(19)中华人民共和国国家知识产权局

(12)实用新型专利

(10)授权公告号 CN 208986966 U
(45)授权公告日 2019.06.14

(21)申请号 201822049267.6

(22)申请日 2018.12.07

(73)专利权人 武汉星际量子信息技术有限责任公司
地址 430000 湖北省武汉市东西湖区径河街道十字东街7号(10)

(72)发明人 王信 梅松 朱智

(74)专利代理机构 深圳市六加知识产权代理有限公司 44372
代理人 向彬

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)

权利要求书1页 说明书6页 附图2页

(54)实用新型名称

一种加密终端以及相应的数据传输系统

(57)摘要

本实用新型公开了一种加密终端以及相应的数据传输系统，该加密终端包括认证工具以及加解密模块，认证工具与加解密模块连接；认证工具用于与加密服务器建立连接，获取加密服务器基于量子随机数所生成的量子密钥；加解密模块用于通过量子密钥对数据进行加密或解密。本实用新型的加密终端采用已有基于量子随机数生成的密钥对数据进行加密，增加了暴力破解的难度，加强了密钥的安全性。已有的认证工具有抗暴力破解功能，认证工具和基于量子随机数生成的密钥相互结合，进一步加强了量子密钥的安全性，提高了数据传输的安全性。

CN 208986966 U

1.一种加密终端,其特征在于,所述加密终端(1)包括认证工具(11)以及加解密模块(12),所述认证工具(11)与所述加解密模块(12)连接;

所述认证工具(11)用于与加密服务器建立连接,获取加密服务器基于量子随机数所生成的量子密钥;

所述加解密模块(12)用于通过量子密钥对数据进行加密或解密。

2.根据权利要求1所述的加密终端,其特征在于,所述加密终端(1)还包括交互模块(13),所述交互模块(13)分别与所述认证工具(11)以及所述加解密模块(12);

所述交互模块(13)用于建立所述加密终端(1)与所述加密服务器之间的通信链路;

所述交互模块(13)还用于传输所述认证工具(11)与所述加解密模块(12)之间的数据流。

3.根据权利要求2所述的加密终端,其特征在于,所述加密终端(1)还包括配置模块(15),所述配置模块(15)与所述交互模块(13)连接;

所述配置模块(15)用于配置所述加密终端(1)的网络地址和所述加密服务器的网络地址。

4.根据权利要求1所述的加密终端,其特征在于,所述加密终端(1)还包括内核收发包模块(14),所述内核收发包模块(14)与所述加解密模块(12)连接;

所述内核收发包模块(14)用于对报文进行分类,确定报文是否需要加密。

5.根据权利要求1～4任一项所述的加密终端,其特征在于,所述认证工具(11)通过所述加密终端(1)上的扩展接口,与所述加密终端(1)建立连接。

6.根据权利要求5所述的加密终端,其特征在于,所述扩展接口包括USB接口、SPI接口或SDIO接口。

7.根据权利要求1～4任一项所述的加密终端,其特征在于,所述加密终端(1)采用路由器web配置架构。

8.根据权利要求1～4任一项所述的加密终端,其特征在于,所述认证工具(11)用于存储初始化根密钥以及加解密算法。

9.根据权利要求8所述的加密终端,其特征在于,所述加解密算法为对称加密算法。

10.一种数据传输系统,其特征在于,所述数据传输系统包括至少一个数据采集终端(3)、至少一个如权利要求1～9任一项所述的加密终端(1)、加密服务器(2)以及数据采集服务器(4);

所述数据采集终端(3)与所述加密终端(1)连接,所述加密终端(1)与所述加密服务器(2)连接,所述加密服务器(2)与所述数据采集服务器(4)连接;

所述加密终端(1)用于对所述数据采集终端(3)获取到的数据进行加密或者解密;

所述加密服务器(2)用于对所述加密终端(1)所发送的经过加密或者解密的数据,进行解密或者加密;

所述数据采集服务器(4)用于存储所述数据采集终端(3)所采集到的数据。

一种加密终端以及相应的数据传输系统

技术领域

[0001] 本实用新型属于数据加解密技术领域，更具体地，涉及一种加密终端以及相应的数据传输系统。

背景技术

[0002] 目前，在通信系统的发送端先把信息加密，再通过TCP/IP协议栈发送出去，接收端从TCP/IP协议栈接收数据后再解密。

[0003] 密钥的传输方案采用非对称密钥加密对称密钥，再用对称密钥加密业务；非对称密钥传输采用明文方式，依靠数学算法的难度来保证密钥的安全，随着计算机运算能力的提高，这种方案的安全性在逐年降低。再者，加密用的密钥是用算法或者热噪声产生的随机数，采用前述方法产生的随机数安全性不高，容易被暴力破解。

