基于 GHZ 态的量子密钥分发协议*

江英华，张仕斌†，昌　燕，杨　帆，邵婷婷
（成都信息工程大学 信息安全工程学院，成都 610225）

摘　要：在用户与用户进行量子密钥分发的时候，随着用户数量的增加，用户之间需要建立大量的量子传输信道。针对减少量子传输信道数量问题进行了研究，设计了一种基于 GHZ 态的量子密钥分发协议。该协议由第三方进行粒子分配，利用三粒子 GHZ 态在 Z 基和 X 基下具有不同的表示特性作为密钥分发的关键点来实现密钥分发，大大减少了量子信道的数量。经过安全性分析表明协议能抵御截获重发攻击、中间人攻击和纠缠攻击，而作为第三方可以是不可信的。

关键词：量子密钥分发；GHZ 态；纠缠特性；X 基；第三方
中图分类号：TN918.1　　**文献标志码**：A　　**文章编号**：1001-3695(2018)03-0889-03
doi:10.3969/j.issn.1001-3695.2018.03.052

Quantum key distribution protocol based on GHZ state

Jiang Yinghua, Zhang Shibing†, Chang Yan, Yang Fan, Shao Tingting
(*College of Information Security Engineering*, *Chengdu University of Information Technology*, *Chengdu* 610225, *China*)

Abstract: As the number of users increases, between users need to set up a large number of quantum transmission channel when the quantum key is distributed. Based on the problem of reducing the number of quantum transmission channels, this paper proposed a quantum key distribution protocol based on GHZ state. The protocol by the third party for the particle distribution. By using three-particle GHZ states under the Z and X had the characteristics of different representations as a key point to realize key distribution, greatly reduced the number of the quantum channel. Through security analysis, this protocol can resist intercepted retransmission attacks, man-in-the-middle attacks, and entangled attacks, and can be untrusted as a third part.
Key words: quantum key distribution; GHZ state; entanglement property; X basis; third part

0　引言

随着量子计算机和分布式计算的发展，传统的密码安全受到巨大的挑战。由于量子具有独特的性质能保证信息的安全，于是研究者们纷纷把目光投向了量子密钥分发（quantum key distribution，QKD）。QKD 的安全性是由量子力学中的海森堡测不准原理、量子不可克隆定理、纠缠粒子的关联性和非定域性等物理特性来保证的。1984 年，Bennett 等人[1]利用单光子的偏振态共同研发了世界上第一个 QKD（BB84 协议）；1992 年，Bennett[2]又提出了使用非正交单光子比特来实现的 QKD（B92 协议）；1991 年，英国牛津大学的 Ekert[3]首次提出利用 Bell 态纠缠特性的 QKD；1992 年 Bennett 等人[4]对 Ekert 的方案进行改进，使之更加简洁，即不使用 Bell 态来实现 QKD。随着量子技术的快速发展，量子身份认证 QIA（quantum identity authentication）也逐渐发展起来[5~7]。与此同时，量子秘密共享 QSS（quantum secret sharing）[8~12]和量子隐私比较 QPC（quantum private comparison）[13~15]也在快速发展中。在应用方面，量子密钥分发可以与身份认证[16]进行结合，将分发之后的密钥（按照协议，密钥为一个二进制字符串）作为分发双方的一个合法的身份 ID，在进行身份认证的时候，双方只需要将各自手中的二进制字符串与对方的二进制字符串作一个简单的同或运算，根据结果就可以识别身份，这样的设计同样可以应用在身份识别的智能卡[17]之中。

传统 QKD 是点对点的密钥分发，用户数为 n 时，用户 U_1 与其他 $n-1$ 个用户进行密钥分发会需要 $n-1$ 条量子信道。当 n 名用户中的任意两名用户需要量子密钥分发时，总共需要 $n!$ 条量子传输信道，结构如图 1 所示。随着用户数的增加，用户之间需要的量子信道会急速增加，这样增加了网络结构复杂度，也极大地提高了成本。基于这个原因，本文设计了一种具有第三方 TP（third part）为其他两名用户进行密钥分发的协议，结构如图 2 所示。这样的设计大大减少了用户之间的量子传输信道，降低了复杂度，同时也减少了成本，具有很大的实际意义。

