量子 B92 协议在联合旋转噪音信道上的安全性分析

黎雷蕾1)，李剑1),\*

1) (北京邮电大学计算机学院, 北京 100876)

**摘要：**为了分析Bennett提出的量子B92协议的安全性，本文提出了一个较好的噪声分析模型。在安全性分析过程中，窃听行为能够通过量子比特误码率的增加而被发现。在不同的噪声水平下，若窃听方想获得相同的信息量，那么它将会导致通过过程中的误码率变大。在本文的分析中，窃听方最多只能在趋近于0.5时获取到31.1%的信息量，但是在获取信息的同时，窃听行为也会被检测出来。总之，我们证明了量子B92协议在用做量子密钥分发，是安全的。

**关键字：**量子B92协议，联合旋转噪音信道，安全性分析，量子比特误码率

# 1.介绍

密码学的目的是确保只有合法的用户Alice和Bob能够通过安全通信读取加密信息，并且未经授权的用户Eve无法读取。一直来，研究人员都致力开发可靠、安全的密码协议，随着信息技术和量子物理学的飞速发展量子密码学已经成为了一个重要而且具有极大吸引力的领域。

量子通信主要包括量子密钥分配(quantum key distribution, QKD)[1]，量子隐形传态(quantum teleportation, QT)[2]，量子密钥共享(quantum secret sharing, QSS)[3]，量子安全直接通信(quantum secure direct communication, QSDC)[4]，等。1984年，C.H. Bennett提出了第一个量子密钥分配协议，即BB84协议[5]，然而BB84协议需要粒子的四种状态，使得其很难被应用到实际生产中。1992年，Bennett创造性地提出了只需要两个非正交态的量子密钥分配方案，这个简洁的方案被称为B92协议[6]。B92提出的两台量子密钥分配协议相比于BB84，它需要的实验设备和实验步骤都比较简单，同时也具有更好的保密通信前景。该协议自从提出以来就备受关注，基于B92协议的信息安全处理方法也是层出不穷。[7-9,9-18]

然而这些方法仅仅处于理论分析状态，很少涉及实践中不可忽视的噪声。在现实的非孤立系统中，环境噪声必然会对量子态产生一定的影响。因此，在噪声环境下，协议的安全性分析至关重要。它可以为协议用于实际生产提供一定的理论基础。

本文提出了一个非常有效的联合旋转噪音分析模型，并利用该模型的信息理论分析了噪声环境下的量子B92协议[19,20]。在一定程度的噪声下，窃听方Eve永远都会被发现，其次，根据互信息理论[21]，Eve可获得的信息范围是在。可以得出结论是：在存在噪声环境下，量子B92协议是安全的，Eve只能获取少部分的密钥信息，以至于她无法获取完整的量子信息密钥，从而无法获取Alice和Bob之间通过量子密钥进行加密的通信信息。

# 2.相关工作

## 2.1 量子B92协议

首先我们先简单地介绍一下C.H. Bennett提出的B92协议[1]，发送者Alice随机地发送或者。其中代表比特0，代表比特1.

Alice通过量子信道向Bob发送相应地量子比特，众所周知，一般来说我们有两组基：Z基 和X基 ，在收到Alice传来的量子比特后，Bob随机地使用或者进行测量。如果用采用得到测量结果, Bob将其记录下来，如果用采用得到测量结果, Bob同样记录下来。其余的测量情况将会被忽略，一直重复这个过程直到通讯结束，如表一所示。

表一 Bob记录的信息

|  |  |  |
| --- | --- | --- |
| 基 | 测量结果 | 记录信息 |
|  |  |  |
|  |  |  |

当量子比特传输完毕，Bob将记录结果转化为0，1的序列，就可以将这个序列用作原始密钥。为了检测是否存在窃听的行为，Alice和Bob公开一部分原始密钥，如果存在误码，说明通信信道遭到窃听，Alice和Bob将终止这次通信，重新建立新的连接。

