第 57 卷 第 4 期 2008 年 4 月
1000-3290/2008/57(04)/2212-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.4,April,2008

基于二进制均匀调制相干态的量子密钥分发方案*

何广强† 郭红斌 李昱丹 朱思维 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)

(2007 年 5 月 23 日收到;2007 年 9 月 30 日收到修改稿)

提出了一种基于二进制均匀调制相干态的量子密钥分发方案. 相对于高斯调制相干态量子密钥分发方案中的高斯信源,二进制信源是最简单的信源,二进制调制是目前数字光纤通信中最普遍的调制方式,技术上容易实现. 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调制参数、解调参数以及信道参数之间的解析表达式.

关键词:量子密钥分发,二进制调制,光束分离攻击

PACC:4250,4230Q,0365

1. 引 言

信息安全在信息社会中发挥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研究取得的重大突破,依赖于数学难题的某些密码算法(如 RSA 等算法)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—7]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[8—10]和对窃听的可检测性,使量子密码具有良好的性能和前景.

连续变量量子密码[11—29]利用高斯态(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,通过振幅调制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. 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(QKD),连续变量 QKD 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引起了各国学者的极大关注.

相干态是最接近经典态的量子态,采用相干态作为量子信号载体的 QKD 方案并不需要光场的非经典性质(如压缩和纠缠等),实验上容易实现,因此相干态是连续变量 QKD 的最佳量子信号载体. 然而,目前所有相干态 QKD 方案中,传输的符号集均服从高斯分布,即采用高斯调制. 当信道是加性高斯白噪声信道,并且发送者采用高斯调制时,通信双方之间的互信息量就是通信双方的信道容量,所以研究高斯调制相干态 QKD 方案具有重要的理论意义,但是实际上合法通信双方之间所传递的互信息量根本无法达到信道容量. 另外,无法制备高速高斯信源成为制约高斯调制相干态 QKD 方案的关键因素. 然而,采用二进制均匀调制的光纤通信是一种高速的通信系统,二进制调制操作简单、传输速率高,所以二进制均匀调制是高速通信系统的首选调制格式.

本文设计了基于二进制均匀调制相干态的 QKD 方案,采用信息论分析了该方案在光束分离攻击情况下合法通信双方之间的秘密信息速率. 本文首先介绍了基于二进制均匀调制相干态的 QKD 协议的工作过程,然后针对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,分析了方案的安全性与调制参数、解调参数以及信道参数之间的关系.

* 上海交通大学青年教师科研启动基金(批准号:A2831B)、国家自然科学基金(批准号:60773085)和上海交通大学本科生研究计划(批准号:T03011030)资助的课题.

† E-mail:gqhe@sjtu.edu.cn

2. 基于二进制均匀调制相干态的 QKD 协议

基于二进制均匀调制相干态的 QKD 协议采用技术上更容易实现的二进制均匀调制格式，其安全性由相干态中固有的量子噪声保证，该协议工作过程分五步完成，如图 1 所示.

第一步：Alice 根据随机比特串 n_1，n_2 应用平移算符 $\hat{D}(\alpha)$于光学模式 $\hat{a}_2$ 上，产生模 $\hat{a}_3$，把服从二进制均匀概率分布的信息 X 或 P 加载到载波 $\hat{a}_2$ 上，其中 $P(X=a)=P(X=-a)=1/2$，$P(P=a)=P(P=-a)=1/2$. 为简化协议分析，本文假设随机变量 X，P 满足相同的二进制均匀概率分布. 随机比特串 n_2 为要传输的随机密钥，根据随机比特串 n_1 选择编码基，若比特串 n_1 的第 i 个比特 $n_1^i=0$，则

$$D(\alpha)=D(x).$$

当 $n_2^i=1$，$x=a$；当 $n_2^i=0$，$x=-a$；若比特串 n_1 的第 i 个比特 $n_1^i=1$，则

$$D(\alpha)=D(jp).$$

当 $n_2^i=1$，$p=a$；当 $n_2^i=0$，$p=-a$.

平移算符

$$\hat{D}(\alpha)=\exp(\alpha\hat{a}_2^{\dagger}-\alpha^{*}\hat{a}_2)$$

作用于模 $\hat{a}_2$，产生变换

$$\hat{a}_3=\hat{D}^{\dagger}(\alpha)\hat{a}_2\hat{D}(\alpha)=\hat{a}_2+\alpha,$$

则

$$\begin{aligned}X_3&=X_2+\mathrm{Re}(\alpha)=X_2+X,\\P_3&=P_2+\mathrm{Im}(\alpha)=P_2+P,\end{aligned}\tag{1}$$

式中正则振幅 X 和正则相位 P 分别定义为

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

$$P=\frac{1}{2j}(\hat{a}-\hat{a}^{\dagger}).$$

两者满足测不准关系，$\Delta X\Delta P\geqslant 1/4$.

