第 57 卷 第 12 期 2008 年 12 月
1000-3290/2008/57(12)/7452-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.12,December,2008
©2008 Chin. Phys. Soc.

多方控制的量子安全直接通信协议的分析及改进*

王天银[1)2)†] 秦素娟[1)] 温巧燕[1)] 朱甫臣[3)]

1)(北京邮电大学网络与交换技术国家重点实验室,北京 100876)

2)(洛阳师范学院数学科学学院,洛阳 471022)

3)(现代通信国家重点实验室,成都 610041)

(2008 年 4 月 25 日收到;2008 年 5 月 24 日收到修改稿)

对一种多方控制的量子安全直接通信协议(WCZT 协议)进行了安全性分析,并利用隐形传态给出了一种新的攻击方法.利用该攻击方法,接收方可以在没有征得任何控制方同意的情况下获得发送方的消息,因此该协议是不安全的.对该协议进行了改进,分析表明改进后的协议能够抵抗这种攻击,可以满足多方控制的量子安全直接通信的目的.

关键词:隐形传态,单光子,多方控制,量子安全直接通信

PACC:0365,4230,4250

1. 引 言

信息系统安全的核心是如何保证信息在系统中的机密性、认证性和完整性,这也是密码学当前和今后相当长一个时期的重要研究课题[1].经典密码体制的安全性大都是基于某些数学难题,然而随着计算机的飞速发展,破译经典密码的难度逐渐降低,特别是目前量子计算机的研究以及一些量子算法的提出[2],对现有的密码体制形成了严峻的挑战,同时也掀起了量子密码学研究的热潮.国内外学者及专家对量子密码进行了深入的研究和探讨,取得了丰富的研究成果[2—27].目前量子密码的研究主要包括量子密钥分配(QKD)[3—11]、量子安全直接通信(QSDC)[12—18]、量子秘密共享[19—24]以及量子数字签名[25—27]等方面.

QKD 即通信双方以量子态为信息载体,利用量子力学原理在通信双方之间建立无条件安全的共享密钥. 然而,在某些特殊情况下需要直接安全传递消息.QSDC 可以实现秘密消息的直接传送而不需要首先建立密钥再对秘密消息进行加密,因而 QSDC 在最近几年得到了迅速发展,许多 QSDC 协议被提出[12—18].

最近,王剑等[16]基于单光子序列秘密顺序重排提出了一种多方控制的量子安全直接通信协议,即 WCZT 协议.该协议可以应用于某些特殊的加密任务,发送方通过量子信道将秘密消息发送给接收方,但是接收方必须征得所有控制方的同意才能恢复出发送方的秘密消息.WCZT 协议使用单光子,实现较为简单且具有较高的效率,因此 WCZT 协议具有一定的应用前景和理论价值.本文利用隐形传态的思想给出了一种新的伪信号替换攻击方法.利用该攻击方法,接收方可以在没有征得任何一个控制方同意的情况下获得发送方的消息,因此 WCZT 协议并没有达到多方控制的目的.为了抵抗这种攻击,本文对 WCZT 协议进行了改进,并对改进后的协议进行了分析.

2. WCZT 协议

假设分区经理 Bob 想要将他的秘密消息直接传给总经理 Alice,Bob 同时要求 Alice 征得所有董事(Charlie, Dick,…,York, Zack)的同意,才能得到秘密消息,同时假定协议中的控制方都是诚实的.

* 国家高技术研究发展计划(批准号:2006AA01Z419)、国家自然科学基金重大研究计划(批准号:90604023,60873191)、现代通信国家重点实验室基金(批准号:9140C1101010601)、北京市自然科学基金(批准号:4072020)、河南省教育厅自然科学基金(批准号:2007120007,2008B120005)和洛阳师范学院青年基金资助的课题.

† E-mail:yinwang790720@yahoo.com.cn

WCZT 协议的具体过程分为 6 步进行.

过程 1　Alice 制备一个包含 n 个光子的有序光子序列$P = [P_1, P_2, \cdots, P_n]$，序列中的每个光子随机地处于以下 4 个态之一：$|0\rangle$，$|1\rangle$，$|+\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle)$，$|-\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle)$，然后将 P 序列发送给 Charlie.

