doi:10.11959/j.issn.1000-436x.2016041

基于测量设备无关协议的量子身份认证方案

董颖娣[1,2]，彭进业[1]，张晓博[1]，张振龙[2]
（1. 西北工业大学电子信息学院，陕西 西安 710072；2. 西安建筑科技大学信息与控制工程学院，陕西 西安 710055）

摘 要：借助测量设备无关量子密钥分配协议的安全性，提出了测量设备无关的量子身份认证协议。在此协议下，认证中心和认证方以共享密钥加密认证信息和认证密钥，将其发送至第三方进行贝尔态测量以提取安全的认证信息，实现认证中心对认证方有效认证，并更新共享密钥。分析协议性能显示，系统在不同攻击下认证过程是安全且有效的。

关键词：量子身份认证；量子密钥分配；测量设备无关；贝尔态测量
中图分类号：TN911 **文献标识码**：A

Quantum identity authentication scheme based on measurement-device-independent quantum key distribution protocol

DONG Ying-di[1,2], PENG Jin-ye[1], ZHANG Xiao-bo[1], ZHANG Zhen-long[2]
(1. School of Electronics and Information, Northwestern Po ytechnical University, Xi'an 710072, China;
2. School of Information and Control Engineering, Xi'an University of Architecture and Technology, Xi'an 710055, China)

Abstract: Utilized to security properties of measurement-device-independent quantum key distribution (MDI-QKD) protocol, quantum identity authentication scheme based on MDI (QIA-MDI) protocol was presented. In this protocol, authentication center (AC) and authentication user have encrypted authentication information and next authenticated key by shared key, and then they transmitted the encrypted information to untrusted third party for Bell-state measurement (BSM). The secret authentication information was obtained through the BSM result, which can verify the communicator identity and update shared key. The security performance of the proposed scheme is extensively analyzed and accordingly con?rmed in the case of attacks.

Key words: quantum identity authentication, quantum key distribution, measurement-device-independent, Bell-state measurement

1 引言

量子密钥分配(QKD, quantum key distribution)协议以量子力学和量子信息论框架中的无条件安全性[1,2]已成为国内外的研究热点[3,4]。量子身份认证(QIA, quantum identity authentication)作为 QKD 系统的重要分支，检测 QKD 协议中通信双方的假冒行为，防止量子比特被攻击者非法获取导致合法用户信息安全性下降。QIA 是 QKD 系统获取安全密钥的前提，为通信双方身份合法性提供重要依据。QIA 利用量子不可克隆性及量子测不准原理[5]对输入者个人信息进行某种方式的处理并与系统中预先存储的个人信息进行比较，从而对个人身份进行肯定或者否定的判定。在此，要求身份认证系统的三重组合[6]中（I 为示证者个人信息集合；T 为信息处理系统；D 为数据库系统）至少有一个具有量子特征，当认证系统三重组合均为量子特征时，即为纯量子身份认证系统。

1999 年，Dusek 等[7]首先提出用经典信息认证算法对量子密钥系统经典消息进行认证的方案，从而达到抗干扰信道的效果，但方案没有充分利用量子的物理性质。2000 年，曾贵华[8,9]利用量子的物理特性，提出了可信赖中心的 QIA，在此基础上进一步研究了无可信赖中心的量子身份认证方案，此方案采用认证密钥加密认证者量子信息以实现对认证方的动态认证过程，认证顺序进行了改进，代替了经典公钥认证

收稿日期：2015-05-04；修回日期：2015-07-20
通信作者：董颖娣，tongxindyd@126.com

方案，弥补了之前方案的不足，但算法过于复杂。同年，周南润等[10]以量子纠缠交换及远距传输的相关性提出了跨中心量子身份认证方案，解决了分布式量子网络中的身份认证问题。2005 年，杨宇光等[11]提出一种多用户量子身份认证和密钥分配方案，该方案利用 EPR 纠缠态和可信服务器实现网络中用户之间的身份认证和密钥分配，但需要对纠缠态存储。张哲砷等[12]提出一个基于 ping-pong 协议量子身份认证方案，该方案安全地实现了认证密钥的更新。2009 年，张兴兰[13]提出一种基于公钥的量子身份认证方案，方案利用可信的认证中心(CA)完成认证，但是该方案的认证过程比较简单不适合在网络中应用。2010 年，李渊华[14]提出基于 W 态的跨中心的量子身份认证方案，实现了客户在分布式量子通信网络中的身份认证。除以上介绍的量子认证方案，利用量子态的非正交性、纠缠态及 GHZ 态进行量子身份认证及量子多方身份认证[15~17]也已相继展开。

