计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2017,26(8):23−28 [doi: 10.15888/j.cnki.csa.005902]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于 Bell 态的量子资源访问控制协议①

谢智海, 张仕斌, 昌　燕, 闫丽丽, 盛志伟, 韩桂华

(成都信息工程大学 信息安全工程学院, 成都 610225)
通讯作者: 张仕斌, E-mail: 498251651@qq.com

摘　要: 在资源访问无处不在的互联网时代, 如何做好对资源的访问控制具有重要的意义. 本文利用二粒子纠缠态 Bell 态的纠缠特性, 提出了基于 Bell 态的资源访问控制协议. 该协议基于量子密钥分发(Quantum Key Distribution-QKD), 设计了一种利用不对等密钥(不经意密钥)实现的量子资源访问控制协议, 同时实现了对资源请求方的身份认证. 本文分析了该协议的安全性, 证明了协议可以实现资源不被非法授权用户访问, 以及特定授权用户只能访问特定资源.

关键词: 资源访问; 量子纠缠; Bell 态; 纠缠单配性

引用格式: 谢智海,张仕斌,昌燕,闫丽丽,盛志伟,韩桂华.基于 Bell 态的量子资源访问控制协议.计算机系统应用,2017,26(8):23–28. http://www.c-s-a.org.cn/1003-3254/5902.html

Quantum Resource Access Control Protocol Based on Bell States

XIE Zhi-Hai, ZHANG Shi-Bin, CHANG Yan, YAN Li-Li, SHENG Zhi-Wei, HAN Gui-Hua

(College of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: In the the Internet era of resource access, it is of great significance how to do a good job of the access control of resources. In this paper, we propose a resource access control protocol based on Bell state by using the entanglement properties of two particles. This protocol combines the quantum key distribution (Key Distribution-QKD Quantum) technology with unequal a key (Key Inadvertently) to achieve a quantum resource access control protocol, and realizes the authentication of the resource request Party in the protocol. At the same time, the security of the protocol is analyzed in this paper, which ensures that the resources are not accessed by unauthorized users and the authorized users can only access specific resources.

Key words: resource access; quantum entanglement; bell states; monogamy property of entanglement

互联网时代的所有的网络行为实际上都是围绕着资源访问产生的. 互联网的爆炸式发展也带来了诸多问题, 其中就包括资源访问问题. 传统的包括访问控制、角色管理等策略, 能在一定程度上实现对资源的访问控制, 但现实情况下并不能得到好的效果, 这主要是由于资源应用场景的多样性、管理的复杂性以及使用的不便性决定的. 然而如何实现对资源的有效访问控制已经成为了一个重要的问题: 资源提供方希望用户不能访问未授权的资源, 并且保证授权的用户能访问到已授权的资源. 由于传统的资源访问控制策略存在上述问题, 如何确定一种更加易于实现和管理的访问控制策略成为资源访问控制的关键问题.

近年来, 伴随着量子通信这种新型通信方式的兴起, 如何在量子通信网络环境中做好资源的访问控制显得尤为重要. 量子通信是经典信息论和量子力学相结合的一门新兴交叉学科, 是利用量子态携带信息的

① 基金项目: 国家自然基金(61572086, 61402058); 四川省科技支撑计划项目(2013GZX0137); 成都市科技惠民项目(2014-HM01-00108-SF)
收稿时间: 2016-12-02; 采用时间: 2017-01-04

全新通信方式, 在通信安全性、计算能力、信息传输、通道容量、测量精度等方面突破经典通信技术的极限, 已成为 21 世纪通信与信息领域发展的新方向和主流. 而在量子通信中, 量子密码学也是量子通信安全保证的一种技术手段. 量子密码学是以量子力学为基础, 其著名的测不准原理和量子相干性保证了量子密码的安全性. 其主要研究方向包括量子密钥分配(QKD)[1-3]、量子安全直接通信(QSDC)[4-7]量子秘密共享(QSS)[8-12]和量子数字签名以及身份认证(QIA)[13-15]等. 1984 年由 C.H.Bennnett 和 G.Brassard 提出的著名的量子密钥分发协议——BB84 协议[16], 随后提出了 B92 协议[17]等其他的量子密钥分发协议. 很多学者研究了基于 QKD 协议的量子身份认证, 如诸如龚晶, 何敏等人[18]提出的基于网络的量子身份认证协议, 张兴兰[19]提出的基于公钥的单向量子身份认证等. 上述协议的提出, 对保障未来量子通信网络中的安全通信具有重要意义. 但是上述协议采取的措施均是对参与通信的实体进行身份认证或者采取密钥分发的手段来保证通信安全. 实际上, 网络通信的实质是最大程度的获取与共享资源, 然而如何实现对资源的访问这方面的研究并不多.

