文章编号:1004-4213(2010)09-1616-5

基于 W 态的跨中心量子网络身份认证方案*

李渊华[1],刘俊昌[1],聂义友[1,2,†]

(1 江西师范大学 物理与通信电子学院,南昌 330022)

(2 江西省光电子与通信重点实验室,南昌 330022)

摘 要:利用量子隐形传态原理和量子纠缠交换技术,提出了基于 W 态的跨中心量子网络身份认证方案,实现了分布式量子通信网络中对客户的身份认证.该方案分为注册阶段和身份认证阶段,认证系统包括主服务器和客户端服务器.客户所有的操作都在客户端服务器上进行,不直接与主服务器进行通信.身份认证全部由服务器根据量子力学原理进行,保证了认证方案的安全性.最后,对该方案进行了安全性分析.

关键词:量子通信;量子身份认证;量子隐形传态;量子纠缠交换;W 态

中图分类号:O431.2;TN918 **文献标识码**:A **doi**:10.3788/gzxb20103909.1616

0 引言

量子通信和量子网络是目前量子信息领域的研究热点,在理论和实验上都取得了巨大的突破,包括量子隐形传态[1-5]、量子密集编码[6-7]以及量子密钥分发[8-9]等.在网络通信中,如电子银行、电子政务等中,常常涉及对用户身份识别的问题,而基于经典加密的身份认证方案从理论上来说不是绝对安全的,且受到潜在的功能强大的量子计算机的威胁[10].因此,人们提出了许多量子身份认证方案.DuŠek 等人[11]将量子密钥分配和经典认证相结合,提出了一种混合量子认证系统.Curty 和 Santos[12]利用一个量子比特作为认证密钥,提出一种安全的二进制经典信息的量子认证协议.Mihara[13]将普通的认证标签和量子密码系统相结合,提出了一种基于可信权威的量子认证方案.通过引入可靠的认证中心,Zeng 等人[14]给出了一些可以同时实施量子密钥分配和量子身份认证的建议.温晓军等人[15]提出了一种基于 GHZ 态量子相干性的网络身份认证方案.最近,Zhou 等人[16]基于 EPR 纠缠对,提出了适用于分布式网络的跨中心量子身份认证方案.

W 纠缠态是一种重要的多粒子(三粒子)纠缠量子体系,许多学者把它用作量子信道来完成量子信息处理任务[3,17-19],并且发现它具有很强的反量子比特丢失的性质,即我们对任何一个粒子进行求迹,其余的两个粒子仍然处于纠缠状态.然而多年来人们对它的研究表明,W 态不能用来完成决定性(概率为 1)的量子隐形传态和超密编码,而只能用来完成概率性的量子隐形传态和超密编码.但文献[19]发现存在另一类 W 纠缠态(见(1)式所示)能够用来完成决定性的量子隐形传态和超密编码任务.文献[20]对这两类 W 纠缠态及其性质做了详细的研究,给出了 W 纠缠态实现概率为 1 的量子隐形传态和超密编码的条件,并发现这一类 W 态也具有强烈的反量子比特丢失的性质.可见 W 类纠缠态是重要的量子态,是值得进一步研究的.

本文提出一种新的基于 W 纠缠态的量子信道的跨中心量子网络身份认证方案.该方案以 W 纠缠态作为量子信道,采用量子隐形传态技术和量子纠缠交换技术,辅之以在经典信道上传送必要的指令信息,实现了理论上安全的量子通信网络中各客户的量子身份认证.

