基于 Bell 态与 Two-qutrit 态无信息泄漏的量子对话协议*

王鹤[1,2],张玉清[2],胡予濮[1],田养丽[1,2],朱珍超[1,2]
(1. 西安电子科技大学 计算机网络与信息安全教育部重点实验室,陕西 西安 710071;
2. 中国科学院研究生院 国家计算机网络入侵防范中心,北京 100049)

摘 要:基于 Einistein-Podolsky-Rosen 纠缠对与量子安全直接通信(QSDC),提出了一个新的基于 Bell 态的量子对话协议。通信双方 Alice 和 Bob 只需要进行一次通信即可实现双方之间秘密的同时交换。该方案利用一个随机比特串和检测光子来实现安全性,能够抵抗截获/重放攻击、特洛伊木马攻击和纠缠攻击等典型攻击。很多近期提出的协议中存在严重的信息泄漏,也就是说任何窃听者都可以从合法通信者的公开声明中提取到部分秘密信息,我们的方案很好地克服了这一问题。协议的效率较高,可以达到66.7%,同时由于纠缠态粒子只需要进行一次传输,该方案更简单易行。将该协议推广到 two-qutrit 态,其安全性仍能得到保证。

关键词:量子对话;Bell 态;Bell 测量;广义 Bell 态
中图分类号:TN918.1 **文献标志码**:A **文章编号**:1001-2486(2012)02-0010-04

Two quantum dialogue schemes based on Bell states and two-qutrit entangled states without information leakage

WANG He[1,2], *ZHANG Yuqing*[2], *HU Yupu*[1], *TIAN Yangli*[1,2], *ZHU Zhenchao*[1,2]
(1. Key Lab of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China;
2. National Computer Network Intrusion Protection Center, Graduate University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: Drawing on the idea of the quantum secure direct communication (QSDC), a novel quantum dialogue scheme based on Bell states is presented in this paper. The proposed scheme can realize authorized parties' secure exchange of their respective secret messages simultaneously only through one communication. In this scheme, a random bit string and checking particles are used to ensure the security; the scheme is secure against eavesdropper's commonly used attacks, such as intercept/resend attack, Trojan horse attack and entanglement attack. A serious problem called "information leakage" or "classical correlation" is found in some quantum dialogue protocols, namely, any eavesdropper can elicit some information about the secret from the classical communication of the legal users. Fortunately, our protocol can discard the drawback "information leakage". In addition, our protocol possesses high efficiency 66.7% and is feasible. Finally, the protocol is applied to the scheme based on two-qutrit entangled states with a secure communication.

Key words: Quantum dialogue; Bell states, Bell measurement, Generalized Bell states

与量子密钥分发(QKD)不同,量子安全直接通信(QSDC)不需要通信双方提前建立密钥[1-2],而是利用量子信道直接传输消息。根据信息的载体不同,可将量子安全直接通信协议分类,例如:基于单光子的和基于纠缠态粒子的协议。然而,QSDC 只能实现单向通信。随着 QSDC 的发展,双向 QSDC[3] 在 2004 年被提出,通信双方可以同时交换彼此的秘密消息,因此也称为量子对话。随后,研究者提出了大量量子对话协议,遗憾的是,在这些量子对话协议中存在严重的信息泄漏(或经典关联)缺陷。

1 基于 Bell 态的量子对话协议

1.1 方案具体过程

首先列出 4 个 Bell 态:

$$|\psi_{00}\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$
$$= \frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle) \quad (1)$$

* 收稿日期:2011-07-28
基金项目:国家自然科学基金资助项目(60970140)
作者简介:王鹤(1987—),女,河南安阳人,博士研究生,E-mail:wanghe666@163.com;
张玉清(通信作者),男,教授,博士,博士生导师,E-mail:zhangyq@gucas.ac.cn

$$|\psi_{01}\rangle = |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$$
$$= \frac{1}{\sqrt{2}}(|+\rangle|-\rangle + |-\rangle|+\rangle) \quad (2)$$
$$|\psi_{10}\rangle = |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$$
$$= \frac{1}{\sqrt{2}}(|+\rangle|+\rangle - |-\rangle|-\rangle) \quad (3)$$
$$|\psi_{11}\rangle = |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$$
$$= \frac{1}{\sqrt{2}}(|-\rangle|+\rangle - |+\rangle|-\rangle) \quad (4)$$

