基于 BB84 协议的量子密钥分发安全门限研究*

赵 楠† 裴昌幸 刘 丹 权东晓 孙晓楠

(西安电子科技大学 综合业务网国家重点实验室, 西安 710071)

(2011 年 1 月 2 日收到;2011 年 3 月 10 日收到修改稿)

本文分析了实际量子密钥分发过程中,量子态可能受到的各种影响因素;建立了相应的信道模型;推得了非理想信道 BB84 协议判别窃听的安全门限公式. 通过计算与仿真,证明该公式用于估计 BB84 协议的安全通信门限更加准确,判断量子密钥分发过程中是否存在窃听更为有效,同时具有提高通信安全性和密钥分发效率的优点.

关键词: 信道模型, BB84 协议, 窃听判别, 安全门限

PACS: 03.67.Hk

1. 引 言

1984 年 Bennett 和 Brassard 提出了第一个量子密钥分发协议[1,2](BB84 协议). 协议的安全性是以量子特性为基础的,并且在此基础上,通过分析接收端误码率[3,4]来判断通信过程是否安全(即是否存在窃听). 量子力学及量子信息理论保证了量子通信过程的绝对安全,但是在实际通信过程中,由于通信设备的非理想性[5,6],以及信道中存在噪声[6],量子信息在传输的过程中会发生改变[7,8],这使得协议中关于接收端判别通信过程是否安全的标准产生偏差.

本文结合量子力学及量子通信理论,通过分析非理想性通信设备及噪声对量子态的影响,以 BB84 协议为例,建立了量子信道模型,通过分析该模型下量子态的变化情况,得出 BB84 协议新的安全通信门限.

2. BB84 协议的理论安全门限

量子密钥分发协议是利用量子态的不可克隆定理[6,7]来防止窃听的. 量子态经过量子信道传递,而经典信道用来传递量子测量的结果,通信双方将部分测量结果进行比较,判断是否有窃听者存在. 窃听者如果在通信过程中进行窃听,就会产生错误概率,进而被接收方发现. 量子密钥分发协议的安全门限是由窃听产生的误码率得出的[5,7].

BB84 协议采用四个非正交态作为量子信息态,且这四个态分属于两组共轭基,每组基内的两个态相互正交. 如果 Alice 和 Bob 是相互独立的发送用户和接收用户,则 Alice 根据共轭编码基随机编码发送光子序列,Bob 随机选取两组共轭基中的任一组作为测量基. Bob 有 1/2 的概率选对测量基,准确测量的概率为 1;同样,Bob 选错测量基的概率同为 1/2, 由不确定性原理,它会得到一个随机的结果,准确测量概率为 1/2, 因此无 Eve 窃听时 Bob 得到的量子比特正确率为 $\frac{1}{2}\times 1+\frac{1}{2}\times\frac{1}{2}=\frac{3}{4}$. Alice 和 Bob 从他们选择相同测量基得到的结果中随机抽取部分结果通过经典信道比对,如果比对的错误率小于事先设定门限值[2],则认为密钥传输过程是安全的. 他们扔掉用于比对的部分结果,余下部分作为筛选码;否则,则认为存在窃听者,废弃传输的结果.

以截获重发窃听为例,如果 Eve 对通信过程进行窃听,随机选取测量基对截获的量子比特进行测量,并随机发送量子比特给 Bob,则 Bob 得到的量子比特正确率为 $\frac{1}{2}\times\frac{3}{4}+\frac{1}{2}\times\frac{1}{2}=\frac{5}{8}$. 存在窃听的

* 国家自然科学基金(批准号:61072067,60672119,60832001),高等学校学科创新引智计划(批准号:B08038),国家重点实验室专项资金(批准号:ISN 1001004)和中央高校基本科研费专项资金(批准号:K50510010004)资助的课题.

† E-mail: zhaonanonline@hotmail.com

理想量子通信信道的安全通信门限 P_m 为 62.5%，当 $P_m \leqslant 62.5\%$ 时，Bob 废弃传输结果，Alice 重发量子比特.