1 基本原理

1.1 隐形传态原理

假设 Alice 和 Bob 共享处于$|W\rangle$纠缠态的三个粒子,其中发送者 Alice 拥有粒子 1 和 2,接收者 Bob 拥有粒子 3.这三个粒子 1、2 和 3 所处的态为

$$|W\rangle_{123}=\frac{1}{2}(|100\rangle_{123}+|010\rangle_{123}+\sqrt{2}|001\rangle_{123}) \quad (1)$$

现在,以该三粒子$|W\rangle$态为量子信道,Alice 要传送一个未知粒子 a 的态给远处的 Bob,粒子 a 的未知态为

$$|\psi\rangle_a=\alpha|0\rangle_a+\beta|1\rangle_a \quad (2)$$

式(2)中$|\alpha|^2+|\beta|^2=1$.处于未知态的粒子 a 与处于$|W\rangle$纠缠态的三个粒子 1、2、3 所构成的量子体系

*国家自然科学基金(60807014)、江西省自然科学基金(2009JX01925)和江西省教育厅科研项目(GJJ09153)资助

†Tel:0791-8120376 Email:nieyiyou@163.com

收稿日期:2009-11-16 修回日期:2009-12-29

的总量子态为

$$|\psi\rangle_{a123}=|\psi\rangle_a\otimes|W\rangle_{123}=(\alpha|0\rangle_a+\beta|1\rangle_a)\otimes\frac{1}{2}(|100\rangle_{123}+|010\rangle_{123}+\sqrt{2}|001\rangle_{123})=\frac{1}{2}[|\eta^+\rangle_{a12}(\alpha|0\rangle_3+\beta|1\rangle_3)+|\eta^-\rangle_{a12}(\alpha|0\rangle_3-\beta|1\rangle_3)+|\xi^+\rangle_{a12}(\beta|0\rangle_3+\alpha|1\rangle_3)+|\xi^-\rangle_{a12}(\beta|0\rangle_3-\alpha|1\rangle_3)] \quad (3)$$

式(3)中$|\eta^\pm\rangle$和$|\xi^\pm\rangle$是$|W\rangle$态纠缠类中的一组正交归一态矢集，具体形式为

$$|\eta^\pm\rangle_{a12}=\frac{1}{2}(|010\rangle_{a12}+|001\rangle_{a12}\pm\sqrt{2}|100\rangle_{a12}) \quad (4)$$

$$|\xi^\pm\rangle_{a12}=\frac{1}{2}(|110\rangle_{a12}+|101\rangle_{a12}\pm\sqrt{2}|000\rangle_{a12}) \quad (5)$$

为实现量子隐形传态，首先，Alice 对自己手中的三个粒子 a、1、2 在正交基$\{|\eta^\pm\rangle,|\xi^\pm\rangle\}$下进行联合投影测量，测量结果为$(|\eta^\pm\rangle,|\xi^\pm\rangle)$中的某一个，每一个结果出现的概率为 1/4. 测量后粒子 3 的量子态为$\alpha|0\rangle_3+\beta|1\rangle_3$，$\alpha|0\rangle_3-\beta|1\rangle_3$，$\alpha|1\rangle_3+\beta|0\rangle_3$和$-\alpha|1\rangle_3+\beta|0\rangle_3$这四个态之一. 然后，Alice 将测量结果通过经典信道告诉 Bob. 根据 Alice 的测量结果，Bob 对自己拥有的粒子 3 分别做 I、σ_z、σ_x、$-i\sigma_y$ 的幺正变换，就得到了要传送的量子态.

1.2　量子纠缠交换原理

纠缠交换的基本原理是：粒子 1、2、3 和粒子 4、5、6 为两组处于$|W\rangle$纠缠态的粒子，通过对粒子 3、4、5 进行适当的操作，使得非纠缠粒子 1、2、6 处于量子纠缠态. 设纠缠粒子 1、2、3 和纠缠粒子 4、5、6 分别处于量子态$|W\rangle_{123}$和$|W\rangle_{456}$，具体为

$$|W\rangle_{123}=\frac{1}{2}(|100\rangle_{123}+|010\rangle_{123}+\sqrt{2}|001\rangle_{123}) \quad (6)$$

$$|W\rangle_{456}=\frac{1}{2}(|100\rangle_{456}+|010\rangle_{456}+\sqrt{2}|001\rangle_{456}) \quad (7)$$

把这 6 个粒子看成一个量子系统，其量子态可表示为

$$|\psi\rangle_{123456}=|W\rangle_{123}\otimes|W\rangle_{456}=\frac{1}{2}(|\eta^+\rangle_{345}|\eta^+_{612}\rangle+|\eta^-\rangle_{345}|\eta^-\rangle_{612}+|\xi^+\rangle_{345}|\xi^+\rangle_{612}-|\xi^-\rangle_{345}|\xi^-\rangle_{612}) \quad (8)$$