第二步：Alice 通过量子信道把调制好的模 $\hat{a}_3$ 从 Alice 端传输到 Bob 端.

第三步：Bob 根据随机比特串 n_3 选择测量基，若比特串 n_3 的第 i 个比特 $n_3^i=0$，Bob 测量模 $\hat{a}_5$（Eve 不存在时，$\hat{a}_5$ 为 $\hat{a}_3$）的 X_5，若比特串 n_3 的第 i 个比特 $n_3^i=1$，Bob 测量模 $\hat{a}_5$ 的 P_5，得到比特 n_4^i.

第四步：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；若 $n_1^i\neq n_2^i$，则丢弃 n_2^i，n_4^i.

第五步：重复上述过程，可得到两个高度相关的信息序列，然后通过密钥协商和保密增强过程可得到安全的秘密密钥.

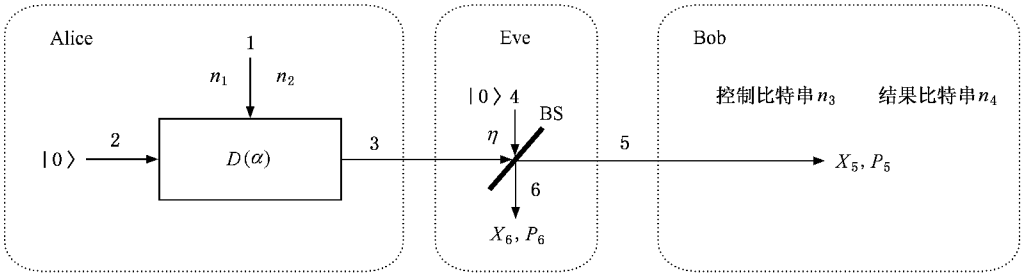

图 1　基于二进制均匀调制相干态的量子密钥分发方案

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. 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. 光束分离攻击策略的物理模型

显然，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 分离信号模 $\hat{a}_3$，本文假设 Eve 具有量子内存技术，她首先利用量子内存存储窃听到的量子信号，等

Alice 和 Bob 之间的经典通信完成后,再采用与 Alice 编码基对应的测量基测量窃取的量子信号. 本文分析最直观也最简单的光束分离攻击策略,Eve 采用光束分离器窃听,窃听装置如图 2 所示.

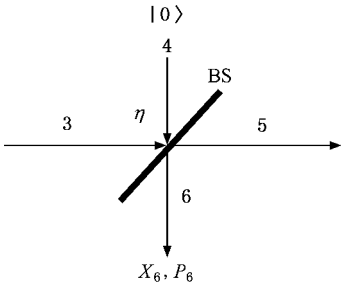

图 2 Eve 的窃听装置示意图

光束分离器对各个光学模式之间的变换关系为

$$\begin{aligned} X_5 &= \sqrt{\eta}X_3 + \sqrt{1-\eta}X_4, \\ P_5 &= \sqrt{\eta}P_3 + \sqrt{1-\eta}P_4, \\ X_6 &= \sqrt{\eta}X_4 - \sqrt{1-\eta}X_3, \\ P_6 &= \sqrt{\eta}P_4 - \sqrt{1-\eta}P_3, \end{aligned} \tag{2}$$

式中 η 为光束分离器的透过率.

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. 若信源 X 为服从二进制均匀概率分布的信源,即 $P(X=a)=P(X=-a)=1/2$,并且连接通信双方的信道为二进制对称信道,则通信双方之间的互信息量为

$$\begin{aligned} I(X,Y) &= 1 + p_e\log_2 p_e \\ &\quad + (1-p_e)\log_2(1-p_e), \end{aligned} \tag{3}$$

式中 p_e 为二进制对称信道所对应的误码率.