然而以上所提身份认证过程均在 QKD 系统中实现，由于 QKD 系统探测单元存在各种非完美性，使系统存在一定的安全漏洞，如针对探测器非完美性的伪态攻击[18]、时移攻击[19]、致盲攻击等，导致认证信息不安全，认证安全性低。为了建立更加安全、高效的身份认证过程，本文提出了基于测量设备无关量子密钥分配协议[20]的量子身份认证(MDI-QIA, measurement-device-independent QIA)方案。在 MDI-QIA 系统中，认证中心和认证方转换共享密钥后对认证信息和认证密钥加密，将量子信息通过量子门加密后发送到不可信第三方（measurement unit），在第三方以分束器、偏振分束器及探测器完成量子态的贝尔测量，并以公开信道公布测量结果；认证中心通过基对比获取认证信息，以此完成对认证方的认证。本文借助测量设备无关协议完成身份认证过程，以此去除认证过程的量子边带攻击，提高认证信息的安全性。

本文主要目的是实现量子测量设备无关协议框架下的身份认证过程。首先刻画出量子身份认证过程框架，并细化了认证协议的步骤；对所提方案进行安全性和有效性分析；数值仿真结果表示该协议在不同攻击下是均是安全的。此研究是测量设备无关技术于身份认证中的典型应用，研究成果对量子保密通信的发展具有一定的推动意义。

2 协议描述

1) 准备阶段

Alice 制备纠缠态粒子对，将粒子$|\gamma_a\rangle$存储，将粒子$|\gamma_b\rangle$传输至 Bob 端作为共享密钥，两粒子之间关系满足

$$|?\rangle=\frac{1}{\sqrt{2}}(|0_a 0_b\rangle+|1_a 1_b\rangle) \tag{1}$$

2) 认证密钥的转换

认证中心与认证方共享密钥定义为量子非正交比特串 $K=\{|k_1\rangle,|k_2\rangle,|k_3\rangle\cdots|k_n\rangle\}$，令 $|k_i\rangle=a_i|0\rangle+b_i|1\rangle(i=1,2,3,\cdots,n)$，在此，$\{a_i,b_i\}\in\left\{\{1,0\},\left\{\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}}\right\},\left\{\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}}\right\},\{0,1\}\right\}$，则 $|k_i\rangle$ 可以转换为 $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ 中任意的量子态，以此作为最后认证判断的标准。

3) 认证过程

量子身份认证框架下，Alice 为可信认证中心，Bob 为需要认证的用户，不可信第三方为参与认证过程的辅助方，实现量子贝尔态测量及转发，测量设备无关协议框架下的量子身份认证过程如图 1 所示。

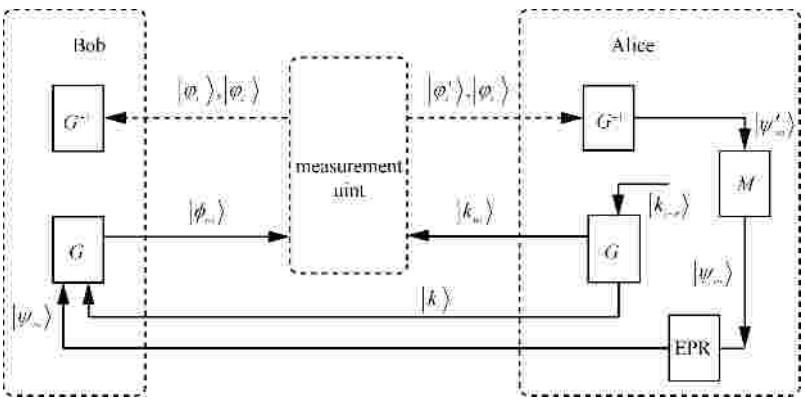

图 1 测量设备无关框架下的量子身份认证

Bob 端将认证量子态$|y_{bi}\rangle$以量子逻辑门 G 转化为$|f_{wi}\rangle$，Alice 端将认证密钥$|k_{i+n}\rangle$以量子逻辑门 G 转化为$|k_{wi}\rangle$，此过程由 Step1 及 Step2 完成。

