物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

量子BB84协议在联合旋转噪音信道上的安全性分析

李剑 陈彦桦 潘泽世 孙风琪 李娜 黎雷蕾

Security analysis of BB84 protocol in the collective-rotation noise channel

Li Jian Chen Yan-Hua Pan Ze-Shi Sun Feng-Qi Li Na Li Lei-Lei

引用信息 Citation: Acta Physica Sinica, 65, 030302 (2016) DOI: 10.7498/aps.65.030302
在线阅读 View online: http://dx.doi.org/10.7498/aps.65.030302
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2016/V65/I3

量子BB84协议在联合旋转噪音信道上的安全性分析*

李剑[1)2)3)] 陈彦桦[1)†] 潘泽世[1)] 孙风琪[1)] 李娜[1)] 黎雷蕾[1)]

1) (北京邮电大学计算机学院, 北京 100876)

2) (中国科学技术大学, 合肥微尺度物质科学国家实验室, 合肥 230026)

3) (通信安全科学与技术重点实验室, 成都 610041)

(2015 年 9 月 21 日收到; 2015 年 10 月 20 日收到修改稿)

多数在理想条件下设计的量子密码协议没有考虑实际通信中噪音的影响, 可能造成机密信息不能被准确传输, 或可能存在窃听隐藏在噪音中的风险, 因此分析噪音条件下量子密码协议的安全性具有重要的意义. 为了分析量子BB84协议在联合旋转噪音信道上的安全性, 本文采用粒子偏转模型, 对量子信道中的联合噪音进行建模, 定量地区分量子信道中噪音和窃听干扰; 并且采用冯·诺依曼熵理论建立窃听者能窃取的信息量与量子比特误码率、噪音水平三者之间的函数关系, 定量地分析噪音条件下量子信道的安全性; 最后根据联合噪音模型及窃听者能窃取的信息量与量子比特误码率、噪音水平三者之间的关系, 定量地分析了量子BB84协议在联合噪音条件下的安全性并计算噪音临界点. 通过分析可知, 在已有噪音水平条件下, 窃听者最多能够从通信双方窃取25%的密钥, 但是Eve的窃听行为会被检测出来, 这样Alice和Bob会放弃当前协商的密钥, 重新进行密钥协商, 直至确认没有Eve的窃听为止. 这个结果说明量子BB84协议在联合旋转噪音信道下的通信是安全的.

关键词: 量子安全通信, 联合旋转噪音, 安全性分析, 量子比特误码率

PACS: 03.67.–a, 03.67.Ac, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.65.030302

1 引 言

在秘密通信过程中, 为了保证只有合法的通信双方Alice和Bob能够获取其中的消息, 并防止窃听者Eve窃取, 通常会对消息进行加密处理. 很多科研人员正在致力于研究安全、可靠的密码通信协议. 随着信息科学技术和量子物理学的快速发展, 量子密码学逐渐成为非常重要的领域之一. 量子密码学和经典密码学有着根本性的不同, 量子密码学是基于量子力学, 与经典密码学相比有着更高的性能和安全性. 随着量子力学的飞速发展, 量子密码学也有了更加广阔的发展前景.

1984年, Bennett和Brassard [1] 首次提出了量子密钥分配协议(quantum key distribution protocol, QKD), 现在被称为BB84协议. 自从这个协议被提出后, 就受到了各界的广泛关注. 1989 年, IBM 公司和蒙特利尔大学第一次完成了量子加密实验 [2], 并从实验角度证明了BB84协议的实用性. 在文献[3]中, 由于使用了极化光子, 实验通信距离达到了1 km.

BB84协议的安全性一直以来都受到学者的关注. 2004年, Boileau等 [4] 提出了基于极化的量子密钥分发协议, 该协议在联合旋转噪音信道上能正常工作; 2004 年, Gottesman 等 [5] 证明在发射

* 国家自然科学基金(批准号: 61472048, 61402058, 61370194)、北京自然科学基金(批准号: 4152038)和中国博士后科学基金(批准号: 2014 M561826)资助的课题.

