论文

具有双向认证功能的多方量子密钥分发

林崧^{①②*}, 王宁^{①②}, 郭躬德^{①②}, 刘晓芬^{①②}

① 福建师范大学数学与计算机科学学院, 福州 350007;

② 福建师范大学, 福建省网络安全与密码技术重点实验室, 福州 350007

*联系人, E-mail: lins95@fjnu.edu.cn

收稿日期: 2014-12-11; 接受日期: 2015-01-23; 网络出版日期: 2015-02-13

国家自然科学基金(批准号: 61202451)和福建省教育厅 A 类重点项目(批准号: JA12062)资助

摘要 基于 Greenberger-Horne-Zeilinger 态的纠缠特性, 设计一个具有双向认证功能的多方量子密钥分发协议. 在协议中, 量子网络中的任意两个用户均可在一个半可信第三方的帮助下, 共享一个安全的会话密钥. 其中, 利用带密钥的单向 hash 函数技术对每个用户的身份进行认证. 最后, 对协议的安全性进行分析, 表明该协议在理论上是安全的.

关键词 量子密码, 多方量子密钥分发, Greenberger-Horne-Zeilinger 态, 身份认证, 半可信第三方

PACS: 03.67.Hk, 03.67.Dd, 03.65.Ud

doi: 10.1360/SSPMA2014-00476

1 引言

量子密钥分发是量子信息领域中最重要应用之一. 它利用量子力学原理使得通信双方之间能够分发一个安全的随机密钥. 1984 年, Bennett 和 Brassard^[1]提出了第一个著名的量子密钥分发协议(BB84). 在该协议中, 两个用户通过交换单粒子来创建一个共享密钥. 随后, 人们提出了许多各具特色的量子密钥分发协议^[2-4]. 其中大部分协议关注的是两个用户之间的密钥分发, 即点对点. 然而, 事实上, 在一个量子网络^[5]中更经常的是进行多对多的密钥分发. 因此, 为了实现这种需求, 人们提出了多用户量子密钥分发协议(Multi-User Quantum Key Distribution, MUQKD), 这成为量子信息领域中一个新的研究热点. 与量子密钥分发协议不同, 多用户量子密钥分发协议

针对一个更为实际的问题, 即在一个拥有 m 个用户的量子网络中两个用户均可进行保密通信. 这就要求网络中的任意两个用户都能够利用已有的通信信道, 执行 MUQKD 协议来实现密钥分发, 进而共享一个安全的会话密钥. 1995 年, Phoenix 等人^[6]提出了第一个 MUQKD 协议. 在该协议中, 两个用户在一个服务端的帮助下通过单粒子传输实现密钥的分发. 随后, 人们对这一问题展开研究, 并得到了一些可喜的理论成果, 他们利用不同的量子特性设计了一些新颖的 MUQKD 方案^[7-12], 如基于高维单粒子、Bell 态、Greenberger-Horne-Zeilinger(GHZ)态的和差分移相等. 随着量子技术地不断发展, 量子密码技术在实验方面也取得了很大进展^[13].

然而, 在量子密码的实际应用过程中, 还存在一个问题需要解决, 即身份认证^[14]. 它是指对一个人身

引用格式: 林崧, 王宁, 郭躬德, 等. 具有双向认证功能的多方量子密钥分发. 中国科学: 物理学 力学 天文学, 2015, 45: 040302

Lin S, Wang N, Guo G D, et al. Multi-user quantum key distribution with mutual authentication (in Chinese). Sci Sin-Phys Mech Astron, 2015, 45: 040302, doi: 10.1360/SSPMA2014-00476

份进行验证的行为, 它能防止攻击者冒充合法用户, 破坏密码系统的安全性. 因此, 身份认证在许多传统或量子密码系统中扮演着重要角色^[15-28]. 在一个 MUQKD 协议中, 存在这样一种情况. 一个恶意的攻击者可以假冒合法用户向其他合法用户分发密钥, 然后就能够与合法用户进行保密通信, 即发送伪造的信息给合法用户或窃取合法用户传递的秘密消息. 因此, 在设计一个实用的 MUQKD 协议时, 就必须考虑用户身份认证问题. 本文对这一问题进行研究, 提出了一个具有双向认证的基于 GHZ 态的 MUQKD 协议. 在该协议中, 三粒子 GHZ 态被用来作为信息载体. 在一个服务中心的协助下, 网络中的两个用户通过对 GHZ 态粒子进行单粒子测量, 从而实现分发一个安全的会话密钥. 同时, 每个用户通过和服务中心之间进行相互认证来证明该用户身份的合法性. 另外值得注意的是, 在本协议中两个用户不需要完全信任服务中心. 也就是说, 该服务中心只要求半可信即可. 这里, 半可信的概念在 Franklin 和 Reiter^[29]的论文中给出了具体的定义, 即意味着允许该服务中心可以采取任何被动和主动攻击, 来窃听两个参与者协商的会话密钥, 对其的唯一限制条件是它不能和任何一个参与者协作进行共谋攻击. 因此, 与第三方可信的一些协议相比, 它降低了系统执行所需的条件, 可进一步提高该协议的实用性.

