第 22 卷 第 4 期
2005 年 12 月

原子核物理评论
Nuclear Physics Review

Vol. 22, No. 4
Dec., 2005

文章编号：1007－4627(2005)04－0382－05

量子安全直接通信研究进展*

邓富国[1,2,3,4]，周　萍[1,2,3]，李熙涵[1,2,3]，李春燕[1,2,3]，周宏余[1,2,3,4]

(1 北京师范大学射线束与材料改性教育部重点实验室，北京 100875；
2 北京师范大学低能核物理研究所，北京 100875；
3 北京师范大学材料科学与工程系，北京 100875；
4 北京市辐射中心，北京 100875)

摘　要：简要地介绍了量子安全直接通信的必要条件，初步介绍了两个量子安全直接通信模型，即 Two-Step 和 Quantum-One-Time-Pad 模型。

关 键 词：量子信息；量子通讯；安全直接通信；Two-step 协议；Quantum-One-Time-Pad 协议

中图分类号：O413.1　　**文献标识码**：A

1　引言

量子信息是最近 20 年发展起来的新型交叉学科，它主要包括量子计算与量子通信，是量子物理学与计算机科学、信息科学相结合的新研究领域。近 20 年来，这门学科无论在理论上还是在实验上，发展都相当迅速。特别是量子通信，它已被称为一门趋于应用的、相对成熟的量子技术，也因此引起了越来越多的部门和科学家的关注。

量子通信主要包括量子密钥分配(QKD)[1－9]、量子离物传态[10,11]、量子机密共享(QSS)[12－21]、量子密集的编码[22,23]和量子安全直接通信(QSDC)[24－37]等。通常把通信双方以量子态为信息载体，利用量子力学原理和各种量子特性，通过量子信道传输，在通信双方之间安全地无泄漏地直接传输有效信息，特别是机密信息的方法，称为量子安全直接通信。量子安全直接通信的概念是 2003 年提出的[24]。在此之前，Beige 等[25]提出了确定的安全通信，Bosrtöm 和 Felbinger[26]于 2002 年提出了一个非安全的安全直接通信模型。到目前已有一些量子安全直接通信的理论模型[24－37]。

2　量子安全直接通信的必要条件

量子安全直接通信作为一个安全的直接通信方式，它应该具有直接通信与安全通信这两大特点，因而它需要满足两个基本要求[24]：(1) 作为合法的接收者 Bob，当他接收到作为信息载体的量子态后，应该能直接读出发送者 Alice 发来的机密信息；对于携带机密信息的量子比特，Bob 不需要与发送者 Alice 交换另外的经典辅助信息。(2) 即使窃听者 Eve 监听量子信道，她也得不到任何机密信息，即她得到的只是一个随机的测量结果。

回顾 QKD，我们就会发现它之所以是一种安全的产生密钥的方式，其本质在于通信的双方 Alice 和 Bob 能够判断是否有人监听了量子信道，而不是窃听者不能监听量子信道。事实上，窃听者是否监听量子信道不是量子力学原理所能束缚的，量子力学原理只能保证窃听者不能得到量子信号的完备信息，使窃听行为会在接收者 Bob 的测量结果中有所表现，即会留下痕迹。由此 Alice 和 Bob 可以判断他们通过量子信道传输得到的量子数据是否可以用于经典一次一密。QKD 正是利用了这一特点来达到安全分配密钥的目的。而 QKD 的安全性分析是一种基于概率统计理论的分析，为此通信双方需要做随机抽样统计分析。QKD 的另一个特征在于 Alice 和 Bob 如果发现有人监听量子信道，那么他们可以抛弃已经传输的结果，从头开始传输量子

收稿日期：2005－08－22

* **基金项目**：国家自然科学基金资助项目(10447106)

作者简介：邓富国(1975－)，男(汉族)，湖南永州人，讲师，博士，从事量子信息、核物理以及生物物理研究；
E-mail：fgdeng@bnu.edu.cn

比特，直到他们得到没有人窃听量子信道的传输结果，这样他们不会泄漏机密信息。

既然量子安全直接通信传输的是机密信息本身，Alice 和 Bob 就不能简单地采用当发现有人窃听时抛弃传输结果的办法来保障机密信息不会泄漏给 Eve。由此，QSDC 的要求要比 QKD 高，使 Alice 和 Bob 必须在机密信息泄漏前就能判断窃听者 Eve 是否监听了量子信道，即能判断量子信道的安全性。量子通信的安全性分析都是基于抽样统计分析，因此，在安全分析前 Alice 和 Bob 需要有一批随机抽样数据。这就要求 QSDC 中的量子数据必需以块状传输[24]。只有这样，Alice 和 Bob 才能从块传输的量子数据中做抽样分析。