† 通信作者. E-mail: cyanhua2010@bupt.edu.cn

源和接收源都存在问题的情况下, BB84 协议仍然是安全的; 2005 年, Watanabe 等 [6] 证明通过随机保密放大, BB84 协议具有安全性, 且在相同错误率的情况下, 经过随机保密放大后的 BB84 协议相对于 Mayers 估计具有更高的密钥传输速率; 2009 年, Wang 等 [7] 从攻击的角度分析了 BB84 协议的安全性, 攻击者可截获发送者的消息, 并发送自己的消息给接收者; 2010 年, Aizan 等 [8] 在 802.11i 无线局域网上实现了 BB84 协议, 从实验的角度证明了在有攻击者存在、且环境噪音比较大的情况下, BB84 协议的安全性, 但缺乏理论支持; 2011 年, Winiarczyk 等 [9] 从量子物理学的角度深入分析了 BB84 协议的安全性, 并较全面地介绍了关于实现 BB84 协议和其他量子系统可能遇到的问题; 2012 年, Buhari 等 [10] 对 BB84 协议进行了仿真模拟, 并在其过程中采取了几套安全攻击方案; 2013 年, Yang 等 [11] 通过形式证明的方法更方便地分析了量子加密协议的安全性; 2014 年, Rostom 等 [12] 提出 OFBD 方法, 改进了 BB84 协议中很重要的一步, 模拟结果表明这种方法更能检测和纠正存在的量子比特错误, 从效率上提高了 25 个百分点; 2014 年, Halip 等 [13] 使用光子模拟光学系统模拟了 BB84 协议, 分别模拟了没有安全攻击的场景和存在一系列安全攻击的场景, 模拟结果符合 BB84 协议; 2015 年, Lucamarini 等 [14] 提出以前的 BB84 安全性证明有一个限制条件, 即 Eve 采用的是联合攻击的手段, 因此他们重新证明了在 Eve 任意形式的攻击情况下 BB84 协议的安全性; 2015 年, Archana 等 [15] 使用 OptSim 5.2 再次成功模拟了使用 BB84 协议进行量子密钥分发; 2015 年, Jasper 等 [16] 提出了新型的量子密钥分发协议, 即时频 (TF) BB84 协议, 成功证明了其在高数据传输率下无条件安全性.

但是这些分析 [5−21] 几乎没有涉及环境噪音的影响, 而这些影响在实际系统中是不能忽略的. 在实际的非孤立系统中, 量子态肯定会受到环境噪音的影响. 因此, 在噪音环境下 BB84 协议的安全性分析就显得尤为重要, 并且这对该协议及其类似协议的实现有着较大的帮助. 由于实际系统中环境噪音的复杂性和不可预测性, 本文主要着眼于联合旋转噪音的分析.

本文提出了联合旋转噪音分析模型, 应用信息理论分析 BB84 协议在噪音环境下的安全性. 由本文分析可知, 当噪音水平 $\varepsilon \leqslant 0.68$, 窃听者 Eve 始终都能被检测出来. 而且 Eve 能够获取的平均互信息量在 0.2 到 0.25 之间. 分析结果表明, BB84 协议在联合旋转噪音环境下通信是安全的. Eve 在窃听过程中只能得到部分密钥信息, 而且会因为窃听行为被检测出来, 这样 Alice 和 Bob 会放弃当前协商的密钥, 重新进行密钥协商, 直至确认没有 Eve 的窃听为止.

简而言之, 本文主要确认了 BB84 协议作为 QKD 在联合噪音环境下是安全的, 并为 BB84 协议等量子通信在噪音环境的安全性分析开辟了新的视角.

2 相关工作

2.1 BB84 协议

Bennett 和 Brassard [2] 1984 年提出的 BB84 协议中有两组基: 一个是 Z 基, $B_Z = \{|0\rangle, |1\rangle\}$; 另一个是 X 基: $B_X = \{|+\rangle, |-\rangle\}$. 发送方 Alice 随机生成二进制比特 (0 或 1), 并随机选择 Z 基或者 X 基, 可得

$$\begin{array}{ccc} \text{基/比特} & 0 & 1 \\ B_Z & |0\rangle & |1\rangle, \\ B_X & |+\rangle & |-\rangle. \end{array} \tag{1}$$

Alice 通过量子信道发送对应的量子比特给 Bob. Bob 得到量子比特后, 随机选择 Z 基或者 X 基进行测量, 并将量子比特转换成对应的二进制比特 (0 或 1). 重复上述操作直到 Alice 的二进制比特发送完毕. 之后 Alice 和 Bob 通过经典信道比较他们所选择的基, 并抛弃他们选择的基不同的测量结果, 保留相同基的测量结果作为原始密钥.