2 准备知识

在一个二维 Hilbert 空间 H^2 中, 一个三粒子 GHZ 态可表示为

$$|\phi_{ijk}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|i\rangle|j\rangle + (-1)^k|1\rangle|i\oplus 1\rangle|j\oplus 1\rangle)_{123}, \quad (1)$$

这里, $i, j, k \in \{0, 1\}$, $i \oplus j \equiv (i + j) \bmod 2$, 且 $MB_z = \{|0\rangle, |1\rangle\}$ 为 H^2 空间上的一组标准正交基. 除此之外, 还存在两组常见的测量基, 分别是

$$MB_x = \left\{ |0_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\},$$

$$MB_y = \left\{ |0_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |1_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \right\}. \quad (2)$$

对一个 GHZ 态的 3 个粒子分别进行某一单粒子投影测量, 则其测量结果具有一定的关联性. 人们经常利用这一特性来设计不同的量子密码协议.

例如, 对一个 GHZ 态 $|\phi_{000}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123}$

中的 3 个粒子都使用 MB_x 进行单粒子测量, 则

$$|\phi_{000}\rangle = \frac{1}{2\sqrt{2}}[(|0_x\rangle|0_x\rangle + |1_x\rangle|1_x\rangle)|0_x\rangle + (|0_x\rangle|1_x\rangle + |1_x\rangle|0_x\rangle)|1_x\rangle]. \quad (3)$$

根据上式可知, 若前两个粒子的测量结果是 $|g_x\rangle_1 |h_x\rangle_2$ 时, 则第 3 个粒子的测量结果肯定是 $|(g \oplus h)_x\rangle_3$. 同理, 若使用测量基 MB_x , MB_y 和 MB_z 分别对 $|\phi_{000}\rangle$ 中的 3 个粒子进行测量时, 也可得到具有一定关联性的结果, 即

$$|\phi_{000}\rangle = \frac{1}{2\sqrt{2}}[(|0_x\rangle|0_y\rangle + |1_x\rangle|1_y\rangle)|1_y\rangle + (|0_x\rangle|1_y\rangle + |1_x\rangle|0_y\rangle)|0_y\rangle]. \quad (4)$$

经过简单计算, 若选择偶数个粒子用 MB_y 基进行测量 (剩余粒子用 MB_x 基测量) 时, 测量结果具有关联性, 具体如表 1 所描述.

3 多方量子密钥分发

在一个量子网络中, 存在一个半可信的第三方 (中心节点) Alice 和 m 个用户 $Bob_i (i = 1, 2, \dots, m)$. 每个用户 Bob_i 拥有其个人的身份信息 ID_i , 并且与 Alice 之间事先共享一个主密钥 K_i . 此外, 这些参与者还协商同意一个带密钥的单向 hash 函数 $h: 2^* \rightarrow 2^{N+3\delta}$. 在该网络中, 任意两个用户 Bob_i 和 Bob_j 通过执行下述协议来实现双向身份认证并分发一个相同的会话密钥 (如图 1 所示). 协议详细步骤描述如下.

步骤 1 Bob_i 和 Bob_j 向 Alice 提出分发会话密钥的请求. 同时, 两个参与者利用量子密钥协议协商一个临时秘密 R_T , 该密钥用于检测 Alice 的窃听行为.

表 1 GHZ 态 3 个粒子测量结果的关联表

Table 1 The relation among the measurement results of three particles in a GHZ state

粒子 2 测量结果	粒子 1 测量结果			
	$ 0_x\rangle_1$	$ 1_x\rangle_1$	$ 0_y\rangle_1$	$ 1_y\rangle_1$
$ 0_x\rangle_2$	$ 0_x\rangle_3$	$ 1_x\rangle_3$	$ 1_y\rangle_3$	$ 0_y\rangle_3$
$ 1_x\rangle_2$	$ 1_x\rangle_3$	$ 0_x\rangle_3$	$ 0_y\rangle_3$	$ 1_y\rangle_3$
$ 0_y\rangle_2$	$ 1_y\rangle_3$	$ 0_y\rangle_3$	$ 1_x\rangle_3$	$ 0_x\rangle_3$
$ 1_y\rangle_2$	$ 0_y\rangle_3$	$ 1_y\rangle_3$	$ 0_x\rangle_3$	$ 1_x\rangle_3$

图 1 MUQKD 协议的通信过程

虚线代表量子通信, 实线代表经典通信

Figure 1 The communications of the presented MUQKD protocol. The dotted lines represent quantum communications, while the solid lines represent classical communications.