[0004] 鉴于此，克服该现有技术所存在的缺陷是本技术领域亟待解决的问题。

发明内容

[0005] 针对现有技术的以上缺陷或改进需求，本实用新型提供了一种加密终端以及相应的数据传输系统，其目的在于，采用已有基于量子随机数生成的密钥对数据进行加密，增加了暴力破解的难度，提高了基于量子随机数产生的密钥的安全性。而且，采用已有认证工具获取加密服务器基于量子随机数生成的量子密钥，在数据发送端和数据接收端采用对称算法进行加密和解密，保证了量子密钥的安全性。认证工具有抗暴力破解功能，进一步加强了量子密钥的安全性，由此解决目前采用非对称密钥加密对称密钥，使得密钥的安全较低，以及由算法或者热噪声产生的随机数的安全性不高，容易被暴力破解的技术问题。

[0006] 为实现上述目的，按照本实用新型的一个方面，提供了一种加密终端，所述加密终端1包括认证工具11以及加解密模块12，所述认证工具11与所述加解密模块12连接；

[0007] 所述认证工具11用于与加密服务器建立连接，获取加密服务器基于量子随机数所生成的量子密钥；

[0008] 所述加解密模块12用于通过量子密钥对数据进行加密或解密。

[0009] 优选地，所述加密终端1还包括交互模块13，所述交互模块13分别与所述认证工具11以及所述加解密模块12连接；

[0010] 所述交互模块13用于建立所述加密终端1与所述加密服务器之间的通信链路；

[0011] 所述交互模块13还用于传输所述认证工具11与所述加解密模块12之间的数据流。

[0012] 优选地，所述加密终端1还包括配置模块15，所述配置模块15与所述交互模块13连接；

[0013] 所述配置模块15用于配置所述加密终端1的网络地址和所述加密服务器的网络地址。

[0014] 优选地，所述加密终端1还包括内核收发包模块14，所述内核收发包模块14与所述加解密模块12连接；

[0015] 所述内核收发包模块14用于对报文进行分类，确定报文是否需要加密。

[0016] 优选地，所述认证工具11通过所述加密终端1上的扩展接口，与所述加密终端1建立连接。

[0017] 优选地，所述扩展接口包括USB接口、SPI接口或SDIO接口。

[0018] 优选地，所述加密终端1采用路由器web配置架构。

[0019] 优选地，所述认证工具11用于存储初始化根密钥以及加解密算法。

[0020] 优选地，所述加解密算法为对称加密算法。

[0021] 按照本实用新型的另一个方面，提供了一种密钥系统，所述密钥系统包括加密终端1以及加密服务器2，所述加密终端1与所述加密服务器2连接；

[0022] 所述加密服务器2包括量子随机数发生器21，所述加密终端1包括认证工具11以及加解密模块12，所述认证工具11与所述加解密模块12连接；

[0023] 所述量子随机数发生器21用于产生量子随机数；

[0024] 所述认证工具11用于与所述加密服务器2建立连接，获取基于量子随机数生成的量子密钥；

[0025] 所述加解密模块12用于通过量子密钥对数据进行加密或解密。

[0026] 按照本实用新型的又一方面，提供了一种数据传输系统，所述数据传输系统包括至少一个数据采集终端3、至少一个本实用新型所述的加密终端1、加密服务器2以及数据采集服务器4；

[0027] 所述数据采集终端3与所述加密终端1连接，所述加密终端1与所述加密服务器2连接，所述加密服务器2与所述数据采集服务器4连接；

[0028] 所述加密终端1用于对所述数据采集终端3获取到的数据进行加密或者解密；

[0029] 所述加密服务器2用于对所述加密终端1所发送的经过加密或者解密的数据，进行解密或者加密；

[0030] 所述数据采集服务器4用于存储所述数据采集终端3所采集到的数据。

[0031] 总体而言，通过本实用新型所构思的以上技术方案与现有技术相比，具有如下有益效果：本实用新型的加密终端采用已有基于量子随机数生成的密钥对数据进行加密，增加了暴力破解的难度，提高了密钥的安全性。而且，采用已有认证工具获取加密服务器基于量子随机数生成的量子密钥，在数据发送端和数据接收端采用已有对称算法进行加密和解密，保证了量子密钥的安全性。认证工具有抗暴力破解功能，认证工具和基于量子随机数生成的密钥相互结合，进一步加强了量子密钥的安全性，提高了数据传输的安全性。