综合 QSDC 的基本要求可得，判断一个量子通信方案是否是一个真正的 QSDC 的 4 个基本依据是[24, 27]：(1) 除因安全检测的需要而相对于整个通信可以忽略的少量的经典信息交流外，接收者 Bob 接收到传输的所有量子态后可以直接读出机密信息，原则上对携带机密信息的量子比特不再需要辅助的经典信息交换；(2)既使窃听者监听量子信道，他也得不到机密信息，他得到的只是一个随机的结果，不包含任何机密信息；(3)通信双方在机密信息泄漏前能够准确判断是否有人监听量子信道；(4) 以量子态为信息载体的量子数据必需以块状传输。

3　量子安全直接通信实例

作为量子安全直接通信的实例，我们介绍一个基于纠缠光子对的 Two-Step 模型[24]和一个基于单光子序列的 Quantum-One-Time-Pad 模型[27]，其它模型限于篇幅，不再赘述。

3.1　Two-Step 量子安全直接通信协议

图 1 给出 Two-Step QSDC 原理示意图[24]，它借鉴了 Long-Liu 2002 QKD 方案[6]的一些物理思想[24]。在 Two-Step QSDC 模型中，信息发送者 Alice 制备一组由纠缠光子对组成的量子信号，即 N 个纠缠光子对，并使它们都处于相同的量子态，如量子态 $|\phi^+\rangle_{AB}=1/\sqrt{2}(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B)$，Bob 接收后将这 N 个纠缠光子对分成两个序列，即从每一纠缠光子对中挑出一个光子，再将所有挑出来的光子组成一个光子序列 S_A，而上述每一纠缠光子对中的另一个光子就可以组成另一个光子序列 S_B。如图 1 所示，用实线连接的两光子表示一纠缠光子对。我们不妨把 S_B 序列叫检测序列，把 S_A 序列叫信息序列[24]。

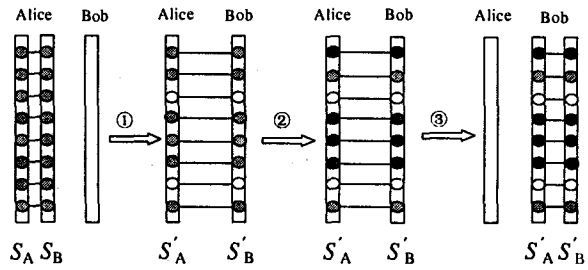

图 1　Two-Step QSDC 的原理示意图

Alice 先将检测序列 S_B 发送给信息接收方 Bob，但她仍然控制信息序列 S_A。Bob 接收到光子序列 S_B 后从中随机地抽取适量的光子，并对其进行单光子测量。这里的单光子测量原理与 BB84-QKD 方案[1]类似，即 Bob 随机地选择两组测量基 σ_z 和 σ_x 中的一组来对每一个抽样光子进行测量并记录测量基信息以及测量结果。测量完后，Bob 用经典信道(如无线电广播等不能被篡改在其中传输的经典信息的信道)告诉 Alice 他在 S_B 中对哪一些光子进行了单光子测量并告知相应的测量基信息及其测量结果。Alice 根据 Bob 所告知的所有信息，在 S_A 中用相同于 Bob 的测量基对与 Bob 的抽样光子相对应的光子(即属于同一纠缠光子对)进行单光子测量，并记录测量结果。Alice 将自己的测量结果与 Bob 所告知的测量结果进行比对，并做出错率分析；如果出错率比预先设定的安全阈值低很多，则表明光子序列 S_B 的传输是安全的，即可以认为没有窃听者监视量子信道；否则，Alice 和 Bob 放弃已经得到的传输结果。S_B 序列的传输主要是为了检测纠缠系统的传输安全，并没有对 S_B 做信息编码，即加载机密信息，这是我们称之为检测序列的主要原因[24]。