本文在上述研究工作的基础上提出了一种基于 Bell 态的量子资源访问控制协议, 协议是在资源请求方(Alice)对资源提供方(Bob)建立资源申请请求之后, Bob 对 Alice 进行身份认证, 并将 Alice 有权限访问的资源通过协商好的不对称密钥加密, 该密钥的特点是, Bob 知道密钥的全部, 而 Alice 只知道部分. 因此未经授权的其他资源的加密密钥只有 Bob 知道, 这样就实现了资源不被非法授权用户访问, 特定授权用户只能访问特定资源, 为在量子通信网络环境下实现对资源的访问控制提供了很好的思路.

1 基于 Bell 态的资源访问控制协议

1.1 场景描述

网络中诸如论文下载、图书馆资源的下载等资源访问的场景不胜枚举. 不同级别的用户所能访问到的资源类别不一样, 这里我们提出一个资源访问控制的量子方案, 帮助资源拥有者和用户实现资源的正确访问, 即, 合法用户只能访问有权限的资源, 不能访问额外的资源. 这里我们假设 Bob 拥有 N 类资源, 用户 Alice 拥有访问第 i 类和第 j 类资源的权限, 因此只能访问该两类资源, 该协议就是要帮助 Alice 和 Bob 安全的完成这个任务. Alice 向 Bob 请求访问授权资源的流程示意图如图 1 所示.

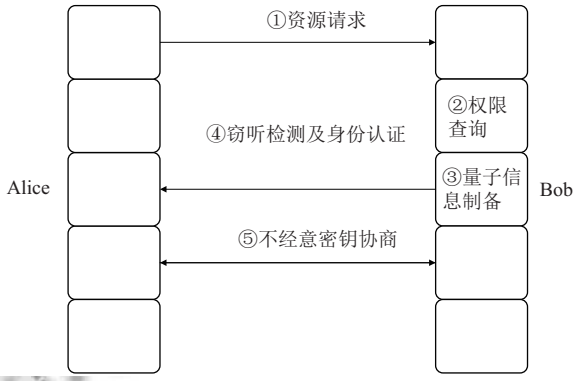

图 1 Alice 向 Bob 请求访问授权资源的流程示意图

1.2 协议描述

基于上述场景, 我们假设 Bob 拥有 N 类资源, 用向量 $S=(S_1,S_2...S_n)$ 描述, 下标代表第 n 类资源, Alice 想要访问第 i 类和第 j 类资源 S_i 和 S_j. 在这里 Alice 和 Bob 事先共享了一串代表 Alice 身份的二进制字符串 $I=(I_1,I_2...I_n)$. 协议中将会使用到的四组 Bell 态表示为:

$$\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}\\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{AB}\\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{AB}\\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)_{AB}
\end{aligned} \tag{1}$$

为方便协议描述, 首先我们定义如下规则:

规则 1. Bob 根据与 Alice 共享的二进制字符串 I, 生成诱惑光子序列, 若 I_i=0, 则随机生成第 i 个诱惑光子|0⟩或|1⟩; 若 I_i=1, 则随机生成第 i 个诱惑光子|+⟩或|−⟩.

规则 2. Alice 和 Bob 根据共享的二进制字符串 I 在相应位约定测量基, 0 对应 Z 基测量, 1 对应 X 基测量.

规则 3. Alice 和 Bob 约定测量结果{|0⟩,|+⟩}编码为“0”, {|1⟩,|−⟩}编码为“1”.

第一步: (1)Alice 向 Bob 提出访问资源 S_i 和资源 S_j 的请求, Bob 在得到该资源请求之后, 查看 Alice 是

否具有访问资源 S_i 和资源 S_j 的请求. 若具有访问权限, 则继续; 否则拒绝. 权限验证成功后 Bob 制备 N 个 Bell 态, 每个态都随机处于公式(1)中的四种状态 $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$之一. 所有 Bell 态的 A 粒子构成粒子序列 PA, 表示为: $P_A=(P_{A_1},P_{A_2}...P_{A_n})$, B 粒子组成$P_B=(P_{B_1},P_{B_2}...P_{B_n})$, 且这两组序列对应粒子是纠缠的.

