(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108683501 A
(43)申请公布日 2018.10.19

(21)申请号 201810171946.2

(22)申请日 2018.03.01

(71)申请人 如般量子科技有限公司
地址 312030 浙江省绍兴市柯桥区柯岩街道余渚村1幢

(72)发明人 富尧 钟一民

(74)专利代理机构 杭州君度专利代理事务所(特殊普通合伙) 33240
代理人 解明铠 刘静静

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)

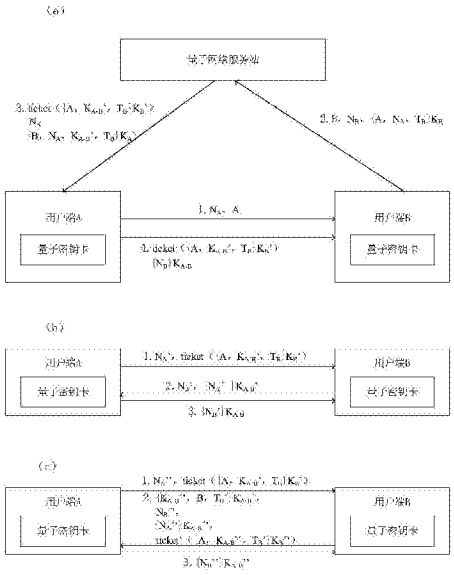
权利要求书2页 说明书10页 附图3页

(54)发明名称

基于量子通信网络的以时间戳为随机数的多次身份认证系统和方法

(57)摘要

本发明公开了一种基于量子通信网络的以时间戳为随机数的多次身份认证系统和方法，系统包括用户端A，用户端B以及量子网络服务站，用户端A向用户端B申请ticket时，用户端B生成时间戳发送至量子网络服务站，量子网络服务站利用该时间戳以及会话密钥生成ticket，再将所述ticket分发给用户端A以及经由用户端A分发给用户端B；所述会话密钥用于在用户端A与用户端B之间实施加密通信且由用户端A和量子网络服务站之间同步生成；各用户端分别配置有量子密钥卡，用于生成真随机数作为ticket分发以及ticket使用时的认证标识。本发明其基于量子通信网络的以时间戳为随机数实施多次认证，进一步提高了安全性，另外改进了会话密钥的生成方式，减少身份认证传递的信息数量。



CN 108683501 A

1.一种基于量子通信网络的以时间戳为随机数的多次身份认证系统，其特征在于，包括用户端A，用户端B以及量子网络服务站，用户端A向用户端B申请ticket时，用户端B生成时间戳发送至量子网络服务站，量子网络服务站利用该时间戳以及会话密钥生成ticket，再将所述ticket分发给用户端A以及经由用户端A分发给用户端B；

所述会话密钥用于在用户端A与用户端B之间实施加密通信且由用户端A和量子网络服务站之间同步生成；各用户端分别配置有量子密钥卡，用于生成真随机数作为ticket分发以及ticket使用时的认证标识。

2.如权利要求1所述的基于量子通信网络的以时间戳为随机数的多次身份认证系统，其特征在于，用户端A向用户端B申请ticket时，包括：

用户端A生成密钥K_A以及会话密钥K_{A-B}并将生成方式通知量子网络服务站，用户端B生成密钥K_B并将生成方式通知量子网络服务站；

用户端A向用户端B发送第一消息以申请ticket，该第一消息中携带有用户端A身份信息以及作为认证标识的真随机数N_A，真随机数N_A为用户端A匹配的量子密钥卡生成。

3.如权利要求2所述的基于量子通信网络的以时间戳为随机数的多次身份认证系统，其特征在于，用户端B生成时间戳发送至量子网络服务站，具体包括用户端B响应于第一消息向量子网络服务站发送第二消息，该第二消息中包括：

作为认证标识的真随机数N_B，真随机数N_B为用户端B匹配的量子密钥卡生成；

用户端B的身份信息；

用来给用户端A颁发信任的指令，包括所述真随机数N_A、用户端A的身份信息以及用户端B生成的时间戳T_B，且该指令通过密钥K_B加密。

4.如权利要求3所述的基于量子通信网络的以时间戳为随机数的多次身份认证系统，其特征在于，所述量子网络服务站依据第二消息中用户端A以及用户端B的身份信息，生成与密钥K_A相同的密钥K_A'，与密钥K_B相同的密钥K_B'，以及与会话密钥K_{A-B}相同的会话密钥K_{A-B}'；

所述量子网络服务站生成携带有所述ticket的第三消息发送给用户端A，该第三消息中包括：

ticket；

真随机数N_B；

利用密钥K_A'加密的：用户端B的身份信息、真随机数N_A、会话密钥K_{A-B}'以及时间戳T_B；

其中所述ticket包括利用密钥K_B'加密的：用户端A的身份信息、会话密钥K_{A-B}'以及时间戳T_B。

5.如权利要求4所述的基于量子通信网络的以时间戳为随机数的多次身份认证系统，其特征在于，所述ticket经由用户端A分发给用户端B时，用户端A先验证第三消息中的真随机数N_A，验证成功后向用户端B发送第四消息，该第四消息中包括ticket以及利用会话密钥K_{A-B}加密的真随机数N_B；

用户端B接收第四消息后验证第四消息中的真随机数N_B。

6.如权利要求1所述的基于量子通信网络的以时间戳为随机数的多次身份认证系统，其特征在于，还包括用户端A依据所述ticket访问用户端B，包括：

用户端A向用户端B发送访问请求，该访问请求中包括作为认证标识的真随机数N_A'，以

及所述ticket，所述真随机数N_A'为用户端A匹配的量子密钥卡生成；

用户端B接收访问请求，验证ticket，验证通过后向用户端A发送验证请求，该验证请求中包括作为认证标识的真随机数N_B'，以及利用会话密钥K_{A-B}加密的真随机数N_A'，真随机数N_B'为用户端B匹配的量子密钥卡生成；

用户端A接收验证请求并对真随机数N_A'进行验证，验证通过后向用户端B发送验证回复，该验证回复中包括利用会话密钥K_{A-B}加密的真随机数N_B'；

用户端B接收验证回复并对真随机数N_B'进行验证。

7.如权利要求1所述的基于量子通信网络的以时间戳为随机数的多次身份认证系统，其特征在于，所述ticket按照预定条件更新，更新时包括：

用户端A向用户端B发送更新请求，该更新请求中包括作为认证标识的真随机数N_A"，以及所述ticket，所述真随机数N_A"为用户端A匹配的量子密钥卡生成；

用户端B接收更新请求，验证ticket，验证通过后向用户端A发送更新回复，该更新回复包括：

更新后的会话密钥K_{A-B}"、用户端B的身份信息和新的时间戳T_B'，且这三者利用更新前的会话密钥K_{A-B}'加密；

作为认证标识的真随机数N_B"，该真随机数N_B"为用户端B匹配的量子密钥卡生成；

利用更新后的会话密钥K_{A-B}"加密的真随机数N_A"；以及

更新后的ticket；

用户端A接收更新回复并对真随机数N_A"进行验证，验证通过后向用户端B发送更新反馈，该更新反馈中包括利用更新后的会话密钥K_{A-B}"加密的真随机数N_B"；

用户端B接收更新反馈并对真随机数N_B"进行验证。

8.如权利要求4所述的基于量子通信网络的以时间戳为随机数的多次身份认证系统，其特征在于，所述量子网络服务站包括量子网络服务站A以及量子网络服务站B，其中用户端A匹配的量子密钥卡颁发自量子网络服务站A，用户端B匹配的量子密钥卡颁发自量子网络服务站B；