从(3)式可知,为计算各方之间的互信息量,先要计算各方之间的误码率. 首先推导各个光学模式所对应的正则算符之间的关系. 根据(1),(2)式,可得模 $\hat{a}_5$ 的正则分量

$$\begin{aligned} X_5 &= \sqrt{\eta}X + \left(\sqrt{\eta}X_2 + \sqrt{1-\eta}X_4\right), \\ P_5 &= \sqrt{\eta}P + \left(\sqrt{\eta}P_2 + \sqrt{1-\eta}P_4\right), \end{aligned} \tag{4}$$

式中 $X_i, P_i \sim N(0,1/4)$, $i=2,4$. 这里 $\Gamma \sim N(\mu, \alpha^2)$ 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. 随机变量 X_5 服从的概率密度函数为

$$\begin{aligned} p(x_5) &= p(x_5 \mid X=a)P(X=a) \\ &\quad + p(x_5 \mid X=-a)P(X=-a) \\ &= \frac{1}{2}\frac{2}{\sqrt{2\pi}}\exp[-2(x_5-\sqrt{\eta}a)^2] \\ &\quad + \frac{1}{2}\frac{2}{\sqrt{2\pi}}\exp[-2(x_5+\sqrt{\eta}a)^2]. \end{aligned} \tag{5}$$

随机变量 P_5 服从相同的概率密度函数,由于 X 和 P 的对称性,本文只讨论 X,即假设 Alice 的编码基和 Bob 的测量基相同. 由于 Eve 拥有量子内存技术,她的测量基总是与 Alice 的编码基相同.

如图 3 所示,本文设 Bob 的判决门限为 m(m 为正数). 这意味着,若 $x_5 > m$,则 $n_4^i = 1$;若 $x_5 < -m$,则 $n_4^i = 0$;若 $-m < x_5 < m$,则 Bob 放弃. Alice 与 Bob 之间的误码率 $p_e(A,B)$ 为

$$\begin{aligned} P_e(A,B) &= P(X=a, X_5 < -m \mid X_5 > m \\ &\quad \cup X_5 < -m) \\ &\quad + P(X=-a, X_5 > m \mid X_5 > m \\ &\quad \cup X_5 < -m) \\ &= 2\frac{P(X=a, X_5 < -m)}{P(X_5 > m) + P(X_5 < -m)} \\ &= 2\frac{P(X_5 < -m \mid X=a)P(X=a)}{P(X_5 > m) + P(X_5 < -m)} \\ &= \left[\frac{1}{2} - \frac{1}{2}\mathrm{erf}(\sqrt{2}(m+\sqrt{\eta}a)\right] \\ &\quad \times \left(1 - \frac{1}{2}\mathrm{erf}[\sqrt{2}(m+\sqrt{\eta}a)] \right. \\ &\quad \left. - \frac{1}{2}\mathrm{erf}[\sqrt{2}(m-\sqrt{\eta}a)]\right)^{-1}, \end{aligned} \tag{6}$$

式中 $\mathrm{erf}(x)$ 为误差函数,

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x \exp(-z^2)\,\mathrm{d}z.$$

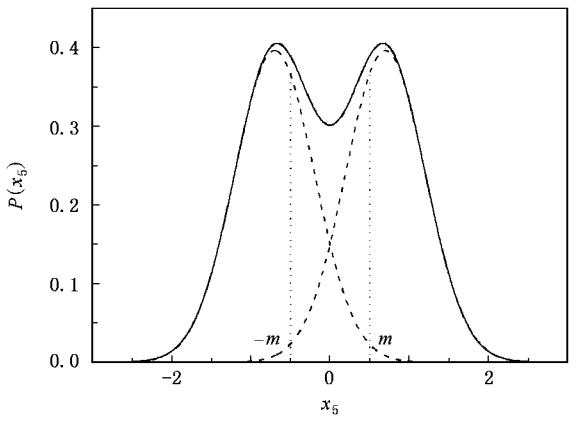

图 3 基于二进制均匀调制相干态的 QKD 解调原理

将(6)式代入(3)式,可以得到合法通信双方

Alice 和 Bob 之间的互信息量

$$I(\alpha,\beta) = 1 + p_e(A,B)\log_2 p_e(A,B) + (1 - p_e(A,B))\log_2(1 - p_e(A,B)). \quad (7)$$

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，在这种情况下窃听者所窃取的信息量为 Eve 与 Alice 之间的互信息量. 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的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. 根据光束分离攻击策略原理(图 2)，由(1)和(2)式可得模 $\hat{a}_6$ 的正则分量 X_6，即

$$X_6 = -\sqrt{1-\eta}X + (-\sqrt{1-\eta}X_2 + \sqrt{\eta}X_4). \quad (8)$$

随机变量 X_6 的概率密度函数为

$$p(x_6) = \frac{1}{2}\frac{2}{\sqrt{2\pi}}\exp[-2(x_6 - \sqrt{1-\eta}a)^2] + \frac{1}{2}\frac{2}{\sqrt{2\pi}}\exp[-2(x_6 + \sqrt{1-\eta}a)^2]. \quad (9)$$

