第 51 卷 第 8 期 2002 年 8 月
1000-3290/2002/51(08)/1684-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.51,No.8,August,2002

非对称二状态量子密钥分配协议最优参量研究

张 权 张尔扬

(国防科技大学电子科学与工程学院,长沙 410073)

(2001 年 10 月 21 日收到;2001 年 12 月 13 日收到修改稿)

通过分析各种情况下 B92 量子密钥分配协议的密钥分配和安全性指标,得出采用非对称信源实现 B92 协议可以在不损失安全性能的前提下极大提高密钥分配的效率.系统分析了非对称 B92 协议参量选择与性能之间的约束关系,给出了各种情况下的最优参量,同时比较了不同情况相应的密钥分配效率和安全性指标,获得了一种实现全局最优的非对称 B92 密钥分配协议.

关键词:非对称二状态量子密钥分配协议,最优参量,量子密码术,量子信息

PACC:0365,0220,0250,4230

1. 引 言

以量子密钥分配[1—3](QKD)为代表的量子密码术是量子信息科学应用于经典通信的成功典范.由于量子密码特别适合光通信环境,同时可以实现经典密码学所追求无条件安全性,量子密钥分配技术日益受到广泛关注.由于量子密码术所具有的重要战略意义,对于 QKD 的研究进展非常迅速.在理论研究方面,BB84 协议的无条件安全性已经被证明[4—6],B92 协议无条件安全性的证明也已经由我们完成,相关论文已投物理学报.在实验方面,IBM 已经在商用光纤上实现了 50km[7] 的 BB84 量子密钥分配实验,我国在量子密钥分配方面的实验研究也已经展开[8].

以 B92 协议为代表的二状态量子密钥分配协议由于所需实验设备较少,操作过程相对简单,因此被认为具有较好的应用前景.另一方面,B92 协议存在的一个突出问题就是密钥分配效率较低.不考虑噪声及窃听干扰时,每发送 4 个物理量子位只能传送 1 比特密钥信息,而 BB84 传送 1 个比特只需 2 个量子位.为了提高 B92 协议的密钥分配效率,可以采用非对称信源实现 B92 协议,即非对称 B92 协议.影响非对称 B92 协议安全性和密钥分配效率的关键参量包括信源参量 p 和量子态相关度 q.本文系统分析了非对称 B92 协议参量选择与性能之间的约束关系,给出了各种情况下的最优参量,同时比较了不同情况相应的密钥分配效率和安全性指标,对于设计实现 B92 量子密钥分配协议具有较强的指导意义.

2. B92 协议分析

在分析 BB84 协议的安全性时 Bennett 等[9] 发现,由于量子不可克隆定理的限制,如果一种测量不会破坏两个非正交状态中的任意一个,那么通过该测量也不可能获得任何能够区分这两个状态的信息.因此,Bennett[2] 指出,任意两个非正交的状态都可以用来实现密钥分配.

设$|u_0\rangle$和$|u_1\rangle$是两个非正交的量子状态,满足

$$0 < |\langle u_0 | u_1\rangle| < 1, \tag{1}$$

式中$|u_0\rangle$和$|u_1\rangle$都是归一化的,即

$$\langle u_0 | u_0\rangle = \langle u_1 | u_1\rangle = 1.$$

算子 $P_0 = 1 - |u_1\rangle\langle u_1|$和 $P_1 = 1 - |u_0\rangle\langle u_0|$分别将量子态投影到与$|u_1\rangle$和$|u_0\rangle$正交的态空间上,即

$$P_0 |u_1\rangle = 0, P_0 |u_0\rangle = |u_0\rangle - |u_1\rangle\langle u_1 | u_0\rangle, \tag{2}$$

$$P_1 |u_0\rangle = 0, P_1 |u_1\rangle = |u_1\rangle - |u_0\rangle\langle u_0 | u_1\rangle. \tag{3}$$

因为$\langle u_i | P_i | u_j\rangle = \left(1 - |\langle u_i | u_{1\oplus i}\rangle|^2\right)\delta_{ij}$,其中 $i,j = 0,1$;"$\oplus$"表示异或,所以根据非 0 的测量结果可以确定量子的初始状态.

利用上述特性，Alice 和 Bob 可以按照以下步骤实现 B92 量子密钥分配.

