}^{\mathrm{Eve}} = \frac{M}{N}$，其中 $M = (1-\eta_1)\eta_4\Sigma^2$，

$$\begin{aligned} N &= -\frac{1}{2}\sqrt{(1-\eta_1)(1-\eta_2)(1-\eta_4)\eta_4}\sinh(2r) \\ &\quad + \frac{1}{2}(\eta_2+\eta_1\eta_4)(1-\cosh^2(r)) \\ &\quad + \frac{1}{2}(1+\eta_2\eta_4)\cosh^2(r) - \frac{1}{4} - \frac{1}{2}\eta_2\eta_4. \end{aligned}$$

所以窃听者所能窃取的信息量为

$$I(\alpha,\varepsilon) = \frac{1}{2}\log_2(1+S_{\mathrm{X}}^{\mathrm{Eve}})$$

$$+\frac{1}{2}\log_2(1+S_{\mathrm{P}}^{\mathrm{Eve}}). \tag{15}$$

由于解析表达式太繁琐，在此不在列出具体的解析表达式，在 3.4 节中采用数值解方式给出合法通信双方之间秘密信息速率图形.

3.4. 秘密信息速率

Maurer 的研究结果[29] 表明，Alice 和 Bob 得到安全密钥的充要条件为

$$\max\{I(\alpha,\beta)-I(\alpha,\varepsilon),\ I(\beta,\alpha)-I(\beta,\alpha)\}>0. \tag{16}$$

当采用正向协商过程时，即以 Alice 的信息为密钥源，Bob 根据协商信息纠正所收到的信息使其与 Alice 的信息一致，Alice 和 Bob 之间的秘密信息速率为

$$\Delta I = I(\alpha,\beta)-I(\alpha,\varepsilon). \tag{17}$$

当采用反向协商过程时，即以 Bob 的信息为密钥源，Alice 根据协商信息纠正自己的信息使其与 Bob 的信息一致，Alice 和 Bob 之间的秘密信息速率为 $\Delta I = I(\beta,\alpha)-I(\beta,\varepsilon)$.

本文采用正向协商过程，把(12) 和(15) 式代入(17) 式，则可得到合法通信双方之间的秘密信息速率.由于秘密信息速率的解析表达式太繁琐，本文采用数值解研究秘密信息速率与各个物理参数之间的关系，分别讨论 r,Σ,η_1,η_2 对秘密信息速率的影响.

1)首先讨论两种特殊情况.第一种特殊情况：当 $\eta_1=\eta_2=1$ 时，即不存在窃听者时，秘密信息速率为 Alice 和 Bob 之间的信道容量，

$$\Delta I = I(\alpha,\beta)=\log_2\left(1+\frac{2\Sigma^2}{e^{-2r}}\right). \tag{18}$$

显然，秘密信息速率随着信号方差 Σ^2 和双模压缩因子 r 的增大而增大.

2)第二种特殊情况.当 $r=0$ 时，基于双模压缩态的量子密钥分发方案就简化为 No-switching 量子密钥分发方案[17—19]，若采用正向协商过程，则秘密信息速率变为

$$\Delta I=\log_2\frac{1+2\eta_1\Sigma^2}{1+2(1-\eta_1)\Sigma^2}. \tag{19}$$

如图 3 所示，秘密信息速率与 η_2 无关，并且当 $\eta_1>0.5$ 时，$\Delta I>0$，即 Alice 和 Bob 可以通过纠错和保密增强获得安全的秘密密钥.

3) 对于一般的情况，为便于讨论，设 $\Sigma=0.5$，$r=1$.如图4所示，对于某一固定的 η_2，秘密信息速率

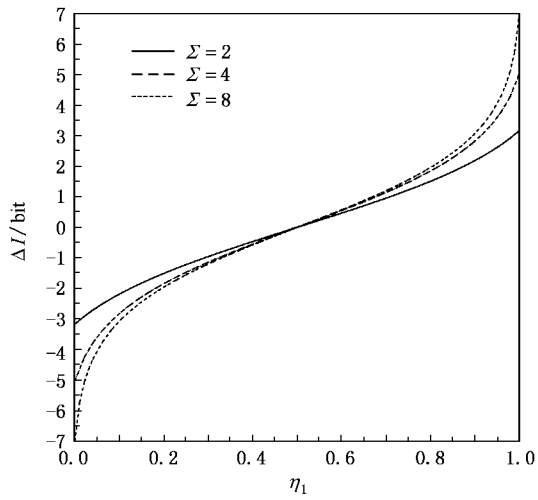

图 3　秘密信息速率 ΔI 与 η_1,Σ 之间的关系($r=0,\Sigma=2,4,6,8$)

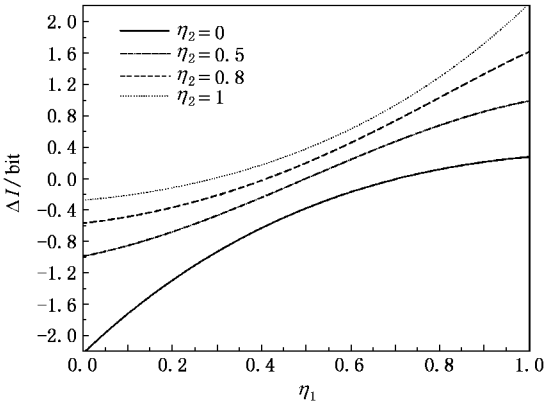

图 4　秘密信息速率 ΔI 与 η_1 之间的关系($r=1,\Sigma=0.5,\eta_2=0,0.5,0.8,1$)

ΔI 随着 η_1 的增大而增大.对某一固定的 η_1，ΔI 随着 η_2 的增大而增大.对于不同的 η_2 值，对应于 $\Delta I=0$ 的 η_1 值 $\eta_1|_{\Delta I=0}$ 不同.η_2 越大，$\eta_1|_{\Delta I=0}$ 越小.这种情况表明在窃听者 Eve 窃听到的信息量一定的情况下，Eve 窃取的参考光越多，他所需要窃取的信号光越少.

