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