1. Alice 选定一个 n 位的随机二进制串 a，当 $a_i = 0$ 时，取 $|\phi\rangle_i = |u_0\rangle$，$a_i = 1$ 时，取 $|\phi\rangle_i = |u_1\rangle$，并按固定的时间间隔将 $|\phi\rangle$ 发送给 Bob.

2. Bob 也选定一个 n 位的随机二进制串 b，当 $b_i = 0$ 时，测量 P_0，当 $b_i = 1$ 时，测量 P_1.

3. Bob 通过公开的经典信道通知 Alice 他在哪些时间片检测到量子态. 当然，Bob 并不透露他测量的究竟是 P_0 还是 P_1.

4. Alice 保留 Bob 检测到量子态的那些时间片所对应的信息比特，从而获得 a 的一个子串 a'.

5. Bob 对于检测到量子态的时间片，根据(4)式译码获得信息串 b'，显然 b' 是 b 的一个子串，在没有误差的前提下，$b' = a'$.

$$\begin{cases} P_0 \mapsto 0, \\ P_1 \mapsto 1, \end{cases} \tag{4}$$

6. Alice 随机公布一些信息比特让 Bob 验证错误概率是否大于特定的门限.

7. 若错误概率大于门限，则表明信道不安全，Alice 和 Bob 可以另选时间进行密钥协商；若错误概率小于门限，则可以确定没有人窃听，Alice 和 Bob 可以将剩余的未公开的信息比特用作密钥.

8. Alice 和 Bob 利用经典纠错码对密钥进行纠错，最后施行保密放大[9]生成最终密钥.

在表 1 中列出了一次完整的 B92 密钥分配过程，最后一行的比特序列就是 Alice 和 Bob 协商得到的密钥.

表 1　B92 量子密钥分配过程

	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}	t_{11}	t_{12}	t_{13}
1	$\|u_0\rangle$	$\|u_1\rangle$	$\|u_1\rangle$	$\|u_0\rangle$	$\|u_1\rangle$	$\|u_1\rangle$	$\|u_1\rangle$	$\|u_0\rangle$	$\|u_1\rangle$	$\|u_0\rangle$	$\|u_1\rangle$	$\|u_0\rangle$	$\|u_0\rangle$
2	P_0	P_1	P_0	P_0	P_1	P_0	P_1	P_0	P_0	P_1	P_1	P_1	P_0
3		√		√				√			√		√
4/5		1		0				0			1		0
6				0							1		
7		1						0					0

由于量子态非正交，即

$$|\langle u_i \mid u_{1\oplus i}\rangle| > 0,$$

Bob 能检测到量子态的概率 $(1 - |\langle u_i | u_{1\oplus i}\rangle|^2) < 1$. 所以在 t_1，t_5，t_7 时间片，虽然测量是正确的，但是 Bob 仍然没有检测到量子态.

如果取 $|u_0\rangle = |\rightarrow\rangle$ 和 $|u_1\rangle = |\nearrow\rangle$ 则

$$1 - |\langle u_0 \mid u_1\rangle|^2 = 1 - \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2},$$

即有 50% 的正确测量将检测不到量子态，考虑到 Bob 选取的二进制串 b 与 a 对应位相同的概率为 50%，所以 B92 的效率是 BB84 的二分之一，为 25%. B92 的校验过程与 BB84 几乎完全相同，区别仅在于存在窃听时的错误概率.

假设 Eve 截获每一个量子位，实施测量后，再根据测量结果制备相应的量子位转发给 Bob. 设 Eve 的随机测量序列为 e，当 $e_i = 0$ 时，测量 P_0，当 $e_i = 1$ 时，测量 P_1. 如果 Eve 在 i 时间片检测到量子态，她可以确定 Alice 在该时间片发送给 Bob 的量子位 $|\phi\rangle_i$，因此 Eve 自己制备一个 $|\phi\rangle_i$ 并发送给 Bob，此时 Eve 的测量没有引入错误，其概率为