为了检测窃听, Alice 和 Bob 可以从原始密钥中选出一部分进行比对, 如果存在错误比特, 则表明信道已被窃听.

2.2 改进的 BB84 协议 [22]

由于环境噪音和窃听带给量子信道传输的影响是等同的, 因此量子比特错误可由环境噪音或者窃听造成, 或者二者兼而有之.

在原始的 BB84 协议中, 量子比特错误只可能由窃听造成, 因此只将量子比特的错误作为是否有窃听者存在的评判标准在噪音环境下就不再适用.

为了保护信息传输, 我们需要改善检测窃听的评判机制. 首先需要根据噪音信道设定一个初始的量子比特误码率$\sigma_{\rm i}$. 如果实际量子比特误码率$\sigma > \sigma_{\rm i}$, 那么不管什么原因引起的, 都认定此次通信过程存在窃听.

这里提及的量子比特误码率指的是原始密钥的误码率. 在计算原始密钥误码率的时候, 需要注意有部分原始密钥会因为BB84协议的设计而丢弃.

2.3 联合旋转噪音水平

为了更加方便地分析BB84协议的安全性, 可以合理地假定环境噪音是常数. 虽然实际环境中噪音的大小随时间而上下波动, 但仍可以根据噪音的最大值进行安全性分析的推导.

理想情况下, 在有噪音的量子信道中, 环境噪音对每一个量子比特产生的影响是一样的. 根据文献[23—25], 环境噪音的影响可被写成如下酉矩阵$\boldsymbol{U}$:

$$\boldsymbol{U} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \tag{2}$$

参数θ的大小根据量子信道的噪音大小设置. 由于假定环境噪音是常数或者是噪音波动的最大值, 和噪音相对应的θ也是常数.

在噪音影响下, 量子态$|0\rangle, |1\rangle, |+\rangle, |-\rangle$如下所示:

$$\begin{aligned}
|0\rangle \rightarrow & \cos\theta|0\rangle - \sin\theta|1\rangle \\
= & \frac{\cos\theta - \sin\theta}{\sqrt{2}}|+\rangle + \frac{\cos\theta + \sin\theta}{\sqrt{2}}|-\rangle, \qquad (3a)\\
|1\rangle \rightarrow & \sin\theta|0\rangle + \cos\theta|1\rangle \\
= & \frac{\cos\theta + \sin\theta}{\sqrt{2}}|+\rangle + \frac{\sin\theta - \cos\theta}{\sqrt{2}}|-\rangle, \qquad (3b)\\
|+\rangle = & \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
\rightarrow & \frac{\cos\theta + \sin\theta}{\sqrt{2}}|0\rangle + \frac{\cos\theta - \sin\theta}{\sqrt{2}}|1\rangle \\
= & \cos\theta|+\rangle + \sin\theta|-\rangle, \qquad (3c)\\
|-\rangle = & \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
\rightarrow & \frac{\cos\theta - \sin\theta}{\sqrt{2}}|0\rangle - \frac{\cos\theta + \sin\theta}{\sqrt{2}}|1\rangle \\
= & \cos\theta|-\rangle - \sin\theta|+\rangle. \qquad (3d)
\end{aligned}$$

不管发射的粒子量子态如何, 最终粒子错误率是常量$\sin^2\theta$. 因此$\varepsilon = \sin^2\theta$可被用来检测噪音的大小. 噪音越大, 偏转角越大, 与之对应的ε也越大, 反之亦然.

3 噪音环境下BB84协议安全性分析

3.1 没有窃听者

根据BB84协议, Alice以0.25的概率发送量子比特$|0\rangle, |1\rangle, |+\rangle, |-\rangle$. 在经过量子信道噪音影响后, Bob的测量结果如表1. P是发送概率, A代表Alice, B代表Bob.

表1 没有窃听者情况下Bob测量结果

Table 1. Outcome of Bob's measurement without eavesdropping.