式中$|\eta^\pm\rangle_{ijk}=\frac{1}{2}(|010\rangle_{ijk}+|001\rangle_{ijk}\pm\sqrt{2}|100\rangle_{ijk})$，$|\xi^\pm\rangle_{ijk}=\frac{1}{2}(|110\rangle_{ijk}+|101\rangle_{ijk}\pm\sqrt{2}|000\rangle_{ijk})$. 现在对粒子 3、4、5 在正交基$\{|\eta^\pm\rangle,|\xi^\pm\rangle\}$下进行联合投影测量，就能获得粒子 1、2、6 所处的纠缠态. 例如，若测量结果是$|\eta^+\rangle_{345}$，则粒子 1、2、6 就处于纠缠态$|\eta^+\rangle_{612}$；如果测量结果分别是$|\eta^-\rangle_{345}$、$|\xi^+\rangle_{345}$、$|\xi^-\rangle_{345}$，则粒子 1、2、6 分别处于$|\eta^-\rangle_{612}$、$|\xi^+\rangle_{612}$、$|\xi^-\rangle_{612}$纠缠态. 这样就实现了粒子 1、2、3 和粒子 4、5、6 之间的纠缠交换.

2　量子身份认证方案

根据$|W\rangle$态的量子隐形传态原理，我们提出一个具有理论安全性的量子身份认证方案. 方案包括注册阶段和认证阶段，认证系统包括主服务器 M 和客户端服务器 U. 各客户所有的操作都在 U 上进行，用户不直接与 M 进行通信，M 和 U 之间的信息交互通过量子隐形传态来实现.

2.1　注册阶段

假设 U 和 M 预先共享处于$|W\rangle$纠缠态的粒子 1、2、3，粒子 1 和 2 属于 U，粒子 3 属于 M.

某一用户个体通过 U 与 M 联系，如果联系是第一次，则先进行注册. 注册时用户在 U 上输入用户姓名、服务类型和用户密码等特征信息. U 根据用户提供的特征信息，制备处于量子态$|\psi\rangle_a$的粒子 a（$|\psi\rangle_a$包含了用户需要提供的所有特征信息），并对粒子 a、1、2 三个粒子在正交基$\{|\eta^\pm\rangle,|\xi^\pm\rangle\}$下进行联合投影测量. 然后通过经典信道把测量结果通告 M. 主服务器 M 再对粒子 3 进行适当的幺正变换，则粒子 3 的量子态就变为$|\psi\rangle_a$，这样 M 就获得了用户的特征信息，并在数据库中储存起来以备今后使用，并通知 U 用户注册成功，注册结束.

2.2　认证阶段

与注册阶段类似，U 和 M 预先共享处于$|W\rangle$态的粒子 1、2、3，用户在客户端 U 输入自己的特征信息. U 据此首先制备处于量子态$|\psi\rangle_a$的粒子 a，然后对粒子 a、1、2 进行联合投影测量，并将测量结果通过经典信道通知 M（主服务器），M 据此对粒子 3 进行相应的幺正变换，得到量子态$|\psi\rangle_a$，获得用户的特征信息，并和数据库中的特征信息进行比较，若完全一致，那么认证通过，否则认证不通过[16].

该量子身份认证方案具有简单、易实现的特点，但客户不能实现跨中心的身份认证. 下面根据文献[16]的思想，利用量子纠缠交换技术，提出基于$|W\rangle$纠缠态的可以实现网络中各客户的身份认证方案，实现跨中心的量子身份认证.

3　跨中心的量子身份认证方案

在网络分布式系统中，M_1、M_2、M_3…为相互信任的认证中心，每个 M_i 负责一定范围的客户端认证业务. 假设用户在 M_1 进行了注册，当他不在 M_1 而在其它（如 M_2）的服务范围内请求认证服务时，就要涉及到跨中心的身份认证. 采用量子纠缠交换技术可以实现跨中心的身份认证，扩大了认证范围.