1　基本原理

Z 基的 $|0\rangle$ 和 $|1\rangle$ 在 X 基的表达式为

收稿日期：2016-11-29；**修回日期**：2017-01-10　**基金项目**：国家自然科学基金资助项目（61572086，61402058）；四川省量子安全通信团队资助项目（sc2016009）

作者简介：江英华（1989-），男，重庆璧山人，硕士研究生，主要研究方向为量子安全通信；张仕斌（1971-），男（通信作者），重庆丰都人，教授，博士，主要研究方向为量子安全通信、网络空间安全（cuitzsb@cuit.edu.cn）；昌燕（1979-），女（蒙古族），内蒙古人，副教授，博士，主要研究方向为量子密码、信息安全；杨帆（1985-），男，四川绵阳人，讲师，博士，主要研究方向为量子安全通信；邵婷婷（1991-），女，山东菏泽人，硕士研究生，主要研究方向为量子安全通信.

$$|0\rangle=\frac{1}{\sqrt{2}}(|+\rangle+|-\rangle),|1\rangle=\frac{1}{\sqrt{2}}(|+\rangle-|-\rangle) \tag{1}$$

X 基的$|+\rangle$和$|-\rangle$在 Z 基的表达式为

$$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),|-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \tag{2}$$

处于 Z 基下的三粒子 GHZ 态的 $\varphi=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}$,在 X 基下的表示方式如下:

$$\varphi=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}=\frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0\rangle+|1\rangle|1\rangle|1\rangle)_{123}=$$

$$\frac{1}{\sqrt{2}}\left(\begin{array}{l}\frac{1}{2}(|+\rangle|+\rangle+|+\rangle|-\rangle+|-\rangle|+\rangle+|-\rangle|-\rangle)\times\frac{1}{\sqrt{2}}(|+\rangle+|-\rangle)+\\ \frac{1}{2}(|+\rangle|+\rangle-|-\rangle|+\rangle-|+\rangle-\rangle+|-\rangle|-\rangle)\times\frac{1}{\sqrt{2}}(|+\rangle-|-\rangle)=\end{array}\right)$$

$$\frac{1}{\sqrt{2}}\left(\begin{array}{l}\frac{1}{2\sqrt{2}}(|+\rangle|+\rangle+|+\rangle|-\rangle+|-\rangle|+\rangle+|-\rangle|-\rangle)(|+\rangle+|-\rangle)+\\ \frac{1}{2\sqrt{2}}(|+\rangle|+\rangle-|-\rangle|+\rangle-|+\rangle|-\rangle+|-\rangle|-\rangle)(|+\rangle-|-\rangle)\end{array}\right)=$$

$$=\frac{1}{2}(|+++\rangle+|+--\rangle+|-+-\rangle+|--+\rangle)_{123} \tag{3}$$

由以上推导结果可知,三粒子 GHZ 态在 X 基的表达为式(3)。式(3)中存在以下关系:当第 1 个粒子为$|+\rangle$时,第 2 和第 3 粒子为$|+\rangle|+\rangle$或者$|-\rangle|-\rangle$,第 2 和第 3 粒子相同;当第 1 个粒子为$|-\rangle$时,第 2 和第 3 粒子为$|+\rangle|-\rangle$或者$|-\rangle|+\rangle$,第 2 和第 3 粒子相反。基于这个特性,设计了本协议。