## 2.2 改进的量子B92协议

需要注意的是，在存在环境噪声的情况下，噪声和窃听造成的误码是无法相互区别的，量子比特误码率可能是由于他们之中任意一个引起的，也可能是它们两个共同作用的结果。

在原始的量子B92协议中，ber仅仅是由于窃听引起的，所以检测ber是否存在就可以判断通信过程中是否存在窃听者了。但是这个协议判断是否存在窃听的方法并不能用于有噪声的环境中，判断是否在噪声环境中存在窃听的方式需要进行改进，才能保护信息。

一个初始的量子比特误码率可以根据量子噪声信道进行设定。如果在通信过程中，量子比特误码率，不管是什么原因造成的，我们都可以认为量子信道存在窃听，是不安全的。

在本文中，ber代表的是原始的密钥比特错误率，在计算ber应该要注意，Bob可能会收到一些空的比特。

2.3 噪声水平

为了使得分析安全性变得简便，可以合理地假设环境噪声是恒定的。即使在实际应用中噪声是会改变的，但是以噪声的最大值作为分析安全性的上限也是合理的。

理想情况下，在联合旋转噪音信道中，噪声会对每个粒子产生相同的影响，从文献中可知[22-24]，噪声会对每个粒子造成一个向左或者向右的角度的偏转，这个影响可以看作如下的酉矩阵：

(1)

在联合信道噪声下，量子状态将会变成如下：

(2)

(3)

(4)

(5)

众所周知，如果没有噪声和Eve的攻击，Bob记录的结果不会出错，因此，该噪声可以定义为Bob记录的平均误差率。将会在下一节给出。

# 3. 量子B92协议在噪声环境下的安全性分析

## 3.1 没有窃听者

Alice以50%的概率随机地发送量子比特和，如果仅存在噪声，那么Bob的测量结果如表二所示；

表二 Bob测量结果。其中P代表发送的概率，A代表Alice、B代表Bob

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| P | A/B |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

考虑到下面情况：当Alice发送而Bob收到；当Alice发送而Bob收到，这意味着存在误码，因此原始密钥的比特错误率可以计算：

(6)

这意味着，当噪声信道中没有窃听时，量子比特错误率应为，根据2.2和2.3节，应该设置成。

(7)

## 3.2 存在窃听者

根据量子计算和量子信息理论，一个合理的假设是在中间人攻击前，噪声已经一次性地对每个粒子都产生了影响[21]，Eve得到的是噪声影响后的量子比特，如表二所示。现在让我们分析一下Eve最多能获取到多少信息，Eve获取的信息可以表示成平均互信息

(8)

由于Alice是随机发送量子比特信息，故:

(9)

根据表二可得:

(10)

根据噪声水平，最大获取的信息量可以改写成:

(11)

### 3.2.1 Eve直接发送测量结果时的错误率

在通信的过程中，Eve截取所有的量子位并且测量他们，在测量结束后，Eve重新直接将测量结果发送给Bob，或着根据测量结果重新制备或者量子比特并将其发送给Bob。

在3.2.1和3.2.2节，我们仅仅讨论噪声影响Alice和Eve。如果没有噪声影响Eve和Bob，那么Bob的接收到的结果可以由表三所示：

在3.2.3节，我们将讨论噪声同时影响Alice和Eve、Eve和Bob。

表三 Bob收到的粒子状态表（Bob和Eve之间无噪声）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| E/B |  |  |  |  |
|  |  | 0 |  |  |
|  | 0 |  |  |  |
|  |  |  |  | 0 |
|  |  |  | 0 |  |

在Bob测量结束后，他将记录下结果并且将其回发给Alice，通过表二和表三，Bob的测量结果可以背表示成表四：

表四 Bob测量结果。其中P代表发送的概率，E代表Eve、B代表Bob

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| P | E/B |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

上表中的概率在计算中并没有起到作用，我们可以忽略它们，通过商标我们可以计算出当前通行系统中的误码率():

(12)