如图 1，假设 M_1 和 M_2 是分布式系统中两个相互信任的认证中心，M_1 和 M_2 之间预先共享处于 $|W\rangle$ 态的三个粒子 4、5、6，其中粒子 6 在 M_1 处，用 $m_{1,6}$ 表示，粒子 4、5 在 M_2 处，用 $m_{2,45}$ 表示；又假设 M_1 和它服务范围内的第 i 个客户端 U_{1i} 之间预先共享处于 $|W\rangle$ 态的三个粒子 1、2、3，其中粒子 3 在 M_1 处，用 $m_{1i,3}$ 表示，粒子 1、2 在 U_{1i} 处，用 $u_{1i,12}$ 表示；M_2 和它服务范围内的第 j 个客户端 U_{2j} 也预先共享处于 $|W\rangle$ 态的三个粒子 1、2、3，其中粒子 3 在 M_2 处，我们用 $m_{2j,3}$ 表示，粒子 1、2 在 U_{2j} 处，用 $u_{2j,12}$ 表示. 用户在 M_1 服务范围内的某个客户端 U_{1i} 上完成了注册，信息存储在 M_1 处. 为了实现跨中心的量子身份认证，用户在注册时，除了输入表征自己身份的特征信息外，还必须把认证中心 M_i 的序列号加到数据库中.

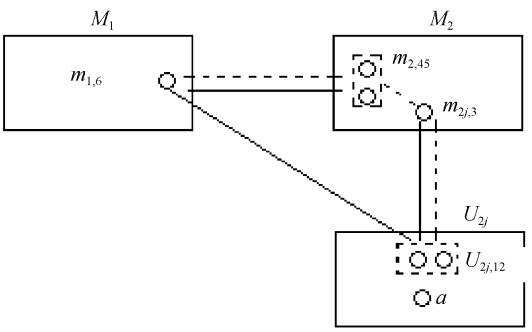

图 1 跨中心量子身份认证示意图

Fig. 1 Schematic diagram of cross-center quantum identity authentication

用户通过 M_2 进行跨中心量子身份认证的具体步骤为：

1) 在 M_2 服务范围内的某个客户端 U_{2j} 上，用户输入表征自己身份的特征信息和注册中心序列号；U_{2j} 通过经典信道把注册中心序列号传给 M_2，并根据用户特征信息制备处于量子态 $|\psi\rangle_a$ 的粒子 a；

2) M_2 根据序列号判断用户是在 M_1 处完成注册的，并决定将认证请求转移到 M_1 处；

3) 利用量子纠缠交换技术，M_2 通过对三个粒子 $m_{2,45}$ 和 $m_{2j,3}$ 在正交基 $\{|\eta^{\pm}\rangle, |\xi^{\pm}\rangle\}$ 下进行联合投影测量，将客户端 U_{2j} 的两个粒子 $u_{2j,12}$ 和 M_1 的一个粒子 $m_{1,6}$ 纠缠起来，并把测量结果通过经典信道告诉 M_1；

根据式(8)，M_2 对三个粒子 $m_{2j,3}$ 和 $m_{2,45}$ 测量的可能结果分别是 $|\eta^+\rangle_{345}$、$|\eta^-\rangle_{345}$、$|\xi^+\rangle_{345}$、$|\xi^-\rangle_{345}$，所以 $m_{1,6}$ 和 $u_{2j,12}$ 三个粒子所处的纠缠态分别对应为 $|\eta^+\rangle_{612}$、$|\eta^-\rangle_{612}$、$|\xi^+\rangle_{612}$、$|\xi^-\rangle_{612}$；再把步骤(1)中 U_{2j} 制备的粒子 a 和这三个粒子看成一个四粒子量子体系，则这个四粒子量子体系所处的可能量子态分别可表示为