其中,$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$。Alice 和 Bob 事先商定这些 Bell 态分别代表 00, 01, 10, 11。假设 Alice 有 N 比特的秘密消息 $m_A = \{a_1, a_2, \cdots, a_N\}$, Bob 的秘密消息为 $m_B = \{b_1, b_2, \cdots, b_M\}$, $a_n, b_m \in \{0,1\}$, $n = 1, \cdots, N$; $m = 1, \cdots, M$。不失一般性,令 $M = N$。

1.1.1　制备量子态

Alice 根据一个随机比特串 $\{k_1, k_2, \cdots, k_N\}$, $k_i \in \{0,1\}$ 和其秘密消息制备 Bell 态序列 $M_A = \{|\psi_{k_1 a_1}\rangle, |\psi_{k_2 a_2}\rangle, \cdots, |\psi_{k_N a_N}\rangle\}$。为了检测窃听,Alice 同时准备两组单光子序列作为样本集合,这些样本光子足够抵御窃听者的统计分析,分别记为 S_1 与 S_2。样本集合中的每个光子均随机处于 $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ 四个量子态中之一。接着 Alice 将这些光子随机插入 M_A 序列中。记录样本光子所在的位置和初始态,最后将 $M_A + S_1 + S_2$ 发送给 Bob。

1.1.2　窃听检测

在确定 Bob 收到 $M_A + S_1 + S_2$ 之后,Alice 和 Bob 进行以下窃听检测过程:

(1) Alice 公布 S_1 中每个光子所在的位置,Bob 随机选取测量基($\{|0\rangle, |1\rangle\}$)或($\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$),对每一个光子进行测量并公开测量基和测量结果。Alice 通过比较测量结果可以确定量子信道中是否存在窃听,如果错误率超过一定的阈值,放弃通信;否则进入下一子步骤。

(2) Alice 公布 S_2 序列中每个光子所在的位置和量子态,Bob 根据 Alice 的声明选取适当的测量基对每个光子进行测量。通过对比测量结果与 Alice 的声明,Bob 可以确定信道中是否存在窃听。如果存在窃听,终止通信;否则继续。通信过程如图 1 所示,图中黑色小球代表 Bell 态的粒子,白色小球和虚线球分别代表 S_2 与 S_1 中的粒子,用实线相连的小球表示处于 Bell 态,虚线相连的小球表示不处于 Bell 态。

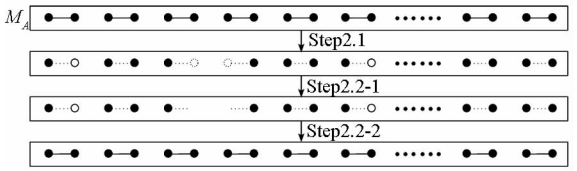

图 1　基于 Bell 态的量子对话过程

Fig. 1　Illustration of quantum dialogue scheme by using Bell states

1.1.3　实现双向通信

(1) 确定信道的安全性之后,Bob 丢弃掉 S_1, S_2 中的粒子并对剩余的粒子进行测量,由测量结果可得到 Alice 的秘密消息和随机比特串 $\{k_1, k_2, \cdots, k_N\}$, $k_i \in \{0,1\}$。

(2) 由(1)中的测量结果、自己的秘密信息与表 1(Alice 和 Bob 之前商定),Bob 公布一个比特串 $\{b'_1, b'_2, \cdots, b'_N\}$。例如,若他的测量结果为 011011……,其秘密消息为 100……,则 Bob 公布 010……。表 1 中的第一行为 Alice 制备的量子态,第一列为 Bob 的秘密消息。

表 1　Alice 制备的量子态、Bob 的秘密与 Bob 的公开消息之间的关系

Tab. 1　Relations of states that Alice prepared, Bob's secret and Bob's statements

	$\|\psi_{00}\rangle$	$\|\psi_{01}\rangle$	$\|\psi_{10}\rangle$	$\|\psi_{11}\rangle$
0	0	1	1	0
1	1	0	0	1