在这种情况下，很明显地有。这说明Eve的测量将会导致Bob的后续测量产生了很大的误差，为了减少误码率，Eve应该选择推断Alice发送的粒子，从而重新制备粒子，而不是直接转发测量结果。

### 3.2.2 Eve重新制备粒子时的错误率

Eve知道Alice仅仅发送或者，为了减小误码率，如果Eve的测量结果不是或者，那么她将会改变量子比特的状态。

根据测量结果，Eve可以推断出Alice发出的粒子状态，忽略粒子测量前的噪声影响。在这种情况下，如果测量结果时,Eve可以认为Alice发送的是，如果测量结果是，那么Eve可以推断出发送的粒子是。根据这个推断，表二，可以改写成表五：

表五 Bob测量结果。其中P代表发送的概率，E代表Eve、B代表Bob

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| P | E/B |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

在计算时是不必要的，所以我们可以忽略它们。Eve 截取所有的量子比特然后测量他们。经过测量后，Eve准备新的量子比特然后将其发送给Bob。发送过程可以描述成表三，而Bob的测量结果可以描述成表五，我们可以计算出:

(13)

### 3.2.3 噪声环境下的进一步分析

3.2.1和3.2.2上面讨论的是噪声只存在于Alice和Eve之间，在本节我们将会考虑噪声在Alice和Eve、Eve和Bob之间。

这种情况下分析Alice到Eve之间的情况将会与3.2.2相同，如表二所示。

当噪声也存在于Bob和Eve之间是，在Eve截取量子比特后，他制备将要发送给Bob的过程可以被描述成表六：

表六 Bob收到的粒子状态概率表（Bob和Eve之间有噪声）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| E/B |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

类似于3.2.2和表五，根据表六，Bob的测量结果如表七所示：

表七 Bob测量结果。其中P代表发送的概率，E代表Eve、B代表Bob

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| P | E/B |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

在计算时是不必要的，所以我们可以忽略它们。我们可以计算出:

(13)