用户端A向用户端B申请ticket时，用户端A生成密钥K_A以及会话密钥K_{A-B}并将生成方式通知量子网络服务站A，用户端B生成密钥K_B并将生成方式通知量子网络服务站B；

量子网络服务站B接收来自用户端B的第二消息，量子网络服务站B依据第二消息中用户端B的身份信息，生成与密钥K_B相同的密钥K_B'；

量子网络服务站B利用密钥K_B'将用来给用户端A颁发信任的指令解密，将解密后的指令连同第二消息中的其它内容通过站间加密传输方式发送给量子网络服务站A；

量子网络服务站A依据用户端A的身份信息，生成与密钥K_A相同的密钥K_A'，以及与会话密钥K_{A-B}相同的会话密钥K_{A-B}'；

量子网络服务站A再相应的生成第三消息发送给用户端A。

9.一种基于量子通信网络的以时间戳为随机数的多次身份认证方法，其特征在于，实施在权利要求1～8任一项所述的多次身份认证系统中。

基于量子通信网络的以时间戳为随机数的多次身份认证系统和方法

技术领域

[0001] 本发明涉及量子通信技术领域，尤其涉及基于量子网络服务站的身份认证的系统和方法。

背景技术

[0002] 身份认证是实现信息安全的基本技术，系统通过审查用户的身份来确认该用户是否具有对某种资源的访问和使用权限，同样也可以进行系统与系统间的身份认证。

[0003] 当前通信网络中身份认证系统普遍采用Kerberos认证方案。Kerberos是一种网络认证协议，其设计目标是通过密钥系统为用户机/服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无需基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意的读取、修改和插入数据。在以上情况下，Kerberos作为一种可信任的第三方认证服务，是通过传统的密码技术(如：共享密钥)执行认证服务的。

[0004] 在Kerberos认证方案中，引入了时间戳timestamp来对重放攻击进行遏止，但是票据有生命周期，在其生命周期的有效时间内仍然可以使用。如果收到消息的时间是在规定允许的范围之内，那么就认为该消息具有新鲜性。但是，在得到许可证后的攻击者可以发送伪造的消息，这样的话，在允许的时间内是很难发现的。

[0005] 现有技术存在的问题：

[0006] (1)现有身份认证技术基于Kerberos认证方案对时间戳的使用导致有出现重放攻击的可能。

[0007] (2)Kerberos协议要求是基于网络中时钟同步，对整个系统时间同步要求高，在大型分布式系统中难以实现。

[0008] (3)现有技术中服务器要分别向两个用户端分发会话密钥，存在一定的安全隐患。

[0009] (4)现有技术中，用户端密钥存储于用户端存储器中，可以被恶意软件或恶意操作窃取。

[0010] (5)现有技术中身份认证所传递的信息数较多，完成一次身份认证需要传递五个信息。

发明内容

[0011] 本发明提供一种身份认证系统，其基于量子通信网络的以时间戳为随机数实施多次认证，进一步提高了安全性，另外改进了会话密钥的生成方式，减少了身份认证所需要传递的信息数量。

[0012] 一种基于量子通信网络的以时间戳为随机数的多次身份认证系统，包括用户端A，用户端B以及量子网络服务站，用户端A向用户端B申请ticket时，用户端B生成时间戳发送至量子网络服务站，量子网络服务站利用该时间戳以及会话密钥生成ticket，再将所述

ticket分发给用户端A以及经由用户端A分发给用户端B；

[0013] 所述会话密钥用于在用户端A与用户端B之间实施加密通信且由用户端A和量子网络服务站之间同步生成；各用户端分别配置有量子密钥卡，用于生成真随机数作为ticket分发以及ticket使用时的认证标识。

[0014] 本发明所述的用户端A与用户端B仅仅是便于区别和描述，A、B并不对用户端本身作出额外限定。

[0015] 用户端的配置的量子密钥卡分别与量子网络服务站存储有相应的量子密钥，用于在用户端与量子网络服务站之间直接或间接的加密传输以及身份认证。

[0016] 作为网络侧的量子网络服务站可以是一个或多个，多个量子网络服务站参与时，整个网络侧可视为一整体，当不同的量子密钥卡归属于不同的量子网络服务站时，不同的量子网络服务站可以通过QKD等方式在站间加密传输数据。

[0017] 由于本发明基于量子网络，在没有特别强调时，所涉及到的随机数均为真随机数，例如量子随机数，所述涉及到的密钥均为量子密钥。

[0018] 用户端A向用户端B申请ticket时，包括：

[0019] 用户端A生成密钥K_A以及会话密钥K_{A-B}并将生成方式通知量子网络服务站，用户端B生成密钥K_B并将生成方式通知量子网络服务站；

[0020] 用户端A向用户端B发送第一消息以申请ticket，该第一消息中携带有用户端A身份信息以及作为认证标识的真随机数N_A，真随机数N_A为用户端A匹配的量子密钥卡生成。

[0021] 用户端B生成时间戳发送至量子网络服务站，具体包括用户端B响应于第一消息向量子网络服务站发送第二消息，该第二消息中包括：

[0022] 作为认证标识的真随机数N_B，真随机数N_B为用户端B匹配的量子密钥卡生成；

[0023] 用户端B的身份信息；

[0024] 用来给用户端A颁发信任的指令，包括所述真随机数N_A、用户端A的身份信息以及用户端B生成的时间戳T_B，且该指令通过密钥K_B加密。

[0025] 所述量子网络服务站依据第二消息中用户端A以及用户端B的身份信息，生成与密钥K_A相同的密钥K_A'，与密钥K_B相同的密钥K_B'，以及与会话密钥K_{A-B}相同的会话密钥K_{A-B}'；

[0026] 所述量子网络服务站生成携带有所述ticket的第三消息发送给用户端A，该第三消息中包括：

[0027] ticket；

[0028] 真随机数N_B；

[0029] 利用密钥K_A'加密的：用户端B的身份信息、真随机数N_A、会话密钥K_{A-B}'以及时间戳T_B；

[0030] 其中所述ticket包括利用密钥K_B'加密的：用户端A的身份信息、会话密钥K_{A-B}'以及时间戳T_B。

[0031] 本发明中例如密钥K_A与相同的密钥K_A'，为了区分生成方的不同通过角标标识，由于采用的是对称加密原理，因此密钥K_A与密钥K_A'在内容上是相同的，用于进行相应的加、解密操作。其它称谓中的角标区分同理；密钥K_A也可简称K_A，其它称谓同理。