(3)根据 Bob 公布的信息与自己制备的量子态,通过表 1,Alice 可以得出 Bob 的秘密消息。

至此,基于 Bell 态的量子对话协议描述完毕,现在通过一个简单的例子加以说明。假如 Alice 与 Bob 的秘密消息分别为 10010110 与 00101110,首先,Alice 用随机数生成器生成一个随机比特串 01110100,之后制备 Bell 态 $|\psi_{01}\rangle|\psi_{10}\rangle|\psi_{10}\rangle|\psi_{11}\rangle|\psi_{00}\rangle|\psi_{11}\rangle|\psi_{01}\rangle|\psi_{00}\rangle$,在得到序列 0110101100110100 后,根据自己的秘密消息和表 1,Bob 公布序列 11001100。Bob 可以得到 Alice 的秘密消息 10010110;与此同时,Alice 根据 Bob 公布的信息和自己制备的量子态可以得到 Bob 的秘密消息 00101110。

1.2 效率分析

我们提出了一个新的基于 Bell 态的量子对话协议。在之前的基于 Bell 态的协议[7-8]中,一般是 Alice(Bob)先发送纠缠态粒子中的一个给 Bob(Alice),Bob(Alice)根据其秘密信息进行相应操作之后,把该粒子序列回发给 Alice(Bob)。我们提出的方案中只需要一次粒子传输,Alice 一次将所有的纠缠态粒子发送给 Bob。这样减少了窃听的可能性,并且简单易行。下面分析该方案的效率,采用 Cabello 在文献[13]中对效率的定义:$\eta = \frac{b_s}{q_t + b_t}$,其中 b_s, q_t, b_t 分别代表可接收到的比特数、通信所用的量子比特数以及 Alice 和 Bob 交换的经典比特数。在我们方案中,b_s, q_t, b_t 分别等于 2, 2, 1, 因此效率为 66.7%。在基于 QKD&OTP 实现的协议中,即便是在 QKD 中,要传输 2 比特的秘密消息,也需要 2 比特量子信息与 2 比特经典信息,效率只有 50%。显然,我们的方案在效率上具有优势。

2 基于 two-qutrit 纠缠态的方案

上节提出的方案可直接推广到 two-qutrit 纠缠态的情况。假设通信双方 Alice 和 Bob 分别有 N 比特秘密消息需要进行交换,具体实施步骤如下:

2.1 制备量子态

假设 Alice 的秘密为 $m_A = \{a_1, a_2, \cdots, a_N\}$, $a_i \in \{0,1,2\}$, Bob 的秘密消息为 $m_B = \{b_1, b_2, \cdots, b_N\}$, $b_j \in \{0,1,2\}$。Alice 制备 N 对纠缠态 $M_A = \{|\psi_{00}^1\rangle, |\psi_{00}^2\rangle, \cdots, |\psi_{00}^N\rangle\}$,上标代表粒子在序列中的位置,$|\psi_{00}^i\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$, $i = 1,2,\cdots,N$。之后 Alice 根据自己的秘密消息和一个随机比特串 $\{k_1, k_2, \cdots, k_N\}$, $k_i \in \{0,1,2\}$,对 $|\psi_{00}^i\rangle$ 进行幺正操作 $U_{k_i a_i}$。Alice 与 Bob 约定幺正操作 $U_{k_i a_i}$ 分别代表秘密消息 $k_i a_i, k_i, a_i \in \{0,1,2\}$。

$$U_{mn} = \sum_{j=0}^{2} e^{2\pi i j m/3} |j + n \bmod 3\rangle\langle j| \quad (5)$$

$$|\psi_{mn}^i\rangle = \frac{1}{\sqrt{3}} \sum_{j=0}^{2} e^{2\pi i j n/3} |j\rangle \otimes |j + n \bmod 3\rangle \quad (6)$$

显然,U_{mn} 将 $|\psi_{00}^i\rangle$ 转换为 $|\psi_{mn}^i\rangle$,即 $U_{mn}|\psi_{00}^i\rangle = |\psi_{mn}^i\rangle$。经过这些操作后,$M_A$ 序列转变为 $M'_A = \{|\psi_{k_1 a_1}^1\rangle, |\psi_{k_2 a_2}^2\rangle, \cdots, |\psi_{k_N a_N}^N\rangle\}$。为了检测量子信道的安全性,Alice 准备足够长的单光子序列 S'_1 和 S'_2,这些单光子随机地处于六个量子态 $|0\rangle$, $|1\rangle$, $|2\rangle$, $\frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$, $\frac{1}{\sqrt{3}}(|0\rangle + e^{2\pi i/3}|1\rangle + e^{4\pi i/3}|2\rangle)$, $\frac{1}{\sqrt{3}}(|0\rangle + e^{4\pi i/3}|1\rangle + e^{2\pi i/3}|2\rangle)$ 中之一。之后 Alice 将 S'_1 和 S'_2 中的单粒子随机插入 M'_A 序列中,记录其初始状态和插入位置,并将 $M'_A + S'_1 + S'_2$ 发送给 Bob。