$$\frac{1}{2}(1 - |\langle u_i \mid u_{1\oplus i}\rangle|^2).$$

若 Eve 在第 j 时间片未检测到量子态，则无法确定 $|\phi\rangle_j$ 为哪个量子态，此时她只能猜测. 如果测量方法错误，那么她检测不到量子态的概率为 100%，相反测量方法正确的话，检测不到量子态的概率为 $|\langle u_0 | u_1\rangle|^2$，考虑到 Eve 的目的是使自己的窃听行为最大程度地隐蔽，Eve 会选择制备一个与自己所用的测量相反的量子位发送给 Bob. 也就是说，如果 Eve 测量 P_0 而没有检测到量子态，她就制备一个 $|u_1\rangle$ 发送给 Bob. 此时，Eve 的测量引入错误概率为 $(|\langle u_0 | u_1\rangle|^2)/2$，当取 $|u_0\rangle = |\rightarrow\rangle$ 和 $|u_1\rangle = |\nearrow\rangle$ 时，Eve 改变了 25% 的量子位. 因此，最后 Alice 和 Bob 进行校验时，错误概率为 8.5% 左右，这也已经远远大于正常的信道错误的概率.

为了提高测量效率，Ekert 等基于广义量子测量(POVM)[10]，改进了 B92 协议的测量方法[11]. Bob 对

他收到的量子位分别实施操作

$$A_0 = \frac{P_0}{1+|\langle u_0 | u_1\rangle|}, A_1 = \frac{P_1}{1+|\langle u_0 | u_1\rangle|}. \tag{5}$$

这样，Bob 检测不到量子态的概率为 $|\langle u_0 | u_1\rangle|$，而在标准 B92 协议中，此概率为 $(1+|\langle u_0 | u_1\rangle|^2)/2$，显然采用上述测量法可以提高 B92 协议的效率.

3. 非对称 B92 协议及最优参量

在上一节我们已经看到，影响 B92 协议效率和可靠性的参量约束是互相关联的，提高有效性的改变可能降低可靠性，反之亦然.通过分析关键约束参量之间的关系，可以得到最优参量选择的约束条件.

设 Alice 选择的信息串是非对称的，即信源模型为

$$\begin{cases} |u_0\rangle : p, \\ |u_1\rangle : 1-p. \end{cases} \tag{6}$$

因此，Bob 在接收测量量子位时，测量方法的选择也应该是非对称，即

$$\begin{cases} A_0 : p, \\ A_1 : 1-p, \end{cases} \tag{7}$$

另外设 $|\langle u_0 | u_1\rangle| = q$.

在没有窃听者的情况下，Bob 获得确定测量结果的概率 $\mathrm{Prob_{cd}}$ 为

$$\begin{aligned} \mathrm{Prob_{cd}} &= p^2(1-q) + (1-p)^2(1-q) \\ &= (1-2p+2p^2)(1-q). \end{aligned} \tag{8}$$

同时，Bob 检测不到量子态的概率 $\mathrm{Prob_u}$ 为

$$\begin{aligned} \mathrm{Prob_u} &= 1 - \mathrm{Prob_{cd}} \\ &= (2p-2p^2) + (1-2p+2p^2)q \\ &= \mathrm{Prob_e} + \mathrm{Prob_{cu}}, \end{aligned} \tag{9}$$

式中 $\mathrm{Prob_e}$ 表示测量方法错误的概率，$\mathrm{Prob_{cu}}$ 表示测量法正确但未检测到量子态的概率.提高 B92 效率的主要办法是增大 $\mathrm{Prob_{cd}}$.

假设存在窃听者 Eve，Eve 当然也知道信源是非对称的，所以她采取的测量策略与 Bob 相同.当 Eve 检测不到量子态时，如上一节所述，她会选择引入错误概率最小的伪造方案，即若 $\mathrm{Prob_e}$ 大于 $\mathrm{Prob_{cu}}$，则 Eve 断定检测不到量子态的原因是测量方法不正确；反之若 $\mathrm{Prob_e}$ 小于 $\mathrm{Prob_{cu}}$，则 Eve 认为检测不到的原因是测量失败；使 Eve 陷入两难抉择的情况发生在 $\mathrm{Prob_e} = \mathrm{Prob_{cu}}$ 时，此时她只能随机地伪造量子位并发送给 Bob，这将引入的量子位错误概率约为 $(1-\mathrm{Prob_{cd}})/2$.同时由于 Eve 不可能事先知道自己在哪些时间片检测不到量子态，所以她没办法控制伪造量子位的概率特性，只能使两种量子态呈随机分布，即在 Eve 伪造错误的量子态中，$|u_0\rangle$ 和 $|u_1\rangle$ 各占二分之一.