(2) Bob 根据规则 1 制备诱惑光子序列 D =(D_1, D_2, ..., D_k). Bob 将 D 随机插入到序列 P_A 中并且记录插入诱惑光子的位置序列$L_t = (L_1,L_2...L_t)$, 组成新的序列 P_A^*. Bob 通过量子信道将 P_A^*发送给 Alice, 当确认 Alice 已经成功接收光子序列 P_A^*之后, Bob 公布位置序列 L_t.

第二步: Alice 收到 Bob 发来的 P_A^*和公布的位置序列 L_t 之后, 抽取出第一步 Bob 插入的诱惑光子, 同时也恢复出序列组 P_A. 根据规则 2 中, 与 Bob 约定好的测量基, Alice 将所有诱惑光子按照顺序测量, 测量结果表示为 R_A, 然后 Alice 公布测量结果 R_A.

Bob 收到 Alice 公布的测量结果 R_A 之后, 根据测量结果, 在做窃听检测的同时, 也对 Alice 进行了身份认证, 这是由于 Bob 在诱惑光子制备和 Alice 测量该诱惑光子选取对应的测量基共同决定. 身份认证详细描述如下.

由于 Alice 和 Bob 共享了一串代表 Alice 身份的二进制字符串 I, Alice 根据第二步能得到 Bob 插入的诱惑光子序列 D, 该光子序列的制备规则是根据规则 1 制备, 测量规则是根据规则 2 测量的. 在该过程中二进制字符串、规则 1 以及规则 2 只有 Alice 和 Bob 知道, 那么 Alice 的测量结果和 Bob 根据诱惑光子序列测量的结果是对应, 这样就实现了身份认证.

如果该结果没有超出提前设定的阈值(窃听检测阈值的范围为(2%, 8.5%)[20]), 则表明不存在窃听者, 同时 Alice 是合法的用户, 协议继续; 否则重新开始.

第三步: Bob 在验证 Alice 的身份和没有窃听者之后, 按如下方式处理:

(1) $P_A=(P_{A_1},P_{A_2}...P_{A_n})$和$P_B=(P_{B_1},P_{B_2}...P_{B_n})$中 $n=i,j$位置

根据规则 2, Bob 对 P_B 序列中的粒子进行测量, Alice 对恢复出来的 P_A 序列中的粒子进行测量, 各自得到测量结果, 然后根据规则 3, Alice 和 Bob 分别对各自的测量结果进行编码, 并保存为$key_{S_i}[1]$和$key_{S_j}[1]$.

(2) $P_A=(P_{A_1},P_{A_2}...P_{A_n})$和$P_B=(P_{B_1},P_{B_2}...P_{B_n})$中 $n\neq i,j$位置

Bob 在 P_B 序列组中, 对$n\neq i,j$时随机选取测量基进行测量, 并且对测量结果编码后保存为$key_n[1]$.

由(1)和(2)我们就做到了 Alice 和 Bob 所知密钥的不对等性的处理.

在得到测量结果之后, 我们按照如下规则对密钥 $key_{s_n}[l]$(l 代表密钥长度)进行密钥拓展:

在资源 S_i 和 S_j 处, Alice 和 Bob 的密钥拓展如下:

$$key_{s_n}[l]=\begin{cases} key_{s_i}[1]\oplus key_{s_j}[1] & l=1 \\ key_{s_n}[l-1]\oplus\left(2^{(l \bmod 2)}-1\right) & l>1 \end{cases} \tag{2}$$

在其他资源处时, Bob 的密钥拓展如下:

$$key_{s_n}[l]=\begin{cases} key_{s_n}[1] & =1 \\ key_{s_n}[l-1]\oplus random(l) & l>1 \end{cases} \tag{3}$$

其中 $random(l)$为在第 l 位用量子随机数发生器随机产生的值, 该值从{0, 1}中选取.

该协议流程如图 2 所示.