P	A/B	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\frac{1}{4}$	$\|0\rangle$	$\frac{\cos^2\theta}{8}$	$\frac{\sin^2\theta}{8}$	$\frac{1-\sin 2\theta}{16}$	$\frac{1+\sin 2\theta}{16}$
$\frac{1}{4}$	$\|1\rangle$	$\frac{\sin^2\theta}{8}$	$\frac{\cos^2\theta}{8}$	$\frac{1+\sin 2\theta}{16}$	$\frac{1-\sin 2\theta}{16}$
$\frac{1}{4}$	$\|+\rangle$	$\frac{1+\sin 2\theta}{16}$	$\frac{1-\sin 2\theta}{16}$	$\frac{\cos^2\theta}{8}$	$\frac{\sin^2\theta}{8}$
$\frac{1}{4}$	$\|-\rangle$	$\frac{1-\sin 2\theta}{16}$	$\frac{1+\sin 2\theta}{16}$	$\frac{\sin^2\theta}{8}$	$\frac{\cos^2\theta}{8}$

考虑到有部分比特会由于BB84协议的设计而抛弃, 原始密钥误码率比较容易得到:

$$ber_0 = \frac{1}{4}\sin^2\theta \times 4 = \sin^2\theta. \tag{4}$$

这就是说, 如果信道没有窃听者存在, 量子比特误码率只由环境噪音$ber_0 = \sin^2\theta$造成. 根据2.1节可知, $\sigma_{\rm i}$应该设置成ber_0:

$$\sigma_{\rm i} = \sin^2\theta. \tag{5}$$

3.2 存在窃听者

根据量子计算和量子信息[26], 合理的通信方式如图1所示. 通信系统开始于量子态和噪音的张量积. 从图1可以看出, 在Eve窃听之前, 环境噪音就开始作用于传输的量子比特. 每一个量子比特所受噪音影响都可看成是一次性效应.

从图1可以看出, Eve在量子比特受环境噪音影响之后进行测量, 因此他的量子态测量结果如表2. P是发送概率, A代表Alice, E代表Eve.

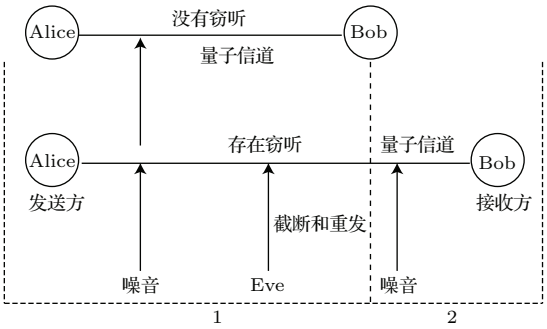

图 1 BB84 协议通信流程图

Fig. 1. Flow Diagram of BB84.

表 2 噪音影响下 Eve 的测量结果

Table 2. Outcome of Eve's measurement effected by noise.

P	A/E	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\frac{1}{4}$	$\|0\rangle$	$\frac{\cos^2\theta}{8}$	$\frac{\sin^2\theta}{8}$	$\frac{1-\sin 2\theta}{16}$	$\frac{1+\sin 2\theta}{16}$
$\frac{1}{4}$	$\|1\rangle$	$\frac{\sin^2\theta}{8}$	$\frac{\cos^2\theta}{8}$	$\frac{1+\sin 2\theta}{16}$	$\frac{1-\sin 2\theta}{16}$
$\frac{1}{4}$	$\|+\rangle$	$\frac{1+\sin 2\theta}{16}$	$\frac{1-\sin 2\theta}{16}$	$\frac{\cos^2\theta}{8}$	$\frac{\sin^2\theta}{8}$
$\frac{1}{4}$	$\|-\rangle$	$\frac{1-\sin 2\theta}{16}$	$\frac{1+\sin 2\theta}{16}$	$\frac{\sin^2\theta}{8}$	$\frac{\cos^2\theta}{8}$

现在分析一下 Eve 能够窃取的信息量. 信息量可由平均互信息 $I(\mathrm{A},\mathrm{E})$ [27] 得到:

$$I(\mathrm{A},\mathrm{E}) = H(\mathrm{A}) - H(\mathrm{A}|\mathrm{E}). \tag{6}$$

因为 Alice 发送量子比特是随机的, 因此 $H(\mathrm{A}) = 1$.