3. 量子通信信道建模

实际量子信道中，存在噪声以及设备影响，量子偏振态在传输的过程中，偏振方向会发生改变. 具体地讲，对于 BB84 协议中的四个非正交态，信道影响将使得 4 个偏振态的相关性发生改变. 而对于 Bob 来说，需要用原先设定的两组共轭基对接受态进行测量，偏振态的改变使测量误码率增加. 增加的误码率会改变 BB84 协议的安全门限，对接收端判断窃听造成相当大的影响，并且使通信效率降低.

量子态在量子信道的传输过程中，与信道发生关联[8—15]，在接收端全部或者部分发生改变，成为新的态. 信道中与量子态发生关联的有非理想型设备和噪声. 这一关系可以用映射来描述. 令信道矩阵为 $\boldsymbol{S}$，噪声矩阵为 $\boldsymbol{N}_\phi$，$\boldsymbol{S}$ 是与信道中非理性设备和量子态间相关情况有关的量，$\boldsymbol{N}_\phi$ 是与噪声和量子态间相关情况有关的量，则接收态为

$$\boldsymbol{\Psi}_i = (\boldsymbol{S} + \boldsymbol{N}_\phi)\boldsymbol{\Phi}_i \quad (i = 1,2,\cdots,n), \tag{1}$$

其中，$\boldsymbol{\Phi}_i$ 表示接收态矩阵；表示同一测量基下的态矩阵，每列元素表示一个发送态.

BB84 协议中，发送态为两组非正交态，则(1)式中，$i = 1,2$.

量子态与信道发生关联，即与非理想设备及噪声发生相关. 相关的程度决定了量子态受信道影响发生变化的情况. 相关系数 $r_1, r_2 (0 \leqslant r_1, r_2 \leqslant 1)$ 分别表示非理想性设备和噪声与量子态的相关情况. 由文献[15]可知，通过波动方程理论及热力学公式建模，可以得出满足不同信道情况的 $\boldsymbol{S}$ 与 r_1 及 $\boldsymbol{N}_\phi$ 与 r_2 的函数关系.

4. 非理想条件下 BB84 协议安全门限

依据 BB84 协议，可令发送态为 $|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle$. 相互正交的两偏振态，可以由同一测量基测得. 令 $\boldsymbol{\Phi}_1, \boldsymbol{\Phi}_2$ 为两 2×2 的发送态矩阵，$\boldsymbol{\Phi}_1$ 的两列元素分别为 $|\phi_1\rangle$ 和 $|\phi_2\rangle$，$\boldsymbol{\Phi}_2$ 的两列元素分别为 $|\phi_3\rangle$ 和 $|\phi_4\rangle$.

在不考虑信道中各种影响的情况下，测量基为

$$M = \boldsymbol{\Phi}_1, K = \boldsymbol{\Phi}_2, \tag{2}$$

则

$$|\mu_1\rangle = |\phi_1\rangle, |\mu_2\rangle = |\phi_2\rangle,$$
$$|\kappa_1\rangle = |\phi_3\rangle, |\kappa_2\rangle = |\phi_4\rangle. \tag{3}$$

令信道及噪声与传输态相关的概率[15]均为 1/2，则

$$SS^\dagger = \frac{1}{2}\begin{bmatrix} 1 & r_1 \\ r_1 & 1 \end{bmatrix},$$
$$\boldsymbol{N}_\phi \boldsymbol{N}_\phi^\dagger = \frac{1}{2}\begin{bmatrix} 1 & r_2 \\ r_2 & 1 \end{bmatrix}, \tag{4}$$

$\boldsymbol{S}^\dagger$ 是 $\boldsymbol{S}$ 的伴随矩阵，$\boldsymbol{N}_\phi^\dagger$ 是 $\boldsymbol{N}_\phi$ 的伴随矩阵.

