Computer Science and Application 计算机科学与应用, 2018, 8(5), 611-618
Published Online May 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.85069

Hans汉斯

Node Trusted Access Model Based on Quantum Trusted Relay Network

Wenguan Ning, Shibin Zhang, Yan Chang

School of Cybersecurity, Chengdu University of Information Technology, Chengdu Sichuan
Email: cuitzsb@cuit.edu.cn

Received: Apr. 15th, 2018; accepted: May 1st, 2018; published: May 9th, 2018

Abstract

The foundation of constructing secure communication is the establishment of trust relationship. The current quantum secure communication protocol and related technologies are based on the premise of trust. In order to solve the problem of trust in quantum communication network, this paper proposes a new scheme based on classical trusted access, based on classical trusted access, and studies the trusted access of nodes in quantum communication network. The trust evaluation system is introduced into the quantum communication network. Relying on the unique characteristics of quantum entanglement and quantum teleportation, it is proposed to borrow the quantum character for trusted access, and its process is described in detail. Finally, according to its feasibility and security, it provides a new idea for the trusted access of quantum communication network.

Keywords

Quantum Communication, Quantum Network, Trusted Access, Trust Evaluation

基于量子可信中继网络的节点可信接入模型

宁文冠，张仕斌，昌　燕

成都信息工程大学，网络空间安全学院，四川 成都
Email: cuitzsb@cuit.edu.cn

收稿日期：2018年4月15日；录用日期：2018年5月1日；发布日期：2018年5月9日

摘　要

构建安全通信的基础是信任关系的建立。目前的量子安全通信协议和相关技术都是以信任为前提来展开

文章引用：宁文冠，张仕斌，昌燕．基于量子可信中继网络的节点可信接入模型[J]．计算机科学与应用，2018，8(5)：611-618. DOI: 10.12677/csa.2018.85069

的。针对量子通信网络中的信任问题，本文提出了以量子可信中继网络为基础，在经典可信接入的基础上，对于量子通信网络内节点的可信接入进行研究。将信任评价体系引入到量子通信网络中。依靠量子纠缠及量子隐形传态等独有的特性提出了借用量子特性进行可信接入，并对其过程进行了详细说明。最后根据其可行性及安全性进行了说明，为量子通信网络的可信接入提供了一种新思路。

关键词

量子通信，量子网络，可信接入，信任评价

1. 引言

量子通信是利用量子物理的特性与信息科技相结合而产生的一门新型学科。量子通信的优势在于它是利用量子态的物理特性来达到绝对的安全性。现阶段随着“墨子号”卫星的成功发射并投入使用，量子通信的发展将进一步提速。相对比经典网络的发展，量子通信网络也和经典网络一样需要面对一些安全性问题。比如网络中节点的信任问题，节点的接入评判标准，以及节点的认证等一系列问题。随着“京沪干线”量子通信网络的投入使用，要保证在接入到量子通信网络中的节点的信任，防止假冒，篡改，欺骗等行为的出现，这是在量子通信应用和网络化的进程中必须要面对和解决的问题。对比经典网络，节点的信任是实现网络通信的基础，在量子通信网络当中也是一样的。目前，大部分量子密钥分配协议[1] [2] [3] [4]都是在通信双方可信的前提下进行的。由此可以发现，量子通信网络当中节点的信任状况是最根本的也是最重要的。到目前为止国内外关于量子通信网络中节点可信接入模型的研究暂时还不是很多。由于它对于整个量子通信网络具有极其重要的意义，所以对于量子通信网络中节点可信接入模型的研究具有相当大的价值，为了使量子通信网络更进一步的发展，这项研究也将成为量子通信当中的重要组成部分。

2. 可信接入的介绍

在经典网络中为了保证接入网络内的节点的安全性，以及接入后不会给网络带来安全隐患，所以需要对接入网络的终端进行严格的认证和信任的评估。为了避免接入的节点对可信网络的安全性产生影响，提出了可信接入的概念。目前有多种接入标准和规范。由思科发起的网络接入控制技术(Network Admission Control, NAC)，用于确保接入网络中的节点是信任关系。微软提出了网络接入保护技术(Network Access Protection, NAP)，来确保接入私有网络的节点的安全性。“可信计算组织”TCG (Trusted Computing Group)提出了可信接入规范(Trusted Network Connection, TNC)，旨在确认接入网络节点的身份及其平台的完整性[5]。相较于 NAC 和 NAP 对节点设备的局限而言，TNC 规范具有不错的开放性，其大概框架如图 1 所示。