Step1　$|f_{wi}\rangle,|k_{i+n}\rangle$首先通过量子逻辑$C_P$转换

$$|f_{wci}\rangle = C_P(|y_{bi}\rangle) \tag{2}$$

量子逻辑C_P在共享密钥$|k_i\rangle$作用下由方程组（3）实现。

$$\begin{cases} C_{P1} = \boldsymbol{I}, & |k_i\rangle = |0\rangle \\ C_{P2} = \boldsymbol{X}, & |k_i\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ C_{P3} = \boldsymbol{H}, & |k_i\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ C_{P4} = \boldsymbol{Z}, & |k_i\rangle = |1\rangle \end{cases} \tag{3}$$

其中，$\boldsymbol{I}$ 表示单位矩阵，$\boldsymbol{H}$ 表示 Hardmard 矩阵，$\boldsymbol{Z}$ 和 $\boldsymbol{X}$ 表示泡利矩阵。同理，$|k_{i+n}\rangle$通过量子逻辑门C_P作用后量子态为$|k_{wci}\rangle$。

Step2　经过量子逻辑门C_P后量子态继续通过式(4)进行归一化。

$$\begin{cases} |f_{wi}\rangle = H(|f_{wci}\rangle) \\ |k_{wi}\rangle = H(|k_{wci}\rangle) \end{cases} \tag{4}$$

量子逻辑门G 的线路表达如图 2 所示。

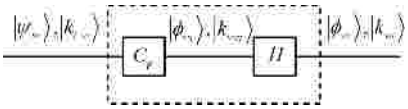

图 2　G 量子逻辑门框架

Step3　Alice 和 Bob 将量子态$|f_{wi}\rangle$、$|k_{wi}\rangle$发送至第三方进行非局域关联后，由偏振分束器、探测器对贝尔态$|j_i^{\pm}\rangle$ (量子态$|j_i^{\pm}\rangle$是由$|f_{wi}\rangle$、$|k_{wi}\rangle$构成的贝尔测量基)进行测量，结果通过经典公开信道反馈至 Alice 与 Bob 端。根据 MDI 的基本原理[21]，Alice 通过贝尔态$|j_i^{\pm}\rangle$获取 Bob 发送的认证量子态$|j_{wi}\rangle$；同理，Bob 可以获取 Alice 发送的量子态$|k_{i+n}\rangle$。

认证中心 Alice 判断 Bob 身份时，首先将量子态$|f_{wi}\rangle$送至量子逻辑门G^{-1}变换为$|y'_{wi}\rangle$，以测量算符同时测量$|y'_{wi}\rangle$、$|y_{ai}\rangle$量子态，当两者测量结果相同，则 Bob 为合法用户，否则，为非法用户，具体步骤如 Step4 及 Step5 所示。

Step4　Alice 端量子$|f_{wi}\rangle$通过量子逻辑门G^{-1}变换，G^{-1}由 Hardmard 门及C_P^{-1}门线性组成。C_P^{-1}逻辑门可以用式(5)表示。

$$\begin{cases} C_{P1}^{-1} = \boldsymbol{I}^{-1}, & |k_i\rangle = |0\rangle \\ C_{P2}^{-1} = \boldsymbol{X}^{-1}, & |k_i\rangle = \dfrac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \\ C_{P3}^{-1} = \boldsymbol{H}^{-1}, & |k_i\rangle = \dfrac{1}{\sqrt{2}}(|1\rangle - |0\rangle) \\ C_{P4}^{-1} = \boldsymbol{Z}^{-1}, & |k_i\rangle = |1\rangle \end{cases} \tag{5}$$

Bob 端将$|k_{wi}\rangle$过量子逻辑门G^{-1}，得到还原的量子态$|k_{i+n}\rangle$作为后继认证密钥。

Step5　在量子测量单元采用同样测量算符 M 对$|y'_{wi}\rangle$及$|y_{ai}\rangle$量子态投影测量[22]，如式(6)所示。

$$\begin{cases} \bar{M}_A = \langle y_{ai}|M|y_{ai}\rangle \\ \bar{M}_W = \langle y'_{wi}|M|y'_{wi}\rangle \end{cases} \tag{6}$$

如满足$\bar{M}_A = \bar{M}_W$，Bob 为合法用户。同理，Bob 端经过计算获得$|k_{i+n}\rangle$将为后续认证的共享密钥，此次认证过程完成。