过程 2　收到 P 序列后，Charlie 首先对序列中的每一个光子随机地选择 I 或 U 进行变换，然后再随机选择 I 或 H 对光子再进行变换.这里

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|,$$

$$U = |0\rangle\langle 1| - |1\rangle\langle 0|,$$

$$H = \frac{\sqrt{2}}{2}(|0\rangle\langle 0| - |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|).$$

Charlie 做完变换后，将 P 序列发送给 Dick，Dick 用同样的方法对 P 序列进行变换，然后再发送给下一个控制方.以此类推，直到 Zack 完成了他对 P 序列的操作后，将 P 序列发送给 Bob.

过程 3　Bob 从 P 序列中选取一个充分大的子集用于窃听检测（C 序列），其他光子构成消息编码序列（M 序列）.Bob 对 C 序列中的每一个光子随机地执行 I 或 U 操作，然后再根据秘密消息的比特值 0 或 1 对 M 序列中的每一个光子执行相应的 I 或 U 操作，从而将秘密消息编码在 M 序列的光子上.

过程 4　执行完随机操作和编码操作后，打乱检测序列和编码序列中光子的顺序，产生一个新的光子序列 $P' = [P'_1, P'_2, \cdots, P'_n]$，然后将 P' 序列发送给 Alice.

过程 5　在确认 Alice 收到 P' 序列后，Bob 首先公布检测序列的位置以及该序列中光子的秘密排列顺序，接着让 Alice 公布检测序列中光子的初态.为防止 Alice 的截取重发攻击，对于每一个采样光子，Bob 随机地选择一个控制方先公布他的 H 操作信息，然后再依次选择其他的控制方公布他们的 H 操作信息，根据控制方公布的信息，Alice 能够选择正确的测量基对采样光子进行测量.测量后，Alice 将她的测量结果告诉 Bob.对于每一个采样光子，Bob 随机地选择一个控制方公布他的 I 和 U 操作信息，再依次选择其他的控制方公布他们的 I 和 U 操作信息.然后 Bob 判断 P 序列在传输过程中产生的错误率，若错误率低于预先设定的门限，就继续执行下一步，否则协议中止.

过程 6　Bob 公布 M 序列中光子的秘密排列顺序，若控制方同意 Alice 恢复 Bob 的秘密消息，则公布他们对 M 序列光子的操作信息.根据公布的信息，Alice 就能够选择正确的测量基对 M 序列的光子进行测量，从而得到 Bob 的秘密消息.

3. WCZT 协议分析

下面介绍本文给出的利用隐形传态思想进行的伪信号替换攻击.

1）当所有控制方对 P 序列按照 WCZT 协议的方法操作完毕后，在过程 2 中当 Zack 传送给 Bob 时，Alice 把 P 序列截获.接着制备 n 个 EPR 对 $|\psi^-\rangle = \frac{\sqrt{2}}{2}(|01\rangle - |10\rangle)_{12}$ 的直积态$\otimes_{i=1}^{n}|\psi_i^-\rangle$，并将所有的 EPR 对 $|\psi_i^-\rangle$（$i = 1, 2, \cdots, n$）中的第一个光子 $p_1^1, p_2^1, \cdots, p_n^1$ 作为 P 序列发送给 Bob，而自己留下$\otimes_i^n|\psi_i^-\rangle$中第二个光子 $p_1^2, p_2^2, \cdots, p_n^2$.

2）Alice 待 Bob 对替换后的 P 序列编码消息并公布消息序列的正确位置和顺序，她将 Bob 编码后传过来的光子（EPR 对中的第一个光子）和手中对应的 EPR 对中的第二个光子进行联合贝尔基测量.若测得结果为原来的态 $|\psi^-\rangle$，则可得出 Bob 做了 I 操作，否则为 U 操作，从而可以成功恢复消息.

当 Bob 公布检测光子的位置和顺序后，Alice 首先将 EPR 对中的第二个光子和截获的 P 序列中对应位置的光子进行联合贝尔基测量.根据测量的结果，对 Bob 传过来的 EPR 对中的第一个光子进行相应的 Pauli 变换（表 1）.