TNC 规范主要可分为两大部分，一部分是对身份的证明，另一部分是对完整性的度量。在身份的证明过程中通过对用户及平台的身份认证来完成身份的证明；在完整性的度量过程中对病毒库完整性，授权软件应用版本，身份归属，安全策略等因素进行检查来确定其结果。其中对身份和完整性的证明过程中均使用到了基于离散数学的公钥密码学。安全性由复杂的数学运算来保证。在量子网络中可以利用量

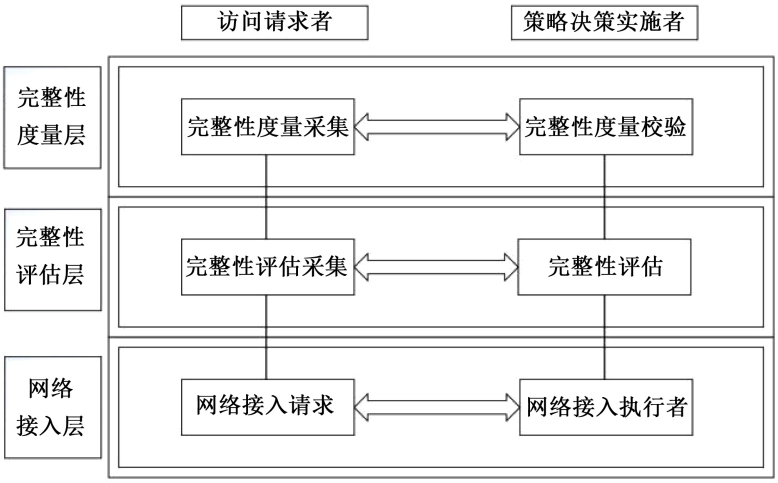

Figure 1. TNC framework
图 1. TNC 框架

子特性来保证其安全性，效率提高的同时又能够抵抗随着计算能力提升而对传统的公钥密码的威胁。同时 TNC 规范中已经对现有的网络访问技术进行了充分的利用(如 802.11x，VPN 等)，使得其在不同的利用场景下能够进行可信网络连接。此处将 TNC 规范应用于量子通信网络中，处理量子网络中节点可信接入的问题。本文在节点遵循 TNC 规范和要求的基础上提出了量子网络中的节点可信接入这一概念。

经典网络中由可信计算组织提出了信任根和信任链的概念[6]。信任根用来进行测量，报告和存储信任度，信任链用来传递组建可信网络。本文将量子网络中可信中继网络定义为一个抽象的大信任根，通过信任根运用度量和报告机制来实现一个自上向下由信任链构建的可信网络。对可信中继网络中的节点文中称为 TTP (Trusted Third Party)，对接入可信网络的节点称为节点 u。TTP 对其下所接入的节点 u 进行可信接入的操作，然后将所辖节点的信任度保存，同时在上层需要的时候进行自下向上的报告。可信中继网络的结构如图 2 所示。信任链在量子网络中通过量子隐形传态来进行传递。在结合 TNC 中身份认证和完整性验证等优点的基础上，提出了将量子身份认证和基于直觉模糊集的量子信任评估模型及信任综合评判模型应用到量子通信网络中，完成基于可信中继量子网络的节点可信接入。

3. 接入流程

节点申请接入可信中继网络时，为了达到上文所提出对身份的证明，首先 TTP 对节点 u 使用量子身份认证来完成对节点身份信息的确认。为了满足对完整性的度量，然后将节点 u 的各个信任属性按照 TNC 规范进行采集后用量子态进行传输。由于节点的各个信任属性具有主观性，变化性，抽象性，所以此处引入直觉模糊集来对各个信任属性进行描述，完成对影响信任度的各个属性的定量描述。最后根据综合评判信任模型对信任度进行计算来完成节点接入可信中继网络的过程。具体流程如图 3 所示。

3.1. 量子身份认证

在进行量子身份认证的过程中将使用单粒子来完成整个认证流程。过程中认为信道为理想状态。认证过程中共使用两组测量基，分别为 X 基和 Z 基。当粒子旋转偏振状态是右旋和左旋时用 $|+\rangle$ 和 $|-\rangle$ 表示，当粒子线性偏振状态是水平和垂直时用 $|0\rangle$ 和 $|1\rangle$ 表示[7]。在节点 u 和 TTP 行量子身份认证之前，双方通过量子秘密共享[8] [9]相互获得对方的二进制身份信息，然后通过对双方的二进制身份信息进行按位异或操作(位数不同则在后补零)产生认证二进制串 ID。TTP 根据二进制认证串 ID 制备一串光子序列 S。其中当