[0032] 所述ticket经由用户端A分发给用户端B时，用户端A先验证第三消息中的真随机数N_A，验证成功后向用户端B发送第四消息，该第四消息中包括ticket以及利用会话密钥

K_{A-B}加密的真随机数N_B；

[0033] 用户端B接收第四消息后验证第四消息中的真随机数N_B。

[0034] 本发明多次身份认证系统还包括用户端A依据所述ticket访问用户端B，包括：

[0035] 用户端A向用户端B发送访问请求，该访问请求中包括作为认证标识的真随机数N_A'，以及所述ticket，所述真随机数N_A'为用户端A匹配的量子密钥卡生成；

[0036] 用户端B接收访问请求，验证ticket，验证通过后向用户端A发送验证请求，该验证请求中包括作为认证标识的真随机数N_B'，以及利用会话密钥K_{A-B}加密的真随机数N_A'，真随机数N_B'为用户端B匹配的量子密钥卡生成；

[0037] 用户端A接收验证请求并对真随机数N_A'进行验证，验证通过后向用户端B发送验证回复，该验证回复中包括利用会话密钥K_{A-B}加密的真随机数N_B'；

[0038] 用户端B接收验证回复并对真随机数N_B'进行验证。

[0039] 所述ticket按照预定条件更新，更新时包括：

[0040] 用户端A向用户端B发送更新请求，该更新请求中包括作为认证标识的真随机数N_A"，以及所述ticket，所述真随机数N_A"为用户端A匹配的量子密钥卡生成；

[0041] 用户端B接收更新请求，验证ticket，验证通过后向用户端A发送更新回复，该更新回复包括：

[0042] 更新后的会话密钥K_{A-B}"、用户端B的身份信息和新的时间戳T_B'，且这三者利用更新前的会话密钥K_{A-B}'加密；

[0043] 作为认证标识的真随机数N_B"，该真随机数N_B"为用户端B匹配的量子密钥卡生成；

[0044] 利用更新后的会话密钥K_{A-B}"加密的真随机数N_A"；以及

[0045] 更新后的ticket；

[0046] 用户端A接收更新回复并对真随机数N_A"进行验证，验证通过后向用户端B发送更新反馈，该更新反馈中包括利用更新后的会话密钥K_{A-B}"加密的真随机数N_B"；

[0047] 用户端B接收更新反馈并对真随机数N_B"进行验证。

[0048] 本发明中各认证标识都是相应的用户端在匹配的量子密钥卡中生成，且为真随机数的形式。

[0049] 会话密钥以及各用户端与量子网络服务站之间的加密通信的密钥，都是通过密钥种子经由指定算法得到，用户端在进行身份认证时，作为密钥种子的量子密钥长期使用或重复使用会有被破解的可能性，为提高本身份认证系统的安全性，密钥种子需要定时更新。

[0050] 用户端与匹配的量子密钥卡建立通信连接后，用户端通过上层应用程序向量子密钥卡发送更新申请，该更新申请同时也发送至量子网络服务站；

[0051] 密钥存储卡接收更新申请后，按预先设定的规则更新密钥种子；

[0052] 量子网络服务站接收更新申请后，按预先与量子密钥卡协商一致的规则更新量子网络服务站内相应存储的密钥种子。

[0053] 本发明中，可选的情况是，用户端A与用户端B两者匹配的量子密钥卡归属于同一量子网络服务站。即均与该量子网络服务站存储有相应的量子密钥，也可视为在局域网环境下。

[0054] 若在广域网环境下，用户端A与用户端B两者匹配的量子密钥卡归属于不同的量子网络服务站，例如：

[0055] 所述量子网络服务站包括量子网络服务站A以及量子网络服务站B，其中用户端A匹配的量子密钥卡颁发自量子网络服务站A，用户端B匹配的量子密钥卡颁发自量子网络服务站B；

[0056] 用户端A向用户端B申请ticket时，用户端A生成密钥K_A以及会话密钥K_{A-B}并将生成方式通知量子网络服务站A，用户端B生成密钥K_B并将生成方式通知量子网络服务站B；

[0057] 量子网络服务站B接收来自用户端B的第二消息，量子网络服务站B依据第二消息中用户端B的身份信息，生成与密钥K_B相同的密钥K_B'；

[0058] 量子网络服务站B利用密钥K_B'将用来给用户端A颁发信任的指令解密，将解密后的指令连同第二消息中的其它内容通过站间加密传输方式发送给量子网络服务站A；

[0059] 量子网络服务站A依据用户端A的身份信息，生成与密钥K_A相同的密钥K_A'，以及与会话密钥K_{A-B}相同的会话密钥K_{A-B}'；

[0060] 量子网络服务站A再相应的生成第三消息发送给用户端A。

[0061] 本发明还提供一种基于量子通信网络的以时间戳为随机数的多次身份认证方法，实施在本发明所述的多次身份认证系统中。

[0062] 由于在多次身份认证系统中已有相关流程的详细描述，因此方法部分不再赘述。

[0063] 现有身份认证技术基于kerberos认证方案对时间戳的使用导致有出现重放攻击的可能，并且整个kerberos协议要求是基于网络中时钟同步，对整个系统时间同步要求高，在大型分布式系统中难以实现。本发明将原方案使用的时间戳改为了真随机数，并使用与用户端B的本地时钟相关联的时间戳，对整个系统的时间同步没有要求。

[0064] 本发明中会话密钥的生成方式为使用量子网络服务站与用户端A同步产生而不是由量子网络服务站直接生成，省去了向用户端B分发会话密钥的过程，降低了分发过程中会话密钥被破解导致消息泄露的可能，提升了安全性。

[0065] 本发明使用量子密钥卡存储用户端密钥而不是用户端存储器，量子密钥卡是独立的硬件设备，被恶意软件或恶意操作窃取密钥的可能性大大降低。本发明中初始身份认证只需要传递四个信息，二次身份认证只需要传递三个信息，减少了身份认证所需要传递的信息数。

附图说明

[0066] 图1为本发明身份认证系统结构图。

[0067] 图2为局域网内身份认证流程图；

[0068] 图中(a)部分示意了用户端A申请ticket的流程；

[0069] 图中(b)部分示意了二次身份认证的流程；

[0070] 图中(c)部分示意了更新ticket的流程。

[0071] 图3为广域网内身份认证流程图；

[0072] 图中(a)部分示意了用户端A申请ticket的流程；

[0073] 图中(b)部分示意了二次身份认证的流程；

[0074] 图中(c)部分示意了更新ticket的流程。

具体实施方式

[0075] 如图1所示，本发明身份认证系统可以包括多个量子网络服务站，不同量子网络服务站之间可以通过QKD方式共享站间量子密钥。

[0076] 量子网络服务站包括：

[0077] 量子服务中心，主要用于通过经典网络与用户侧的各用户端通信连接以及与其他量子网络服务站通信连接；经典网络包括但不限于电信网、互联网、广播电视网或者其他通信网络等。