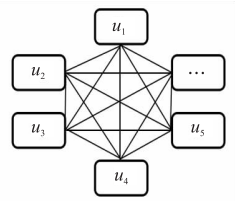

图1 无中心节点结构图

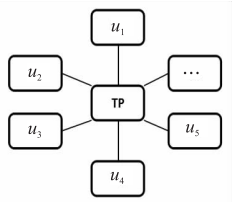

图2 有中心节点结构图

2 协议描述

a)TP 制备 n 对处于 $\varphi=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{123}$的三粒子 GHZ 态,把第 1(2,3)个粒子抽取出来按顺序编成序列 S_1(S_2,S_3)。TP 在量子序列 S_1 和 S_2 相同位置插入相同状态的诱惑粒子(诱惑粒子包含$|0\rangle$,$|1\rangle$,$|+\rangle$和$|-\rangle$)。TP 保留 S_3,把 S_1 发送给 U_1,S_2 发送给 U_2。

b)U_1 收到 S_1,U_2 收到 S_2 之后,通知 TP。TP 接到通知之后,公布诱惑粒子的位置和相对应的基($|1\rangle$和$|0\rangle$选择 Z 基,$|+\rangle$和$|-\rangle$选择 X 基)。U_1,U_2 分别抽出相应位置的诱惑粒子,选择相应的测量基检测其状态。若出现错误的测量结果低于阈值,进行下一步;若出现错误的测量结果高于阈值,放弃此次通信。

c)TP 使用 X 基对自己手中 S_3 进行测量,然后公布测量结果。

d)U_1 使用 X 基测量自己手中 S_1 序列,按照$|+\rangle$编码为 1,$|-\rangle$编码为 0 的规则生成一个二进制密钥序列 k_1。

e)U_2 使用 X 基测量自己手中 S_2 序列,按照$|+\rangle$编码为 1,$|-\rangle$编码为 0 的规则生成一个二进制密钥序列 k_2。U_2 再根据 TP 公布的 s_3 的测量结果对自己手中 k_2 进行修正。修正规则如下:

(a)若 TP 公布的 S_3 中第 i 位测量结果为$|+\rangle$,则 k_2 对应的第 i 位的二进制数不变;

(b)若 TP 公布的 S_3 中第 i 位测量结果为$|-\rangle$,则 k_2 对应的第 i 位的二进制数取反(1 变为 0,0 变为 1)。

3 协议分析

3.1 协议的正确性分析

当 TP 用 X 基随机对自己手中 S_1 进行测量之后,根据三粒子 GHZ 态 $\varphi=\frac{1}{\sqrt{2}}(|000\rangle+|111|\rangle)_{123}$的纠缠特性,$S_2$ 和 S_3 会发生相应的变化。具体而言,对 S_3 进行测量之后,当 S_3 中的第 k 位的粒子为$|+\rangle$时,S_2 和 S_3 中相应位置的粒子状态为$|+\rangle|+\rangle$或者$|-\rangle|-\rangle$;当 S_1 中的第 k 位的粒子为$|-\rangle$时,S_2 和 S_3 中相应位置的粒子状态为$|+\rangle|-\rangle$或者$|-\rangle|+\rangle$。穷举这四种情况,并且对相应状态按照$|+\rangle$编码为 1,$|-\rangle$编码为 0 的规则进行编码,如表 1 所示。

表 1 协议举例

序列	取值			
S_3	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$
S_1	$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$
U_1 编码序列 k_1	1	0	1	0
S_2	$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$
U_2 编码序列 k_2	1	0	0	1
U_2 修正序列 k_2	1	0	1	0

由表 1 可知,无论 S_3 中的粒子处于$|+\rangle$或者$|-\rangle$,只要 U_1 和 U_2 使用 X 基对自己手中的粒子序列 S_1 和 S_2 进行测量,根据编码规则,分别形成二进制密钥序列 k_1 和 k_2。U_2 再根据 TP 公布的测量结果对 k_2 进行修正,修正规则为:若 TP 公布的 S_1 中第 i 位测量结果为$|+\rangle$,则 k_2 对应的第 i 位的二进制数不变;若 TP 公布的 S_1 中第 i 位测量结果为$|-\rangle$,则 k_2 对应的第 i 位的二进制数取反(1 变为 0,0 变为 1)。操作完成之后,$k_1=k_2$,此时 U_1 和 U_2 就得到相同的密钥 k_1。