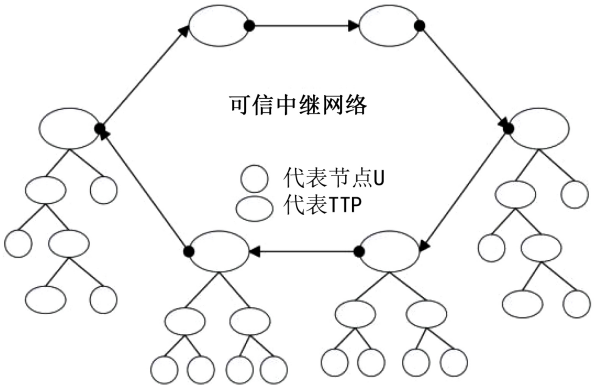

Figure 2. Trusted relay network
图 2. 可信中继网络

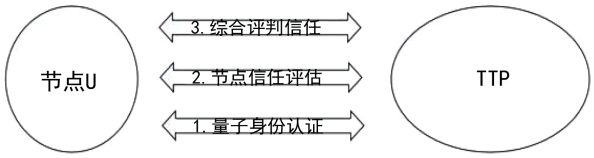

Figure 3. Flow chart
图 3. 流程图

ID 的第 i 位为 0 时，生成第 i 个光子$|0\rangle$或$|1\rangle$；当 ID 的第 i 位为 1 时，生成第 i 个光子$|+\rangle$或$|-\rangle$。再根据上述规则制备若干位诱惑光子序列 S’并插入到光子序列 S 中。双方约定根据 ID 的第 i 位信息来对测量基进行选取。其中当 ID 的第 i 位为 0 时，选取 Z 基；其中当 ID 的第 i 位为 1 时，选取 X 基。节点 u 在收到 TTP 发送的光子序列 S 后，TTP 向节点 u 公布光子序列 S 中诱惑粒子的位置。根据 TTP 公布的诱惑粒子位置，节点 u 将 S’提取出来，然后根据相互约定的规则选取测量基对诱惑光子序列 S’和光子序列 S 按顺序进行测量。最后将测量结果进行公布。如果诱惑粒子的测量结果没有超过窃听检测的阈值范围，TTP 根据光子序列 S 的测量结果来完成对节点 u 的身份认证。根据上述规则，TTP 对节点 u 的认证过程如图 4 所示。

3.2. 基于可信中继网络的节点信任评估

当节点身份认证成功之后，就可以对节点进行信任评估了。量子通信网络中信任的评估具有主观性，变化性，抽象性等特点，因此无法准确的对信任进行描述和刻画[10]。此处借助直觉模糊集理论对量子通信网络中的信任问题进行建模，在文献[10]的研究基础上结合可信中继网络实现对接入网络的节点的信任评估，然后利用量子隐形传态对节点的信任属性值进行安全传递。

在量子通信中，量子态可以用$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$来表示。其中$|\alpha|^2+|\beta|^2=1$。考虑到量子通信网络中，信任具有随机性、多样性和模糊性等不确定性因素，因此拟借助于直觉模糊集中的隶属度和非隶属度，来对节点隶属于某个属性的程度(隶属度)进行刻画。此处可以将节点的信任值的各个属性用量子态来进行表示：$|\psi\rangle_{u_i}=\cos\theta_j|0\rangle+\sin\theta_j|1\rangle$。其中 u_i 表示第 i 个节点，$\cos^2\theta_j$ 是 u_i 对第 j 个属性的隶属度，$\sin^2\theta_j$ 是 u_i 对第 j 个属性的非隶属度，且满足关系 $\cos^2\theta_j+\sin^2\theta_j=1$。由此来实现将节点的信任度用量子态的形式进行表示。同时借助于量子隐形传态来实现信任值的传递。

TTP 与用户 $u_i\,(i=1,2,\cdots,n)$ 之间共享一对 Bell 粒子，将其中粒子 1 归节点 $u_i\,(i=1,2,\cdots,n)$ 所有，粒子 2 归 TTP，所有四种 Bell 态表示如下：