步骤 2 Alice 产生一个随机数 r_A , 并通过经典信道告诉 Bob_i 和 Bob_j . 同时, Alice 制备 $N=n+3\delta$ 个三粒子 GHZ 态, 其初始量子态均为 $|\phi_{000}\rangle$. 按顺序从每个 GHZ 态中抽出一个粒子构成一个有序粒子串, 这样就可得到 3 个粒子串, 记为 $S_i = \{s_i^1, s_i^2, \dots, s_i^N\}$, $S_j = \{s_j^1, s_j^2, \dots, s_j^N\}$ 和 $S_A = \{s_A^1, s_A^2, \dots, s_A^N\}$. 最后, Alice 分别将粒子串 S_i 和 S_j 通过量子信道传给 Bob_i 和 Bob_j , 并保留粒子串 S_A .

步骤 3 $\text{Bob}_i(\text{Bob}_j)$ 产生随机数 $r_i(r_j)$, 进而计算 $b_i = h_{k_i}(ID_i \| r_i \| r_A)$ ($b_j = h_{k_j}(ID_j \| r_j \| r_A)$), 并根据该值对粒子串 $S_i(S_j)$ 中的 $n+2\delta$ 个粒子进行投影测量. 当 $b_i^k(b_j^k)=0$ ($k=1, 2, \dots, N$) 时, $\text{Bob}_i(\text{Bob}_j)$ 选择 MB_x 基对粒子 $s_i^k(s_j^k)$ 进行测量, 否则选择 MB_y 基. 测量结束后, $\text{Bob}_i(\text{Bob}_j)$ 得到相应的测量结果 $V_i = \{v_i^1, v_i^2, \dots, v_i^N\}$ ($V_j = \{v_j^1, v_j^2, \dots, v_j^N\}$). 剩余的 δ 个粒子作为样本粒子保留在 $\text{Bob}_i(\text{Bob}_j)$ 手上用于对 Alice 进行窃听检测. 这里, 样本粒子的选择由两参与者共享的临时秘密 R_T 决定. 另外, 他们通过经典信道告诉 Alice 随机数值 $r_i(r_j)$.

步骤 4 Alice 计算 hash 值 b_i 和 b_j , 进而得到 $b_A = b_i \oplus b_j$. 当 $b_A^k = 0$ ($k=1, 2, \dots, N$) 时, 选择 MB_x 基对粒子 s_A^k 进行测量, 否则选择 MB_y 基. 这样, Alice 就得到她的测量结果 $V_A = \{v_A^1, v_A^2, \dots, v_A^N\}$, 并根据该值计

算她的公开信息 $P_A = \{p_A^1, p_A^2, \dots, p_A^N\}$,

$$p_A^k = \begin{cases} v_A^k, & \text{若 } (b_i^k=0) \text{ 且 } (b_j^k=0); \\ v_A^k \oplus 1, & \text{则.} \end{cases} \quad (5)$$

步骤 5 Bob_i 对 Bob_j 的身份进行认证. 他从测量结果中随机选择 δ 个, 要求 Bob_j 公开他的测量结果. 判断等式 $v_i^k = p_A^k \oplus v_j^k$ 是否成立, 得到相应的错误率. 若错误率低于门限值, 则 Bob_i 认为与他进行密钥分发的用户确实是 Bob_j ; 否则, 他认为 Bob_j 是假冒的, 并终止协议.

步骤 6 像步骤 5 一样, Bob_j 从剩余结果中选择 δ 个样本对 Bob_i 的身份进行认证.

步骤 7 Bob_i 和 Bob_j 利用样本粒子对 Alice 进行窃听检测. 当 Alice 对 GHZ 态 $|\phi_{000}\rangle$ 中的一个粒子用 MB_x 基或 MB_y 基进行测量后, 则剩余的两个粒子就塌缩到某一两粒子最大纠缠态上,

$$\begin{aligned} |\phi_{000}\rangle &= \frac{1}{\sqrt{2}}|0_x\rangle \otimes |\phi_0^+\rangle + \frac{1}{\sqrt{2}}|1_x\rangle \otimes |\phi_0^-\rangle \\ &= \frac{1}{\sqrt{2}}|0_y\rangle \otimes |\phi_1^-\rangle + \frac{1}{\sqrt{2}}|1_y\rangle \otimes |\phi_1^+\rangle, \end{aligned} \quad (6)$$

这里, $|\phi_0^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\phi_1^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm i|11\rangle)$.

两个参与者要求 Alice 公布她的测量信息. 这样, 他们就可以知道他们手中的粒子所处的量子态, 即 4 个量子态 $|\phi_0^\pm\rangle$, $|\phi_1^\pm\rangle$ 中的一个. 然后, Bob_i 和 Bob_j 就使用与 EPR 协议^[2]类似的方法来判断手中的粒子是否处于这一最大纠缠态. 当粒子处于态 $|\phi_0^\pm\rangle$ 时, Bob_i 和 Bob_j 随机选择 $MB_x \otimes MB_x$ 基或 $MB_z \otimes MB_z$ 基进行测量. 当粒子处于态 $|\phi_1^\pm\rangle$ 时, Bob_i 和 Bob_j 随机选择 $MB_x \otimes MB_y$ 或 $MB_z \otimes MB_z$ 作为测量基. 最后, 他们根据测量结果的关联性对 Alice 进行窃听检测. 若错误率高于门限值, 则 Bob_i 和 Bob_j 认为 Alice 存在窃听行为并终止协议.