4. 结　　论

本文提出了一种基于双模压缩态的量子密钥分发方案，双模压缩态的模间关联性保证了方案的安全性.安全性分析表明，该方案能有效抵抗光束分离攻击策略.合法通信双方之间的秘密信息速率 ΔI 随着双模压缩因子 r(纠缠对的完善程度)的增大而增大，随着信号调制方差的增大而增大.对于特定的

纠缠系统(即双模压缩态的压缩因子一定的情况下),当量子信道的透过率满足一定的条件时,合法通信双方通过纠错和保密增强可以得到安全的秘密密钥.

[1] Zeng G H 2006 *Quantum Cryptography* (Science Press) (in Chinese) [曾贵华 2006 量子密码学(科学出版社)]

[2] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[3] Song J, Zhang S, Zhu A D 2007 *Chinese Physics* **16** 621

[4] He G Q, Zeng G H 2005 *Chinese Physics* **14** 541

[5] Chen J J, Han Zh F, Zhao Y B, Gui Y Zh, Guo G C 2007 *Acta Phys. Sin.* **56** 5 (in Chinese) [陈进建、韩正甫、赵义博、桂有珍、郭光灿 2007 物理学报 **56** 5]

[6] Lo H K, Chau H F 1999 *Science* **283** 2050

[7] Shor P W, Preskill J 2000 *Phys. Rew. Lett.* **85** 441

[8] Mayers D 2001 *J. ACM* **48** 351

[9] Braunstein S L, Loock P van 2005 *Rev. Mod. Phys.* **77** 513

[10] Ralph T C 1999 *Phys. Rev.* A **61** 010303 (R)

[11] Ralph T C 2000 *Phys. Rev.* A **62** 062306

[12] Hillery M 2000 *Phys. Rev.* A **61** 022309

[13] Reid M D 2000 *Phys. Rev.* A **62** 062308

[14] Gottesman D, Preskill J 2001 *Phys. Rev.* A **63** 022309

[15] Cerf N J, Lévy M, Assche G Van 2001 *Phys. Rev.* A **63** 052311

[16] Silberhorn Ch, Ralph T C, Lütkenhaus N, Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901

[17] Silberhorn Ch, Korolkova N, Leuchs G 2002 *Phys. Rev. Lett.* **88** 167902

[18] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[19] Grosshans F, Assche G Van, Wenger J, Brouri R, Cerf N J, Grangier P 2003 *Nature* (London) **421** 238

[20] Weedbrook Ch, Lance A M, Bowen W P, Symul T, Ralph T C, Lam P K 2004 *Phys. Rev. Lett.* **93** 170504

[21] Weedbrook Ch, Lance A M, Bowen W P, Symul T, Ralph T C, Lam P K 2003 *Phys. Rev.* A **73** 022316

[22] Lance A M, Symul T, Sharma V, Weedbrook Ch, Ralph T C, Lam P K 2005 *Phys. Rev. Lett.* **95** 180503

[23] He G Q, Zhu J, Zeng G H 2006 *Phys. Rev.* A **73** 012314

[24] Grosshans F, Cerf N J 2004 *Phys. Rev. Lett.* **92** 047905

[25] Iblisdir S, Assche G Van, Cerf N J 2004 *Phys. Rev. Lett.* **93** 170502

[26] Navascués M, Bae J, Cirac J I, Lewestein M, Sanpera A, Acín A 2005 *Phys. Rev. Lett.* **94** 010502

[27] Grosshans F 2005 *Phys. Rev. Lett.* **94** 020504

[28] Grosshans F, Cerf N J 2005 *Quantum information and communication* **3** 535

[29] Maurer U M 1993 *IEEE Trans. Inf. Theory* **39** 733

Quantum key distribution using two-mode squeezd states *

He Guang-Qiang† Yi Zhi Zhu Jun Zeng Gui-Hua

(*The State Key Laboratory on Fiber-Optic Local Area Networks and Advanced Optical Communication Systems*, *Electronic Engineering Department*, *Shanghai Jiaotong University*, *Shanghai* 200240, *China*)

(Received 20 December 2006; revised manuscript received 18 March 2007)

Abstract

A quantum key distribution scheme using two-mode squeezed states is proposed in this paper. The security of the proposed scheme against beam splitter attack is analyzed using Shannon information theory. The analytical expression of the secret information rate is given in terms of squeezed factor and channel parameters. The mode-mode correlation of two-mode squeezed states guarantees the security of the proposed scheme.

Keywords: quantum key distribution, two-mode squeezed state, beam splitter attack

PACC: 4250, 4230Q, 0365

* Project supported by SJTU Young Teacher Foundation (Grant No. A2831B) and SJTU PRP (Grant No. T03011030) and the National Natural Science Foundation of China (Grant No. 60472018).

† E-mail: gqhe@sjtu.edu.cn