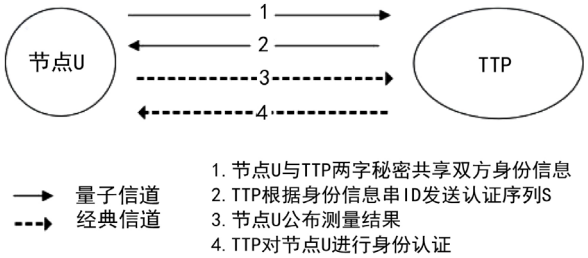

Figure 4. Node U and TTP for quantum authentication
图 4. 节点 U 与 TTP 进行量子身份认证过程

$$\left|\phi^{+}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)_{12};\ \left|\phi^{-}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right)_{12};$$

$$\left|\psi^{+}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right)_{12};\ \left|\psi^{-}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle-\left|10\right\rangle\right)_{12}$$

u_i 将自身的信任属性制备成量子态$\left|\alpha\right\rangle_U=\cos\theta\left|0\right\rangle+\sin\theta\left|1\right\rangle$(即要隐形传态的量子态)，借助于量子信道隐形传态给 TTP。具体过程如下：

1) u_i 对量子态$\left|\alpha\right\rangle_U$和 Bell 态进行直积操作。

具体做法是：u_i 将其制备成的量子态$\left|\alpha\right\rangle_U=\cos\theta\left|0\right\rangle+\sin\theta\left|1\right\rangle$，与他们共享的处于纠缠态中的量子态$\left|\phi^{+}\right\rangle_{12}=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)_{12}$的粒子 1 和粒子 2 进行“⊗”运算，得到一个三粒子态$\left|\varphi\right\rangle_U$。过程如下。

$$\left|\varphi\right\rangle_U=\left|\alpha\right\rangle_u\otimes\left|\phi^{+}\right\rangle_{12}=\left(\cos\theta\left|0\right\rangle+\sin\theta\left|1\right\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)_{12}$$

2) u_i 对粒子 1 和量子态$\left|\alpha\right\rangle_U$进行测量。判断其结果处于四种 Bell 态中的哪一种。此处对量子信息进行编码。用经典信息二进制 00、01、10 和 11 分别代表u_i的测量结果$\left|\phi^{+}\right\rangle_{U1}$、$\left|\phi^{-}\right\rangle_{U1}$、$\left|\psi^{+}\right\rangle_{U1}$、$\left|\psi^{-}\right\rangle_{U1}$四个状态，并将结果(经典信息)发送给 TTP。此处将$\left|\varphi\right\rangle_U$按对应的四个 Bell 态展开得到：

$$\begin{aligned}\left|\varphi\right\rangle_U=1/2\Big[&\left|\phi^{+}\right\rangle_{U1}\left(\cos\theta\left|0\right\rangle_2+\sin\theta\left|1\right\rangle_2\right)+\left|\phi^{-}\right\rangle_{U1}\left(\cos\theta\left|0\right\rangle_2-\sin\theta\left|1\right\rangle_2\right)\\&+\left|\psi^{+}\right\rangle_{U1}\left(\cos\theta\left|1\right\rangle_2+\sin\theta\left|0\right\rangle_2\right)+\left|\psi^{-}\right\rangle_{U1}\left(\cos\theta\left|1\right\rangle_2-\sin\theta\left|0\right\rangle_2\right)\Big]\end{aligned}$$

3) TTP 根据收到的测量结果，对他拥有的粒子 2 做对应的操作，即可恢复出u_i信任值的原始量子态$\left|\alpha\right\rangle_U=\cos\theta\left|0\right\rangle+\sin\theta\left|1\right\rangle$。并规定当 TTP 收到$u_i$发送的经典信息 00、01、10、11 时，做相对应酉变换，即可得到u_i信任值的原始量子态$\left|\alpha\right\rangle_U$，对应关系如表 1 所示。

4) TTP 根据恢复出的$\left|\alpha\right\rangle_U=\cos\theta\left|0\right\rangle+\sin\theta\left|1\right\rangle$，计算出$u_i$的信任值，并根据计算出的信任值评判是否信任$u_i$，同时将$u_i$的信任值保存(更新)在 TTP 所属的本地数据库中。