$$|\psi\rangle_a\otimes|\eta^+\rangle_{612}=(\alpha|0\rangle_a+\beta|1\rangle_a)\otimes\frac{1}{2}(|010\rangle_{612}+|001\rangle_{612}+\sqrt{2}|100\rangle_{612})=\frac{1}{2}[|\eta^+\rangle_{a12}(\alpha|0\rangle_6+\beta|1\rangle_6)+$$
$$|\eta^-\rangle_{a12}(\alpha|0\rangle_6-\beta|1\rangle_6)+|\xi^+\rangle_{a12}(\beta|0\rangle_6+\alpha|1\rangle_6)+|\xi^-\rangle_{a12}(\beta|0\rangle_6-\alpha|1\rangle_6)] \tag{9a}$$

$$|\psi\rangle_a\otimes|\eta^-\rangle_{612}=(\alpha|0\rangle_a+\beta|1\rangle_a)\otimes\frac{1}{2}(|010\rangle_{612}+|001\rangle_{612}-\sqrt{2}|100\rangle_{612})=\frac{1}{2}[|\eta^+\rangle_{a12}(\alpha|0\rangle_6-\beta|1\rangle_6)+$$
$$|\eta^-\rangle_{a12}(\alpha|0\rangle_6+\beta|1\rangle_6)+|\xi^+\rangle_{a12}(\beta|0\rangle_6-\alpha|1\rangle_6)+|\xi^-\rangle_{a12}(\beta|0\rangle_6+\alpha|1\rangle_6)] \tag{9b}$$

$$|\psi\rangle_a\otimes|\xi^+\rangle_{612}=(\alpha|0\rangle_a+\beta|1\rangle_a)\otimes\frac{1}{2}(|110\rangle_{612}+|101\rangle_{612}+\sqrt{2}|000\rangle_{612})=\frac{1}{2}[|\eta^+\rangle_{a12}(\alpha|1\rangle_6+\beta|0\rangle_6)+$$
$$|\eta^-\rangle_{a12}(\alpha|1\rangle_6-\beta|0\rangle_6)+|\xi^+\rangle_{a12}(\alpha|0\rangle_6+\beta|1\rangle_6)+|\xi^-\rangle_{a12}(-\alpha|0\rangle_6+\beta|1\rangle_6)] \tag{9c}$$

$$|\rangle\psi_a\otimes|\xi^-\rangle_{612}=(\alpha|0\rangle_a+\beta|1\rangle_a)\otimes\frac{1}{2}(|110\rangle_{612}+|101\rangle_{612}-\sqrt{2}|000\rangle_{612})=\frac{1}{2}[|\eta^+\rangle_{a12}(\alpha|1\rangle_6-\beta|0\rangle_6)+$$
$$|\eta^-\rangle_{a12}(\alpha|1\rangle_6+\beta|0\rangle_6)+|\xi^+\rangle_{a12}(-\alpha|0\rangle_6+\beta|1\rangle_6)+|\xi^-\rangle_{a12}(\alpha|0\rangle_6+\beta|1\rangle_6)] \tag{9d}$$

4) M_2 告诉 U_{2j} 可以进行下一步操作，于是 U_{2j} 对三个粒子 a、$u_{2j,12}$ 在正交基 $\{|\eta^{\pm}\rangle, |\xi^{\pm}\rangle\}$ 下进行联合投影测量，U_{2j} 测量的可能结果分别为 $|\eta^+\rangle_{a12}$、$|\eta^-\rangle_{a12}$、$|\xi^+\rangle_{a12}$、$|\xi^-\rangle_{a12}$；

5) U_{2j} 将测量结果通过经典信道传给 M_2，M_2 再将这一结果通过经典信道传给 M_1；

6) 为了获得 $|\psi\rangle_a$ 和用户的特征信息，根据 M_2 和 U_{2j} 的测量结果，M_1 对粒子 $m_{1,6}$ 做适当的幺正变换，即获得了 $|\psi\rangle_a$. 例如：M_2 的测量结果为 $|\eta^+\rangle_{345}$，而 U_{2j} 的测量是 $|\xi^+\rangle_{a12}$，则 M_1 处的粒子 $m_{1,6}$ 的量子态为 $\beta|0\rangle_6+\alpha|1\rangle_6$，于是 M_1 把幺正变换 σ_x 作用于这个粒子，则这个粒子的量子态就变成粒子 a 的量子态 $|\psi\rangle_a$，获得用户的特征信息；

7) M_1 把获得的用户特征信息与数据库中的记录进行比较，若完全一致，则认证通过；若不完全一致，则认证不通过[16]；

8) M_1 把认证结果和必要的指令告诉 M_2，根据认证结果和指令，M_2 决定是否给用户提供相应的服务.