$$\begin{aligned} &H(\mathrm{A}|\mathrm{E}) \\ =&\left(-\sum_{a,e} P(\mathrm{A},\mathrm{E})\log_2 P(\mathrm{A}|\mathrm{E})\right)/2 \\ =&-\left(\frac{\cos^2\theta}{8}\log_2\frac{\cos^2\theta}{2}+\frac{\sin^2\theta}{8}\log_2\frac{\sin^2\theta}{2}\right. \\ &+\frac{1-\sin 2\theta}{16}\log_2\frac{1-\sin 2\theta}{4} \\ &\left.+\frac{1+\sin 2\theta}{16}\log_2\frac{1+\sin 2\theta}{4}\right)\times\left(\frac{4}{2}\right) \\ =&-\left(\frac{\cos^2\theta}{4}\log_2\frac{\cos^2\theta}{2}+\frac{\sin^2\theta}{4}\log_2\frac{\sin^2\theta}{2}\right. \\ &+\frac{1-\sin 2\theta}{8}\log_2\frac{1-\sin 2\theta}{4} \\ &\left.+\frac{1+\sin 2\theta}{8}\log_2\frac{1+\sin 2\theta}{4}\right). \end{aligned} \tag{7}$$

那么

$$\begin{aligned} I(\mathrm{A},\mathrm{E}) =&H(\mathrm{A}) - H(\mathrm{A}|\mathrm{E}) \\ =&\left(\frac{\cos^2\theta}{4}\log_2\frac{\cos^2\theta}{2}+\frac{\sin^2\theta}{4}\log_2\frac{\sin^2\theta}{2}\right. \\ &+\frac{1-\sin 2\theta}{8}\log_2\frac{1-\sin 2\theta}{4} \\ &\left.+\frac{1+\sin 2\theta}{8}\log_2\frac{1+\sin 2\theta}{4}\right)+1. \end{aligned} \tag{8}$$

根据噪音水平表达式 $\varepsilon = \sin^2\theta$, 有

$$\begin{aligned} &I(\mathrm{A},\mathrm{E}) \\ =&\left(\frac{1-\varepsilon}{4}\log_2\frac{1-\varepsilon}{2}+\frac{\varepsilon}{4}\log_2\frac{\varepsilon}{2}\right. \\ &+\frac{1-2\sqrt{\varepsilon(1-\varepsilon)}}{8}\log_2\frac{1-2\sqrt{\varepsilon(1-\varepsilon)}}{4} \\ &\left.+\frac{1-2\sqrt{\varepsilon(1+\varepsilon)}}{8}\log_2\frac{1-2\sqrt{\varepsilon(1+\varepsilon)}}{4}\right) \\ &+1. \end{aligned} \tag{9}$$

之后 Eve 将拦截到的量子比特再次发送给 Bob. 再次发送过程仍将受到环境噪音影响, 结果列于表 3. E 代表 Eve, B 代表 Bob.

根据表 2 和表 3, Bob 的测量结果可写成表 4 的形式. A 代表 Alice, B 代表 Bob, P 是发送概率, Ab 是 Alice 选择的测量基, Bb 是 Bob 选择的测量基, 且

$$\begin{aligned} y =&2\times\left(\frac{\cos^2\theta}{8}\times\frac{\sin^2\theta}{2}+\frac{\cos^2\theta}{2}\times\frac{\sin^2\theta}{8}\right. \\ &+\frac{1-\sin 2\theta}{16}\times\frac{1-\sin 2\theta}{4} \\ &\left.+\frac{1+\sin 2\theta}{16}\times\frac{1+\sin 2\theta}{4}\right) \\ =&\frac{8\sin^2\theta\times(1-\sin 2\theta)+1}{16}. \end{aligned} \tag{10}$$

表 3 第二次噪音影响后 Bob 的测量结果

Table 3. Outcome of Bob's measurement effected by second noise.

E/B	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\|0\rangle$	$\frac{\cos^2\theta}{2}$	$\frac{\sin^2\theta}{2}$	$\frac{1-\sin 2\theta}{4}$	$\frac{1+\sin 2\theta}{4}$
$\|1\rangle$	$\frac{\sin^2\theta}{2}$	$\frac{\cos^2\theta}{2}$	$\frac{1+\sin 2\theta}{4}$	$\frac{1-\sin 2\theta}{4}$
$\|+\rangle$	$\frac{1+\sin 2\theta}{4}$	$\frac{1-\sin 2\theta}{4}$	$\frac{\cos^2\theta}{2}$	$\frac{\sin^2\theta}{2}$
$\|-\rangle$	$\frac{1-\sin 2\theta}{4}$	$\frac{1+\sin 2\theta}{4}$	$\frac{\sin^2\theta}{2}$	$\frac{\cos^2\theta}{2}$

表 4 经过两次噪音影响和攻击影响后 Bob 的测量结果

Table 4. Outcome of Bob's measurement effected by two noise and attack.