[0078] 量子密钥分发设备，主要用于通过QKD方式实现站间量子密钥的共享。

[0079] 真随机数发生器，用于接收用户侧密钥管理服务器提出的申请用户侧密钥的请求，生成用户侧密钥，并发送给用户侧密钥管理服务器；此处采用的为真随机数发生器。其优选为量子真随机数发生器，也可以为基于电路的真随机数发生器、基于物理源的真随机数发生器以及其他种类的真随机发生器。

[0080] 用户侧密钥管理服务器，存放、管理从真随机数发生器生成的用户侧密钥，可以接入可移动式的量子密钥卡，实现发卡、登记、拷贝用户侧密钥，还可以接收量子服务中心提出的申请用户侧密钥请求，发送相应长度的用户侧密钥给量子服务中心。量子密钥卡的详细内容请见申请号为

[0081] “201610846210.6”的专利。

[0082] 其中量子服务中心包括：身份认证服务器，票据许可服务器，还可根据需要设置其他服务器，例如数字签名服务器、签名验证服务器、加解密服务器等。

[0083] 身份认证服务器用于实现用户在接受消息认证、数字签名等服务前与量子网络服务站的相互身份认证。身份认证服务器内部具有采用PCI总线接口的加密卡，用于存储身份认证协议，包括密钥生成算法、认证函数、加密传输协议。

[0084] 票据许可服务器用于实现用户在获得与量子网络服务站的相互身份认证后，为用户分发其访问某一用户的申请的许可。

[0085] 各量子网络服务站下配置有用户端，例如图中的用户端1～用户端n，本说明书中不同的服务器或其他装置在硬件上也可以根据需要进行整合。

[0086] 用户端为接入量子网络服务站的设备，可为移动终端，或为固定终端。当为移动终端时，量子密钥卡优选为量子SD卡；当为固定终端时，量子密钥卡优选为USBkey或主机加密板卡。

[0087] 当用户前往所在区域的量子网络服务站进行注册登记，获批后得到量子密钥卡(具有唯一的量子密钥卡ID)。量子密钥卡存储了用户注册登记信息，还内置有身份认证协议，至少包括密钥生成算法以及认证函数，或其他与身份认证相关的算法。

[0088] 网络侧的各个量子网络服务站也相应的存有认证协议，若协议中各算法存在两种以上，量子密钥卡在与量子网络服务站通信时会将算法标号发送给量子网络服务站，供量子网络服务站选取。

[0089] 量子密钥卡中的用户侧密钥可能下载自不同的量子网络服务站，因此可按不同来源存在不同的密钥种子集中，用户端可按预先设定的规则取用密钥种子以生成密钥。不同的密钥种子集具有唯一的密钥种子ID，其指向的量子网络服务站中存储有相应的密钥种子。

[0090] 量子密钥卡从智能卡技术上发展而来，是结合了量子物理学技术、密码学技术、智

能卡技术和USB技术的身份认证产品。量子密钥卡的内嵌芯片和芯片操作系统可以提供私钥的安全存储和密码算法等功能。由于其具有独立的数据处理能力和良好的安全性，量子密钥卡成为量子真随机数私钥的安全载体。每一个量子密钥卡都有硬件PIN码保护，PIN码和硬件构成了用户使用量子密钥卡的两个必要因素。即所谓“双因子认证”，用户只有同时取得保存了相关认证信息的量子密钥卡和用户PIN码，才可以登录系统。即使用户的PIN码被泄露，只要用户持有的量子密钥卡不被盗取，合法用户的身份就不会被仿冒；如果用户的量子密钥卡遗失，拾到者由于不知道用户PIN码，也无法仿冒合法用户的身份。

[0091] 实施例1，局域网内同属于一个量子网络服务站的两个用户端身份认证

[0092] 以下步骤中，在各用户端侧涉及的加解、密操作，都在所匹配的量子密钥卡中进行。身份认证服务器和票据许可服务器涉及的加、解密操作，是在量子网络服务站的加解密服务器中完成。

[0093] 当用户端A、用户端B都同属于一个量子网络服务站时，身份认证过程中所涉及的量子密钥卡在该本地量子网络服务站注册颁发。具体步骤参见图2，图中，大括号内表示被加密的部分，括号内表示传输的多个内容，用逗号隔开，后面紧跟的内容表示使用的密钥，如$\{A,N_A,T_B\}K_B$表示使用K_B加密A、N_A和T_B。若未使用大括号，则表示是明文传输。

[0094] 图2中各部分的1、2、3、4分别表示该部分中的流程顺序，在图2的(a)部分中，1、2、3、4也分别对应下文中的message1～message4。

[0095] 每条message中，若包括多个部分，则每个部分作为一行表示，例如message3分为3行表示，即包括三个部分，其中第三部分为$\{B,N_A,K_{A-B}',T_B\}K_A'$，其余部分以及其余附图同理。

[0096] 具体步骤文字描述如下：

[0097] 1.用户端A申请Ticket。参见图2中(a)部分。

[0098] 用户端A和用户端B分别与量子网络服务站进行密钥同步：用户端A匹配的量子密钥卡根据所存储的密钥种子SA以及卡内随机数发生器所产生的随机数R1结合密钥生成算法AS得到密钥K_A(以下简称K_A，其它同理省去汉字部分作为简称)。

[0099] 用户端A匹配的量子密钥卡根据所存储的密钥种子SA以及卡内随机数发生器所产生的随机数R2分别结合密钥生成算法AS得到与用户端B之间的会话密钥K_{A-B}。将随机数R1、R2以及密钥生成算法ID和密钥种子ID传递给量子网络服务站；并通知量子网络服务站进行密钥同步。

[0100] 用户端B匹配的量子密钥卡根据所存储的密钥种子SB以及卡内随机数发生器所产生的随机数R3结合密钥生成算法BS得到密钥K_B。将随机数R3以及密钥生成算法ID和密钥种子ID传递给量子网络服务站；并通知量子网络服务站进行密钥同步。

[0101] 用户端A和用户端B两者与量子网络服务站之间的密钥同步可以按照设定的条件或周期预先进行。

[0102] 1.1用户端A生成真随机数并发送给用户端B：用户端A匹配的量子密钥卡生成真随机数N_A。将N_A与A的身份信息(图2中message1中的A)作为明文形式的message1发送给用户端B。

[0103] 步骤1.1应理解为message1中至少包括真随机数N_A与A的身份信息，用户端A为了表达申请ticket以及message1在网络中的传输，可以在message1的封装过程中，选择相应