附图说明

[0032] 为了更清楚地说明本实用新型实施例的技术方案，下面将对本实用新型实施例中所需要使用的附图作简单地介绍。显而易见地，下面所描述的附图仅仅是本实用新型的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0033] 图1是本实用新型实施例提供的一种加密终端的结构示意图；

[0034] 图2是本实用新型实施例提供的另一种加密终端的结构示意图；

[0035] 图3是本实用新型实施例提供的一种密钥系统的结构示意图；

[0036] 图4是本实用新型实施例提供的一种数据传输系统的结构示意图。

具体实施方式

[0037] 为了使本实用新型的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本实用新型进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本实用新型，并不用于限定本实用新型。

[0038] 此外，下面所描述的本实用新型各个实施方式中所涉及到的技术特征只要彼此之间未构成冲突就可以相互组合。

[0039] 实施例1：

[0040] 目前，密钥的传输方案采用非对称密钥加密对称密钥，再用对称密钥加密业务；非对称密钥传输采用明文方式，依靠数学算法的难度来保证密钥的安全，随着计算机运算能力的提高，这种方案的安全性在逐年降低。再者，加密用的密钥是用算法或者热噪声产生的随机数，采用前述方法产生的随机数安全性不高，容易被暴力破解。

[0041] 为解决前述问题，本实施例提供一种加密终端，该加密终端采用已有基于量子随机数产生量子密钥对数据进行加密或者解密，量子密钥的安全性较高，而且已有认证工具有抗暴力破解的功能，二者相互结合，进一步提高了量子密钥的安全性。采用该加密终端对数据进行加密和解密时，可以有效提高数据传输的安全性。

[0042] 下面参阅图1，说明本实施例的加密终端的实现方式之一。

[0043] 本实施例的加密终端1包括认证工具11以及加解密模块12，所述认证工具11用于与加密服务器建立连接，获取加密服务器基于量子随机数所生成的量子密钥；所述加解密模块12用于通过量子密钥对数据进行加密或解密。

[0044] 其中，认证工具11在本领域内可以称作为Q盾，其工作原理与银行U盾相似。在实际使用中，所述认证工具11通过所述加密终端1上的扩展接口，与所述加密终端1建立连接。其中，所述扩展接口包括USB(Universal Serial Bus，简写为USB)接口、SPI(Serial Peripheral Interface，简写为SPI)接口或SDIO(Secure Digital Input and Output Card，简写为SDIO)接口。

[0045] 所述认证工具11用于存储初始化根密钥以及加解密算法，其中，所述加解密算法为对称加密算法，并对基于量子随机子随机数生成的量子密钥进行解密。

[0046] 在实际使用过程中，认证工具11首先在加密服务器侧进行初始化，获取初始根密钥以及加解密算法。其中，加密服务器用于依据初始根密钥加密量子随机数，生成量子密钥信息，加密终端1用于依据初始根密钥对量子密钥信息进行解密。获取相应的量子随机数。在实际应用场景下，初始根密钥存储在认证工具11中，初始根密钥还存储在加密服务器中，使得加密终端1以及加密服务器均知晓该初始根密钥。在认证工具11初始化完成后，认证工具11与加密终端1建立连接，从而保证加密终端1能够基于初始根密钥对量子密钥信息进行解密，获取相应的量子随机数，从而对数据进行加密。

[0047] 其中，所述认证工具11获取到量子随机数后，将量子随机数发送至加解密模块12，加解密模块12通过量子随机数对数据进行加密或者解密。加解密模块12主要处理加密解密工作，加密处理时，只加密IP层的负载部分(IPPAYLOAD)，其中IP头(IPHEAD)和MAC头保持明文，这部分提供在IP网络中传输时的路由信息，加密后的报文包，在IP的负载部分增加加密

头和负载密文，并转发出去。例如，明文信息为“MAC IPHEAD IPPAYLOAD CRC”，经过加密后的密文信息为“MAC IPHEAD CRYPTHEAD CRYPTFLOW CRC”。