步骤 8 最后, 剩余 n 个测量结果相互关联, 即 $v_i^k = v_j^k \oplus p_A^k$. 这样, 两个参与者就可得到生密钥 $K_S = v_i^k$, 然后对这些经典比特进行纠错和保密放大, 最终得到一个安全的会话密钥.

协议中使用了基于块传输的方法. 该方法于 2002 年由 Long 和 Liu^[30]在设计量子安全直接通信两

步方案中首次提出, 随后许多量子通信协议都采用该方法来传输信号粒子^[31,32]. 该方法要求对粒子进行存储, 文献[33]表明, 量子存储在当前技术条件下是可以实现的. 此外, 协议的执行还需涉及单粒子酉操作^[34]、纠缠态制备^[35]和粒子探测器^[36], 这在目前实验条件下也是可行的.

4 安全性分析

为了分析所提协议的安全性, 对以下两种常见攻击情形进行讨论. 一个是假冒用户攻击, 即攻击者冒充某一合法用户的身份与另一个合法用户执行协议, 进而窃取主密钥或会话密钥; 另一个是半可信第三方攻击. 在该攻击中, Alice 利用参与协议执行的便利, 窃取有关会话密钥的部分或全部信息. 下面分别对这两种攻击情形进行细致地讨论.

4.1 假冒 Bob_j 攻击

在协议中, 两个用户执行的操作是一样的. 因此, 不失一般性, 可设攻击者冒充 Bob_j (记为 Bob_j^{*}) 进行攻击, 其目的是窃取主密钥 K_j 或会话密钥 K_S . 根据攻击目的不同, 分成两种情形进行分析.

若 Bob_j^{*} 想要窃取会话密钥 K_S , 他就必须设法通过步骤 5 的身份认证. 但是, 这是不可能的. 在步骤 2 中, Bob_j^{*} 收到粒子串 S_j . 然而, 该串中的每一个粒子都处于最大混合态 $(|0\rangle\langle 0| + |1\rangle\langle 1|)/2$, 则 Bob_j^{*} 无法利用手中的粒子窃取任何信息. 同时, 由于 Bob_j^{*} 不知道真正 Bob_j 的主密钥 K_j , 因此他就无法计算出 hash 值 b_j 并对这些粒子进行适当的测量. 在进行身份认证时, Bob_j^{*} 会被要求公布他的测量结果. 这样, 他就不得不随机选择一个测量基进行测量. 在这种情形下, 他的攻击行为不可避免地会引入错误. 通过简单计算, 可得该错误率为 25%. 因此, 该攻击行为将会被 Bob_j 发现. 这就意味着, Bob_j^{*} 无法冒充 Bob_j 来窃取会话密钥 K_S .

从上述分析可知, 若攻击者窃取了某一用户的主密钥, 则他就可以假冒该用户执行协议, 进而获得会话密钥. 因此, Bob_j^{*} 的另一个攻击目标是窃取 Bob_j 的主密钥 K_j . 由于由通信噪声引起的错误和由攻击行为引起的错误对参与者而言是无法区分的, 并且主密钥显然是需要重复使用的, 无法实时更新. 因此, 如果 Bob_j^{*} 的攻击能获得主密钥, 那么即使他的

攻击行为被检测出来, 这也破坏了协议的安全性. 从某种意义上说, 该攻击比上述攻击对协议具有更强的危害性. 接下来, 就对这一类型攻击的情况进行简要的分析.

在协议中, 主密钥是用于计算 hash 值, 然后根据 hash 值对粒子进行测量. 这里, 经典 hash 函数的安全性是基于计算复杂性的. 随着一些新颖的经典或量子算法的提出^[37-41], 一些著名的 hash 函数被攻破, 变成不安全的. 一旦该 hash 函数的明文对被 Bob_j^{*} 所得到, 他就很有可能利用这些先进算法来窃取主密钥 K_j . 因此, 这就将成为该协议的一个安全薄弱点. 这里, ID_j, r_j, r_A 是公开的. 故而, 攻击的关键在于 Bob_j^{*} 能否利用手中的粒子和公开的信息来获得 b_j 的值. 然而, 这是不可行的. 因为在协议中所有公布的信息都只涉及测量结果, 而关于测量基的信息是保密的. 而且, 传输的粒子均处于最大混合态, 这也无法给 Bob_j^{*} 提供任何有用信息. 在这种情况下, Bob_j^{*} 是无法取得 b_j 的值. 因此, 本协议能抵抗这种类型的攻击.

