文章编号：0253-2239(2009)06-1680-04

基于三粒子 W 态的身份认证

胡 杏[1] 郁季军[2] 宁小玲[3] 刘 玉[2]

([1]华中科技大学计算机科学与技术学院，湖北 武汉 430074；[2]华中科技大学电子与信息工程系，湖北 武汉 430074
[3]中国科学院武汉物理与数学研究所，湖北 武汉 430074)

摘要 无认证中心的认证协议一般由通信双方相互认证，事先共享纠缠态或身份密钥，结构简单，但不适于扩展成通信网络。通过引入可信第三方认证中心，并利用三粒子 W 纠缠态的稳健性，提出了一个基于 W 态的身份认证协议，使得合法通信用户可以在认证中心的协助下进行安全身份认证，身份认证的同时即完成了纠缠粒子的分发。认证完成后，合法通信用户可安全共享 EPR 纠缠态并在第三方的控制下进行量子直传通信。针对窃听者常用攻击手段进行了安全性分析，结果表明在身份认证过程中可以有效的抵御伪装攻击，截取重发攻击与纠缠攻击等。基于第三方的通信结构具有可扩展性、实用性和受控性。

关键词 量子光学；量子通信；量子身份认证；W 纠缠态；隐形传态

中图分类号 O413 **文献标识码** A **doi**：10.3788/AOS20092906.1680

Quantum Identity Authentication Using Three-Particle W state

Hu Xing[1] Yu Jijun[2] Ning Xiaoling[3] Liu Yu[2]

([1] *College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, Hubei* 430074, *China*
[2] *Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan, Hubei* 430074, *China*
[3] *Wuhan Institute of Physics and Mathematics, Chinese Academic of Sciences, Wuhan, Hubei* 430074, *China*)

Abstract Some quantum identity authentication (QIA) protocols enable both communication parties to authenticate each other by sharing entanglement or identity keys beforehand and they always go without a certificated authority (CA). Such kind of authentication structure is simple but not easy to extend into integrated network. An authority-based secure QIA protocol is proposed using the robust entanglement of W state. With the help of CA, two legitimated communication parties can identify each other faithfully and simultaneously share the entangled particles for later controlled communication. Security analysis shows that QIA remains secure even confront with several typical individual attacks. The authority-based model ensures the security complete with expandability, practicality and controllability.

Key words quantum optics; quantum communication (QC); quantum identity authentication (QIA); W entangled state; teleportation

1 引 言

自从 Bennett 和 Brassard 在 1984 年提出基于量子力学分发密钥的量子密钥分配(QKD)协议 BB84[1]以来，量子信息学经过多年的研究取得了丰富的成果[2]。量子密码协议不断涌现，Ekert 于 1991 年提出用 EPR 纠缠对进行密钥分发[3]。2002