## 3.3 数据分析

我们可以得到的图像，如下图所示：

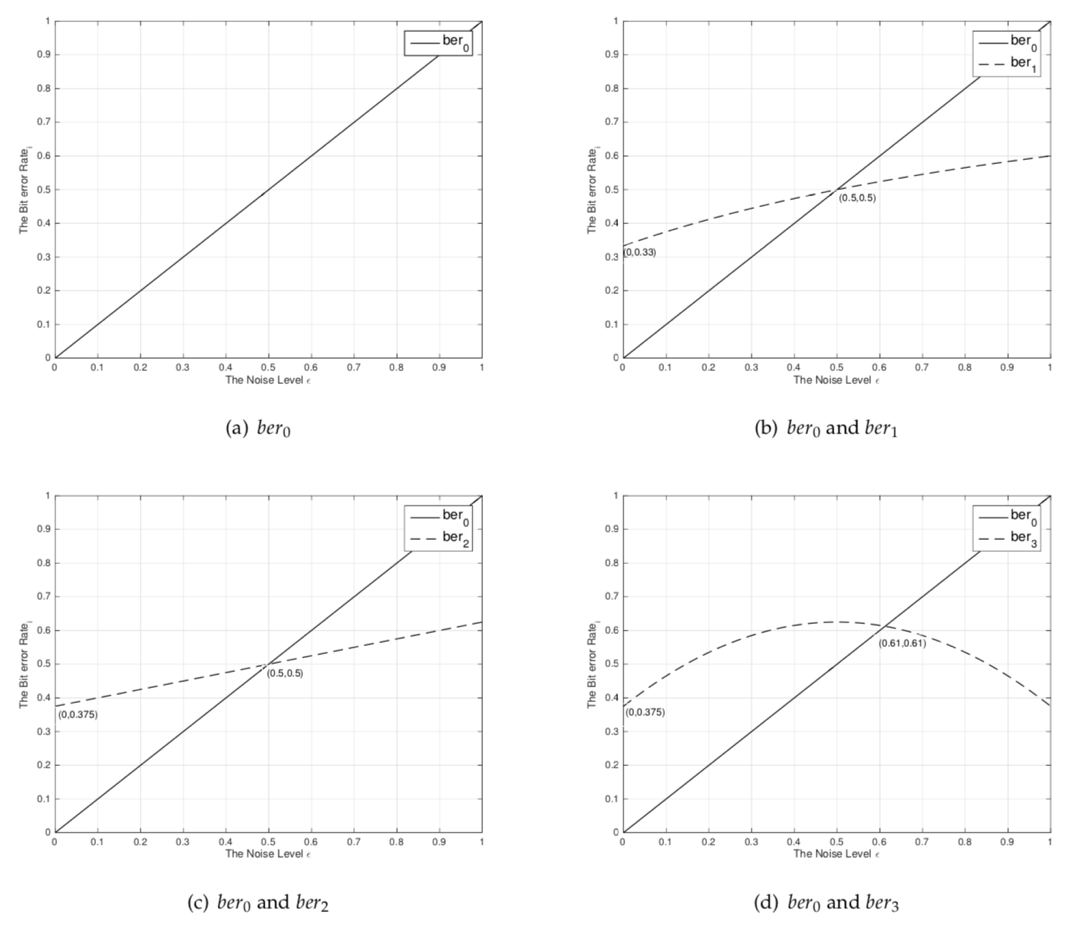


图 1 与的关系；其中是仅仅由环境噪声造成的误码率。是Eve截取转发量子比特造成的误码率；是Eve重新制备量子比特造成的误码率；两方均存在噪声时Eve窃听引起的误码率。

根据分析，最接近真实环境，当环境噪声水平时，有，这意味着Eve的窃听将会被检测出来。即使信道中没有噪声，Eve的攻击仍然会造成的误码率。当噪声环境水平时，意味着由于通信环境太差而无法检测到窃听，这时候应该避免通信，分析这种情况没有意义。