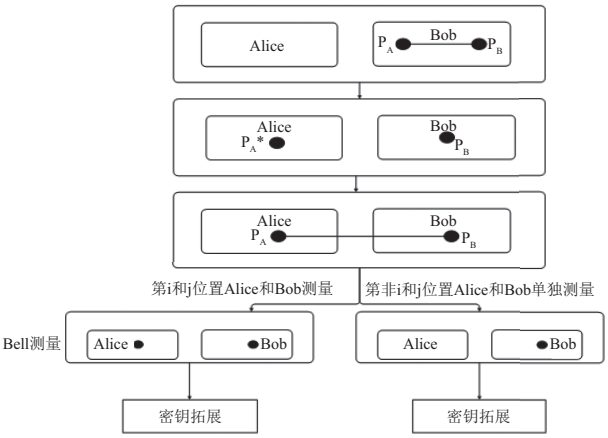

图 2 协议执行流程

1.3 实例分析

为了更好的理解该协议, 下面举例说明该协议. 分析该协议之前做如下假设.

假设 1: Alice 和 Bob 共享的二进制字符串为(011000101…).

假设 2: Bob 制备的 Bell 态粒子中在第 i 位和第 j 位的 Bell 态均为Φ^+.

下面举例在第 i=4 和第 j=7 位, 其他只取第 3 位详

细描述该协议.

Bob 在制备好含有 N 个二粒子 Bell 态, 假设我们按照假设 1 和规则 1 制备如下诱惑光子为{|0⟩,|+⟩,|−⟩,|0⟩....}. 同时, Bob 定义好位置序列$L_t=(L_1,L_2...L_t)$, 这里我们假设前 4 个诱惑光子插入的位置分别为序列组 P_A 的第 2 位、第 3 位、第 5 位和第 7 位, 序列组 P_A 在插入诱惑光子之后序列组 P_A^*各位置变化如表 1 所示.

表 1 插入诱惑光子之后位置变化

P_A	P_A^*
P_{A_1}	P_{A_1}
P_{A_2}	|0⟩
P_{A_3}	|+⟩
P_{A_4}	P_{A_2}
P_{A_5}	|−⟩
P_{A_6}	P_{A_3}
P_{A_7}	|0⟩
…	…

Bob 将序列组 P_A^*和位置序 L_t 发送给 Alice, Alice 抽取出诱惑光子, 恢复出了量子序列组 P_A 之后, 根据和 Bob 共享的二进制字符串 I, 以及在每一位约定的测量基做窃听检测, 并且公布检测结果. 若 Alice 通过了窃听检测, 进行下一步.

Bob 和 Alice 在量子序列组 P_B^*和 P_A^*中的第 i=4 位和第 i=7 位(即P_{A_4}和P_{B_4})进行 Bell 测量. 测量方式如下:

(1) 第 i=4 位和第 j=7 位

由于共享的二进制序列第 4 位为 0, 即选取 Z 基在该位同时做 Bell 测量; 共享的二进制序列第 7 位为 1, 即选取 X 基在该位同时做 Bell 测量. 假设 Bob 在第 i=4 位的结果 0, 在第 i=7 位的结果为 1, 根据量子纠缠性和表 2, Alice 得到在第 i=4 位的结果为 0, 在第 i=7 位的结果为 1.

表 2 Φ^+下 Bell 测量结果和编码结果

测量基	Alice测量结果	Bob测量结果	编码结果
X基	0	0	0
X基	1	1	1
Z基	|+⟩	|+⟩	0
Z基	|−⟩	|−⟩	1

(2) 第 i=3 位

在第 i=3 位, Bob 自行选择测量基测量, 假设在该位的 Bell 态为Φ^-, 选取 X 基测量. 假设在该位测量之后编码得到的结果为 0. Bob 和 Alice 将得到的结果分别做密钥拓展. 这里在对第 i = 3、第 i = 4 和第 i = 7 位, 我们根据第三步密钥拓展规则, 拓展出前 5 位密钥, 其中我们假设在第 i=3 位的量子随机随机数发生器产生的其他四位的值位(1001). 密钥拓展结果如表 3 所示.

表 3 密钥拓展结果

l	$key_{s_4}[l]$和$key_{s_7}[l]$	$key_{s_3}[l]$
1	1	0
2	1	1
3	0	1
4	1	1
5	0	0
…	…	…

2 协议安全性分析

2.1 外部窃听攻击

1) 截获-重发攻击

在诱惑光子检测(1.2 第一步)中, 由于插入了从{|0⟩,|1⟩,|+⟩,|−⟩}(其中$|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$)中随机选取的诱惑光子$D=(D_1,D_2...D_k)$, 假设攻击者 Eve 截获了 P_A^*序列, 由于插入诱惑光子是随机选取并且插入的位置序列$L_t=(L_1,L_2...L_t)$是随机的, 单个光子选择正确的基(X 基或 Z 基)得到正确结果的概率为$\frac{1}{2}$, 那么通过诱惑光子检测的概率为$\left(\frac{1}{2}\right)^k$($k$ 为插入诱惑光子个数). 设窃听检测阈值为 p 的范围为(2%, 8.5%), 当 k≥6 时, Eve 通过窃听检测的概率为小于等于 1.5625%, Eve 被发现的概率大于等于 0.94375, 所以 Eve 进行截获-重发攻击是能够被发现的.