3　安全性分析及协议效率

安全性分析是判断身份认证过程是否正确的判断标准。协议从经典攻击和量子攻击 2 方面研究所提方案的安全性，并讨论身份认证的初始阶段及认证阶段的安全性能；最后讨论了协议的执行效率。

3.1　协议攻击分析

在经典攻击策略条件下，攻击者以中间人方式攻击信道，或者借助合法通信者间的经典过程窃取信息，从而获得所谓的边信息[9]。量子密码通信过程中假定攻击者是不能同时获得量子信道和经典信道的信息，即使攻击者得到不可信第三方的贝尔态测量后经典信息，由于测量设备无关协议的安全属性，攻击者即使得到经典信息也无法精确得到认证中心 Alice 及认证方 Bob 中发送的量子态信息，即无法精确获取认证密钥及认证信息，从而无法实现攻击策略。

在量子攻击条件下，在量子身份认证的初始阶段，攻击者 Eve 以截获攻击共享密钥，由于共享密钥采用非正交的量子比特，由量子不可克隆定理及量子力学的测不准原理保证，攻击者不能同时精确

复制非正交的量子比特，即不诚实的攻击者不能复制 Alice 与 Bob 之间共享密钥，从而保证了后继认证过程的安全性。

在量子认证阶段，攻击者以截获/重发攻击或者纠缠攻击获取信息。首先分析截/转发攻击，假设窃听者 Eve 以幺正操作截获 Bob 的认证信息，但认证信息是以共享密钥加密的，由于 Eve 无法获取共享密钥，则其无法精确得到 Bob 认证信息。

由于纠缠攻击比其他攻击更具有威胁性[23]，其认证方与认证中心之间的交互的密钥率最低，考虑在此攻击条件下的系统安全密钥率更具有可行性。在 MDI-QIA 系统中，经过量子逻辑门 G 后量子态为 $|f_{wi}\rangle=a_i|0\rangle+b_i|1\rangle$、$|k_{wi}\rangle=c_i|0\rangle+d_i|1\rangle$。攻击者 Eve 以辅助态 $|e\rangle$ 干扰 $|f_{wi}\rangle$，以 $|h\rangle$ 干扰 $|k_{wi}\rangle$，量子衍变过程[17]如下。

$$U(|0\rangle,|e\rangle)=\sqrt{F}|0e_{00}\rangle+\sqrt{D}|1e_{01}\rangle \tag{7a}$$

$$U(|1\rangle,|e\rangle)=\sqrt{D}|0e_{10}\rangle+\sqrt{F}|1e_{11}\rangle \tag{7b}$$

$$\begin{aligned}U(|+\rangle,|e\rangle)=&\frac{1}{2}|+\rangle(\sqrt{D}|e_{10}\rangle+\sqrt{F}|e_{11}\rangle+\\&\sqrt{D}|e_{01}\rangle+\sqrt{F}|e_{00}\rangle)+\frac{1}{2}|-\rangle(\sqrt{D}|e_{10}\rangle-\\&\sqrt{F}|e_{11}\rangle-\sqrt{D}|e_{01}\rangle+\sqrt{F}|e_{00}\rangle)\end{aligned} \tag{7c}$$

$$\begin{aligned}U(|-\rangle,|e\rangle)=&\frac{1}{2}|+\rangle(\sqrt{D}|e_{01}\rangle-\sqrt{F}|e_{11}\rangle-\\&\sqrt{D}|e_{10}\rangle+\sqrt{F}|e_{00}\rangle)+\frac{1}{2}|-\rangle(\sqrt{F}|e_{11}\rangle-\\&\sqrt{D}|e_{10}\rangle-\sqrt{D}|e_{01}\rangle+\sqrt{F}|e_{00}\rangle)\end{aligned} \tag{7d}$$

$$U(|0\rangle,|h\rangle)=\sqrt{F_1}|0h_{00}\rangle+\sqrt{D_1}|1h_{01}\rangle \tag{8a}$$

$$U(|1\rangle,|h\rangle)=\sqrt{D_1}|0h_{10}\rangle+\sqrt{F_1}|1h_{11}\rangle \tag{8b}$$