3.3. 模糊综合评判信任模型

本节将利用模糊综合评判信任模型对接入节点的信任值进行判断，确认其信任值是否符合接入标准。首先对评判模型中所需要的语意集进行定义。属性集$X=\{x_1,x_2,\cdots,x_m\}$,其中每个子集x_i代表节点信任类型的各个属性。评价集$D=\{d_1,d_2,\cdots,d_n\}$，其中每个子集d_i代表节点每个属性的不同评价等级。根据属性集和评价集获得评判矩阵$R=\left(r_{ij}\right)_{m\times n}$。最后根据对节点不同属性的权重构建权重集合$W=\{w_1,w_2,\cdots,w_m\}$。

Table 1. The unitary transformation of classical information
表 1. 经典信息对应的酉变换

U 公布的经典信息	粒子 2 的状态	TTP 做对应的酉变换
00	$\cos\theta\|0\rangle+\sin\theta\|1\rangle$	$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$
01	$\cos\theta\|0\rangle-\sin\theta\|1\rangle$	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
10	$\cos\theta\|1\rangle+\sin\theta\|0\rangle$	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
11	$\cos\theta\|1\rangle-\sin\theta\|0\rangle$	$\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$

通过上文按照 TNC 规范采集并通过隐形传态传递到 TTP 的属性信任值，对节点属性集进行定义。例如历史通信成功率，病毒库完整性，授权软件应用版本，身份归属，安全策略等对信任值进行影响的属性。分别对这五个属性定义属性集 $X=\{x_1,x_2,x_3,x_4,x_5\}$，并设定权重集合分别为 0.5，0.2，0.1，0.1，0.1。确定评价集分别为 1，0.9，0.8，0.7 对应“完全符合”，“很符合”，“一般符合”，“不符合”。其中属性集，权重集，评价集可根据实际网络的要求而进行设定，以符合具体的需求。此处将节点 u 的各个属性集相对应的评价集通过上文所介绍的量子态发送给 TTP。节点各个属性所对应的评价集如表 2 所示。

由节点 u 各属性集对应的评价集经计算可获得评价矩阵 R 如下：

$$\begin{pmatrix}0.3 & 0.7 & 0 & 0\\ 0.4 & 0.5 & 0.1 & 0\\ 0.5 & 0.5 & 0 & 0\\ 0.2 & 0.3 & 0.45 & 0.05\\ 0.3 & 0.3 & 0.25 & 0.15\end{pmatrix}$$

TTP 通过对算子的选取来计算出评价向量 $I=W\cdot R=(0.33,0.56,0.09,0.02)$。最后通过评价集与评价向量进行量化，将节点 u 的信任值计算出。$D\cdot I^{\mathrm{T}}=0.92$。TTP 根据自身的接入标准设置一个阈值用来判断节点是否接入。假设该阈值为 0.90，则节点 u 接入成功。

4. 安全性分析

在整个量子网络中节点可信接入的过程可能会面临一些安全性问题。本小节将对文中不同流程进行安全性分析。

Table 2. Each attribute of the node corresponds to the evaluation set
表 2. 节点各个属性所对应的评价集

	完全符合	很符合	一般符合	不符合
历史通信成功率	30	70	0	0
病毒库完整性	40	50	10	0
授权软件应用版本	50	50	0	0
身份归属	20	30	45	5
安全策略	30	30	25	15

4.1. 身份认证的安全性

在进行量子身份认证的过程中，当窃听者截获到认证串光子序列，并对认证串进行测量想获取认证信息时。由于认证过程中使用到的两个不同的偏振态。根据量子测不准原理导致其无法正确的确定测量结果，并会导致对结果产生影响。例如假设认证串光子序列 S 的长度为 n 位，窃听者 Eve 对认证串光子序列 S 的每一位测量基的正确选取的概率为 1/2。在认证串光子序列 S 长度为 n 的情况下，窃听者 Eve 要对认证串光子序列 S 完全准确的获得测量结果的概率只有 1/2n。当认证串光子序列 S 的长度越长，窃听者 Eve 获得正确结果的概率越小。测量结果无法满足预期结果，从而认证失败。若是在非理想信道下则可根据实际情况设定一个阈值来进行判断[11]。从而保证认证过程当中不受外部的攻击。

4.2. 信任评估的安全性

在节点将自身的各个属性通过量子态完成传输的过程中，如果存在外部窃听者 Eve 进行截获攻击，由于处于缠态中的量子比特是由节点 u 所制备，窃听者 Eve 无法获得任何量子比特信息。当窃听者 Eve 截获到节点 u 通过经典信道发给 TTP 的信息(窃听者 Eve 得到节点 u 的测量结果，该过程中经典信道的测量结果其实已经是编码过后的信息)，但因为窃听者 Eve 没有量子纠缠态中的量子比特信息，所以即使他截取到经典信道中的测量结果，他也不能通过酉变换(因为窃听者 Eve 并不知道测量信息所对应的酉变换是什么)来恢复出携带信息的量子态 $|\alpha\rangle_U$。这样窃听者 Eve 就不能由量子态中获取任何节点的信息。因此保证了不被外部窃听者所攻击。