2.2 窃听检测

在确认 Bob 收到 $M'_A + S'_1 + S'_2$ 之后,通信双方 Alice 与 Bob 进行如下窃听检测:

(1) Alice 公布 S'_1 中粒子所在的位置,Bob 随机选取测量基 $\{|0\rangle, |1\rangle, |2\rangle\}$ 或者 $\{\frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), \frac{1}{\sqrt{3}}(|0\rangle + e^{2\pi i/3}|1\rangle + e^{4\pi i/3}|2\rangle), \frac{1}{\sqrt{3}}(|0\rangle + e^{4\pi i/3}|1\rangle + e^{2\pi i/3}|2\rangle)\}$ 对每个粒子进行测量,公布测量基和测量结果。通过对比公布的测量结果和自己的记录,Alice 可以确定信道中是否存在窃听。如果错误率超过一定的阈值,通信终止;否则进入下一个子步骤。

(2) Alice 公布 S'_2 中每个粒子所在的位置及其量子态,Bob 选择合适的测量基进行测量,通过对比 Alice 公布的量子态和测量结果,Bob 可以确定信道中是否存在窃听。

2.3 实现双向通信

(1) 在确认信道安全之后,Bob 依次对剩余的粒子进行测量,可以得出 Alice 所进行的幺正操作,从而得到 Alice 的秘密消息 $\{a_1, a_2, \cdots, a_N\}$ 和随机比特串 $\{k_1, k_2, \cdots, k_N\}$。

(2) 根据(1)的测量结果和表 2,Bob 公布消息 $\{b'_1, b'_2, \cdots, b'_N\}$。

表 2 Alice 所做的幺正操作,Bob 的秘密与 Bob 声明消息的关系

Tab. 2 Relations of unitary operation that Alice performed, Bob's secret and Bob's statements

	U_{00}	U_{01}	U_{02}	U_{10}	U_{11}	U_{12}	U_{20}	U_{21}	U_{22}
0	0	1	2	1	2	0	2	0	1
1	1	2	0	2	0	1	0	1	2
2	2	0	1	0	1	2	1	2	0

(3) 根据 Bob 的声明和自己所做的幺正操作,Alice 通过表 2 可恢复出 Bob 的秘密消息。

3 安全性分析

安全性是量子通信的一个重要因素。我们所

提出的基于 Bell 态的量子对话协议的安全性基于 1.1.1 节与 1.1.2 节,攻击者 Eve 可采取的典型攻击方式包括截获/重放攻击、特洛伊木马攻击以及纠缠攻击。下面给出针对这些攻击方式的详细分析过程。基于 two-qutrit 的方案的安全性分析与此类似。

截获/重放攻击:假设 Eve 截获了 Alice 发送的 $M_A + S_1 + S_2$,测量每一对粒子之后,Eve 根据测量结果重新发送一个光子序列给 Bob。由于 Eve 不知道单光子所在的位置,Eve 的测量破坏了 Alice 所制备 Bell 态的纠缠性。因此这种攻击将在窃听检测的时候被检测出来,Eve 也无法获得任何信息。

特洛伊木马攻击:特洛伊木马攻击有两种攻击方式,由 Cai 等提出的不可见光子攻击和由 Li 等提出的延迟光子攻击。在 Bob 的所有装置之前添加一个滤波器(这种滤波器只允许波长接近于所操作粒子的波长的光子通过),就可以抵抗不可见光子特洛伊木马攻击。为了抵抗延迟光子特洛伊木马攻击,可在系统中引入光子数目分割器(PNS: 50/50),将每个信号分割成两份。

纠缠攻击:在混合光子序列到达 Bob 之前,通过纠缠引诱光子,Eve 可能窃取部分信息。Eve 制备一个 Bell 态序列,并截获由 Alice 发送的光子序列,将两个光子序列进行纠缠操作之后发送给 Bob。对于量子远程传态,在 Bell 态光子中编码的秘密信息可以转变为 Eve 传送给 Bob 的 Bell 态粒子对中的传送光子,当然这样就会造成扰动。由于 Eve 不知道单光子的位置,因此他不能推导出 Alice 的秘密消息。