$$\begin{aligned}U(|+\rangle,|h\rangle)=&\frac{1}{2}|+\rangle(\sqrt{D_1}|h_{10}\rangle+\sqrt{F_1}|h_{11}\rangle+\\&\sqrt{D_1}|h_{01}\rangle+\sqrt{F_1}|h_{00}\rangle)+\frac{1}{2}|-\rangle(\sqrt{D_1}|h_{10}\rangle-\\&\sqrt{F_1}|h_{11}\rangle-\sqrt{D_1}|h_{01}\rangle+\sqrt{F_1}|h_{00}\rangle)\end{aligned} \tag{8c}$$

$$\begin{aligned}U(|-\rangle,|h\rangle)=&\frac{1}{2}|+\rangle(\sqrt{D_1}|h_{01}\rangle-\sqrt{F_1}|h_{11}\rangle-\\&\sqrt{D_1}|h_{10}\rangle+\sqrt{F_1}|h_{00}\rangle)+\frac{1}{2}|-\rangle(\sqrt{F_1}|h_{11}\rangle-\\&\sqrt{D_1}|h_{10}\rangle-\sqrt{D}|h_{01}\rangle+\sqrt{F_1}|h_{00}\rangle)\end{aligned} \tag{8d}$$

D、D_1 为 Eve 对 $|f_{wi}\rangle,|k_{wi}\rangle$ 干扰度，F、F_1 为保真度。由 $\langle e_{00}|e_{10}\rangle+\langle e_{01}|e_{11}\rangle=0$ 及 $\langle h_{00}|h_{10}\rangle+\langle h_{01}|h_{11}\rangle=0$，可知 $\langle e_{00}|e_{10}\rangle=\langle e_{01}|e_{11}\rangle=\langle e_{00}|e_{01}\rangle=\langle e_{10}|e_{11}\rangle=0$，$\langle h_{00}|h_{10}\rangle=\langle h_{01}|h_{11}\rangle=\langle h_{00}|h_{01}\rangle=\langle h_{10}|h_{11}\rangle=0$。由 $F+D=1$ 及 $F_1+D_1=1$ 可以得到，$\langle e_{00}|e_{11}\rangle=\cos x$，$\langle h_{00}|h_{11}\rangle=\cos x'\langle e_{10}|e_{01}\rangle=\cos y,\langle h_{10}|h_{01}\rangle=\cos y',0\le x,x',y,y'\le\frac{\pi}{2}$，量子态 $|f_{wi}\rangle=G[|y_{bi}\rangle]$，$|k_{wi}\rangle=G[|k_{i+n}\rangle]$ 满足 $|a_i|^2=|b_i|^2=|c_i|^2=|d_i|^2=\frac{1}{2}$，$\cos y=\cos y'=0$ 则

$$D=\frac{1-\cos x}{2-\cos x}，\quad D_1=\frac{1-\cos x'}{2-\cos x'} \tag{9}$$

在 $\frac{D}{D_1}=\frac{F}{F_1}$ 条件下，Eve 检测 $|y_{wi}\rangle$、$|k_{wi}\rangle$ 的最大概率表示为

$$P_D=\frac{1}{2}+\frac{1}{2}\left[1-\left(\frac{D_1}{D}\right)^2\right]^{\frac{1}{2}}=\frac{1}{2}[1+D+\sqrt{D(2-3D)}] \tag{10}$$

由信息论定理知，Eve 可以获取信息量如式(11)所示。

$$I^{\text{Eve}}=1+f(D)\text{lb}(f(D))+(1-f(D))\text{lb}(1-f(D)) \tag{11}$$

图 3 展示了 MDI-QIA 框架下信息传输过程中，Eve 干扰度 D 与其获取的信息量 I 之间的关系，当 D 为 0 时，信息量为 0，随着 D 的逐渐增加，信息量 I 与之缓慢增加，当 D 取最大值，Eve 获取的最大信息量为 0.5。由于传输信道中认证信息由不同贝尔基 00、01、10、11 构成，在此 Eve 获取 $|00\rangle$ 的概率为 P_D，以概率 c 认定 $|y_{wi}\rangle,|k_{wi}\rangle$ 为 00，则认定 $|y_{wi}\rangle,|k_{wi}\rangle$ 为 01 的概率为 1-c，由此可知，在认证密钥传输过程中 Eve 获得的概率如式(12)所示。