在确保检测序列 S_B 安全传输的情况下，Alice 根据自己所需传输的信息，每两比特位对应地选择 4 个幺正操作 $\{U_0=I, U_1=\sigma_z, U_2=\sigma_x, U_3=i\sigma_y\}$ 中的一个来对序列 S'_A(即在 S_A 中扣除用于安全性检测后的所有光子) 中的每一个光子依次做相应的幺正操作，从而完成对量子态的机密信息编码过程。这也是我们称 S_A 为信息序列的原因。4 个幺正操作 U_0，U_1，U_2 和 U_3 可以分别代表编码 00，01，10 和 11。当然，在编码过程中，Alice 需要在随机

的位置进行适量的安全检测编码，即加入一些为下一次安全检测服务的随机编码[24]。

随后，Alice 将编码后的 S'_A 序列发送给 Bob，Bob 对 S'_A 序列和与之对应的 S'_B 序列（即在 S_B 中扣除用于安全性检测后的所有光子）中对应的纠缠光子对做贝尔基联合测量，从而读出 Alice 所做的操作信息，即 Alice 对光子序列中的每一个光子分别采用了什么局域幺正操作，也就得到了 Alice 所需传输的机密信息。

为了检查 S'_A 序列的传输安全性，在量子态传输完后，Alice 告诉 Bob 她对哪一些纠缠粒子对进行了安全检测编码以及编码的数值；Bob 在其测量结果中挑出这一些检测编码数据，并与 Alice 告知的结果进行比对，分析出错率。实际上，这是 Alice 和 Bob 做第二次安全性分析。

事实上，在第一次安全分析成功的情况下，由于 Eve 无法同时得到光子序列 S_A 和 S_B，因而她已经无法得到机密信息。这是纠缠系统的量子特性局限了她对机密信息的窃听，纠缠量子系统的特性要求 Eve 只有对整个纠缠体系做联合测量才能读出 Alice 做的局域幺正操作。第二次安全性分析主要是为了判断窃听者是否在 S_A 序列传输过程破坏了 S_A 与 S_B 序列的量子关联性，从而判断是否值得对已经传输的结果做纠错等数据后处理。

3.2 Quantum-One-Time-Pad QSDC 协议

Quantum-One-Time-Pad QSDC 借鉴了经典一次一密中密钥完全随机的思想，也继承了 Two-Step QSDC 中的量子数据块状传输的思想[27]。如果能在通信双方 Alice 和 Bob 之间安全地共享一串量子态，那么 Alice 就可以在量子态上加载机密信息。如果对 Eve 而言量子态是完全随机的，那么这样的机密信息加载从原理上讲具有与一次一密一样的安全性，即绝对安全。

与 Two-Step QSDC 类似，Quantum-One-Time-Pad QSDC 需要分 3 步完成[27]：(1) Alice 和 Bob 之间安全地共享一串量子态，即共享一串处于不同偏振状态的光子，我们不妨称之为创建一串量子密钥；(2)在量子密钥上做机密信息加载并加入冗余信息，我们称之为对机密信息用量子密钥加密得到量子密文；(3)机密信息的发送方 Alice 将量子密文发送给接收方 Bob，Bob 解密量子密文并做安全性分析。

Quantum-One-Time-Pad QSDC 的实验原理如图 2 所示[27]。图中的 SR 表示量子态存储器(或光学延迟装置)，CE 表示安全检测过程，Switch 是控制开关，由 CM，M1 和 M2 组成的装置完成机密信息加载与量子信号返回量子信道的功能。