2) Eve 冒充 Alice 获取 Alice 想要的资源

这里是指 Eve 冒充 Alice 获得 Bob 授权的两类资源的访问, 在进行诱惑光子检测时, 由于选取测量每一个诱惑光子的测量基是根据 Alice 在和 Bob 共享的二进制字符串$I=(I_1,I_2...I_n)$选取的, 如果 Eve 想要代替 Alice 与 Bob 进行通信, 假设诱惑光子的个数为 k, 那么 Eve 通过身份认证概率为$\left(\frac{1}{2}\right)^k$; 假设该协议中密钥长度为 l, Eve 得到完整密钥的概率为$\left(\frac{1}{2}\right)^l$; 并且 Eve 由于不知道 Alice 访问 Bob 资源的哪两位, 猜测出该两位资源概率为$\frac{1}{C_m^2}$. 那么 Eve 得到第 i 位和第 j 位资源概率为$\left(\frac{1}{2}\right)^k*\left(\frac{1}{2}\right)^l*\frac{1}{C_m^2}$. 根据表 4, 当 k=7, l=11, m=11 时,

Eve 得到 Alice 访问资源的概率 p_a 为$\left(\frac{1}{2}\right)^7*\left(\frac{1}{2}\right)^{11}*\frac{1}{C_{11}^2}=$ 0.000007%. Eve 不能访问对应资源的概率为 99.999993%, 不能访问的概率非常高.

表 4 Eve 冒充 Alice 获取 Alice 想要资源的概率

k	l	m	p_a(%)
6	10	10	0.000034
6	10	11	0.000028
6	11	11	0.000014
7	10	10	0.000017
7	10	11	0.000014
7	11	11	0.000007

3) Eve 想得到 Bob 中除 Alice 访问的其他资源

该分析是指 Eve 想访问 Bob 的除 Alice 授权访问的资源(即$n\neq i,j$), 假设 Eve 通过了 Bob 的身份认证, 那么 Eve 只能知道 Bob 在不经意密钥拓展(第三步(2))中key_n[1]的密钥结果. 由于当密钥位置 l>1 时的密钥拓展结果只有 Bob 知道, 对该类资源加密时采用的是量子随机数发生器来产生真随机数, 那么每一类资源得到的概率为$\left(\frac{1}{2}\right)^l$, 且 Eve 访问正确资源类的概率为$\left(\frac{1}{m-2}\right)$, 那么最终 Eve 产生的所有资源都能得到的概率 p_b 为$\left(\frac{1}{2}\right)^l*\left(\frac{1}{m-2}\right)$. 根据表 5, 当 l=12, m=11, 则 Eve 能得到 Bob 中除 Alice 访问的其他资源的概率约为 0.002713%, 即不能访问其他资源概率为 99.997287%. 因此, Eve 想访问 Bob 除 Alice 访问的其他资源的概率非常低.

表 5 Eve 想访问除 Alice 访问的其他资源

l	m	p_b(%)
10	10	0.012207
10	11	0.010851
11	10	0.006104
11	11	0.005425
12	10	0.003052
12	11	0.002713

2.2 Alice 攻击

Alice 攻击的目的就是访问除权限以外的额外的资源. 由于该协议是允许 Alice 访问特定的资源类, 假设 Alice 想要猜测出其他所有类资源的信息, 并且每一类资源的长度为 l. 针对每一类资源而言, 资源类不被 Alice 授权时($n\neq i,j$), 且 l≥2 时的密钥拓展方式只有 Bob 知道, 那么 Alice 只能猜测出其余的 l-1 位的密钥, 被猜测出来的概率为$\left(\frac{1}{2}\right)^{(l-1)}$; 对应密钥访问正确的资源类的概率为$\left(\frac{1}{m-2}\right)$, 那么剩余($m$-2)类资源被全部猜测出来的概率为$\left(\frac{1}{2}\right)^{(l-1)}*\left(\frac{1}{m-2}\right)$. 由表 5 分析可以看出, 当 l 和 m 足够大时, Alice 想获取未被授权资源的概率极低.