的协议方式以及通过标识符等方式告知用户端B申请ticket，后续的多处消息传输以及二次身份认证和更新ticket过程中同理，本发明重点在于真随机数和ticket生成方式以及运用的改进，消息的封装以及网络传输方式本身可以采用现有技术。

[0104] 1.2用户端B生成真随机数并发送给量子网络服务站：用户端B匹配的量子密钥卡生成真随机数N_B。将N_B与用户端B的身份信息和用户端B生成的一个给量子网络服务站用来给A颁发信任的指令作为message2发送给量子网络服务站。指令详细说明用户端A是信息的主动申请者并提供从用户端A收到的真随机数N_A，指令还包括用户端B生成的时间戳T_B。T_B是一个带有时间起点的时间戳，作为随机数来使用。之后过程中在用户端B收到时间戳T_B后，用户端B会检查这个时间起点与是否与当前的相符并检查时间戳是否在可允许的范围内。整个指令使用K_B加密。

[0105] 1.3量子网络服务站分发会话密钥：量子网络服务站根据密钥生成算法ID和密钥种子ID，在当前量子网络服务站内找出对应的密钥种子SA'、和密钥生成算法AS'，结合随机数R1运算得到与密钥K_A相同的密钥K_A'。

[0106] 结合随机数R2运算得到与密钥K_{A-B}相同的密钥K_{A-B}'。

[0107] 量子网络服务站根据密钥生成算法ID和密钥种子ID，在当前量子网络服务站内找出对应的密钥种子SB'和密钥生成算法BS'，结合随机数R3运算得到与密钥K_B相同的密钥K_B'。

[0108] 量子网络服务站使用K_B'解密指令，然后将用户端A的身份信息、K_{A-B}'、以及T_B使用K_B'加密，作为message3中的ticket发送给用户端A。message3中还包括N_B和使用K_A'加密的用户端B的身份信息、N_A、K_{A-B}'以及T_B。

[0109] 1.4用户端A发送ticket：用户端A使用K_A解密message3的最后一部分(参见图2，即$\{B, N_A, K_{A-B}', T_B\}K_A'$)，验证随机数$N_A$和message1中的是否相同。认证通过后把ticket连同用K_{A-B}加密的随机数N_B一起作为message4发送给用户端B，向用户端B证明自己的身份。用户端B解密后验证N_B。

[0110] 2.二次身份认证。参见图2中(b)部分。

[0111] 2.1用户端A申请二次认证：用户端A生成一个新的随机数N_A'，和ticket一起发送给B。

[0112] 2.2用户端A和用户端B完成双向认证：用户端B收到用户端A的二次认证申请后，验证ticket，通过后再生成一个新的随机数N_B'，用与上文相同的方法完成AB间的双向认证。用户端B解密ticket并验证T_B即检查这个时间起点与是否与当前的相符并检查时间戳是否在可允许的范围内。验证后，使用得到的K_{A-B}'加密N_A'，与N_B'一起发给用户端A，A解密后验证N_A'，再用K_{A-B}加密N_B'发送给用户端B，用户端B解密后验证N_B'，完成双向身份认证。

[0113] 3.更新ticket。参见图2中(c)部分。

[0114] 3.1用户端A申请更新ticket：用户端A生成一个新的随机数N_A"，和ticket一起发送给B。

[0115] 3.2用户端B分发新的ticket：用户端B认证ticket后，生成一个新的随机数N_B"和新的密钥K_B"。对K_{A-B}'进行运算生成K_{A-B}"，也可以重新生成K_{A-B}"。使用K_{A-B}'加密K_{A-B}"，用户端B的身份信息和新的时间戳T_B'，连同新生成的N_B"、用K_{A-B}"加密的N_A"、以及新的ticket'一起发送给用户端A。ticket'用密钥K_B"加密，内容如下：

[0116] ①新的AB会话密钥K_{A-B}”；

[0117] ②A的身份信息；

[0118] ③B新生成的时间戳T_B’。

[0119] 3.3用户端A得到新的ticket并与用户端B完成双向验证：用户端A收到信息后使用K_{A-B}解密第一部分，得到K_{A-B}”。使用K_{A-B}”解密第三部分完成对N_A”的验证。然后使用K_{A-B}”加密N_B”并发送给用户端B，用户端B解密后验证N_B”，完成双向身份认证。

[0120] 本系统中用户端B也可以为与A不匹配的量子网络服务站B，通过用户端A、与用户端A匹配的量子网络服务站A和量子网络服务站B三者之间的信息传递完成用户端A与量子网络服务站B相互之间的身份认证。由于需要站间通信，因此各交换中心以及量子网络服务站分别设有量子密钥分发设备，可通过QKD方式实现站间密钥的共享。1.2中message2的传递可使用量子网络服务站A与量子网络服务站B各自的量子密钥分发设备实现站间量子密钥的共享，使得明文形式的message2在量子网络服务站A和量子网络服务站B实现传递。量子网络服务站A与量子网络服务站B之间如果还要通过其他网络节点中转，则直接通信连接的两量子网络服务站(或网络节点)之间通过相应的量子密钥分发设备形成的站间量子密钥，并依次中转传送密文。站间量子密钥的分发是利用量子力学基本原理实现的异地密钥共享的方式，优选为BB84协议。

[0121] 用户在进行身份认证时，密钥种子长期使用或重复使用会有被破解的可能性，为提高本身份认证系统的安全性，密钥种子需要定时更新。

[0122] 本实施例中的更新方式为：

[0123] 用户端与匹配的量子密钥卡建立通信连接后，用户端通过上层应用程序向量子密钥卡发送更新申请，该更新申请同时也发送至量子服务中心。

[0124] 密钥存储卡接收更新申请后，按预先设定的规则更新密钥种子，例如将一部分使用过的密钥种子做失效标识，不再使用，而启用新的密钥种子。

[0125] 量子服务中心接收更新申请后，按预先与量子密钥卡协商一致的规则更新量子网络服务站内相应存储的密钥种子，实现与量子密钥卡的时时对应。本发明中各实施例的密钥种子的更新方法均采用上述方法。

[0126] 实施例2，广域网内的两个用户端的身份认证

[0127] 如图3所示，当用户端A、用户端B不属于同一个量子网络服务站时，身份认证过程中所涉及的量子密钥卡分别在该用户端所属的量子网络服务站注册颁发。本实施例中的系统架构区别于实施例1之处为应用在广域网中，一级交换中心是一个地级市或相当大小区域的量子网络核心站，二级交换中心是一个县级市或相当大小区域的量子网络核心站，量子网络服务站是一个乡镇或街道办事处相当大小区域的量子通信接入站点。

[0128] 一级交换中心和下属的多个二级交换中心以星型网络结构相连，二级交换中心可以和多个下属的量子网络服务站以星型网络结构相连。

[0129] 由于需要站间通信，因此各交换中心以及量子网络服务站分别设有量子密钥分发设备，可通过QKD方式实现站间密钥的共享。本实施例中量子网络服务站的其他设备以及关于量子密钥卡的描述可参见实施例1。