4.2 半可信 Alice 攻击

协议中, 中心节点 Alice 并非完全可信. 除了不能和其他用户勾结之外, 她可以利用参与协议的便利条件来窃取会话密钥. 由于她本身是合法的, Alice 能够轻易躲避步骤 5 和 6 的身份认证检测. 同时, Alice 负责信号粒子的初始制备, 她可以不按协议规定产生 GHZ 态 $|\phi_{000}\rangle_{LLA}$ 而是制备某一特殊纠缠态. 然后, 在协议结束时, 利用手中的粒子窃取关于会话密钥 K_S 的部分或全部信息. 因此, 她比外部攻击者具有更强的攻击能力^[42,43]. Alice 通常执行的攻击策略描述如下.

不失一般性, 可设 Alice 制备 3 个粒子 I, J, A , 其所处的量子态为

$$|\Psi\rangle_{LLA} = |00\rangle|\lambda_{00}\rangle + |01\rangle|\lambda_{01}\rangle + |10\rangle|\lambda_{10}\rangle + |11\rangle|\lambda_{11}\rangle, \quad (7)$$

其中,

$$\langle\lambda_{00}|\lambda_{00}\rangle + \langle\lambda_{01}|\lambda_{01}\rangle + \langle\lambda_{10}|\lambda_{10}\rangle + \langle\lambda_{11}|\lambda_{11}\rangle = 1. \quad (8)$$

在步骤 4 中, 她对粒子 A 进行测量, 并根据测量结果发布相应的经典消息 p_A^k . 最后, Alice 根据 Bob_i 和 Bob_j 的测量基信息, 以及她的测量结果, 来窃取会话密钥. 接下来, 对这一攻击情形进行分析.

假设 Bob_i 和 Bob_j 的测量结果为 $|0_x\rangle_i$ 和 $|0_x\rangle_j$, 那么 Alice 手中的粒子 A 就塌缩到如下量子态:

$$|\psi_{00}\rangle = |\lambda_{00}\rangle + |\lambda_{01}\rangle + |\lambda_{10}\rangle + |\lambda_{11}\rangle. \quad (9)$$

这种情况发生的概率为

$$p_{0x0x} = \frac{1}{4} \langle \psi_{00} | \psi_{00} \rangle. \quad (10)$$

在步骤 4 时, Alice 对粒子 A 进行某一 POVM 测量. 不妨设该测量为

$$\Pi = \{\Pi_0, \Pi_1, \Pi_2 = I - \Pi_0 - \Pi_1\}, \quad (11)$$

这里, 当测量结果为 $\Pi_1|\varphi\rangle$ 时, Alice 公布 $p_A^k=0$; 当测量结果为 $\Pi_1|\varphi\rangle$ 时, Alice 公布 $p_A^k=1$. 在这种情况下, 为了不引入错误, 则该测量就必须满足如下条件:

$$(|\psi_{00}\rangle, \Pi_0|\psi_{00}\rangle) = 1. \quad (12)$$

同理, 当两个用户的测量结果为 $|0_x\rangle|1_x\rangle$, $|1_x\rangle|0_x\rangle$ 和 $|1_x\rangle|1_x\rangle$ 时, 可推出下列限制条件:

$$\begin{aligned} (|\psi_{01}\rangle, \Pi_1|\psi_{01}\rangle) &= 1, (|\psi_{10}\rangle, \Pi_1|\psi_{10}\rangle) = 1, \\ (|\psi_{11}\rangle, \Pi_0|\psi_{11}\rangle) &= 1, \end{aligned} \quad (13)$$

其中

$$\begin{aligned} |\psi_{01}\rangle &= |\lambda_{00}\rangle - |\lambda_{01}\rangle + |\lambda_{10}\rangle - |\lambda_{11}\rangle, \\ |\psi_{10}\rangle &= |\lambda_{00}\rangle + |\lambda_{01}\rangle - |\lambda_{10}\rangle - |\lambda_{11}\rangle, \\ |\psi_{11}\rangle &= |\lambda_{00}\rangle - |\lambda_{01}\rangle - |\lambda_{10}\rangle + |\lambda_{11}\rangle, \end{aligned} \quad (14)$$

相应的发生概率为

$$\begin{aligned} p_{0x1x} &= \frac{1}{4} \langle \psi_{01} | \psi_{01} \rangle, p_{1x0x} = \frac{1}{4} \langle \psi_{10} | \psi_{10} \rangle, \\ p_{1x1x} &= \frac{1}{4} \langle \psi_{11} | \psi_{11} \rangle. \end{aligned} \quad (15)$$

由于 Alice 需要根据两个用户的测量基信息和她的测量结果, 来窃取密钥. 显然, 如果下式成立, 则 Alice 是无法获得有关 K_S 的任何信息.