在基于 Bell 态的量子对话协议中,Bob 只公布了 1 比特的消息。例如,对 $|\psi_{k_1a_1}\rangle$ 来说,Bob 在最后公布 b'_1,然而 Eve 由于不知道 $|\psi_{k_1a_1}\rangle$ 的初始状态,所以不能获得任何秘密信息。假设 Bob 最后公布的消息是 $b'_1 = 0$,如果 Eve 猜测初始状态为 $|\psi_{k_1a_1}\rangle = |\psi_{00}\rangle$,那么秘密消息为 $a_1 = 0, b_1 = 0$;若猜测 $|\psi_{k_1a_1}\rangle = |\psi_{01}\rangle$,则秘密消息为 $a_1 = 1, b_1 = 1$;若猜测 $|\psi_{k_1a_1}\rangle = |\psi_{10}\rangle$,则秘密消息为 $a_1 = 0, b_1 = 1$;若猜测 $|\psi_{k_1a_1}\rangle = |\psi_{11}\rangle$,则秘密消息为 $a_1 = 1, b_1 = 0$。显然,有 4 种不确定性,相当于 $-\sum p_i \log_2 p_i = -4 \times \frac{1}{4}\log_2 \frac{1}{4} = 2$ 比特的秘密信息,即最大的不确定性,也就是 2 比特的秘密消息 a_1, b_1 都是安全的。这就说明我们提出的方案中不存在信息泄露。同样对于基于 two-qutrit 的方案,Bob 公布 1 比特信息 b'_i,Eve 不知道 U_{mn},也就不能得到任何秘密信息。假设 Bob 公布的为 0,Eve 猜测 $U_{mn} = U_{00}$,则秘密消息为 $a_i = 0, b_i = 0$。一共有 9 种不确定性,相当于 $-\sum p_i \log_2 p_i = -9 \times \frac{1}{9}\log_2 \frac{1}{9} > 2$ 比特的秘密信息。因此该方案中也不存在信息泄露。

4　总结

提出了分别基于 Bell 态与 two-qutrit 纠缠态的量子对话协议,这两个协议均能实现通信双方的秘密通信;能抵抗攻击者的典型攻击,如截获/重放攻击、特洛伊木马攻击和纠缠攻击;方案中不存在信息泄漏。因为粒子在通信双方之间只需要进行一次传输,所以所提出的协议更简单易行。

参考文献(References)

[1] Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. Physical Review A, 2002, 65(3): 032302.

[2] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing [C]// Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1884: 175 - 179.

[3] Nguyen B A. Quantum dialogue [J]. Physics Letters A, 2004, 328(1): 6 - 10.

[4] Man Z X, Zhang Z J, Li Y. Quantum dialogue revisited [J]. Chinese Physics Letters, 2005, 22(1): 22 - 24.

[5] Ji X, Zhang S. Secure quantum dialogue based on single-photon [J]. Chinese Physics, 2006, 15(7): 1418 - 1420.

[6] Yang Y G, Wen Q Y. Quasi-secure quantum dialogue using single photons [J]. Science in China Series G, 2007, 50(5): 558 - 562.

[7] Shi G F, Xi X Q, Tian X L, et al. Bidirectional quantum secure communication based on a shared private Bell state [J]. Optics Communications, 2009, 282(12): 2460 - 2463.

[8] Shi G F. Bidirectional quantum secure communication scheme based on bell states and auxiliary particles [J]. Optics Communications, 2010, 283(24): 5275 - 5278.

[9] Gao F, Guo F Z, Wen Q Y, et al. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication [J]. Science in China Series G, 2008, 51(5): 559 - 566.

[10] Tan Y G, Cai Q Y. Classical correlation in quantum dialogue [J]. International Journal of Quantum Information, 2008, 6(2): 325 - 329.

[11] Cai Q Y, Li B W. Deterministic secure without using entanglement [J]. Chinese Physics Letters, 2004, 21(4): 601 - 603.

[12] Li C Y, Zhou H Y, Wang Y, et al. Secure quantum key distribution network with Bell states and local unitary operations [J]. Chinese Physics Letters, 2005, 22(5): 1049 - 1052.

[13] Cabello A. Quantum key distribution in Holevo limit [J]. Physical Review Letters, 2000, 85(26): 5635 - 5638.