收稿日期：2008-08-04；**收到修改稿日期**：2008-10-30

基金项目：国家航天科技创新基金(20060110)和华中科技大学大学生科技创新基金资助课题。

作者简介：胡 杏(1988—)，女，主要从事量子保密通信方面的研究。E-mail：XingHu.cs@gmail.com

导师简介：刘 玉(1957—)，女，教授，主要从事量子保密通信、信息安全和嵌入式系统等方面的研究。E-mail：liuyu@hust.edu.cn

年 Beige 等人用 EPR 纠缠对构造了首个量子明文直传(QSDC)协议[4]，使得明文可以通过量子信道传输。不久，Bostrom 和 Felbinger 使用纠缠态构造了更易操作的乒乓协议[5,6]，还有量子对话协议[7]。然而，无论是 QKD、QSDC 还是量子对话协议(QD)，都要求密钥、明文传递给特定的用户，其安全性必须以通信双方身份合法为基础，量子身份认证(QA)正是在此需求下不断发展[8~11]。M. Dusek 提出了结合经典消息认证算法的量子身份认证协议[8]，此后不同的文献采用了不同的认证方案。根据是否存在第三方认证中心可分为不依赖于第三方[12]和依赖于第三方[13]的认证方案。根据共享信息类型的不同也可以分为共享信息型[7,14]，共享纠缠态型[15]等。量子信道也不单一，例如 EPR 对[12]、GHZ 态等。由 Lee，Lim，Yang 提出了利用 CHZ 态实现结合量子身份认证的安全直传通信，随后 Zhang 等人对此协议进行了改进使其能够抵御中间人攻击[16]。需要注意的是，GHZ 态处于最大纠缠态，但易损。另一种不同与 GHZ 态的多粒子纠缠态 W 态引起了人们的兴趣。Dür 指出 W 态虽然不处于最大纠缠态，但比 GHZ 态更强健，在丢失一个粒子的情况下具有最好的稳健性[17]。并且，由于可以直接使用 W 态，而不用从 W 态中提取 GHZ 态，所以更加便于实验实现。目前已经提出了多种基于 W 态的 QSDC 协议[18~20]。在此，提出了一种基于三粒子 W 态的身份认证协议。

2　基于 W 态的身份认证协议

认证过程由 Alice，Bob 和 Trent 三方共同完成，其中 Trent 为可信认证中心(CA)，由其制备和分发粒子，协助 Alice 和 Bob 完成身份认证和受控量子安全通信。

在身份认证过程中，Trent 事先分别与 Alice 和 Bob 共享他们的身份密钥 ID_A、ID_B 和单值散列函数 $H_A(X)$、$H_B(X)$，并由 $K=H(ID)$ 得到操作秘密信息 K_A、K_B，以保证身份密钥不直接用于编码，降低被窃取的可能性。

通信模型如图 1 所示，以 Alice 发起认证和通信请求为例。

首先，Alice 发起认证需求并在经典信道上通知 Trent。Trent 制备足够多 $|W\rangle$ 态粒子序列 $\boldsymbol{P}=\{W_1、W_2、\cdots、W_n\}$，其中

$$|W_i\rangle=\frac{1}{\sqrt{3}}(|001\rangle+|010\rangle+|100\rangle)_{ATB},\quad(1)$$

并根据与 Alice(Bob)共享的操作秘密信息 K_A、K_B 分别对 A(B)粒子进行操作。若 $K_A(K_B)=0$，则进行 $\boldsymbol{H}$ 操作；若 $K_A(K_B)=1$，则进行 $\boldsymbol{ZH}$ 操作，粒子态变为

$$|W\rangle_1=\{(1-K_A)\boldsymbol{H}+K_A\boldsymbol{ZH}\}_A\otimes\{(1-K_B)\boldsymbol{H}+K_B\boldsymbol{ZH}\}_B|W\rangle,\quad(2)$$

操作完毕，将粒子发往 Alice(Bob)。

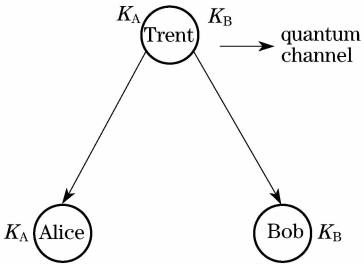

图 1　通信模型框图

Fig. 1　Communication Scenario

然后，Alice(Bob)根据 $K_A(K_B)$ 对收到的粒子进行恢复性操作，若 $K_A(K_B)=0$，则进行 $\boldsymbol{H}$ 操作，若为 $K_A(K_B)=1$，则进行 $\boldsymbol{HZ}$ 操作，粒子态变为

$$|W\rangle_2=\{(1-K_A)\boldsymbol{H}+K_A\boldsymbol{HZ}\}_A\otimes\{(1-K_B)\boldsymbol{H}+K_B\boldsymbol{HZ}\}_B|W\rangle_1=|W\rangle,\quad(3)$$

由式(3)可知，恢复操作完成后，在无窃听的情况下，Alice、Bob、Trent 手中的粒子应该还原成 $|W\rangle$ 粒子。若三人随机选择同样的子集 $C(C\subseteq P)$ 并分别对三粒子进行测量，要求 Bob 和 Trent 先后公布测量结果，则 Alice 可根据测量结果是否出现非法态来判断 Eve 的存在。若 Alice 检查公布的结果发现出现不符合三粒子 $|W\rangle$ 态的特征，如 110，则意味着错误。当误码率超过一定限度，可认为对方身份不合法或认证过程中存在 Eve，应重新开始认证。