$$P_{xx0}^0 = P_{xx0}^1, \quad (16)$$

其中, P_{xxd}^d ($d=0, 1$) 表示当 Bob_i 和 Bob_j 选择 MB_x 基对粒子 I 和 J 进行测量, 且 Alice 的测量结果为 0 时, 会话密钥为 d 的概率. 根据公式(12)和(15), 可知

$$P_{xx0}^0 = p_{0x0x}, P_{xx0}^1 = p_{1x1x}. \quad (17)$$

简单计算, 由公式(12)和(13)可推得

$$\begin{aligned} &((|\lambda_{00}\rangle + |\lambda_{11}\rangle), (|\lambda_{01}\rangle + |\lambda_{10}\rangle)) \\ &+ ((|\lambda_{01}\rangle + |\lambda_{10}\rangle), (|\lambda_{00}\rangle + |\lambda_{11}\rangle)) = 0, \end{aligned}$$

$$\langle \lambda_{00} | \lambda_{11} \rangle + \langle \lambda_{11} | \lambda_{00} \rangle = 0, \langle \lambda_{01} | \lambda_{10} \rangle + \langle \lambda_{10} | \lambda_{01} \rangle = 0. \quad (18)$$

进而, 根据公式(12), (15)和(18), 可得

$$p_{0x0x} = p_{1x1x}. \quad (19)$$

同时, 由公式(17)和(19), 可知等式(16)成立. 同理, 可得以下等式:

$$\begin{aligned} P_{xx1}^0 &= P_{xx1}^1, P_{yy0}^0 = P_{yy0}^1, P_{xy0}^0 = P_{xy0}^1, \\ P_{xy1}^0 &= P_{xy1}^1, P_{yx0}^0 = P_{yx0}^1, P_{yx1}^0 = P_{yx1}^1. \end{aligned} \quad (20)$$

因此, 半可信第三方 Alice 在不引入错误的条件下无法得到关于会话密钥的任何信息.

除了上述攻击外, Alice 还可以采取一个更为巧妙的攻击方法, 即她发送的不是一个三粒子态. 这时, 她可以分别制备两个两粒子纠缠态, 如 $|\varphi_0^+\rangle_{A_1B_1} \otimes |\varphi_0^+\rangle_{A_2B_2}$. 在步骤 2 中, Alice 将粒子 B_1 和 B_2 分别传给两个参与者, 并保留粒子 A_1 和 A_2 . 然后, 在步骤 4 中她根据 r_i 和 r_j 的值知道 Bob_i 和 Bob_j 的测量基, 并用相同的基对手中的粒子 A_1 和 A_2 进行测量. 根据粒子 A_1 和 A_2 的测量结果, Alice 就能够推出 Bob_i 和 Bob_j 的测量结果. 在此基础上, Alice 通过公布假信息使得步骤 5 和 6 的身份认证顺利完成. 同时, 她也可根据 A_1 和 A_2 的测量结果来窃取会话密钥. 但是, 该攻击是不成功的, 它将在步骤 7 的窃听检测中被发现.

因为 R_T 是由 Bob_i 和 Bob_j 秘密协商得到, 所以它不为 Alice 所知. 在这种情况下, 当 Alice 采用上述攻击时, 她就无法得到样本粒子的位置. 若某一对 B_1 和 B_2 被选中为样本粒子, Alice 按照攻击策略对粒子 A_1 和 A_2 进行单粒子测量, 这就使得粒子 B_1 和 B_2 不存在任何的关联性, 这将不可避免的在步骤 7 的窃听检测中引入错误.

5 结束语

本文提出一个基于 GHZ 态的可认证多方量子密钥分发协议. 在该协议中, 一个半可信的第三方制备信息载体, 并将 GHZ 态中的两个粒子传输给量子网络中的两个用户. 利用 GHZ 态的关联性, 两个用户通过对收到的粒子进行单粒子测量来共享一个安全的会话密钥. 这里, 基于带密钥单向 hash 函数技术, 设计了两个身份认证过程对两个用户的身份进行验证. 最后, 本文对协议的安全性也进行详细讨论. 分析表明, 本协议能够抵御内部攻击者的一些常见攻

击, 因此协议在理论上是安全的.

在方案实现方面, 两个用户只需进行单粒子测量, 且无需量子存储, 这在目前的实验水平下是比较容易实现的. 但是, 中心节点必须具有制备三粒子 GHZ 态的能力, 虽然这在实验上已取得成功, 但制备的成功率比较低, 这就使得本方案的实用性受到一定限制. 因此, 下一步将通过寻找一些较容易制备

的量子态来解决该问题, 如单粒子量子态等. 此外, 方案的执行需要一个半可信中心节点的参与, 这也使得本方案在实用性方面受到限制. 例如, 对于一些稍显复杂的网络结构, 如树型、mesh 型等, 就没有中心节点. 因此, 如何在无第三方参与或第三方不可信的情形下实现带认证功能的多方量子密钥分发也是未来研究的一个主要问题.