如果存在外部攻击者 Eve 截获到节点 u 发送给 TTP 处于纠缠态中的粒子 2，根据量子测不准原理和量子不可克隆定理，如果攻击者 Eve 去测量粒子 2，就会导致粒子 2 的量子态塌缩，进而无法恢复出携带节点 u 信息的量子态 $|\alpha\rangle_U$；如果攻击者 Eve 希望通过一些操作恢复出携带节点 u 信息的量子态 $|\alpha\rangle_U$，也会导致对粒子 2 的量子态塌缩。因为攻击者 Eve 并不知道测量结果及其所对应的酉变换是什么。从而保证了该过程的安全性。

此外，在本文中提出的量子可信中继网会将其接入的节点的信任度进行记录，在上层需要的时候由下向上进行汇报和传递，同时也避免了节点的抵赖情况的发生。

5. 小节

本文借助经典网络中可信接入的手段，利用量子可信中继网络来完成节点的可信接入。使用对单粒子的操作来实现量子身份认证，并通过直接模糊集理论及量子隐形传态来完成对节点的信任评估，最后通过综合评判模型来实现对节点接入的判定。将 TNC 标准结合到量子通信网络中研究并提出了基于量子可信中继网络节点可信接入模型，为量子通信网络中信任问题的研究提供了一种新思路。

基金项目

国家自然科学基金(61572086, 61402058)；四川省科技计划项目(拨款号：20717YY168)；国家重点研究发展计划(2017YFB0802302)；四川量子安全通信创新团队(17TD0009)；四川省学术和技术领导人培训资金支持项目(2016120080102643)，成都信息工程大学中青年学术研究基金(J201511)。

参考文献

[1] Bennett, C.H. and Brassard, G. (1984) Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, 175-179.

[2] Ekert, A.K. (1991) Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, **67**, 661-663. https://doi.org/10.1103/PhysRevLett.67.661

[3] 徐兵杰, 刘文林, 毛钧庆, 等. 量子通信技术发展现状及面临的问题研究[J]. 通信技术, 2014, 47(5): 463-468.

[4] Sasaki, M., Fujiwara, M., Ishizuka, H., *et al.* (2011) Field Test of Quantum Key Distribution in the Tokyo QKD Network. *Optics Express*, **19**, 10387-10409. https://doi.org/10.1364/OE.19.010387

[5] Zhang, H., Chen, L. and Zhang, L. (2010) Research on Trusted Network Connection. *Jisuanji Xuebao* (*Chinese Journal of Computers*), **33**, 706-717. https://doi.org/10.3724/SP.J.1016.2010.00706

[6] Zhang, H.G., Han, W.B., Lai, X.J., *et al.* (2015) Survey on Cyberspace Security. *Science China Information Sciences*, **58**, 1-43. https://doi.org/10.1007/s11432-015-5433-4

[7] Arrazola, J.M. and Lütkenhaus, N. (2014) Quantum Communication with Coherent States and Linear Optics. *Physical Review A*, **90**, Article ID: 042335. https://doi.org/10.1103/PhysRevA.90.042335

[8] Shi, R.H., Huang, L.S., Yang, W., *et al.* (2010) Quantum Secret Sharing between Multiparty and Multiparty with Bell States and Bell Measurements. *Science China Physics*, *Mechanics & Astronomy*, **53**, 2238-2244. https://doi.org/10.1007/s11433-010-4181-0

[9] Sun, Y., Xu, S.W., Chen, X.B., *et al.* (2013) Expansible Quantum Secret Sharing Network. *Quantum Information Processing*, **12**, 2877-2888. https://doi.org/10.1007/s11128-013-0570-4

[10] 张仕斌, 许春香. 基于云模型的信任评估方法研究[J]. 计算机学报, 2013, 36(2): 422-431.

[11] Chang, Y.J., Tsai, C.W. and Hwang, T. (2013) Multi-User Private Comparison Protocol Using GHZ Class States. *Quantum Information Processing*, **12**, 1077-1088. https://doi.org/10.1007/s11128-012-0454-z