Ab	P	A/B	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	Bb
$B_{\rm Z}$	0.25	$\|0\rangle$	x	y	0	0	$B_{\rm Z}$
$B_{\rm Z}$	0.25	$\|1\rangle$	y	x	0	0	$B_{\rm Z}$
$B_{\rm X}$	0.25	$\|+\rangle$	0	0	x	y	$B_{\rm X}$
$B_{\rm X}$	0.25	$\|-\rangle$	0	0	y	x	$B_{\rm X}$

通信过程中的量子比特误码率 ber 如下所示:

$$\begin{aligned} ber =& y + y + y + y \\ =& 4 \times \left(\frac{8\sin^2\theta \times (1 - \sin 2\theta) + 1}{16} \right) \\ =& \frac{8\sin^2\theta \times (1 - \sin 2\theta) + 1}{4}. \end{aligned} \tag{11}$$

又由于 $\varepsilon = \sin^2\theta$, 因此

$$ber = \frac{8\varepsilon(1-\varepsilon) + 1}{4}. \tag{12}$$

3.3 表达式和数据的分析

首先需要分析的是窃听者被检测的概率, 因为这对协议的安全性非常重要.

根据 2.1 节的改进 BB84 协议, 不管什么原因, 如果 $ber > \sigma_{\rm i}$, 那么量子信道就不再安全, 存在窃听者. 从图 2 可以看出, 当噪音水平 $\varepsilon \leqslant 0.68$, $ber \geqslant \sigma_{\rm i}$, Eve 会由于量子比特误码率的增加而被检测出来. 当 $\varepsilon = 0$, 表示信道中没有噪音. 此时如果有窃听者存在, 则量子比特误码率为 0.25; 如果没有窃听者存在, 则量子比特误码率为 0.

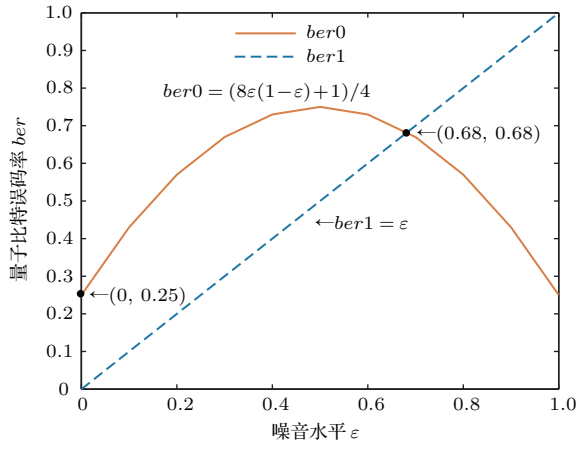

图 2 量子比特误码率和噪音水平的关系

Fig. 2. The relation of qubit error rate and noise level.

当噪音水平 $\varepsilon \geqslant 0.5$, 表明通信环境非常糟糕, 环境噪音使得量子比特传输极易产生错误. 因此选择通信信道时应避免这种信道, 对这种信道的安全性分析没有意义. 有一点需要注意, Eve 可能不会窃听所有的在量子信道传输的量子比特, 量子比特误码率体现在图 2 中的曲线、直线和纵坐标三条线形成的区域中. 正如图 1 所示, 有窃听的 BB84 协议过程可被分成两个部分: 第一部分等同于没有窃听时 Alice 和 Bob 的通信过程, 且第二部分造成的量子比特误码率必须为非负的. 这就是为什么量子比特误码率体现在上述区域中的原因, 且在该区域中窃听者也能被检测出来.

接下来考虑 Eve 能从截断重发攻击中窃取到多少信息量. 根据 (9) 式, 可得图 3. 从图 3 可看出, Eve 能窃取的信息量在 0.2 到 0.25 之间. 随着噪音水平 ε 增加, 窃取信息量 I(A, E) 呈现出三角波的形式.

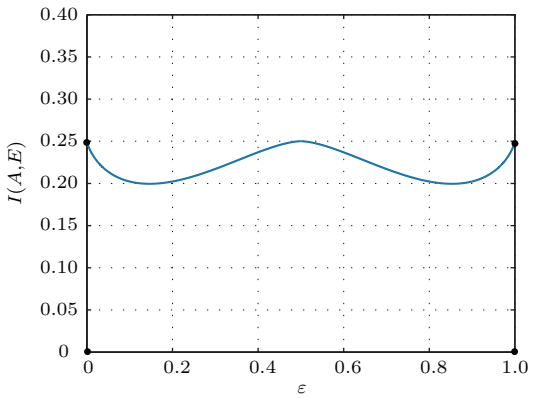

图 3 Eve 能窃取的最大信息量

Fig. 3. The maximal information Eve can gain.