从协议安全性的角度考虑，对 Eve 最不利的情况，对于协议的安全性最有利.此时考虑 Bob 的测量过程，在 Eve 错误伪造的那部分量子位中，Bob 测量“正确”并获得确定测量结果的概率为 $(1-q)/2$，这部分测量结果对于 Alice 和 Bob 的校验过程而言，就是由 Eve 的窃听造成的错误.比特错误概率

$$P_{\mathrm{be}} = \frac{1-\mathrm{Prob_{cd}}}{2} \cdot \frac{1-q}{2} = \frac{(1-\mathrm{Prob_{cd}})(1-q)}{4}$$

越大，Eve 越容易被发现，协议的可靠性也越高，在不引起混淆的情况下，本文将混合使用比特错误概率和可靠性两个概念.又由 $\mathrm{Prob_e} = \mathrm{Prob_{cu}}$，可以推出

$$q = \frac{1}{1-2p+2p^2} - 1. \tag{10}$$

综上所述，得到 B92 密钥分配协议的最优约束条件为

$$\begin{cases} \max_{0<p<1}((2p-1)^2), \\ \max_{0<p<1}\left(p(1-p)\dfrac{1-4p+4p^2}{1-2p+2p^2}\right). \end{cases} \tag{11}$$

由图 1 可见，当 $p = \frac{1}{2}\left(\sqrt{\sqrt{2}-1}+1\right) \approx 0.82$ 时，正确测量的概率（即密钥分配效率）大于 41%，而 Eve 造成的比特错误概率仍然达到 8.2%.可见在非对称 B92 密钥分配协议中，采用上述最优策略，可以在不损失安全性要求的情况，密钥传输效率提高 65% 以上.

如果不满足 $\mathrm{Prob_e} = \mathrm{Prob_{cu}}$，则 Eve 可以采取非对称的伪造策略，即 $\mathrm{Prob_e}/\mathrm{Prob_u}$ 的量子位按照测量方法错误来对待，而 $\mathrm{Prob_{cu}}/\mathrm{Prob_u}$ 的量子位按照测量方法正确但测量失败来对待，由此引入的量子位错误概率为

$$\frac{2\mathrm{Prob_e}\mathrm{Prob_{cu}}}{\mathrm{Prob_u}} = \frac{2(2p-2p^2)(1-2p+2p^2)q}{1-(1-2p+2p^2)(1-q)}. \tag{12}$$

相应地 Bob 和 Alice 在校验过程中发现比特错误概率为

$$P_{\mathrm{be}} = \frac{2(2p-2p^2)(1-2p+2p^2)q}{1-(1-2p+2p^2)(1-q)} \cdot \frac{1-q}{2} = \frac{(2p-2p^2)(1-2p+2p^2)q(1-q)}{1-(1-2p+2p^2)(1-q)}. \tag{13}$$

此时(13)式的极值点包括

$$\begin{cases} p = \dfrac{1}{2}, \\ P = \dfrac{1}{2} \pm \dfrac{\sqrt{1-q^2-2\sqrt{q}+2q^{3/2}}}{2(1-q)}. \end{cases} \tag{14}$$