参考文献

- 1 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In: The Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. Bangalore: IEEE Press, 1984. 175–179
- 2 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. *Rev Mod Phys*, 2002, 74: 145–195
- 3 Li H W, Chen W, Huang J Z, et al. Security of quantum key distribution (in Chinese). *Sci Sin-Phy Mech Astron*, 2012, 42: 1237–1255 [李宏伟, 陈巍, 黄靖正, 等. 量子密码安全性研究. *中国科学: 物理学 力学 天文学*, 2012, 42: 1237–1255]
- 4 Long G L, Wang C, Li Y S, et al. Quantum secure direct communication (in Chinese). *Sci Sin-Phy Mech Astron*, 2011, 41: 332–342 [龙桂鲁, 王川, 李岩松, 等. 量子安全直接通信. *中国科学: 物理学 力学 天文学*, 2011, 41: 332–342]
- 5 Wu H, Zhao Y K, Zhao Y, et al. Field application and security management of a telephone network and a high speed data transmission system with practical ber quantum cryptography (in Chinese). *Sci Sin Inf*, 2014, 44: 312–321 [吴华, 赵于康, 赵勇, 等. 实用化光纤量子加密电话网络和高速数据传输系统——现场应用与安全管理. *中国科学: 信息科学*, 2014, 44: 312–321]
- 6 Phoenix S J D, Barnett S M, Townsend P D, et al. Multi-user quantum cryptography on optical networks. *J Mod Opt*, 1995, 42: 1155–1163
- 7 Li C Y, Li X H, Deng F G, et al. Efficient quantum cryptography network without entanglement and quantum memory. *Chin Phys Lett*, 2006, 23: 2896–2899
- 8 Xue P, Li C F, Guo G C. Conditional efficient multiuser quantum cryptography network. *Phys Rev A*, 2002, 65: 022317
- 9 Deng F G, Liu X S, Ma Y J, et al. A theoretical scheme for multi-user quantum key distribution with N Einstein-Podolsky-Rosen pairs on a passive optical network. *Chin Phys Lett*, 2002, 19: 893–896
- 10 Hong C H, Heo J O, Khym G L, et al. Quantum channels are sufficient for multi-user quantum key distribution protocol between users. *Opt Commun*, 2010, 283: 2644–2646
- 11 Guo Y, Shi R, Zeng G. Secure networking quantum key distribution schemes with Greenberger-Horne-Zeilinger states. *Phys Scripta*, 2010, 81: 045006
- 12 Wang W Y, Wang C, Wen K, et al. Quantum key distribution network based on differential phase shift. *Chin Phys Lett*, 2007, 24: 1463–1466
- 13 Stucki D, Walenta N, Vannel F, et al. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibers. *New J Phys*, 2009, 11: 075003
- 14 Sandor I. Quantum communications: Explained for communication engineers. *IEEE Commun Mag*, 2013, 51: 28–25
- 15 Dušek M, Hadeřka O, Hendrych M, et al. Quantum identification system. *Phys Rev A*, 1999, 60: 149–156
- 16 Zeng G, Zhang W. Identity verification in quantum key distribution. *Phys Rev A*, 2000, 61: 022303
- 17 Mihara T. Quantum identification schemes with entanglements. *Phys Rev A*, 2002, 65: 052326
- 18 Lee H, Lim J, Yang H J. Quantum direct communication with authentication. *Phys Rev A*, 2006, 73: 042305
- 19 Zhang Z, Zeng G, Zhou N, et al. Quantum identity authentication based on ping-pong technique for photons. *Phys Lett A*, 2006, 356: 199–205
- 20 Cederlof J, Larsson J A. Security aspects of the authentication used in quantum cryptography. *IEEE Trans Inform Theor*, 2008, 54: 1735–1741
- 21 Wang M J, Pan W. Quantum secure direct communication based on authentication. *Chin Phys Lett*, 2008, 25: 3860–3863
- 22 Yen C A, Horng S J, Goan H S, et al. Quantum direct communication with mutual authentication. *Quantum Inform Comput*, 2009, 9: 376–394
- 23 Fung C H F, Ma X F, Chau H F. Practical issues in quantum-key-distribution postprocessing. *Phys Rev A*, 2010, 81: 012318
- 24 Yang J, Wang C, Zhang R. Quantum secure direct communication with authentication expansion using single photons. *Commun Theor Phys*,