4 结 论

从 3.3 节可以看出, 随着噪音水平 ε 增加, 当 $\varepsilon \leqslant 0.5$ 时, 量子比特误码率呈现增长趋势. 也就是说 Eve 想要窃听信道而不被检测出来是不可能的, 因为窃听会导致量子比特误码率 ber 的增加, 而没有窃听时 $ber0 = \varepsilon_{\rm i}$. 即使 Eve 只窃听部分量子比特, 仍然能被检测出来. 而且 Eve 能够窃取的最大信息量不超过 0.25, 也就是说 Eve 能窃取最多 1/4 的密钥信息. 但是这没有任何意义, 因为这将导致 Eve 的窃听行为被检测出来, 且得到的是不完整的密钥, 不是 Alice 和 Bob 的通信信息. Eve 被检测出来后, Alice 和 Bob 会放弃当前协商的密钥, 重新进

行密钥协商, 直至没有Eve窃听. 此时Alice 和Bob通信的密钥信息不会被任何第三方拥有, 他们间的通信信息也不会被任何第三方破译出来.

总而言之, 在联合旋转噪音信道上, BB84协议作为量子密钥分发协议是安全的. 本文证明了BB84协议同样可安全地适用于联合旋转噪音信道上. 协议能够保证密钥传输的安全性, 同样能确保使用该密钥传输消息的安全性. 本文的研究结果将为BB84协议在通信和信息处理领域的应用开辟新的视角.

参考文献

[1] Bennett C H, Brassard G 1984 *Theor. Comput. Sci.* **560** 175

[2] Bennett C H, Bessette F, Brassard G, Salvail L, Smolin J 1992 *J. Cryptology* **5** 3

[3] Muller A, Breguet J, Gisin N 1993 *Europhys. Lett.* **23** 383

[4] Boileau J C, Gottesman D, Laflamme R, Poulin D, Spekkens R W 2004 *Phys. Rev. Lett.* **92** 017901

[5] Gottesman D, Hoi-Kwong L, Lu kenhaus N, Preskill J 2002 *Quant. Inf. Comput.* **4** 325

[6] Watanabe S, Matsumoto R, Uyematsu T 2005 *Int. J. Quantum. Inf.* **4** 935

[7] Wang Y, Wang H D, Li Z H, Huang J X 2009 *Computer Science and Information Technology* Beijing, August 8–11, 2009 p438

[8] Aizan N H K, Zukarnain Z A, Zainuddin H 2010 *Network Applications Protocols and Services (NETAPPS)* Kedah, September 22–23, 2010 p130

[9] Winiarczyk P, Zabierowski W 2011 *CAD Systems in Microelectronics (CADSM)* Polyana-Svalyava, February 23–25, 2011 p23

[10] Buhari A, Zukarnain Z A, Subramaniam S K, Zainuddin H, Saharudin S 2012 *Industrial Electronics and Applications (ISIEA)* Bandung, September 23–26, 2012 p84

[11] Yang F, Hao Y J 2013 *Wavelet Active Media Technology and Information Processing (ICCWAMTIP)* Chengdu, December 17–19, 2013 p29

[12] Rostom R, Bakhache B, Salami H, *Awad A* 2014 *Mediterranean Electrotechnical Conference (MELECON)* Beirut, April 13–16, 2014 p350

[13] Halip N H M, Mokhtar M, Buhari A 2014 *Photonics (ICP)* Kuala Lumpur, September 2–4, 2014 p29

[14] Lucamarini M, Dynes J F, Frohlich B, Zhiliang Y, Shields A J 2015 *Select. Topics in Quantum Electron.* **21** 6601408

[15] Archana B, Krithika S 2015 *Electronics and Communication Systems (ICECS)* Coimbatore, February 26–27, 2015 p457

[16] Jasper R, Nicolas P, Ronald F 2015 *Broadband Coverage in Germany 9th ITG Symposium Proceedings* Berlin, Germany, April 20–21, 2015 p1