由于窃听者 Eve 无法猜测 Bob 所采用的判决门限，她最好的办法是把判决门限设为 0. 因此，如果 Eve 收到的 $X_6 > 0$，她认为 Alice 发送的为 1 若 $X_6 < 0$，她认为 Alice 发送的为 0. 在这种情况下，Alice 和 Eve 之间的误码率为

$$P_e(A,E) = P(X = a, X_6 < 0) + P(X = -a, X_6 > 0) = \frac{1}{2} - \frac{1}{2}\mathrm{erf}(\sqrt{2(1-\eta)}\,a). \quad (10)$$

将(10)式代入(3)式，可得 Alice 与 Eve 之间的互信息量

$$I(\alpha,\varepsilon) = 1 + p_e(A,E)\log_2 p_e(A,E) + (1 - p_e(A,E))\log_2(1 - p_e(A,E)). \quad (11)$$

3.4. 秘密信息速率

Maurer[30] 的研究结果表明，Alice 和 Bob 得到安全密钥的充分条件为

$$\max\{I(\alpha,\beta) - I(\alpha,\varepsilon), I(\beta,\alpha) - I(\beta,\varepsilon)\} > 0. \quad (12)$$

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 与 Bob 之间的秘密信息速率为

$$\Delta I = I(\alpha,\beta) - I(\alpha,\varepsilon). \quad (13)$$

本文采用正向协商过程，把(7)和(11)式代入(13)式，则可得到合法通信双方之间的秘密信息速率. 当 $\Delta I > 0$ 时，Alice 和 Bob 可以通过密钥协商和保密增强提取出秘密密钥，因此 $\Delta I > 0$ 为 QKD 安全性判据. 从(3)式可知，互信息量 $I(X,Y)$ 是误码率 p_e 的减函数. 因此安全判据可重写为 $p_e(A,B) < p_e(A,E)$，即要求合法通信双方 Alice 与 Bob 之间的误码率小于 Alice 与窃听者 Eve 之间的误码率.

图 4 为基于二进制均匀调制相干态的 QKD 的安全边界，当 $b = \frac{m}{a} = 0$ 时，即 $m = 0$ 时，安全判据要求 $\eta > 0.5$，与基于高斯调制相干态的 QKD 在正向协商下的安全性条件相同[20].

Bob 设置的判决门限 m 与方案的通信效率以及安全性密切相关，m 越大，方案越安全，但是其通信效率越低. 这里，设通信效率为

$$r = P(X_5 > m) + P(X_5 < -m) = 1 - \frac{1}{2}\mathrm{erf}\left(\frac{ab + \sqrt{\eta}a}{\sqrt{2}\sigma}\right) - \frac{1}{2}\mathrm{ref}\left(\frac{ab - \sqrt{\eta}a}{\sqrt{2}\sigma}\right). \quad (14)$$

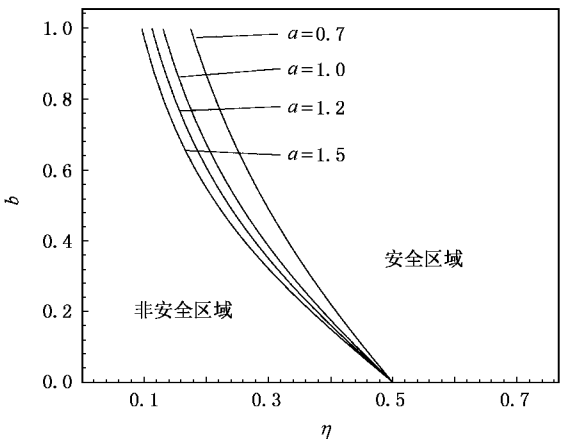

图 4　基于二进制均匀调制相干态的 QKD 安全边界

图 5 上方的曲面为通信效率 r 与 a，b 的关系，下方的曲面为秘密信息速率 ΔI 与 a，b 的关系. 由图 5 可见，r 越大，则 ΔI 越小，η 为其他值时情况一样. 因此，r 越高，秘密信息速率 ΔI 越小，即通信效率越高，方案越不安全. 可以通过调节 Bob 端的判决门限 m 值，来平衡方案的安全性与通信效率之间的关系. 因此，需要根据实际情况选择合适的 a 和