表 1　EPR 对中光子的 Pauli 变换

测量结果	$\|\varphi^+\rangle$	$\|\varphi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
Pauli 变换	$i\sigma_y$	σ_x	σ_z	I

由隐形传态理论可知，若 Bob 对检测光子进行的是 I 操作，进行上述操作后，显然 EPR 对中第一个光子的态刚好就是所有控制方和 Bob 对 P 序列中对应位置光子操作后的态.若 Bob 对检测光子进行的是 U 操作，这一结论也成立.

不失一般性，假定经过所有控制方操作后，P 序列中某个光子的态为 $(\alpha|0\rangle + \beta|1\rangle)_3$，Alice 在过程 2 中用 EPR 对 $|\psi^-\rangle = \frac{\sqrt{2}}{2}(|01\rangle - |10\rangle)_{12}$ 的第一个光子对该光子进行替换.在 Alice 未进行替换攻击的情况下，光子 $(\alpha|0\rangle + \beta|1\rangle)_3$ 的态最后应为

$(\beta|0\rangle-\alpha|1\rangle)_3$.在 Alice 进行伪信号替换攻击的情况下,检测光子的载体由光子$(\alpha|0\rangle+\beta|1\rangle)_3$变为对应的 EPR 对中的第一个光子,而 Alice 可以将对应的 EPR 对中第一个光子变为$\beta|0\rangle-\alpha|1\rangle$.

由我们的攻击方法可知,Bob 对光子$\alpha|0\rangle_3+\beta|1\rangle_3$进行的 U 变换,实际作用在 EPR 对$|\psi^-\rangle=\frac{\sqrt{2}}{2}(|01\rangle-|10\rangle)_{12}$中第一个光子上,所以经过 Bob 操作后,由 EPR 对$|\psi^-\rangle$和检测光子$\alpha|0\rangle_3+\beta|1\rangle_3$组成的复合系统为

$$
\begin{aligned}
&-\frac{\sqrt{2}}{2}(|00\rangle+|11\rangle)_{12}\otimes(\alpha|0\rangle+\beta|1\rangle)_3\\
&=-\frac{1}{2}[(\alpha|0\rangle+\beta|1\rangle)_1\otimes|\varphi^+\rangle_{23}\\
&\quad+(\alpha|0\rangle-\beta|1\rangle)_1\otimes|\varphi^-\rangle_{23}\\
&\quad+(\beta|0\rangle+\alpha|1\rangle)_1\otimes|\psi^+\rangle_{23}\\
&\quad+(\beta|0\rangle-\alpha|1\rangle)_1\otimes|\psi^-\rangle_{23}]\\
&=-\frac{1}{2}[\mathrm{i}\sigma_y(\beta|0\rangle-\alpha|1\rangle)_1\otimes|\varphi^+\rangle_{23}\\
&\quad-\sigma_x(\beta|0\rangle-\alpha|1\rangle)_1\otimes|\varphi^-\rangle_{23}\\
&\quad+\sigma_z(\beta|0\rangle-\alpha|1\rangle)_1\otimes|\psi^+\rangle_{23}\\
&\quad+I(\beta|0\rangle-\alpha|1\rangle)_1\otimes|\psi^-\rangle_{23}].
\end{aligned}
$$

因此,此时进行联合贝尔基测量并进行相应 Pauli 变换后,EPR 对中第一个光子的态也刚好就是所有控制方和 Bob 对原来 P 序列中光子$\alpha|0\rangle_3+\beta|1\rangle_3$操作后的态.Alice 总可以把经过所有控制方和 Bob 变换后的检测光子的未知态成功地传递到对应 EPR 对中第一个光子上.这样 Alice 就可以利用 EPR 对中第一个光子作为检测光子进行过程 5 中的窃听检测,并且不会引入任何错误,从而成功地躲避窃听检测.

上述攻击没有考虑 Bob 对光子序列的顺序打乱,事实上打乱顺序对上述攻击是无效的.因为在检测窃听和恢复消息前,Bob 要公布检测光子序列和编码光子序列的正确位置和顺序,所以打乱顺序对于 Alice 的攻击是没有作用的.