4　安全性分析

本方案共享的处于$|W\rangle$态的三个粒子采用量子密钥分发(QKD)的方案进行分发，因此本方案的安全性和 QKD 的安全性是一样的，是无条件安全的.

在身份认证的整个过程中，用户的所有操作都在客户端服务器上进行，服务器制备的表征用户特征信息的量子态$|\psi\rangle_a$在进行联合投影测量后被破坏，因此可以确保用户离开客户端服务器后其身份信息不会泄漏. 在量子信道上传送的量子态$|\psi\rangle_a$，除服务器以外，对任何人都是未知的(连用户自己也不知道). 根据不可克隆原理，未知的量子态不能克隆，因此这个方案在理论上是安全的. 另外，如果在量子信道上传送的量子态被攻击者改变，则结果将被改变，这表明攻击者的行为能被测定. 如果攻击者窃听量子信道，则$|W\rangle$态的纠缠性一定会被破坏，因此$|\psi\rangle_a$态不能传送到目的地. 在量子密码中，纠缠攻击是一种可能的攻击技巧. 但在本方案中，由于$|\psi\rangle_a$是未知的和秘密的，通过纠缠攻击不可能得知$|\psi\rangle_a$，因而不可能获得任何有用的客户信息. 纠缠攻击只会破坏原有粒子之间的纠缠性，导致认证不通过. 不知道用户密码和量子态$|\psi\rangle_a$的具体情况的攻击者，是不可能冒充通过认证的. 在经典信道上，传递的信息只是一些指令性的信息，不涉及用户的身份信息，因此，攻击者不可能从经典信道上得到有关用户的身份信息进行攻击.

从本文分析可知，所提出的方案是安全的.

5　结论

本文利用量子隐形传态原理和量子纠缠交换技术，详细介绍了基于$|W\rangle$态的跨中心量子网络身份认证方案. 该方案分为注册阶段和身份认证阶段，认证系统包括主服务器和客户端服务器. 客户所有的操作都在客户端服务器上进行，不直接与主服务器进行通信. 在注册阶段，用户在客户端服务器上输入反映自己特征的身份信息，并储存在相应的主服务器上，以备今后认证使用；在认证阶段，除用户在客户端服务器上输入反映自己特征的身份信息外，其他所有的身份认证过程全部由服务器根据量子力学原理进行，保证了认证方案的安全性，实现了分布式量子通信网络中对客户的身份认证. 就目前的技术来说，制备纠缠量子态已不成问题，但量子态的长期记忆和粒子间纠缠的长时间保持是个问题，如这一问题得以解决，上述方案就能应用和推广.

参考文献

[1] BENNET C H, BRASSARD G, CREPEAU C, *et al*. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rc6en channels[J]. *Phys Rev Lett*, 1993, **70**(13): 1895-1899.

[2] BOUWMEESTER D, PAN J W, MATTLE K, *et al*. Experimental quantum teleportation[J]. *Nature*, 1997, **390**: 575-579.

[3] SHI B S, TOMITA A. Teleportation of an unknown state by W state[J]. *Phys Lett A*, 2002, **296**(4-5): 161-164.

[4] CAI Xin-hua, NIE Jian-jun, GUO Jie-rong. Entanglement translation and quantum teleportation of the single-photon entangled state[J]. *Acta Photonica Sinica*, 2006, **35**(5): 776-778.

[5] XIONG Xue-shi, FU Jie, SHEN Ke. Controlled teleportation of an unknown two-particle partly entangled state[J]. *Acta Photonica Sinica*, 2006, **35**(5): 780-782.
熊学仕，付洁，沈柯. 二粒子部分纠缠未知态的量子受控传递[J]. 光子学报，2006，**35**(5)：780-782.