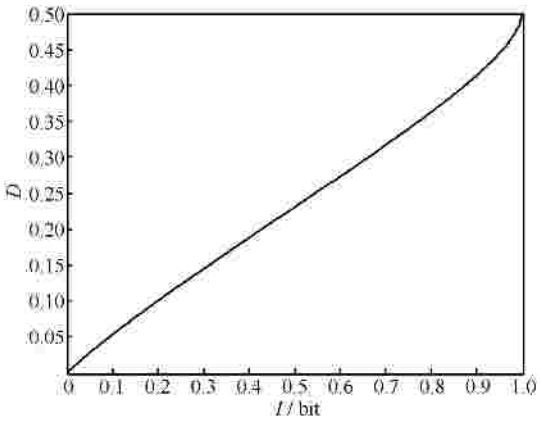

图 3 干扰度 D 和信息量 I 关系曲线

$$P_S = P_D\frac{c}{2} + P_D\left(1-\frac{c}{2}\right) = \frac{1}{4}[1 + D + \sqrt{D(2-3D)}] \quad (12)$$

以此类推，Eve 获得 n bit 认证密钥传输概率如式(13)所示。

$$P = \left[P_D(1-D)\right]^{\frac{n}{2}} = [\frac{1}{4}(1 + D + \sqrt{D(2-3D)})(1-D)]^{\frac{n}{2}} \quad (13)$$

图 4 所示为 Eve 在信息传输过程中获取传输密钥的概率，定义系统身份认证密钥率为 n，Eve 干扰度为 D，可以看出 Eve 选择不同 D 值时，随着传输密钥率 n 增加时，Eve 获取的信息量逐渐减小，最后趋近于 0，这一结果说明 MDI-QIA 框架中身份认证过程是安全的，随着身份认证密钥信息传输率增加，Eve 获取信息量逐步减小。

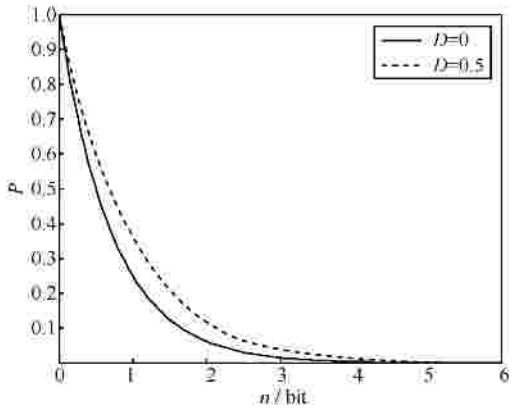

图 4　P 与干扰度 D 及 n 的函数曲线

3.2　MDI-QIA 协议效率

Yang 等[24]对于协议的比特效率定义为 $h = \frac{c}{n}$，c 表示协议中交换的经典认证密钥总数，n 是协议完成认证过程需要的量子比特总数，计算经典认证密钥数量与量子比特总数即可获知协议效率。所提的 MDI-QIA 框架中完成认证过程所需量子比特数目为 4，协议交换经典比特数为 2，因此协议的效率为 $h = \frac{1}{2}$。

4　结束语

本文提出基于测量设备无关框架下的量子身份认证协议，借助测量设备无关协议的属性，提高了量子身份认证过程的准确性和有效性。安全性能仿真结果显示，在最强辅助纠缠攻击下，随着认证密钥传输量的增加，而 Eve 对认证信息的窃取量逐渐减小；且方案在本次协议认证后能自动更新共享密钥，以一次一密方式保证了身份认证过程的绝对安全性。

参考文献：

[1] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Phys Rev Lett, 2000, 85: 441-446

[2] GOTTESMAN D, LO H K, LUTKENHAUS N, et al. Security of quantum key distribution with imperfect devices[J]. Quantum Infor Comput, 2004, 4: 325-329.

[3] PAUL J, DAVID E, SÉBASTIEN K J. High bit rate continuous-variable quantum key distribution[J]. Phys Rev A, 2014, 90(4): 042329-042335.

[4] ZHOU R R, YANG L. Quantum election scheme based on anonymous quantum key distribution[J]. Chin Phys B, 2012, 21(8): 080301-080309.

[5] ALEXANDER S, ZUREK W H. Quantum discord cannot be shared[J]. Phys Rev Let, 2013, 111(4): 040401-040406.

[6] 曾贵华. 量子保密通信[M]. 北京: 高等教育出版社, 2006.
ZENG G H. Quantum private communication[M]. Beijing: Higher Educaiton Press, 2006.