[17] Zhao N, Pei C X, Liu D, Quan D X, Sun X N 2011 *Acta Phys. Sin.* **60** 090307 (in Chinese) [赵楠, 裴昌幸, 刘丹, 权东晓, 孙晓楠 2011 物理学报 **60** 090307]

[18] Chen M J, Liu X 2011 *Chin. Phys. B* **20** 100305

[19] Zhou F, Yong H L, Li D D, Yin J, Ren J G, Peng C Z 2014 *Acta Phys. Sin.* **63** 140303 (in Chinese) [周飞, 雍海林, 李东东, 印娟, 任继刚, 彭承志 2014 物理学报 **63** 140303]

[20] Ma H Q, Wei K J, Yang J H, Li R X, Zhu W 2014 *Chin. Phys. B* **23** 100307

[21] Zhao L Y, Li H W, Yin Z Q, Chen W, You J, Han Z F 2014 *Chin. Phys. B* **23** 100304

[22] Ren C B, Xu Q L, Ren G Z 2003 *Comput. Eng. Appl. J.* **13** 177

[23] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2007 *Chin. Phys.* **16** 277

[24] Li X H, Deng F G, Zhou H Y 2008 *Phys. Rev.* **78** 022321

[25] Niu H C, Ren B C, Wang T J, Hua M, Deng F G 2012 *Internal J. Theor. Phys.* **51** 2346

[26] Nielsen M A, Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) chaper 8

[27] Zeng G H, Wang X M, Zhu H W 2000 *J. China Inst. Commun.* **21** 70

Security analysis of BB84 protocol in the collective-rotation noise channel*

Li Jian[1)2)3)] Chen Yan-Hua[1)†] Pan Ze-Shi[1)] Sun Feng-Qi[1)] Li Na[1)] Li Lei-Lei[1)]

1) (*School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China*)

2) (*Hefei National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Hefei 230026, China*)

3) (*Science and Technology on Communication Security Laboratory, Chengdu 610041, China*)

(Received 21 September 2015; revised manuscript received 20 October 2015)

Abstract

Most of quantum cryptography protocols are designed under the ideal conditions without considering the impact of noise in actual communication; thus they may result in that the confidential information cannot be transmitted to the receiver accurately or eavesdroppers can steal the confidential information by mixing in noise. Therefore, analyzing the security of quantum cryptography protocols under noise conditions is of great significance. For the purpose of analyzing the security of quantum BB84 protocol in collective-rotation noise, firstly this paper introduces the quantum BB84 protocol, and considers the influence of environmental noise on it. An explanation should be stated that in a noise environment, the effects of noise and eavesdropping cannot be distinguished between each other. So the mechanism for which the error bit is simply used as the criterion to judge whether there exists eavesdropping in the BB84 protocol, cannot be used in the noise environment. The mechanism to judge whether there exists eavesdropping in quantum noise channel needs to be modified and improved for protecting the information. An initial qubit error rate can be set according to the noisy quantum channel. If the qubit error rate σ of the quantum communication channel is larger than that, it can be determined that the quantum channel is not secure and exists eavesdropping, no matter what the reason is. And on this basis, the collective-rotation noise model will be established in quantum channel by using the particle deflection model and distinguish the noise from the eavesdropping in quantum channel quantitatively, and the relationship of the amount of information that eavesdroppers can steal, the quantum bits error rate and the noise level will be analyzed by using the von Neumann entropy. Finally, the noise critical point will be calculated by using the collective noise model and the relationship between the amount of information that eavesdroppers can steal, at the quantum bits error rate, and the noise level. Through the analysis, we can know that in the existing noise level, the most of the eavesdropping can steal 25% of the key from the communication. However, the Eve's eavesdropping behavior will be detected, so that Alice and Bob will give up the current consultation key, and restart the key negotiation. This result shows that the quantum BB84 protocol is safe and secure in the collective-rotation noise channel. The research results of this paper will enrich the theory of quantum cryptography, and the innovation of security detection methods in quantum cryptographic protocols will help promote the process of practical quantum cryptography.

Keywords: quantum security communication, collective-rotation noise, security analysis, quantum bit error rate

PACS: 03.67.–a, 03.67.Ac, 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.65.030302

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61472048, 61402058, 61370194), the Beijing Natural Science Foundation, China (Grant No. 4152038), and the China Postdoctoral Science Foundation Funded Project (Grant No. 2014M561826).

† Corresponding author. E-mail: cyanhua2010@bupt.edu.cn