[6] BENNET C H, WIESNER S. Communication via one and two-particle operators on einstein- podolsky-rosen states[J]. *Phys Rev Lett*, 1992, **69**(20): 2881-2884.

[7] HAO J C, LI C F, GUO G C. Controlled dense coding using the Greenberger-Horne-Zeilinger state [J]. *Phys Rev A*, 2001, **63**(5): 054301-054303.

[8] EKERT A K. Quantum cryptography based on Bell's theorem [J]. *Phy Rev Lett.*, 1991, **67**(6): 661-663.

[9] GOBBY C, YUAN Z L, SHIELDS A J. Quantum key distribution over 122 km of standard telecom fiber[J]. *Appl Phys Lett*, 2004, **84**(19): 3762-3764.

[10] NIELSEN M A, CHUANG I L. Quantum computation and quantum information[M]. Cambridge: Cambridge University Press, 2000.

[11] DUŠE K M, HADERKA O, HENDRYCH M, *et al*. Quantum identification system[J]. *Phys Rev A*, 1999, **60**(1): 149-156.

[12] CURTY M, SANTOS D J. Quantum authentication of classical messages[J]. *Phys Rev A*, 2001, **64**(6): 062309.

[13] MIHARA T. Quantum identification schemes with entanglements[J]. *Phys Rev A*, 2002, **65**(5): 052326.

[14] ZENG G H, ZHANG W P. Identity verification in quantum key distribution[J]. *Phys Rev A*, 2000, **61**(2): 022303.

[15] WEN Xiao-jun, LIU Yun, ZHANG Zhen-jiang. Identification scheme in quantum communication network[J]. *Journal of Beijing Jiaotong University*, 2004, **28**(5): 66-68.
温晓军，刘云，张振江. 量子通信网络中的身份认证方案[J]. 北京交通大学学报，2004，**28**(5)：66-68.

[16] ZHOU N R, ZENG G H, ZENG W J, *et al*. Cross-center quantum identification scheme based on teleportation and entanglement swapping[J]. *Opt Commun*, 2005, **254**(4-6): 380-388.

[17] CABELLO A. Bell's theorem with and without inequalities for the three-qubit Greenberger-Horne-Zeilinger and W states [J]. *Phys Rev A*, 2002, **65**(3): 032108.

[18] GORBACHEV V N, RODICHKINA A A, TRUBILKO A I, *et al*. On preparation of the entangled W-states from atomic ensenbles[J]. *Phys Lett A*, 2003, **310**(5-6): 339-343.

[19] AGRAWAL P, PATI A. Perfect teleportation and superdense coding with W-states[J]. *Phys Rev A*, 2006, **74**(6): 062320.

[20] LI L Z, QIN D W. The states of W-class as shared resources for perfect teleportation and superdense coding[J]. *J Phys A: Math Theor*, 2007, **40**(35): 10871-10885.

Quantum Identification Scheme of Cross-center Based on W-state

LI Yuan-hua[1], LIU Jun-chang[1], NIE Yi-you[1, 2]

(1 *Department of physics, Jiangxi Normal University, Nanchang* 330022, *China*)

(2 *Key Laboratory of Photoelectronic & Telecommunication of Jiangxi Province, Nanchang* 330022 *China*)

Abstract: Using the quantum teleportation and quantum entanglement swapping, a quantum identification scheme of Cross-center based on W-state is proposed, and the identification for user in distributed network is realized. The scheme includes register phase and authentication phase, and the whole system consists of main server and client server. All the operations of any user are processed at client server and there is no direct communication between user and main server. All authentications are processed by servers based on the principles of quantum mechanics, and its security is guaranteed by quantum mechanism. Finally, the security of the quamtum identification scheme is analyzed.

Key words: Quantum communication; Quantum identification; Quantum teleportation; Quantum entanglement swapping; W-state

LI Yuan-hua was born in 1984. Now he is pursuing the M. S. degree, and his research interests focus on quantum optics and quantum information.

NIE Yi-you was born in 1963. As a professor, his research interests focus on quantum optics, quantum computation and quantum information.