3.2 协议的安全性分析

3.2.1 截获/重发攻击和中间人攻击

当信道不安全,存在截获重发攻击和中间人攻击时,由于 TP 向 U_1 发送的 S_1 和向 U_2 发送的 S_2 中插入了相同的诱惑粒子,窃听者不知道诱惑粒子插入的位置和状态,那么他只能随机地选择基进行测量。根据量子测不准定理,当窃听者选错基对窃听粒子进行测量之后,诱惑粒子的状态会发生不可逆的变化。TP 公布诱惑粒子的位置和状态之后,由于 TP 插入 S_1 和 S_2 中诱惑粒子的位置和状态是相同的,那么用户 U_1 和 U_2 都可以根据 TP 公布的诱惑粒子的位置把诱惑粒子抽取出来,然后根据 TP 公布的基对诱惑粒子进行测量。用户公布测量结果,TP 将诱惑粒子的初始状态与之比对。如果出现错误的测量结果低于阈值,则不存在截获/重发攻击和中间人攻击;测量出现错误的测量结果高于阈值,则存在截获/重发攻击和中间人攻击,放弃此次通信。

3.2.2 纠缠攻击

由于用户 U_1、U_2 具有等效性,假设窃听者 Eva 对任意一个用户的窃听过程是一样的。先假设窃听者 Eva 对用户 U_1 的粒子进行截获,并对 S_1 进行纠缠,选用的附加粒子为 g,其初始状态为$|0\rangle$。当 Eva 截获了 S_1,将 S_1 中的粒子经过控制非门与 g 进行纠缠。S_1 中的粒子为控制位,附加粒子 g 为靶位,有如下关系式。

$$|0\rangle_{s_1}|0\rangle_g \rightarrow |0\rangle_{s_1}|0\rangle_g \tag{4}$$

$$|1\rangle_{s_1}|0\rangle_g \rightarrow |1\rangle_{s_1}|1\rangle_g \tag{5}$$

由式(4)可知,当控制位粒子状态为$|0\rangle$时,靶位粒子状态不变。当控制位粒子状态为$|1\rangle$时,靶位粒子状态改变($|0\rangle$变为$|1\rangle$)。但是由于本文随机插入了诱惑粒子,诱惑粒子包括$|0\rangle$,$|1\rangle$,$|+\rangle$和$|-\rangle$。由于 Eva 并不知道诱惑粒子的状态,在与$|+\rangle$和$|-\rangle$进行纠缠的时候,关系如下:

$$|+\rangle_{s_1}|0\rangle_g \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_{s_1}|0\rangle_g \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{s_1 g} \tag{6}$$

$$|-\rangle_{s_1}|0\rangle_g \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)_{s_1}|0\rangle_g \rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{s_1 g} \tag{7}$$

由式(6)(7)可知,诱惑粒子的状态已经被改变,当用户 U_1 进行窃听检测的时候会发现存在窃听行为而放弃通信。

如果 Eva 对处于纠缠态的粒子进行攻击,窃听者的任何干扰必然引入错误,从而可以检测到窃听者的存在。当没有错误引入的时候,总粒子只能处于 GHZ 三重态与窃听者的辅助量子态的直积态。但是直积态表明辅助粒子与 GHZ 三重态之间没有任何关联性,所以窃听者不会获得任何有用的信息,由此证明纠缠攻击是不会成功的。

3.2.3 对 TP 的分析

在协议中 TP 需要做两件事情:a)插入诱惑粒子,公布诱惑粒子的位置和状态,确定量子信道的安全;b)使用 X 基对量子序列 S_3 进行测量。在协议中,TP 对量子序列 S_3 进行测量以后,由表 1 可知,当 TP 手中的粒子为$|+\rangle$,它只知道 U_1 和 U_2 手中的粒子状态是相同,但具体是$|+\rangle|+\rangle$或者$|-\rangle|-\rangle$,TP 并不知道(为$|+\rangle|+\rangle$的概率为 50%,为$|-\rangle|-\rangle$的概率为 50%)。当手中粒子为$|-\rangle$时,TP 只知道用户手中的粒子为$|+\rangle|-\rangle$或者$|-\rangle|+\rangle$,但具体是哪一种状态 TP 并不知道(为$|+\rangle|-\rangle$的概率为 50%,为$|-\rangle|+\rangle$的概率为 50%)。所以用户手中的粒子状态对于 TP 来说都是不知道的。这样就保证了 TP 不能知道用户手中量子序列的状态,从而保证了密钥的安全。