- 2010, 54: 829–834
- 25 Zhou N R, Wang L J, Ding J, et al. Quantum deterministic key distribution protocols based on the authenticated entanglement channel. *Phys Scripta*, 2010, 81: 045009
- 26 Huang P, Zhu J, Lu Y, et al. Quantum identity authentication using gaussing-modulated squeezed states. *Int J Quantum Inform*, 2011, 9: 701–721
- 27 Yang Y G, Tian J, Xia J, et al. Quantum authenticated direct communication using Bell states. *Int J Theor Phys*, 2013, 52: 336–344
- 28 Yuan H, Liu Y M, Pan G Z, et al. Quantum identity authentication based on ping-pong technique without entanglements. *Quantum Inf Process*, 2014, 13: 2535–2549
- 29 Franklin M K, Reiter M K. Fair exchange with a semi-trusted third party. In: *The Proceedings of the 4th ACM conference on Computer and communications security*. New York: Association for Computing Machinery, 1997. 1–5
- 30 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A*, 2002, 65: 032302
- 31 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys Rev A*, 2003, 68: 042317
- 32 Long G L, Deng F G, Wang C, et al. Quantum secure direct communication and deterministic secure quantum communication. *Front Phys China*, 2007, 2: 251–272
- 33 Zhou Z Q, Li C F. Solid state quantum memory (in Chinese). *Chin Sci Bull*, 2013, 58: 287–293 [周宗权, 李传锋. 固态量子存储. *科学通报*, 2013, 58: 287–293]
- 34 Lin Q. Optical realization of universal unitary operation of single partite polarization encoded qudit (in Chinese). *Sci Sin-Phy Mech Astron*, 2014, 44: 317–325 [林青. 普适单体偏振高维量子态么正操作的光学实现. *中国科学: 物理学 力学 天文学*, 2014, 44: 317–325]
- 35 Ye X L, Lin Q. Heralded generation of asymmetric polarized entangled qutrits (in Chinese). *Sci Sin-Phy Mech Astron*, 2013, 43: 626–633 [叶欣露, 林青. 非对称偏振三维纠缠态的预警制备. *中国科学: 物理学 力学 天文学*, 2013, 43: 626–633]
- 36 Wang G W, Xu Y Q, Niu Z C. Development of high-performance novel low-dimensional structure antimonide infrared FPAs: Challenges and solutions (in Chinese). *Sci Sin-Phy Mech Astron*, 2014, 44: 368–389 [王国伟, 徐应强, 牛智川. 新型低维结构锑化物红外探测器的研究与挑战. *中国科学: 物理学 力学 天文学*, 2014, 44: 368–389]
- 37 Wang X Y, Yu H B. How to break MD5 and other hash functions. In: Cramer R, ed. *Advances in Cryptology—EUROCRYPT 2005*. Berlin Heidelberg: Springer-Verlag, 2005. 19–35
- 38 Wang X Y, Yin Y L, Yu H B. Finding Collisions in the Full SHA-1. In: Shoup V, ed. *Advances in Cryptology—CRYPTO 2005*. Berlin Heidelberg: Springer-Verlag, 2005. 17–36
- 39 Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring. In: *The Proceedings of the 35th Annual Symposium of Foundation of Computer Science*. New York: Institute of Electrical and Electronics Engineers, 1994. 124–134
- 40 Grover L K. A fast quantum mechanical algorithm for database search. In: *The Proceedings of the 28th Annual ACM Symposium on Theory of Computing*. New York: Association for Computing Machinery, 1996. 212–219
- 41 Hao L, Long G L. Experimental implementation of a fixed-point duality quantum search algorithm in the nuclear magnetic resonance quantum system. *Sci China-Phys Mech Astron*, 2011, 54: 936–941
- 42 Gao F, Qin S J, Wen Q Y, et al. A simple participant attack on the Bradler-Dusek protocol. *Quantum Inform Comput*, 2007, 7: 329–334
- 43 Lin S, Gao F, Guo F Z, et al. Comment on “Multiparty quantum secret sharing of classical messages based on entanglement swapping”. *Phys Rev A*, 2007, 76: 036301

Multi-user quantum key distribution with mutual authentication

LIN Song^{1,2*}, WANG Ning^{1,2}, GUO GongDe^{1,2} & Liu XiaoFen^{1,2}

¹ School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China;

² Key Lab of Network Security and Cryptography, Fujian Normal University, Fuzhou 350007, China

Based on the entanglement feature of Greenberger-Horne-Zeilinger states, a multi-user quantum key distribution with mutual authentication is proposed. In the protocol, a semi-trusted third party, who may misbehave on its own but will conspire with none of the participants, is introduced to help arbitrary two users on a quantum network to achieve this secure task. Firstly, the third party prepares a three-particle entangled state. Then, he keeps one particle in his hand, and sends two particles to these two users respectively. Meanwhile, a keyed one-way hash function is utilized to generate an authentication message, in terms of which three parties respectively make an appropriate single-particle measurement on the particles in their hands. According to the measurement results, the third party can verify the identity of one user. It implies that one user is able to authenticate the other user with the assistance of the third party. After that, two participants use the remainder measurement results to generate a common session key. Moreover, the practical implementation of the presented protocol is discussed, which illustrates that this protocol is feasible under the current techniques. In the end, the security of the presented protocol is analyzed. It is shown that this protocol is secure in theory by proving that the presented protocol can stand against several common attacks.

quantum cryptography, multi-user quantum key distribution, Greenberger-Horne-Zeilinger state, authentication, semi-trusted third party

PACS: 03.67.Hk, 03.67.Dd, 03.65.Ud

doi: 10.1360/SSPMA2014-00476