当 $p = 1/2$ 时,(13)式简化为

$$P_{\mathrm{be}} = \frac{(1-q)q}{2(1+q)}. \tag{15}$$

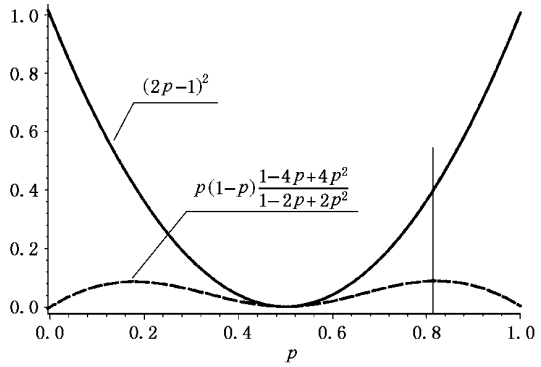

图 1　非对称 B92 协议最优约束

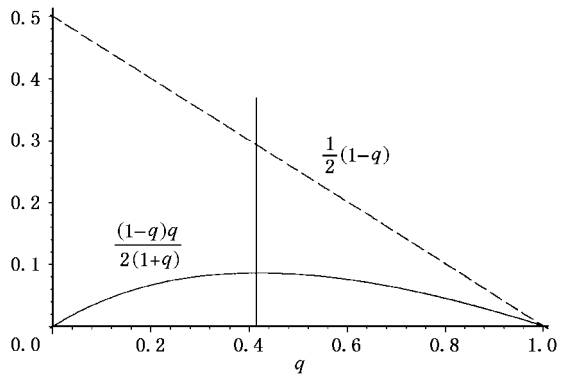

图 2　$p = \frac{1}{2}$ 时比特错误概率和密钥分配效率曲线

(15)式在 $q = 0.41$ 时达到极大值 0.086,即 Eve 的测量造成比特错误概率为 8.6%,此时密钥分配效率 $\mathrm{Prob}_{\mathrm{cd}} = (1-q)/2$ 约为 29.5%. 图 2 中显示了当 $p = 1/2$ 时比特错误概率与密钥分配效率和 q 之间的关系,可见随着 $q \to 0$,密钥分配效率逐步提高,但是最高不可能超过 50%.

当 $p = \frac{1}{2} + \frac{\sqrt{1-q^2-2\sqrt{q}+2q^{3/2}}}{2(1-q)}$ 时,在 $q = 0.39$ 处 P_{be} 取极大值为 0.09,即 Eve 引入的比特错误概率约为 9%,此时 $p = 0.74$,故密钥分配效率

$$\mathrm{Prob}_{\mathrm{cd}} = 1 - \sqrt{q} \approx 38\%.$$

当 $p = \frac{1}{2} - \frac{\sqrt{1-q^2-2\sqrt{q}+2q^{3/2}}}{2(1-q)}$ 时,q 的极值点仍为 0.39,因此错误概率与 $p = \frac{1}{2} + \frac{\sqrt{1-q^2-2\sqrt{q}+2q^{3/2}}}{2(1-q)}$ 时相同,此时 $p = 0.26$,密钥分配效率同样为 38%. 图 3 中显示了当 $p = \frac{1}{2} + \frac{\sqrt{1-q^2-2\sqrt{q}+2q^{3/2}}}{2(1-q)}$ 时比特错误概率和密钥分配效率与 q 之间的关系. 随着 $q \to 0$,密钥分配效率逐步提高,当密钥分配效率达到 70%,比特错误概率仍有 5%.

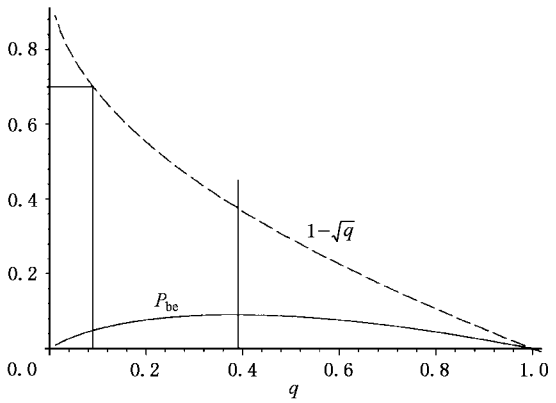

图 3　$p = \frac{1}{2} + \frac{\sqrt{1-q^2-2\sqrt{q}+2q^{3/2}}}{2(1-q)}$ 时比特错误概率和密钥分配效率曲线

以上讨论了 B92 量子密钥分配协议的三种参量选择方案,即

1. $\mathrm{Prob}_{\mathrm{e}} = \mathrm{Prob}_{\mathrm{cu}}$ 且 $p = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1-q}{1+q}}$

$$\begin{cases} p \approx 0.82, \\ q \approx 0.41; \end{cases} \tag{16}$$

2. $\mathrm{Prob}_{\mathrm{e}} \neq \mathrm{Prob}_{\mathrm{cu}}$ 且 $p = \frac{1}{2}$

$$\begin{cases} p \approx 0.5, \\ q \approx 0.41; \end{cases} \tag{17}$$

3. $\mathrm{Prob}_{\mathrm{e}} \neq \mathrm{Prob}_{\mathrm{cu}}$ 且 $p = \frac{1}{2} + \frac{\sqrt{1-q^2-2\sqrt{q}+2q^{3/2}}}{2(1-q)}$

$$\begin{cases} p \approx 0.74, \\ q \approx 0.39. \end{cases} \tag{18}$$

在图 4 和 5 中，我们比较了上述三种 B92 协议的参量选择方案，其中实线表示方案 1，虚线表示方案 2，点划线表示方案 3. 由图 4 可以看到，方案 1 的效率最高，方案 3 稍次，方案 2 最差. 可靠性方面，方案 1 和 2 完全相同(图 5 中重合)，而方案 3 稍优于方案 1 和 2.