分别对 $\boldsymbol{S}$ 和 $\boldsymbol{N}_\phi$ 进行奇异值分解(SVD)，得

$$S = V_S \sum\nolimits_S W_S^\dagger = V_S \begin{bmatrix} \sqrt{\frac{1+r_1}{2}} & 0 \\ 0 & \sqrt{\frac{1-r_1}{2}} \end{bmatrix} W_S^\dagger, \tag{5}$$

$$N_\phi = V_{N_\phi} \sum\nolimits_{N_\phi} W_{N_\phi}^\dagger = V_{N_\phi} \begin{bmatrix} \sqrt{\frac{1+r_2}{2}} & 0 \\ 0 & \sqrt{\frac{1-r_2}{2}} \end{bmatrix} W_{N_\phi}^\dagger, \tag{6}$$

$\boldsymbol{V}_S, \boldsymbol{V}_{N\phi}, W_S^\dagger, \boldsymbol{W}_{N\phi}^\dagger$ 均为 2×2 实正交矩阵. 如果 $\boldsymbol{S}$ 和 $\boldsymbol{N}_\phi$ 的奇异值分别为 σ_s 和 σ_{N_ϕ}，则 S 和 N_ϕ 可表示为

$$S = A\sigma_s, N_\phi = B\sigma_{N_\phi}, \tag{7}$$

其中，$A = \boldsymbol{V}_S \boldsymbol{W}_S^\dagger$，$\mathrm{B} = \boldsymbol{V}_{N\phi} W_{N\phi}^\dagger$.

由(1)式得

$$\boldsymbol{\Psi}_i = (A\sigma_s + B\sigma_{N_\varphi})\boldsymbol{\Phi}_i \quad (i = 1,2). \tag{8}$$

接收态与测量态之间的均方误差[16,17]可以表示为

$$E = \sum_{i=1}^{2} \langle e_i | e_i \rangle, \tag{9}$$

其中，$|e_i\rangle = |\psi_i\rangle - |\mu_i\rangle$，或者 $|e_i\rangle = |\psi_i\rangle - |\kappa_i\rangle$.

E_1，E_2 分别为接收端用正确测量基测量时，两非正交测量基下的均方根误差，则

$$E_1 = \boldsymbol{\Psi} - M,$$
$$E_2 = \boldsymbol{\Psi} - K. \tag{10}$$

由(2)，(8)，(9)，(10)式得

$$E_1 = (A\sigma_s + B\sigma_{N_\phi} - \boldsymbol{I})\boldsymbol{\Phi}_1,$$
$$E_2 = (A\sigma_s + B\sigma_{N_\phi} - \boldsymbol{I})\boldsymbol{\Phi}_2, \tag{11}$$
$$E_1' = E_2' = A\sigma_s + B\sigma_{N_\phi} - \boldsymbol{I}, \tag{12}$$

其中，$\boldsymbol{I}$ 为单位矩阵.

因为 $\langle \phi_i | \phi_i \rangle = 1$，令 E_1 为进行一次测量的均

方误差,由(11)式得

$$E_t = p|E_1'|^2 + (1-p)|E_2'|^2, \quad (13)$$

$|E_1'|^2$, $|E_2'|^2$ 分别为不同测量基测量的均方误差;p 为 Bob 选择正确测量基的概率,$1-p$ 为 Bob 选择错误测量基的概率. 由 BB84 协议可知, $p = 1/2$.

由(9)式得

$$E_t = \frac{1}{2}(|E_1'|^2 + |E_2'|^2). \quad (14)$$

Bob 选择正确测量基检测的正确概率为 $\sum_{i=1}^{2}|\langle\psi_i|\mu_i\rangle|^2$, $|\langle\psi_i|\mu_i\rangle|^2$ 表示接收态 $|\psi_i\rangle$ 与测量态 $|\mu_i\rangle$ 重叠的概率.

对(9)式进行奇异值分解,可得[18—20]

$$|\mu_i\rangle \equiv (\Psi\Psi^{\dagger})^{-1/2}|\psi_i\rangle. \quad (15)$$

则 $|\langle\psi_i|\mu_i\rangle|^2 \propto (1-E_t)$, $|\langle\psi_i|\mu_i\rangle|^2$ 可以用接收态与测量基本矢量均方误差描述.

依据 BB84 协议,理想情况下,Bob 选择正确测量基测准确接收量子态的概率为 1/2, 实际由于存在非理想性设备及噪声影响,则选择正确测量基测准确接收量子态的概率为

$$P_r = 1 - E_t. \quad (16)$$

错误选择测量基时得到正确结果的概率 P_w 仍为 1/2.