Eve能够获得的最大信息量如下图所示：

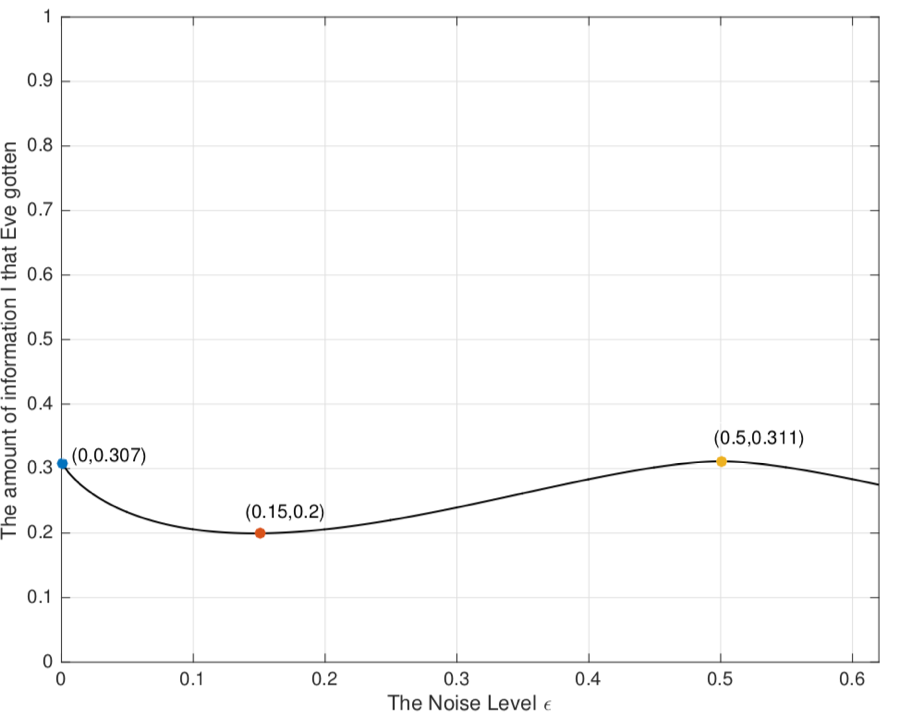


图 2 Eve获得的信息量与噪声水平之间的关系

从图2我们可以看出，当时，Eve可以获得最大信息量：，Eve至少可以获得的信息量为，当时，通信环境太差，双方应该放弃此次通信。在这里我们也不做讨论。

# 4 总结

从3.3节分析，在一定的噪声水平范围内，随着噪声水平的提高，误码率也跟着上升，对于Eve，她的窃听必然会导致误码率的上升，在不被发现的前提下窃听密钥信息是不可能的。从图2可知，Eve能够获取到的最大信息量为0.311，这表明Eve仅仅能获得Alice和Bob之间公共密钥的31.1%，而不是完整的密钥，这对于解密来说意义不大；并且为了获得密钥，也会导致她的窃听行为被检测出来。

总之，本文证明了量子B92协议作为量子密钥分配协议时安全的。换言之，该协议可以保护在信道中传输的密钥和通过密钥加密的信息。在理论分析量子B92协议的安全性的同时，我们还提出了一种分析噪声信道的安全性的新思路。

# 参考文献

1. C.H. Bennett, Physical Review Letters 68(21), 3121 (1992)
2. V.M. Rodney, V.M. Rodney, Quantum Key Distribution (2008)
3. D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, Nature  390(390), 575 (1997)
4. G. Guo, Proc Spie 59(3), 101 (2002)
5. C. Wang, F.G. Deng, G.L. Long, Optics Communications 253(1), 15 (2006)
6. C.H. Bennett, G. Brassard, Lecture Notes in Computer Science 196, 475 (1984)
7. A.D. Stojanovic, R.V. Ramos, P.S. Matavulj, Optical and Quantum Electronics 48(5),  1 (2016)
8. Y. Chang, S.B. Zhang, J.M. Zhu, Quantum Information Processing 16(3), 86 (2017)
9. S. Chen, L.V. Hongjun, G. Xie, Chinese Journal of Quantum Electronics (2016)
10. B.B. Su, Y.Y. Zhou, X.J. Zhou, in IEEE International Conference on Cloud Computing and Big Data Analysis (2016), pp. 189–192
11. R. Matsumoto, in IEEE International Symposium on Information Theory Proceedings (2014), pp. 351–353
12. Z. Quan, Acta Physica Sinica 51(7), 1446 (2002)
13. R. Matsumoto, pp. 351 – 353 (2013)
14. Z. Quan, T. ChaoJing, Z. ShenQiang, Acta Physica Sinica 51(7), 1439 (2002)
15. R. Etengu, F.M. Abbou, H.Y. Wong, A. Abid, N. Nortiza, A. Setharaman, Journal of  Optical Communications 32(1), 37 (2011)
16. L. Wan, Y. Huang, C. Huang, Physica B Condensed Matter 510, 22 (2017)
17. Y. Chang, S.B. Zhang, J.M. Zhu, Quantum Information Processing 16(3), 86 (2017)
18. Z.Zhiyong,W.Yanbo,H.Min,W.Jian,ChineseJournalofQuantumElectronics33(1),  44 (2016)
19. H.K. DONG, L. DONG, X.M. XIU, Y.J. GAO, International Journal of Quantum In-  formation 8(08), 1389 (2010)
20. M. Zou, G. Zhang, Proc Spie 5631, 181 (2005)
21. J. Li, Y.H. Chen, Z.S. Pan, F.Q. Sun, N. Li, L.L. Li, Acta Physica Sinica -Chinese  Edition- 65(3) (2016)
22. D. Fu-Guo, L. Xi-Han, L. Chun-Yan, Z. Ping, Z. Hong-Yu, Chinese Physics 16(2), 277  (2007)
23. X.H. Li, F.G. Deng, H.Y. Zhou, Phys. Rev. A 78, 022321 (2008)
24. H.C. Niu, B.C. Ren, T.J. Wang, M. Hua, F.G. Deng, International Journal of Theoretical  Physics 51(8), 2346 (2012)