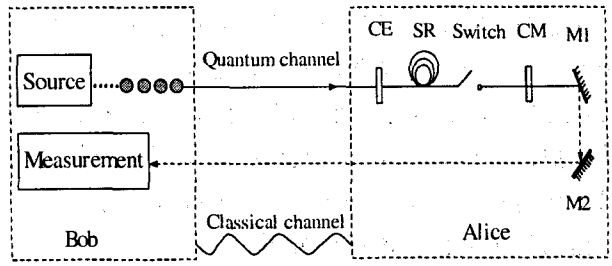

图 2 Quantum-One-Time-Pad QSDC 的实验原理图

在 Quantum-One-Time-Pad QSDC 中，机密信息的接收方 Bob 制备一串单光子序列 S，并将 S 中的每一个光子的量子态随机地制备成 $|H\rangle=|0\rangle$，$|V\rangle=|1\rangle$，$|u\rangle=1/\sqrt{2}(|0\rangle+|1\rangle)$ 或 $|d\rangle=1/\sqrt{2}(|0\rangle-|1\rangle)$。它们分别是测量基 σ_z 和 σ_x 的本征态。Bob 将光子序列 S 发给 Alice，Alice 先存储光子序列，然后从 S 中随机地抽取一些光子作为抽样数据进行安全检测测量，即可以类似于 BB84-QKD 方案[1]随机地选择 σ_z 或 σ_x 对光子进行测量，从而完成第一次安全检测。这一过程是一个创建安全量子密钥的过程。

如果通信双方 Alice 和 Bob 能够确定在 S 光子序列传输过程中没有人监听量子信道，那么他们就共享了一串量子态。不同于经典密码的地方在于：Alice 并没有对这一串共享的光子做测量，因而她不知道这一串光子的量子态。如果他们不能判断 S 光子序列的传输安全性，他们只能放弃他们得到的传输结果，与 QKD 一样经过经典处理后[5]，从头开始新的光子串传输。

为了能让 Bob 准确地得到 Alice 加载到光子上的机密信息，Alice 对共享的光子序列 S 的编码不宜改变测量基信息，详细原理参考文献[9, 27]。因而 Alice 可以选择两个不改变测量基信息的量子幺正操作 I 和 $i\sigma_y$ 来完成对光子序列的信息编码，然后将光子序列 S 发回给 Bob，由他做单光子测量来读出 Alice 的编码信息。这两个幺正操作可以分别代表编码 0 和 1，从而与经典的机密信息一一对应。

类似于 Two-Step QSDC 方案，为了检测光子序列 S 从 Alice 返回 Bob 过程的安全性，Alice 需要多加入一些冗余编码，即随机地在 S 序列中选择一些光子并随机地选择量子操作 I 和 $i\sigma_y$ 完成冗余编码[27]。

4　结论与讨论

由于量子信道中存在的噪声和损耗，量子安全直接通信也需要进行量子机密放大处理。在量子密钥分配中，最后的测量结果是确定的经典信息，因此作为后处理的机密放大处理可以是一个完全经典的过程，即可以通过对传输后得到的裸码进行机密放大，从而蒸馏出一些安全的随机二进制串[5]。但量子安全直接通信传输的是机密信息本身，因而不能简单地使用经典中的机密放大处理方法。对于基于纠缠对的量子安全直接通信模型所需要的量子机密放大可以用量子纠缠纯化来完成[24]。对基于单光子的 QSDC[27]，我们最近也设计了一个量子机密放大处理方法，见文献[28]。总之，从原理上讲，量子安全直接通信是完全可能做到非常的安全。

最近，人们根据量子离物传态和量子纠缠转移等量子技术设计了一些 QSDC 模型[31—36]，与以上两个模型相比，它们大都需要大量的经典信息交换，更接近一些特殊的 QKD 模型，当然这些QSDC模型也有一些很好的优点，譬如借助于量子态存储器使需要传输量子态的距离变得更短等。

参　考　文　献：

[1] Bennett C H, Brassad G. Proc IEEE Int Conf on Computers, Systems and Signal Processing, Bangalore, India. New York: IEEE, 1984, 175.

[2] Ekert A. Phys Rev Lett, 1991, **67**: 661.

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

[4] Bennet C H. Phys Rev Lett, 1992, **68**: 3 121.

[5] Gisin N, Ribordy G, Tittel W, *et al*. Rev Mod Phy, 2002, **74**: 145.

[6] Long G L, Liu X S. Phys Rev, 2002, **A65**: 032302.

[7] Zhang Y S, Li C F, Guo G C. Phys Rev, 2001, **A64**: 024302.

[8] Deng F G, Long G L. Phys Rev, 2003, **A68**: 042315.

[9] Deng F G, Long G L. Phys Rev, 2004, **A70**: 012311.

[10] Bennett C H, *et al*. Phys Rev Lett, 1993, **70**: 1 895.

[11] Deng F G, Li C Y, Li Y S, *et al*. Phys Rev, **A** (accepted).

[12] Hillery M, Bužek V, Berthiaume A. Phys Rev, 1999, **A59**: 1 829.