4 结束语

本协议基于三粒子 GHZ 态 $\varphi = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123}$ 在 X 基下的特殊性质,设计了本协议。该协议通过第三方的辅助,对任意两名用户进行密钥分发,解决了多用户之间密钥分发需要大量量子传输信道数量的问题。经过协议分析,证明了协议的可行性。安全性分析表明本协议能抵御截获重发攻击、中间人攻击和纠缠攻击。同时对第三方 TP 的信任问题进行了分析,表明了协议不需要一个可信的第三方。

参考文献:

[1] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing[C]//Proc of IEEE International Conference on Computers Systems and Signal Processing. 1984: 175-179.

[2] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992,68(21): 3121-3124.

[3] Ekert A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991,67(6): 661-663.

[4] Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell's theorem[J]. Physical Review Letters, 1992,68(5): 557-559.

[5] 曾文杰, 周南润, 曾贵华. 基于隐形传态的跨中心量子身份认证方案[J]. 光电子·激光, 2005,16(1): 94-97.

[6] 杨宇光, 张兴. 利用秘密共享的多方同时量子身份认证[J]. 中国科学: 物理学 力学 天文学, 2008(2): 165-170.

[7] 李渊华, 刘俊昌, 聂义友. 基于 W 态的跨中心量子网络身份认证方案[J]. 光子学报, 2010,39(9): 1616-1620.

[8] Shi J H, Zhang S L, Zhang H L, *et al*. One-insider attack of quantum secret sharing protocol with collective eavesdropping check[J]. Quantum Information Processing, 2014,13(1):33-42.

[9] Chen R K, Zhang Y Y, Shi J H, *et al*. A multiparty error-correcting method for quantum secret sharing[J]. Quantum Information Processing, 2014,13(1):21-31.

[10] Shi Weimin, Zhang Janbiao, Zhou Yihua, *et al*. A non-interactive quantum deniable authentication protocol based on asymmetric quantum cryptography[J]. Optik - International Journal for Light and Electron Optics, 2016,127(20):8693-8697.

[11] Tsai C W, Hwang T. Multi-party quantum secret sharing based on two special entangled states[J]. Science China Physics, Mechanics & Astronomy, 2012,55(3): 460-464.

[12] 谢朝任, 蔡家纬, 黄宗立. Quantum secret sharing using GHZ-like state[J]. 理论物理, 2010,54(12): 1019-1022.

[13] Liu Wenjie, Liu Chao, Liu Zhihao, *et al*. Erratum to: same initial states attack in Yang et al.'s quantum private comparison protocol and the improvement[J]. International Journal of Theoretical Physics, 2014,53(3):271-276.

[14] Chen Y T, Hwang T. Comment on the "quantum private comparison protocol based on bell entangled states"[J]. International Journal of Theoretical Physics, 2014,53(3): 837-840.

[15] Wang Yukun, Zhang Jie, Huang Wei, *et al*. A quantum private comparison protocol with splitting information carriers[J]. International Journal of Theoretical Physics, 2015,54(1): 281-291.

[16] Wang Ding, He Debiao, Wang Ping, *et al*. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment[J]. IEEE Trans on Dependable and Secure Computing, 2015, 12(4):428-442.

[17] Wang Ding, Wang Ping. Two birds with one stone: two-factor authentication with security beyond conventional bound[J]. IEEE Trans on Dependable and Secure Computing, 2016, *PP*(99): 1-22.