[0130] 例如一级交换中心和下属的二级交换中心分别利用量子密钥分发设备实现站间量子密钥的共享，二级交换中心和下属的的量子网络服务站分别利用量子密钥分发设备实

现站间量子密钥的共享，量子密钥分发设备可以是一套也可以是至少两套集成。

[0131] 两个一级交换中心之间由于距离较远，可采用量子中继站的方式实现站间量子密钥共享。

[0132] 本实施例中，用户端A与用户端B要进行身份认证，用户端A归属于量子网络服务站A，即相对于用户端A而言，其当前量子网络服务站为与用户端A通信连接的量子网络服务站A；同理用户端B归属于量子网络服务站B。本实施例区别于实施例1的具体部分为密钥K_A'的获取与传输方式。

[0133] 具体步骤参见图3，文字描述如下：

[0134] 1.用户端A申请Ticket。参见图3中(a)部分。

[0135] 用户端A和用户端B分别与量子网络服务站进行密钥同步：用户端A匹配的量子密钥卡根据所存储的密钥种子SA以及卡内随机数发生器所产生的随机数R1分别结合密钥生成算法AS得到密钥K_A(以下简称K_A，其它同理省去汉字部分作为简称)。用户端A匹配的量子密钥卡根据所存储的密钥种子SA以及卡内随机数发生器所产生的随机数R2分别结合密钥生成算法AS得到与用户端B之间的会话密钥K_{A-B}。将随机数R1、R2以及密钥生成算法ID和密钥种子ID传递给量子网络服务站；并通知量子网络服务站进行密钥同步。用户端B匹配的量子密钥卡根据所存储的密钥种子SB以及卡内随机数发生器所产生的随机数R3结合密钥生成算法BS得到密钥K_B。将随机数R3以及密钥生成算法ID和密钥种子ID传递给量子网络服务站；并通知量子网络服务站进行密钥同步。

[0136] 1.1用户端A生成真随机数并发送给用户端B：用户端A匹配的量子密钥卡生成真随机数N_A。将N_A与A的身份信息作为明文形式的message1发送给用户端B。

[0137] 1.2用户端B生成真随机数并发送给量子网络服务站B：用户端B匹配的量子密钥卡生成真随机数N_B。将N_B与B的身份信息和B生成的一个给量子网络服务站用来给A颁发信任的指令作为message2发送给量子网络服务站B。指令详细说明A是信息的主动申请者并提供从用户端A收到的随机数N_a，指令还包括用户端B生成的时间戳T_B。T_B是一个带有时间起点的时间戳，作为随机数来使用，在B收到时间戳T_B后，B会检查这个时间起点与是否与当前的相符并检查时间戳是否在可允许的范围内。整个指令使用K_B加密。

[0138] 1.3量子网络服务站分发会话密钥：量子网络服务站B根据密钥生成算法ID和密钥种子ID，在当前量子网络服务站内找出对应的密钥种子SB'和密钥生成算法BS'，结合随机数R3运算得到与密钥K_B相同的密钥K_B'。

[0139] 量子网络服务站A根据密钥生成算法ID和密钥种子ID，在当前量子网络服务站内找出对应的密钥种子SA'和密钥生成算法AS'，结合随机数R1运算得到与密钥K_A相同的密钥K_A'。结合随机数R2运算得到与密钥K_{A-B}相同的密钥K_{A-B}'。

[0140] 量子网络服务站B使用K_B'解密指令，得到A，N_A和T_B。

[0141] 量子网络服务站A与量子网络服务站B利用各自的量子密钥分发设备实现站间量子密钥的共享，使得明文形式的B，N_B，A，N_A，T_B，K_B'作为message3在量子网络服务站B加密后发送至量子网络服务站A。再经解密恢复出明文形式的信息。

[0142] 量子网络服务站A与量子网络服务站B之间如果还要通过其他网络节点中转，则直接通信连接的两量子网络服务站(或网络节点)之间通过相应的量子密钥分发设备形成的站间量子密钥，并依次中转传送密文。

[0143] 站间量子密钥的分发是利用量子力学基本原理实现的异地密钥共享的方式，优选为BB84协议。

[0144] 1.4量子网络服务站A并通过真随机数发生器生成用户端A和用户端B的会话密钥K_{A-B}。将A的身份，K_{A-B}以及T_B使用K_B'加密，作为message4中的ticket发送给你给用户端A。message4中还包括N_B和使用K_A'加密的B的身份信息、N_A、K_{A-B}以及T_B。

[0145] 1.5用户端A发送ticket：用户端A使用K_A解密message4的最后一部分，验证随机数N_A和message1中的是否相同。然后用把ticket连同用K_{A-B}加密的随机数N_B一起作为message5发送给用户端B，向用户端B证明自己的身份。用户端B解密后验证N_B。

[0146] 2.二次身份认证。参见图3中(b)部分。

[0147] 2.1用户端A申请二次认证：用户端A生成一个新的随机数N_A'，和ticket一起发送给B。

[0148] 2.2用户端A和用户端B完成双向认证：用户端B收到用户端A的二次认证申请后，生成一个新的随机数N_B'，用户端B解密ticket并验证T_B后，使用得到的K_{A-B}'加密N_A'，与N_B'一起发给用户端A，A解密后验证N_A'，再用K_{A-B}加密N_B'发送给用户端B，用户端B解密后验证N_B'，完成双向身份认证。

[0149] 3.更新ticket。参见图3中(c)部分。

[0150] 3.1用户端A申请更新ticket：用户端A生成一个新的随机数N_A"，和ticket一起发送给B。

[0151] 3.2用户端B分发新的ticket：用户端B认证ticket后，生成一个新的随机数N_B"和新的密钥K_B"。对K_{A-B}'进行运算生成K_{A-B}"，也可以重新生成K_{A-B}"。使用K_{A-B}'加密K_{A-B}"，B的身份信息和新的时间戳T_B'，连同新生成的N_B"、用K_{A-B}"加密的N_A"、以及新的ticket'一起发送给用户端A。ticket'用密钥K_B"加密，内容如下：

[0152] ①AB的会话密钥K_{A-B}"；

[0153] ②A的身份信息；

[0154] ③B生成的时间戳T_B'。

[0155] 3.3用户端A得到新的ticket并与用户端B完成双向验证：用户端A收到信息后使用K_{A-B}解密第一部分，得到K_{A-B}"。使用K_{A-B}"解密第三部分完成对N_A"的验证。然后使用K_{A-B}"加密N_B"并发送给用户端B，用户端B解密后验证N_B"，完成双向身份认证。

[0156] 以上公开的仅为本发明的实施例，但是本发明并非局限于此，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。显然这些改动和变型均应属于本发明要求的保护范围保护内。此外，尽管本说明书中使用了一些特定的术语，但这些术语只是为了方便说明，并不对本发明构成任何特殊限制。