4. WCZT 协议的改进

下面对 WCZT 协议进行少许改进,从而可以避免本文提出的攻击.

1) 在过程 1 中,将 P 序列的制备由 Alice 改为 Bob.

2) 在过程 2 中,所有控制方的操作由 I 或 U 两种改为 $I,\sigma_x,\mathrm{i}\sigma_y,\sigma_z$四种.

3) 收到 P 序列后,Bob 首先进行窃听检测.方法如下:首先,Bob 从 P 序列中随机选取一个充分大的子集作为检测光子集.接着,对所有的检测光子随机进行 X 或 Z 基测量.然后,公布检测光子的位置(但不公布检测结果)并要求所有控制方公布他们的操作信息.最后,Bob 判断 P 序列传输过程中产生的错误率,若错误率低于预先设定的门限,继续执行下一步,否则协议中止.

4) Bob 用 WCZT 协议的编码方法对剩下的光子序列进行编码,并随机选择 l' 个光子(随机地处于过程 1 中四种态之一)随机插入编码序列以进行窃听检测,组成一个新的光子序列 $P'=[P'_1,P'_2,\cdots,P'_{n'}]$,然后将 P'序列发送给 Alice.

5) 在确认 Alice 收到 P'序列后,Bob 首先公布检测光子的位置,然后 Alice 和 Bob 利用 BB84 协议的窃听检测方法进行窃听检测,若错误率低于他们预先设定的门限,Bob 公布消息序列中每一个光子的初始态,否则协议中止.

6) 若所有控制方都同意 Alice 恢复 Bob 的秘密消息,则控制方公布他们的操作信息.根据公布的操作信息和 Bob 公布的消息序列中光子的初始态,Alice 就能够选择正确的测量基对消息序列的光子进行测量,从而得到 Bob 的秘密消息.

5. 改进后的协议分析

由以上所述可知,所有控制方的幺正操作由 WCZT 协议中的 I 或 U 两种操作改为 $I,\sigma_x,\mathrm{i}\sigma_y,\sigma_z$,这样再经过幺正操作 I 或 H 后,就变为八种幺正操作.如果这八种幺正操作分别作用在任何一个单粒子态或任何纠缠态的一个粒子上,则该量子态将变为八种不可能完全正交的态,因此不可能正确区分.这样做的目的是为了抵抗类似文献[21,22]所给出的伪信号的 EPR 对攻击.可是仅进行这样的改进仍然不能抵抗本文提出的利用隐形传态思想进行的伪信号替换攻击,所以也做了一些改进.Bob 在编码前首先对光子进行类似 BB84 的窃听检测方法,保证光子在编码前没有被进行替换,从而防止了本文提出的攻击.最后,Alice 和 Bob 可以检测编码后的光子是否受到攻击,若受到攻击就可被检测到,这时 Alice得不到消息,攻击者也得不到消息,但破坏了这

次通信.

6. 结　论

本文对 WCZT 协议进行了安全性分析，并利用隐形传态给出了一种新的伪信号替换攻击方法.利用该攻击方法，接收方可以在不征得任何控制方同意的情况下成功获得发送方的消息，从而证明了 WCZT 协议是不安全的.最后对 WCZT 协议进行了改进，并证明了改进后的协议可以抵抗本文提出的攻击.

[1] Schneier B 1996 *Applied Cryptography*：*Protocols*，*Algorithms*，*and Source Code in C*（New York：Wiley）

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

[3] Bennett C H，Brassard G 1984 *Proceedings IEEE of International Conference on Computers*，*Systems and Signal Processing*（New York：IEEE Press）p175

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

[5] Ekert A K 1991 *Phys*. *Rev*. *Lett*. **67** 661

[6] Yang L，Wu L A，Liu S H 2002 *Acta Phys*. *Sin*. **51** 2446（in Chinese）[杨　理、吴令安、刘颂豪 2002 物理学报 **51** 2446]