3 结束语

本文提出了一种基于 Bell 态实现的资源访问控制协议. 该协议通过将 QKD 协议和现实生活中资源访问的密钥不对等性结合起来, 通过 Alice 和 Bob 事先共享的二进制字符串, 在进行窃听检测的同时也对 Alice 的身份进行了认证. 同时通过两者提前协商好的测量结果, 进行对应的密钥拓展之后, 将资源进行加密发送给 Alice, Alice 对相应的资源解密即可. 根据上述协议, 在实现 Alice 访问有权限的资源之前对其进行了身份认证, 并且设计了一种基于量子的一个利用不对等密钥(不经意密钥)的资源访问控制协议.

参考文献

1 Buttler WT, Hughes RJ, Lamoreaux SK, *et al*. Daylight quantum key distribution over 1.6 km. Physical Review Letters, 2000, 84(24): 5652–5655. [doi: 10.1103/PhysRevLett.84.5652]

2 Ekert AK. Quantum cryptography based on Bell's theorem. Physical Review Letters, 1991, 67(6): 661–663. [doi: 10.1103/PhysRevLett.67.661]

3 Kurtsiefer C, Zarda P, Halder M, *et al*. Quantum cryptography: A step towards global key distribution. Nature, 2002, 419(6909): 450.

4 Long GL, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. Physical Review A, 2002, 65(3): 032302. [doi: 10.1103/PhysRevA.65.032302]

5 Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Physical Review A, 2003, 68(4): 042317. [doi: 10.1103/PhysRevA.68.042317]

6 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(4): 332–342.

7 Chang Y, Xu CX, Zhang SB, *et al*. Quantum secure direct communication and authentication protocol with single photons. Chinese Science Bulletin, 2013, 58(36): 4571–4576. [doi: 10.1007/s11434-013-6091-9]

8 Xiao L, Long GL, Deng FG, *et al*. Efficient multiparty quantum-secret-sharing schemes. Physical Review A, 2004, 69(5): 052307. [doi: 10.1103/PhysRevA.69.052307]

9 Yang YG, Wen QY. Threshold quantum secret sharing between multi-party and multi-party. Science in China Series G: Physics, Mechanics and Astronomy, 2008, 51(9): 1308–1315. [doi: 10.1007/s11433-008-0114-6]

10 Zhang ZR, Liu WT, Li CZ. Quantum secret sharing based on quantum error-correcting codes. Chinese Physics B, 2011, 20(5): 050309. [doi: 10.1088/1674-1056/20/5/050309]

11 Sun Y, Xu SW, Chen XB, *et al*. Expansible quantum secret sharing network. Quantum Information Processing, 2013, 12(8): 2877–2888. [doi: 10.1007/s11128-013-0570-4]

12 Bell BA, Markham D, Herrera-martí DA, *et al*. Experimental demonstration of graph-state quantum secret sharing. Nature Communications, 2014, (5): 5480.

13 Dušek M, Haderka O, Hendrych M, *et al*. Quantum identification system. Physical Review A, 1999, 60(1): 149–156. [doi: 10.1103/PhysRevA.60.149]

14 Zeng GH, Zhang WP. Identity verification in quantum key distribution. Physical Review A, 2000, 61(2): 022303. [doi: 10.1103/PhysRevA.61.022303]

15 Gao F, Qin SJ, Guo FZ, *et al*. Cryptanalysis of quantum secure direct communication and authentication scheme via Bell states. Chinese Physics Letters, 2011, 28(2): 020303. [doi: 10.1088/0256-307X/28/2/020303]

16 Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 2014, 560: 7–11.

17 Bennett CH. Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 1992, 68(21): 3121–3124. [doi: 10.1103/PhysRevLett.68.3121]

18 龚晶, 何敏, 邓元庆, 等. 基于网络的量子身份认证方案. 量子光学学报, 2009, 15(4): 336–341.

19 张兴兰. 基于公钥的单向量子身份认证. 科学通报, 2009, 54(10): 1415–1418.

20 Chang YJ, Tsai CW, Hwang T. Multi-user private comparison protocol using GHZ class states. Quantum Information Processing, 2013, 12(2): 1077–1088. [doi: 10.1007/s11128-012-0454-z]