[13] Karlsson A, Koashi M, Imoto N. Phys Rev, 1999, **A59**: 162.

[14] Deng F G, Zhou H Y, Long G L. Phys Lett, 2005, **A337**: 329.

[15] Xiao L, Long G L, Deng F G, *et al*. Phys Rev, 2004, **A69**: 052307.

[16] Guo G P, Guo G C. Phys Lett, 2003, **A310**: 247.

[17] Deng F G, Long G L, Zhou H Y. Phys Lett, 2005, **A340**: 43.

[18] Deng F G, Long G L, Wang Y, *et al*. Chin Phys Lett, 2004, **21**: 2 097.

[19] Zhang Z J, Li Y, Man Z X. Phys Rev, 2005, **A71**: 044301.

[20] Li Y M, Zhang K S, Peng K C. Phys Lett, 2004, **A324**: 420.

[21] Deng F G, Zhou H Y. Phys Rev, **A** (accepted).

[22] Bennett C H, Wiesner S J. Phys Rev Lett, 1992, **69**: 2 881.

[23] Liu X S, Long G L, Tong D M, *et al*. Phys Rev, 2002, **A65**: 022304.

[24] Deng F G, Long G L, Liu X S. Phys Rev, 2003, **A68**: 042317.

[25] Beige A, Englert B G, Kurtsiefer C, *et al*. Acta Phys Pol, 2002, **A101**: 357.

[26] Boström K, Felbinger T. Phys Rev Lett, 2002, **89**: 187902.

[27] Deng F G, Long G L. Phys Rev, 2004, **A69**: 052319.

[28] Deng F G, Long G L. e-print quant-ph/0408102.

[29] Wang C, Deng F G, Li Y S, *et al*. Phys Rev, 2005, **A71**: 044305.

[30] Cai Q Y, Li B W. Chin Phys Lett, 2004, **21**: 601.

[31] Gao T. Z Naturforsch, 2004, **A59**: 597.

[32] Gao T, Yan F L, Wang Z X. Nuovo Cimento, 2004, **B119**: 313.

[33] Yan F L, Zhang X Q. Eur Phys J, 2004, **B41**: 75.

[34] Man Z X, Zhang Z J, Li Y. Chin Phys Lett, 2005, **22**: 18.

[35] Gao T, Yan F L, Wang Z X. Chin Phys, 2005, **14**: 893.

[36] Zhang Z J, Man Z X, Li Y. Phys Lett, 2004, **A333**: 46.

[37] Xue P, Guo G C. J Phys, 2004, **B37**: 711.

Progress on Study of Quantum Secure Direct Communication*

DENG Fu-guo[1,2,3,4], ZHOU Ping[1,2,3], LI Xi-han[1,2,3],
LI Chun-yan[1,2,3], ZHOU Hong-yu[1,2,3,4]

(1 *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing* 100875, *China*;
2 *Institute of Low Energy Nuclear Physics, Beijing Normal University, Beijing* 100875, *China*;
3 *Department of Material Science and Engineering, Beijing Normal University, Beijing* 100875, *China*;
4 *Beijing Radiation Center, Beijing* 100875, *China*)

Abstract: The requirements of quantum secure direct communication (QSDC) are briefly introduced. Two QSDC schemes i. e. , the Two-Step QSDC scheme and the Quantum-One-Time-Pad QSDC scheme, are discussed in brief.

Key words: quantum communication; secure direct communication; secure direct commurication; Two-Step scheme; Quantum-One-Time-Pad-schem

(上接第 372 页)

Anomalous Diffusion: Directional Passing over the Saddle Point of a Potential**

BAO Jing-dong

(*Department of Physics, Beijing Normal University, Beijing* 100875, *China*)

Abstract: Directional transport of a particle in a non-Ohmic environment passing over the saddle point of a potential is considered and the analytical expression of the passing probability is obtained. Our results has shown that both overshooting and backflow are observed in the case of subdiffusion. This is a possible for understanding slow increasing of the fusion probability with the center-of-mass energy.

Key words: anomalous diffusion; passing probability; overshooting; backflow

* **Foundation item**: National Natural Science Foundation of China(10447106)

** **Foundation item**: National Natural Science Foundation of China(10235020, 10075007); Project of Trans-century Training Programmer Foundation for the Talents, Ministry of Education, China