通过图 4 和 5 还可以看出，当效率均为 60% ，方案 1 的比特错误概率达到 7.6% ，而方案 3 为 6.8% ；当比特错误概率均为 8% ，方案 1 的效率达到 56% ，而方案 3 为 52% ，可见，方案 1 在总体性能上优于第三种方案.

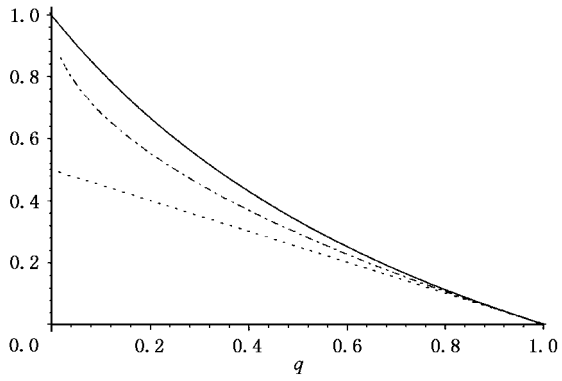

图 4 B92 三种参量方案的密钥分配效率比较

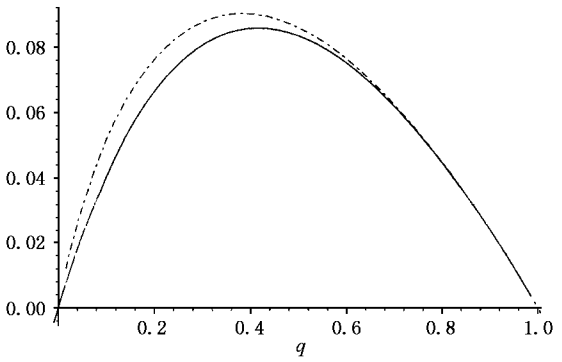

图 5 B92 三种参量方案的可靠性比较

4. 结 论

在非对称 B92 量子密钥分配协议中，可以通过适当选取信源参量和量子态相关度参量，在不损失安全性能的前提下，使密钥分配效率提高 65% 以上. 由于比特错误概率为 7.6% 时，密钥分配效率可以达到 60% ，因此如果信道条件较好，即在完成部分密钥分配后，发现错误概率较小，可以适当增大 p，以进一步提高密钥分配效率.

[1] Bennett C H and Brassard G 1984 *Proc. IEEE International Conf. Computers, Systems, and Signal Processing* p175

[2] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

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

[4] Lo H K and Chau H F 1999 *Science* **283** 2050

[5] Mayers D 1996 *Proc. Crypto.* p343

[6] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[7] Hughes R J, Morgan G L and Peterson C G 2000 *J. Mod. Opt.* **47** 533

[8] Liang *et al* 2001 *Acta Phys. Sin.* **50** 1429(in Chinese)[梁 创等 2001 物理学报 **50** 1429]

[9] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[10] Busch P, Pekka L and Mittelstaedt P 1991 *The Quantum Theory of Measurement* (New York: Springer-Verlag) p57

[11] Ekert A K, Huttner B, Palma G M and Peres A 1994 *Phys. Rev.* A **50** 1047

Optimum parameters for biased two-state quantum key distribution protocol

Zhang Quan　Zhang Er-Yang

(*School of Electronical Science and Technology, National University of Deference Technology, Changsha* 410073, *China*)

(Received 21 October 2001; revised manuscript received 13 December 2001)

Abstract

By analyzing the efficiency and security of B92 quantum key distribution (QKD) protocol, we concluded that efficiency can be greatly improved using biased state source without loss of security. We studied the constraint relations between parameters and performance of the biased B92 schem. The optimum parameters for a variety of scenarios were presented. Meanwhile, the efficiency and security for these scenarios were compared with each other in detail. In conclusion, we have obtained a globally optimal biased B92 QKD scheme whose performance outgo the standard B92.

Keywords: biased two-state quantum key distribution protocol, optimum parameter, quantum cryptography, quantum information

PACC: 0365, 0220, 0250, 4230