[7] Long G L，Liu X S 2002 *Phys*. *Rev*. A **65** 032302

[8] He G Q，Yi Z，Zhu J，Zeng G H 2007 *Acta Phys*. *Sin*. **56** 6427（in Chinese）[何广强、易　智、朱　俊、曾贵华 2007 物理学报 **56** 6427]

[9] Yang Y G，Wen Q Y，Zhu F C 2007 *Chin*. *Phys*. B **16** 910

[10] He G Q，Guo H B，Li Y D，Zhu S W，Zeng G H 2008 *Acta Phys*. *Sin*. **57** 2212（in Chinese）[何广强、郭红斌、李昱丹、朱思维、曾贵华 2008 物理学报 **57** 2212]

[11] Mi J L，Wang F Q，Lin Q Q，Liang R S 2008 *Chin*. *Phys*. B **17** 1178

[12] Bostrom K，Felbinger T 2002 *Phys*. *Rev*. *Lett*. **89** 187902

[13] Deng F G，Long G L，Liu X S 2003 *Phys*. *Rev*. A **68** 042317

[14] Deng F G，Long G L 2004 *Phys*. *Rev*. A **69** 052319

[15] Wang J，Zhang Q，Tang C J 2006 *Phys*. *Lett*. A **358** 256

[16] 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]

[17] Song J，Zhu A D，Zhang S 2007 *Chin*. *Phys*. B **16** 621

[18] Man Z X，Xian Y J 2007 *Chin*. *Phys*. B **16** 1197

[19] Hillery M，Buzek V，Berthiaume A 1999 *Phys*. *Rev*. A **59** 1829

[20] Guo G P，Guo G C 2003 *Phys*. *Lett*. A **310** 247

[21] Deng F G，Li X H，Zhou H Y，Zhang Z J 2006 *Phys*. *Rev*. A **73** 049901

[22] Qin S J，Gao F，Wen Q Y，Zhu F C 2006 *Phys*. *Lett*. A **357** 101

[23] Yang Y G，Wen Q Y，Zhu F C 2006 *Acta Phys*. *Sin*. **55** 3255（in Chinese）[杨宇光、温巧燕、朱甫臣 2006 物理学报 **55** 3255]

[24] Li Y，Zeng G H 2007 *Chin*. *Phys*. B **16** 2875

[25] Lee H，Hong C，Kim H，Lim J，Yang H J 2004 *Phys*. *Lett*. A **321** 295

[26] Zeng G H，Keitel C H 2002 *Phys*. *Rev*. A **65** 042312

[27] Yang Y G 2008 *Chin*. *Phys*. B **17** 415

Analysis and improvement of multiparty controlled quantum secure direct communication protocol *

Wang Tian-Yin[1)2)†] Qin Su-Juan[1)] Wen Qiao-Yan[1)] Zhun Fu-Chen[3)]

1)(*State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

2)(*School of Mathematical Science*, *Luoyang Normal University*, *Luoyang* 471022, *China*)

3)(*National Laboratory for Modern Communications*, *Chengdu* 610041, *China*)

(Received 25 April 2008; revised manuscript received 24 May 2008)

Abstract

The security of a multiparty controlled quantum secure direct communication protocol (WCZT protocol) is analyzed and a new attack with teleportation is advanced. Using this attack, the receiver can gain access to the sender's secret message without the permission of any controller; therefore, this protocol is not secure. An improved version of this protocol is proposed and the security analysis shows that the improved protocol can resist the said attack and thus the goal of multiparty controlled quantum secure communication is warranted.

Keywords: teleportation, single photon, multiparty controlled, quantum secure direct communication

PACC: 0365, 4230, 4250

* Project supported by the National High Technology Development Program of China (Grant No. 2006AA01Z419), the Major Program of the National Natural Science Foundation of China (Grant Nos. 90604023, 60873191), the Scientific Research Foundation of National Laboratory for Modern Communications, China (Grant No. 9140C1101010601), the Natural Science Foundation of Beijing, China (Grant No. 4072020), the Natural Science Foundation of the Education Bureau of Henan Province, China (Grant Nos. 2007120007, 2008B120005) and the Youth Foundation of Luoyang Normal University, China.

† E-mail: yinwang790720@yahoo.com.cn