由上可见，量子身份认证的同时完成了 $|W\rangle$ 态的分发，认证完成后，三方即共享 $|W\rangle$ 纠缠粒子序列 $M(M=P-C)$，Alice 和 Bob 可利用这些纠缠粒子在 Trent 的控制下进行通信。具体地，对 $|W\rangle$ 变形有

$$|W\rangle=\frac{1}{\sqrt{3}}(|01\rangle+|10\rangle)_{AB}|0\rangle_T+\frac{1}{\sqrt{3}}|00\rangle_{AB}|1\rangle_T,\quad(4)$$

由式(4)可见当 Trent 测量结果为 $|0\rangle_T$ 时，M 序列相应位置上 A、B 粒子处于纠缠态 $|\phi^+\rangle=(1/\sqrt{2})(|10\rangle+|01\rangle)$。当 Alice 和 bob 要求通信时，只要 Trent 告知处于纠缠的粒子的位置信息，Alice 和 Bob 即可利用任意基于共享纠缠态的方法[4,5,6]进行直传通信[21]。公式(4)也反映出 Alice 和 Bob 之间

的通信是受 Trent 控制的[22]，即没有 Trent 手中的粒子信息，通信双发无法进行确定性的通信。

3 身份认证及受控通信安全性分析

以上认证及通信过程都是在没有 Eve 的理想情况下进行的。这里将考虑有 Eve 的存在。对身份认证过程，分为伪装攻击、截取重发攻击和纠缠攻击三种典型攻击方式证明其安全性，并将对直传通信的受控特性进行分析，如图 2 所示。

3.1. 伪装攻击

当 Eve 伪装成 Bob 希望通过认证时即伪装攻击。可以发现 Bob 被 Eve 隔离，并不知道 Alice 发起身份认证。由于 Eve 不知道 Bob 的身份密钥 ID_B 和散列函数 $\boldsymbol{H}_B(\boldsymbol{X})$，则不知道操作信息 K_B。在恢复操作的步骤时，若 Eve 选错操作，由于 $(\boldsymbol{HZ})\boldsymbol{H}=\boldsymbol{H}(\boldsymbol{ZH})=\boldsymbol{X}$，相当于 Eve 对 B 粒子进行了 $\boldsymbol{X}$ 操作，态变成为

$$|W\rangle_e=\frac{1}{\sqrt{3}}(|000\rangle+|011\rangle+|101\rangle)_{ATB}. \quad (5)$$

可见 Eve 选错操作时会以 1 的概率使纠缠态坍塌到非法态上，从而通过比对测量结果必然可以检测出 Eve 的存在。考虑到 Eve 选对操作和选错操作的概率各为 0.5，故检测出 Eve 的概率为 0.5。

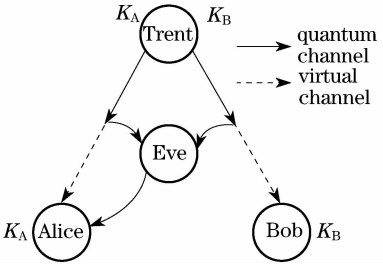

图 2 伪装攻击和截取重发攻击模型

Fig. 2 Camouflage attack and intercept-resend attack scenario

3.2 截取-测量-重发攻击

进一步，为提高伪装成功的概率，Eve 可能进行截取-测量-重发攻击，如截取 A、B 粒子进行联合测量，并根据测量结果制备粒子 A_E、B_E 并将 A_E 重新发给 Alice，自己保留 B_E，此时 Bob 仍不知道 Alice 发起认证。