无窃听时,实际通信过程中,Bob 得到量子比特的正确率为

$$P = \frac{1}{2}P_r + \frac{1}{2}P_w = \frac{1}{2}(1-E_t) + \frac{1}{4}. \quad (17)$$

由(12),(14),(17)式得

$$P = \frac{1}{2}\left[1 - \left|A\sqrt{\frac{(1+r_1)(1-r_1)}{4}} + B\sqrt{\frac{(1+r_2)(1-r_2)}{4}} - 1\right|^2\right] + \frac{1}{4}. \quad (18)$$

当存在窃听(截获-重发)时,Bob 选择正确测量基得到正确量子比特的概率为 $\frac{P_r}{2}+\frac{1}{4}$, 由(16)式,存在窃听时,实际量子通信信道的安全通信门限 P_m 为

$$P_m = \frac{1}{2}\left(\frac{P_r}{2}+\frac{1}{4}\right)+\frac{1}{4} = \frac{1}{4}\left[1 - \left|A\sqrt{\frac{(1+r_1)(1-r_1)}{4}} + B\sqrt{\frac{(1+r_2)(1-r_2)}{4}} - 1\right|^2\right] + \frac{3}{8}. \quad (19)$$

根据不同信道情况,确定 P_m 值. 当通信双方进行密钥协商后,接收端得到正确量子比特概率低于 P_m 时,就可确定存在窃听.

5. 仿真结果及分析

P 和 P_m 是与相关系数 r_1 和 r_2 有关的量. 这里只考虑 A,B 均为 1 的情况[15],此时,信道和噪声对量子态造成影响的权值相同,仿真结果如图 1 所示.

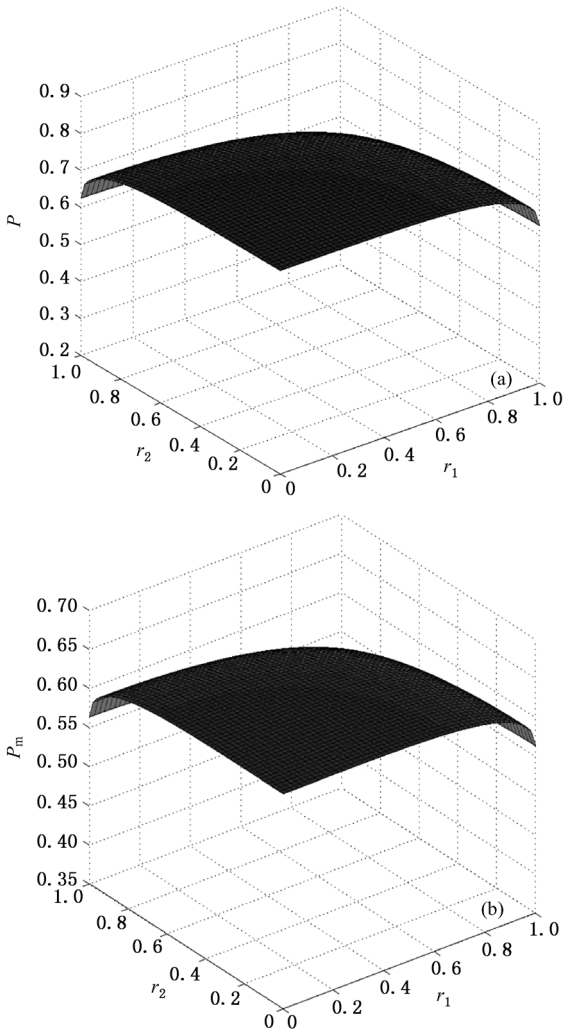

图 1 P 和 P_m 随 r_1 和 r_2 变化情况

由图 1(a)可以看出,在 r_1 和 r_2 均为 0 时,P 约为 0.75. 由图 1(b)可以看出,在 r_1 和 r_2 均为 0 时,P_m 约为 0.625,即符合理想条件下的 P_m 值. 而随着 r_1 和 r_2 值的增加,P 和 P_m 的值不断减小. 令 $P_{e1} = 1 - P$, $P_{e2} = 1 - P_m$,图 2 给出 P_{e1}, P_{e2} 与相关系数 r_1

和 r_2 的关系曲线.