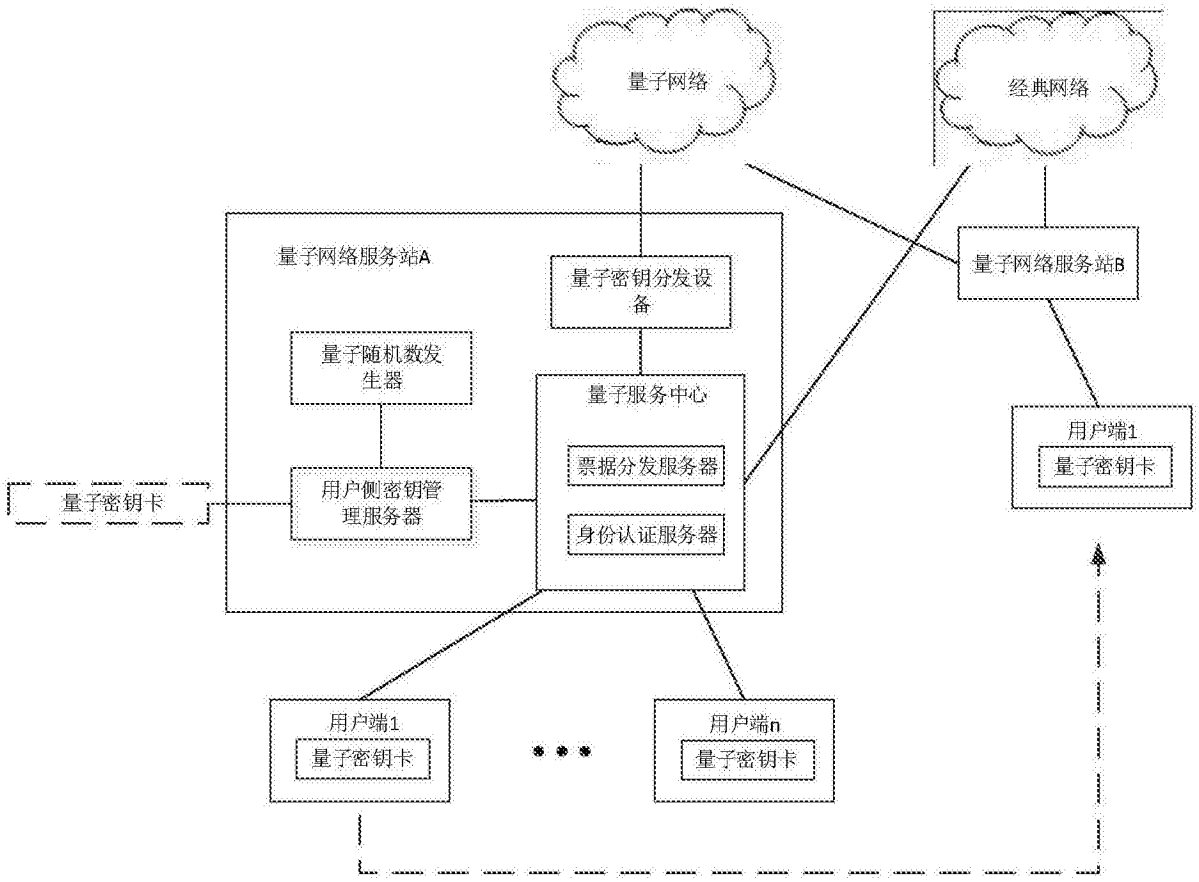

量子网络
经典网络
量子网络服务站A
量子密钥分发设备
量子网络服务站B
量子随机数发生器
量子服务中心
用户端1
量子密钥卡
票据分发服务器
量子密钥卡
用户侧密钥管理服务器
身份认证服务器
用户端1
量子密钥卡
用户端n
量子密钥卡