[7] DUSEK M, HANDERKA O, HENDRYCH M. Quantum identification system[J]. Phys Rev A, 1999, 60(1):149-156.

[8] ZENG G H, ZHANG W P. Identity verification in quantum distribution[J]. Phys Rev A, 2000, 61:022303-022308.

[9] 曾贵华. 不依赖于第三方的动态量子身份认证方案[J]. 电子学报, 2004, 32(7):1148-1152.
ZENG G H. Quantum identity authentication without trusted-party[J]. Acta Electronica Sinca, 2004, 32(7):1148-1152.

[10] ZHOU N R, ZENG G H, ZENG W J, et al. Cross-center quantum identification based on teleportation and entanglement swapping[J]. Optics Communications, 2005, 254: 380-388.

[11] 杨宇光, 温巧燕, 朱甫臣.一种网络多用户量子认证和量子身份认证方案[J]. 物理学报, 2005, 54(9): 3995-4000.
YANG Y G, WEN Q Y, ZHU F C. A theoretical scheme for m lti-user quantum authentication and key distribution in a network[J]. Acta Physica Sinca, 2005, 54(9): 3995-4000.

[12] ZHANG Z S, ZENG G H, ZHOU N R, et al. Quantum identity authentication based on ping-pong technique for photons[J]. Phys Let A, 2006, 356:199-205.

[13] 张兴兰. 基于公钥的单向量子身份认证[J]. 科学通报, 2009, 59(10):1415-1418.
ZHANG X L. One-way quantum identity authentication based on public key[J]. Chinese Sci Bull, 2009, 54(10):1415-1418.

[14] 李渊华, 刘俊昌, 聂义友. 基于纠缠交换和团簇态实现二粒子任意态的可控隐形传态[J]. 光子学报, 2010, 39(11):1615-1616.
LI Y H, LIU J C, NIE Y Y. Controlled teleportation of an arbitrary two-particle state by using a four-qubit cluster state and entanglement swapping[J]. Acta Photonica Sinca, 2010, 39(11):1615-1616.

[15] YANG Y G, WANG H Y, JIA X. A quantum protocol for (*t*, *n*)-threshold identity authentication based on greenberger-horne-zeilinger states[J]. Theor Phys, 2013, 52: 524-530.

[16] HUANG P, ZHU J, LU Y, et al. Quantum identity authentication using gaussian-modulation squeezed state[J]. International Journal of Quantum Information, 2011, 9(2): 701-721.

[17] YANG Y G, TIAN J, XIA J. Quantum authenticated direct communication using bell states[J]. Theor Phys, 2013, 52: 336-344.

[18] MAKAROV V, SKAAR J. Hacking commercial quantum cryptography systems by tailored bright illumination[J]. Nature Photonics, 2010, 214(4): 686-689.

[19] ZHAO Y, FUNG C H F, QI B. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key- distribution systems[J]. Phys Rev A, 2008, 78: 042333-042340.

[20] LO H K, CURTY M, QI B. Measurement-device-independent quantum key distribution[J]. Phys Rev Let, 2012, 108: 130508-13514.

[21] TANG Z Y, LIAO Z F, XU F H, et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution[J]. Phys. Rev. Let, 2014, 112(19): 190503-190511.

[22] **马瑞霖**. **量子密码通信**[M]. **北京**: **科学出版社**, 2006.
MA R L. Quantum cryptograghy communication[M]. Beijing: Science Press, 2006.

[23] GARCIA-PATRON R, CERF N J. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution[J]. Physical Review Letters, 2006, 97:190503-190510.

[24] YANG C W, TSAI C W, HWANG T. Fault tolerant two-step quantum secure direct communication protocol against collective noises[J]. Sci. China G:Phys. Mech. Astron,2011, 54(3):496-501.

作者简介：

董颖娣（1978-），女，陕西西安人，西北工业大学博士生，主要研究方向为量子密码通信。

彭进业（1964-），男，湖南娄底人，西北工业大学教授，主要研究方向为量子密码通信及图像处理等。

张晓博（1975-），男，陕西西安人，西北工业大学博士生，主要研究方向为模式识别与量子通信。

张振龙（1980-），男，陕西韩城人，西安建筑科技大学博士生，主要研究方向为数字图像处理。