其中 $|\phi^{\pm}\rangle=(1/\sqrt{2})(|00\rangle+|11\rangle)$，$|\psi^{\pm}\rangle=(1/\sqrt{2})(|01\rangle+|10\rangle)$。由表 1 知，若 Eve 测得 ψ^- 或 ψ^+ 时，可确切地知道 Trent 手中的粒子状态为 $|1\rangle$。此时必须保证传递给 Alice 的粒子在 Alice 进行恢复操作 $\boldsymbol{H}$ 或 $\boldsymbol{HZ}$ 后变为 $|0\rangle$，但分析知 Eve 不能以 1 的概率成功。若 Eve 测得 ϕ^- 或 ϕ^+ 时，Eve 不能够知道 Trent 手中的粒子状态，只能猜测。经过分析，可以以比较高的概率发现 Eve 的存在，当粒子数目很大时，协议渐进安全。

表 1 Eve 纠缠攻击获取信息表

Table 1 Eve's information from entanglement attack

Results of Eve's joint measurements on A and B	Trent's operations on A and B (C_A/C_B)	State of Trent's particle
ϕ^+	$\boldsymbol{H}/\boldsymbol{H}$、$\boldsymbol{ZH}/\boldsymbol{ZH}$	$\|1\rangle$
	$\boldsymbol{ZH}/\boldsymbol{H}$、$\boldsymbol{H}/\boldsymbol{ZH}$	$\|0\rangle$
ϕ^-	$\boldsymbol{H}/\boldsymbol{H}$、$\boldsymbol{ZH}/\boldsymbol{ZH}$	$\|0\rangle$
	$\boldsymbol{ZH}/\boldsymbol{H}$、$\boldsymbol{H}/\boldsymbol{ZH}$	$\|1\rangle$
ψ^+	$\boldsymbol{H}/\boldsymbol{H}$、$\boldsymbol{ZH}/\boldsymbol{ZH}$	$\|1\rangle$
ψ^-	$\boldsymbol{ZH}/\boldsymbol{H}$、$\boldsymbol{H}/\boldsymbol{ZH}$	$\|1\rangle$

3.3 纠缠攻击

在 Trent 将 A 粒子发送给 Alice 的途中，Eve 可将其预先制备的粒子和 A 粒子进行关联操作，如以 Alice 手中量子位为控制位，Eve 手中粒子为靶位进行 CNOT 操作，以求获得信息。不失一般性，设 $K_A=K_B=0$，经 Eve 操作后整个粒子态为

$$\boldsymbol{H}_A\otimes\boldsymbol{H}_B|W\rangle_{ATB}|0\rangle_E\xrightarrow{\text{CNOT}}(1/\sqrt{2})\times(|W'\rangle_{ATB}|-\rangle_E+|W\rangle_{ATB}|+\rangle_E), \quad (6)$$

其中 $|W'\rangle=(1/\sqrt{3})(|000\rangle+|101\rangle+|110\rangle)$，若 Eve 测量结果为 $|-\rangle$ 时，一定会造成错误，可见 Eve 若进行纠缠攻击有 1/2 的概率被发现。但不管 Eve 是否被发现，它都不能窃取关于 K_A、K_B 的任何信息，如图 3 所示。

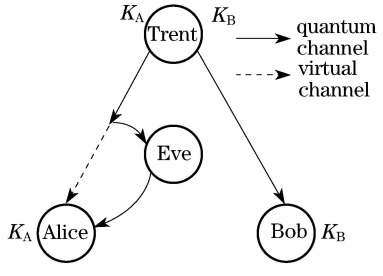

图 3 纠缠攻击模型

Fig. 3 Entanglement attack scenario

4 结 论

介绍了一种基于 W 态的身份认证和直传通信方案，通过对 Eve 采用的典型攻击手段对身份认证的安全性进行了分析。协议可以抵御截取重发、纠缠等攻击，能以较高的概率探测出 Eve。引入第三方认证中心提高了协议的实用价值，具有一定的应用前景。

参 考 文 献

1 C. H. Bennett, G. Brassard. Quantum cryptography: public key distribution and coin tossing [C]. *IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984): 175～179

2 Wang Juxia, Yang Zhiyong, An Yuying. Quantum information transfer via multi-photon interaction [J]. *Acta Optica Sinica*, 2007, **27**(8): 1508～1512
王菊霞,杨志勇,安毓英. 利用多光子相互作用实现量子信息传递[J]. 光学学报, 2007, **27**(8): 1508～1512