图1

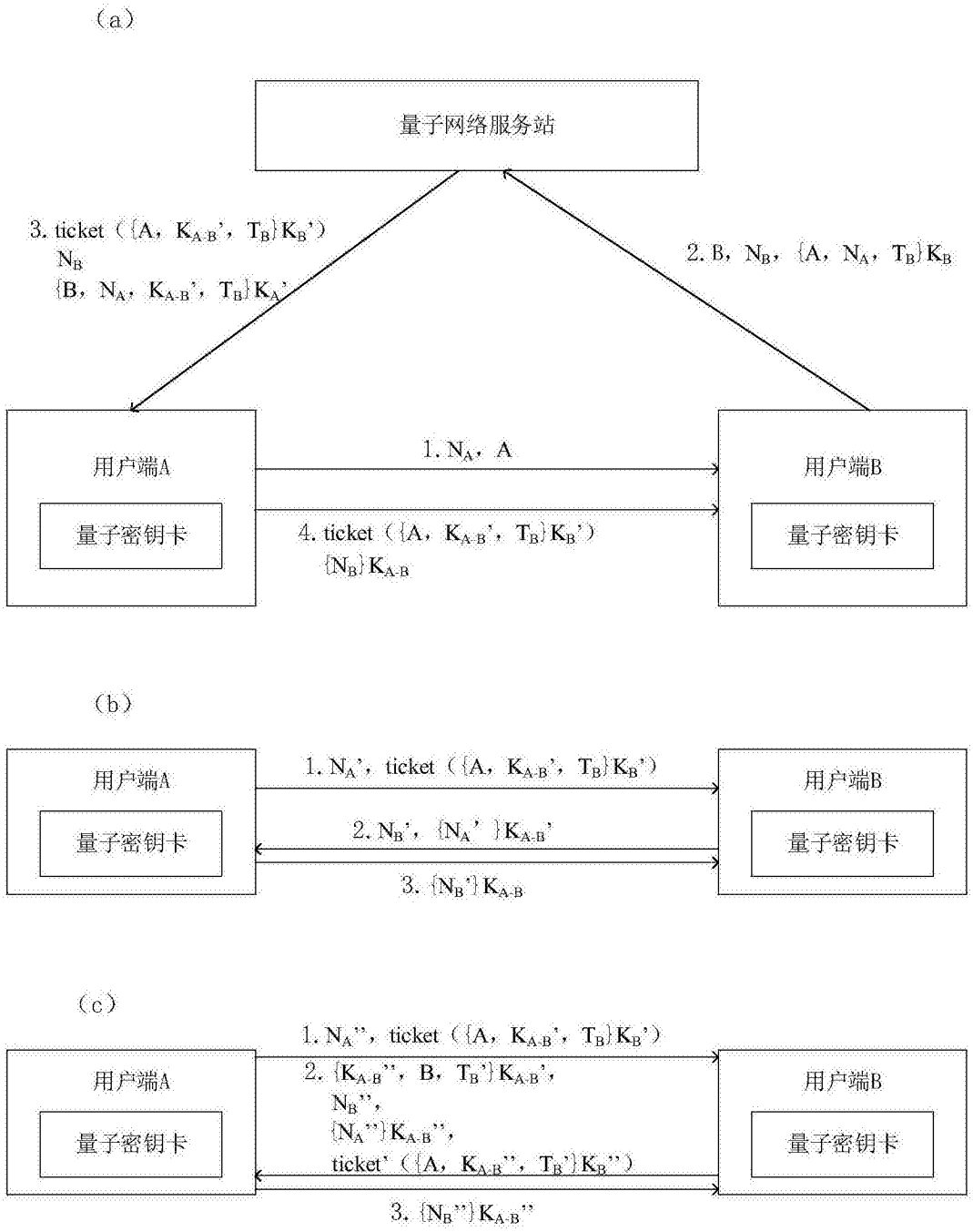

(a)
量子网络服务站
3. ticket ({A, K_{A-B}', T_B}K_B')
N_B
{B, N_A, K_{A-B}', T_B}K_A'
2. B, N_B, {A, N_A, T_B}K_B
用户端A
量子密钥卡
1. N_A, A
4. ticket ({A, K_{A-B}', T_B}K_B')
{N_B}K_{A-B}
用户端B
量子密钥卡
(b)
用户端A
量子密钥卡
1. N_A', ticket ({A, K_{A-B}', T_B}K_B')
2. N_B', {N_A' }K_{A-B}'
3. {N_B'}K_{A-B}
用户端B
量子密钥卡
(c)
用户端A
量子密钥卡
1. N_A'', ticket ({A, K_{A-B}', T_B}K_B')
2. {K_{A-B}'', B, T_B'}K_{A-B}',
N_B'',
{N_A''}K_{A-B}'',
ticket' ({A, K_{A-B}'', T_B'}K_B'')
3. {N_B''}K_{A-B}''
用户端B
量子密钥卡

图2

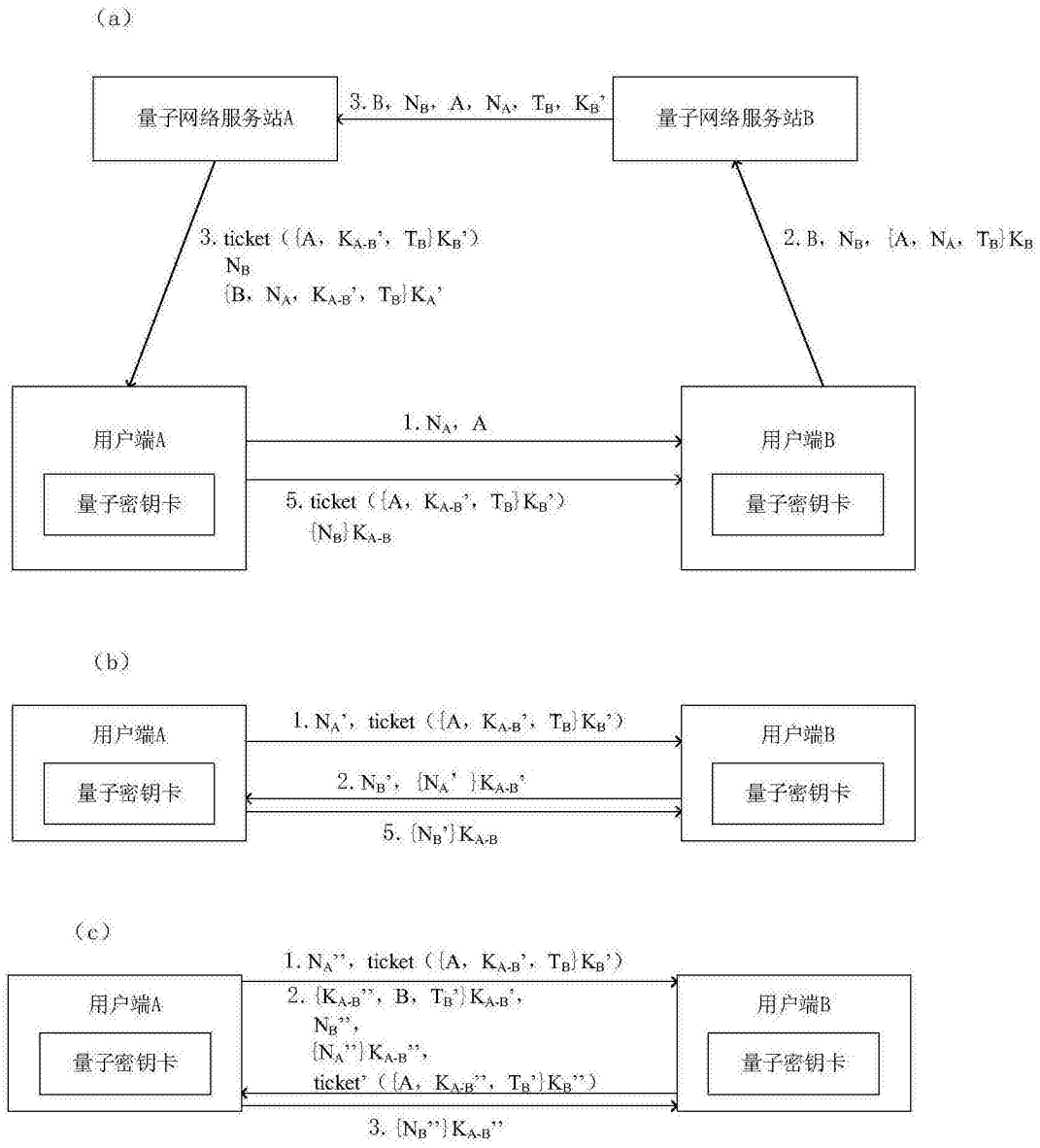

（a）
量子网络服务站A
3. B，N_B，A，N_A，T_B，K_B'
量子网络服务站B
3. ticket（{A，K_{A-B}'，T_B}K_B'）
N_B
{B，N_A，K_{A-B}'，T_B}K_A'
2. B，N_B，{A，N_A，T_B}K_B
用户端A
量子密钥卡
1. N_A，A
5. ticket（{A，K_{A-B}'，T_B}K_B'）
{N_B}K_{A-B}
用户端B
量子密钥卡
（b）
用户端A
量子密钥卡
1. N_A'，ticket（{A，K_{A-B}'，T_B}K_B'）
2. N_B'，{N_A' }K_{A-B}'
5. {N_B'}K_{A-B}
用户端B
量子密钥卡
（c）
1. N_A''，ticket（{A，K_{A-B}'，T_B}K_B''）
用户端A
量子密钥卡
2. {K_{A-B}''，B，T_B'}K_{A-B}'，
N_B''，
{N_A''}K_{A-B}''，
ticket'（{A，K_{A-B}''，T_B'}K_B''）
3. {N_B''}K_{A-B}''
用户端B
量子密钥卡

图3