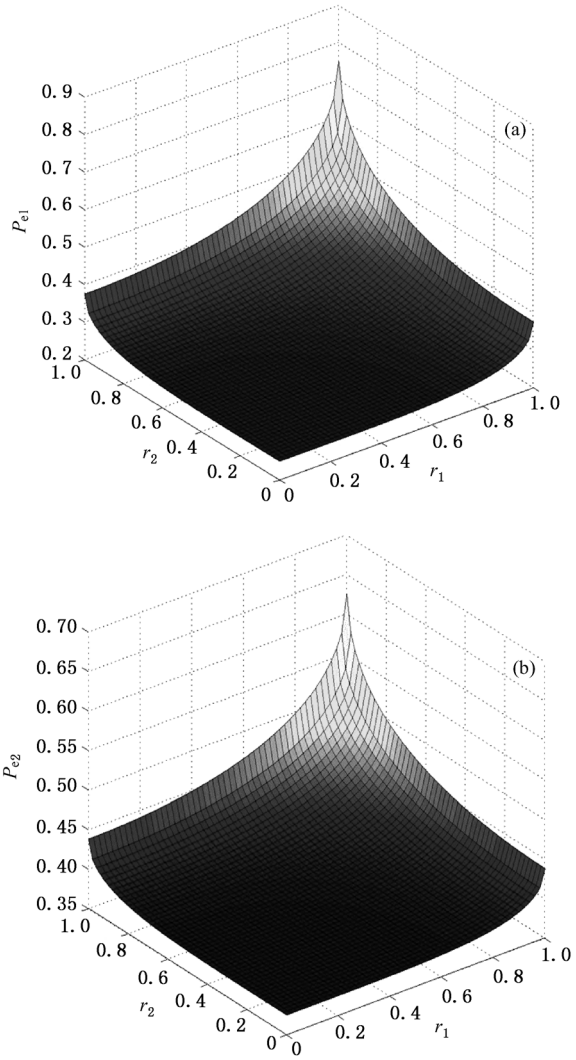

图 2 P_{e1} 和 P_{e2} 随 r_1 和 r_2 变化情况

由图 2 可以看出,在 r_1 和 r_2 均为 1 时,P_{e1} 接近 0.75, P_{e2} 接近 0.625.

根据 r_1 和 r_2 值的不同,可以得到存在窃听时接收端得到正确量子比特的概率,即安全通信门限;以此可以判断窃听者 Eve 是否存在.

考虑一种特殊情况,当 $r_2 = 0$ 时,噪声与量子态不相关,即噪声不对量子态的偏转角造成影响.

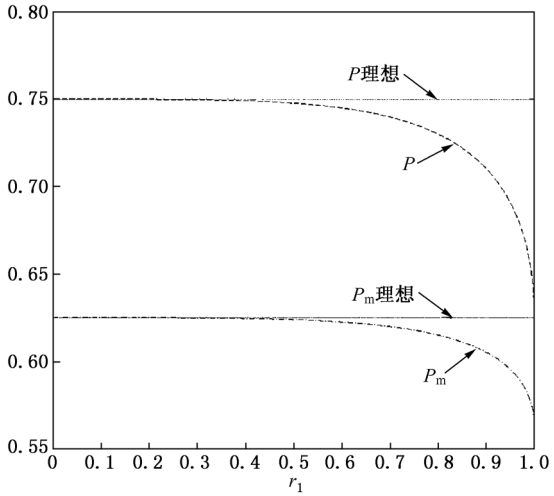

图 3 P_m, P, P_m 理想和 P 理想的变化曲线

由图 3 可以看出, $r_2 = 0$ 时, P, P_m, P 理想和 P_m 理想的变化曲线. P 理想和 P_m 理想为 BB84 协议理论安全门限和理想情况下无 Eve 窃听时 Bob 得到的量子比特正确率. 由图可以看出,随着 r_1 值从 0 增加到 1, P 从 0.75 减小到 0.625 , P_m 从 0.625 减小到约 0.57. 如果在 $r_1 = 1$ 时,用 BB84 协议理论安全门限判别窃听,那么在 P_m 为 0.57—0.625 之间的安全量子通信过程也将被认为存在窃听,发送端则重发量子比特,这将极大地降低通信效率.