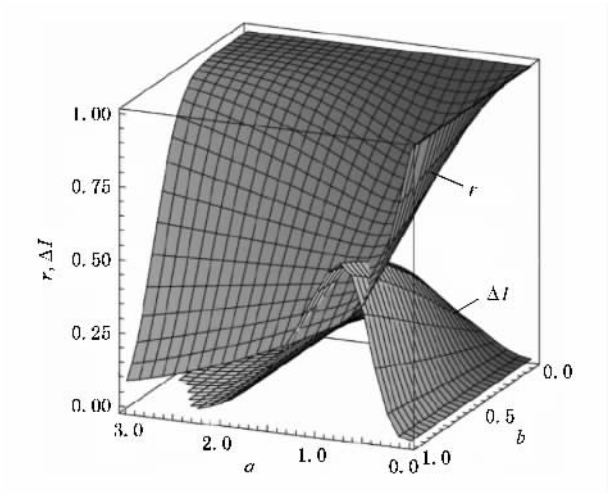

图 5 $\Delta I, r$ 与 a, b 的关系 $\eta = 0.6$

b 的值,即根据需要的安全等级选择合适的调制参数和解调参数,来保证方案的安全.

4. 结 论

本文提出了一种基于二进制均匀调制相干态的 QKD 方案,相干态的量子噪声保证了方案安全性.采用信息论计算了该方案在光束分离攻击策略下的秘密信息速率,得到了安全边界,并给出了安全判据与调制参数、解调参数以及窃听策略之间的关系.只要方案所采用的调制参数和解调参数在安全区域内,方案可以抵抗光束分离攻击. Bob 的判决门限值越大,则方案越安全,但是方案的通信效率就越低.

[1] Zeng G H 2006 *Quantum Cryptography* (Beijing: Science Press) (in Chinese) [曾贵华 2006 量子密码学 (北京 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 *Chin. Phys.* **16** 621

[4] He G Q, Zeng G H 2005 *Chin. Phys.* **14** 541

[5] He G Q, Yi Z, Zhu J, Zeng G H 2007 *Acta Phys. Sin.* **56** 6427 (in Chinese) [何广强、易 智、朱 俊、曾贵华 2007 物理学报 **56** 6427]

[6] Feng F Y, Zhang Q 2007 *Acta Phys. Sin.* **56** 1924 (in Chinese) [冯发勇、张 强 2007 物理学报 **56** 1924]

[7] Liu S H, Wang F Q, Zheng L M 2007 *Acta Phys. Sin.* **56** 2180 (in Chinese) [刘颂豪、王发强、郑力明 2007 物理学报 **56** 2180]

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

[9] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441

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

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

[12] Ralph T C 1999 *Phys. Rev.* A **61** R010303

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

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

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

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

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

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

[19] Silberhorn C, Korolkova N, Leuchs G 2002 *Phys. Rev. Lett.* **88** 0167902

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

[21] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J, Grangier P 2003 *Nature* **421** 238

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

[23] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C, Lam P K 2006 *Phys. Rev.* A **73** 022316

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

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

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

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

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

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

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

Quantum key distribution using binary-modulated coherent states *

He Guang-Qiang†　Guo Hong-Bin　Li Yu-Dan　Zhu Si-Wei　Zeng Gui-Hua
(*State Key Laboratory on Fiber-optic Local Area Networks and Advanced Optical Communication Systems*, *Department of Electronic Engineering*, *Shanghai Jiaotong University*, *Shanghai* 200240, *China*)
(Received 23 May 2007; revised manuscript received 30 September 2007)

Abstract

A quantum key distribution (QKD) scheme using binary-modulated coherent states is proposed in this paper. Compared with Gaussian sources of QKD using Gaussian-modulated coherent states, the binary sources of the proposed scheme are the simplest sources, and the binary modulation is the most usual modulation format in the digital optical-fiber communication. 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 modulation-demodulation parameters and channel parameters. The quantum noise of coherent states guarantees the security of the proposed scheme.

Keywords: quantum key distribution, binary modulation, beam splitter attack
PACC: 4250, 4230Q, 0365

* Project supported by the Young Teacher Scientific Research Foundation of Shanghai Jiaotong University, China (Grant No. A2831B), the National Natural Science Foundation of China (Grant No. 60773085) and the Participation in Research Program of Shanghai Jiaotong University, China (Grant No. T03011030).

† E-mail: gqhe@sjtu.edu.cn