3 A. K. Ekert. Quantum cryptography based on bell's theorem [J]. *Phys. Rev. Lett.*, 1991, **67**(6): 661～663

4 A. Beige, B. G. Englert, Kurtsiefer *et al*.. Secure communication with a publicly know key[J]. *Acta Phys. Pol.* A, 2002, **101**(3): 357～368

5 Kim Boström, Timo Felbinger. Deterministic secure direct communication[J]. *Phys. Rev. Lett.*, 2002, **89**(18): 187902-1～4

6 Wang Xiaoxin, Liu Yu, Wang Changqiang. Experimental scheme of secure plaintext transmission with quantum direct communication[J]. *Acta Optica Sinica*, 2005, **25**(3): 425～428 (in Chinese)
王晓鑫,刘　玉,王长强. 安全传送明文的量子直传实验方案设计[J]. 光学学报, 2005, **25**(3): 425～428

7 Piao Guangchun, Zhang Shou. Controlled quantum dialogue based on W state [J]. *Chin. J. Quant. Electron.*, 2007, **24**(3): 311～315

8 Miloslav Dušek, Ondřej Haderka, Martin Hendrych *et al*.. Quantum identification system[J]. *Phys. Rev. A*, 1999, **60**(1): 149～156

9 Takashi Mihara. Quantum identification schemes with entanglements [J]. *Phys. Rev. A*, 2002, **65**: 052326-1～052326-4

10 Wim van Dam. Comment on "Quantum identification schemes with entanglements" [J]. *Phys. Rev. A*, **68**: 026301-1～026301-4

11 He Guangqiang, Zeng Guihua, Zhu Jun. An integrable optic-fiber coherent state quantum identification system [J]. *Chin. J. Lasers*, 2007, **34**(7): 924～929 (in Chinese)
何广强,曾贵华,朱　俊. 可光纤集成的相干态量子身份认证系统[J]. 中国激光, 2007, **34**(7): 924～929

12 Guihua Zeng, Weiping Zhang. Identity verification in quantum key distribution [J]. *Phys. Rev. A*, 2000, **61**: 022303-1～022303-5

13 Hwayean Lee, Jongin Lim, HyungJin Yang. Quantum direct communication with authentication [J]. *Phys. Rev. A*, 2006, **73**: 042305-1～042305-4

14 D. Ljunggren, M. Bourennane, A. Karlsson. Authority-based user authentication in quantum key distribution[J]. *Phys. Rev. A*, 2000, **62**: 022305-1～022305-6

15 Shi Baosen, L Jian, Liu Jinming *et al*.. Quantum key distribution and quantum authentication based on entangled state [J]. *Phys. Lett. A*, 2001, **281**: 83～87

16 Zhanjun Zhang, Jun Liu, Dong Wang *et al*.. Comment on "Quantum direct communication with authentication"[J]. *Phys. Rev. A*, 2007, **75**: 026301-1～026301-4

17 W. Dür, G. Vidal, J. I. Cirac. Three qubits can be entangled in two inequivalent ways[J]. *Phys. Rev. A*, 2000, **62**: 062314-1～062314-5

18 Cao Haijing, Song Heshan. Quantum secure direct communication with W State[J]. *Chin. Phys. Lett.*, 2006, **23**(2): 290～292

19 Liu Jun, Liu Yimin. Revisiting quantum secure direct communication with W state[J]. *Chin. Phys. Lett.*, 2006, **23**(10): 2652～2655

20 Yuan Hao, Liu Yimin, Zhang Wen *et al*.. Eavesdropping on quantum secure communication with W state in noisy channel[J]. *Commun. Theor. Phys.* 2008, **49**(1): 103～106

21 C. Bennett, G. Brassard, C. Crepeau *et al*.. Teleporting an unknown quantum state via dual classical and EPR channels[J]. *Phys. Rev. Lett.*, 1993, **70**: 1895～1899

22 Yue Li, Yu Liu, Quantum secure direct communication based on supervised teleportation [C]. *SPIE*, 2007, **6827**: 682707～682714