6. 结 论

本文通过分析量子态在实际量子通信信道中所受影响,建立了量子信道模型;以 BB84 协议为例,对其安全门限进行了分析,推得了实际量子通信中判别窃听的安全门限公式. 通过仿真,证明了该公式能够有效地判断量子密钥分发过程中是否存在窃听. 进一步研究将对不同量子密钥分发协议及不同窃听方法攻击的判别安全门限作深入分析.

[1] Bennett C H, Brassard G 1984 *Int. Conference on Computers, Systems, and Signal Processing* (Bangalore: IEEE) pp 175—179

[2] Bennett C H, Shor P W 1998 *IEEE Trans. Inform. Theory* **44** 2724

[3] Holevo A S 1973 *J. Multivar. Anal.* vol. 3, pp 337—394

[4] Yuen H P, Kennedy R S, Lax M 1975 *Trans. Inform. Theory* vol. IT-21, pp125—134

[5] Klimovitch G V 2001 *Prov. IEEE Int. Symp. Information Theory* (Washington DC) p123

[6] Peres A 1990 *Foundations Phys.* vol. 20, pp1441—1453

[7] Su R K 2003 *Quantum Mechanics* (Beijing: Higher Education Press) p84—123 (in Chinese) [苏汝铿 2003 量子力学 第二版 (北京 高等教育出版社) 第 84—123 页]

[8] Bostrom K, Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[9] Chen J, Li Y, Wu G, Zeng H P 2007 *Acta Phys. Sin.* **56** 5243 (in Chinese) [陈 杰、黎 遥、吴 光、曾和平 2007 物理学报 **56** 5243]
[10] Wang C, Deng F G, Li Y S 2005 *Phys. Rev.* A **71** 044305
[11] Wang J, Chen H Q, Zhang Q, Tang C J 2007 *Acta Phys. Sin.* **56** 673 (in Chinese) [王 剑、陈皇卿、张 权、唐朝京 2007 物理学报 **56** 673]
[12] Kholeyo A S 1979 *Probl. Pered. Inform.* (Russian) **15** 247
[13] Concha J I, Poor H V 2002 *Int. Conf. Quantum Communication, Measurement and Computing* (the United States)
[14] Zhu C H, Pei C X, Quan D X, Chen N, Yi Y H 2009 *Acta Phys. Sin.* **58** 2184 (in Chinese) [朱畅华、裴昌幸、权东晓、陈 南、易运晖 2009 物理学报 **58** 2184]
[15] Concha J L, Poor H V 2004 *Int. IEEE Transactions on Information Theory*
[16] Ban M, Kurukowa K, Momose R, Hirota O 1997 *Int. J. Theor. Phys.* **36** 1269
[17] Nelson L B, Poor H V 1995 *IEEE Trans. Commun.* **43** 2803
[18] Noam Elron, Eldar U C 2005 quant-ph/0501084v2 19
[19] Kraus K 1971 *Ann. Phys.* **64** 311
[20] He P S, You W L, Tian G S 2011 *Chin. Phys.* B **20** 017503

Quantum key distribution secure threshold based on BB84 protocol*

Zhao Nan† Pei Chang-Xing Liu Dan Quan Dong-Xiao Sun Xiao-Nan
(*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071, *China*)
(Received 2 January 2011; revised manuscript received 10 March 2011)

Abstract

Quantum state in the channel is affected by several factors, which will bring detection error and make secure threshold of quantum distribution protocol unable to judge whether eavesdropping exists. We analyze the factors in real quantum channel, which affects the quantum state, develop a channel model, and derive a judging eavesdrop secure threshold formula of BB84 protocol based on an imperfect channel. Through calculating and simulating, the formula is proved to be more accurate to estimate the secure threshold of the BB84 protocol and more effective to judge eavesdropping. Meanwhile, this method can improve the security and the efficiency of key distribution.

Keywords: channel model, BB84 protocol, judge eavesdrop, secure threshold
PACS: 03.67.Hk

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61072067, 60672119, 60832001), the 111 Project (Grant No. B08038), ISN (Grant No. 1001004), and the Fundamental Research Funds for the Central Universities (Grant No. K50510010004).
† E-mail: zhaonanonline@hotmail.com