[0048] 其中，密文中只包含加密使用的秘钥的ID，秘钥的实际值已经经过前面交互保存在加密终端1和加密服务器上，双方收到密文后，根据秘钥ID查找对应秘钥值对密文进行解密处理。

[0049] 本实施例的加密终端1主要用于实现与加密服务器之间的身份认证、向加密服务器申请量子密钥、接收来自于加密服务器的数据配置信息、初始根密钥更新、会话密钥更新、根据客户配置筛选报文并对筛选中的报文进行加解密处理等功能。下面结合图2，进一步说明本实施例的加密终端的实现方案之一。

[0050] 所述加密终端1还包括交互模块13，所述交互模块13分别与所述认证工具11、所述加解密模块12以及加密服务器连接；所述交互模块13用于建立所述加密终端1与所述加密服务器之间的通信链路；所述交互模块13还用于传输所述认证工具11与所述加解密模块12之间的数据流。所述交互模块13具体为客户端协议报文交互模块，在实际使用中，包括加密终端1的认证，交互模块13首先和加密服务器建立会话链接，并从认证工具11中读取认证信息后，向加密服务器发起双向认证请求。在认证过程的中，申请报文中的关键信息是用初始根秘钥加密处理的。交互模块13接收到的认证通过确认报文中，含有用初始根秘钥加密的会话秘钥和秘钥ID信息，然后通过会话秘钥和初始根秘钥双重加密申请应用秘钥，并从加密服务器申请密钥和配置，通过netlink向内核传送密钥和配置信息。

[0051] 进一步地，所述加密终端1还包括内核收发包模块14，所述内核收发包模块14与所述加解密模块12连接；所述内核收发包模块14用于对报文进行分类，确定报文是否需要加密。举例而言，所述内核收发包模块14可以依据源端的MAC(Media Access Control，简写为MAC)地址、目的端MAC地址、源端网络地址、目的端网络地址、源端的端口信息、目的端的端口信息或者协议标志等，对报文进行分类，选择性进行加密或者解密。

[0052] 内核收发包模块14对于接收和发送的报文进行解析，并按配置规则返回是否需要加密解密处理，同时，完成密文报文长度和校验值等相关部分的调整。在实际使用中，如果收到的明文报文长度就是满MTU(Maximum Transmission Unit)的情况下，密文增加了加密头部分，整个密文报文势必会大于网络MTU，因此，内核收发包模块14要对报文进行分片操作和相关校验值的重新计算，避免密文在网络中传输过程中因为MTU和校验值等信息被丢弃。

[0053] 所述加密终端1还包括配置模块15，所述配置模块15与所述交互模块13连接，所述配置模块15用于配置所述加密终端1的网络地址和所述加密服务器的网络地址。

[0054] 在实际使用中，配置模块15的表现形式为web页面配置模块15，可以通过web页面配置加密终端1的WAN口IP地址和加密服务器的IP地址，通过web网页可以配置加密终端1的WAN口的IP地址和服务器的IP地址。不同的应用场景和网络实现设备的IP地址规划不同，为了让整个网络的IP互通性不受到破坏，加密终端1采用路由器web配置架构，可以通过web页面配置加密终端1的网络地址和加密服务器的网络地址，便于密钥系统上电后，加密终端1与加密服务器建立会话链接，可以使得加密终端1可以产品化，能够灵活配合加密服务器完成加解密的操作。

[0055] 为了提高加密终端1的容错能力，加密终端1中保存三组动态更新的{量子密钥ID，

量子密钥}，每次进行业务报文加密操作时，选择中间的一组量子密钥进行加密，解密时根据需要解密的报文中携带的密钥ID值，从这三组中查找对应的量子密钥，时刻保存三组量子密钥，增强了加密终端1的容错能力。

[0056] 在此，需要强调的是，本实施例中关于量子密钥的生成过程、对数据加密解密的过程以及对于数据传输的过程等涉及方法流程的步骤，均为本领域的常规手段。为了使得本实施例的密钥系统的实现过程较为清楚，方对相应的方法进行了简要说明。

[0057] 实施例2：

[0058] 本实施例还提供一种密钥系统，如图3所示，该密钥系统包括加密服务器2以及上述实施例1的加密终端1，所述加密服务器2包括量子随机数发生器21，所述加密终端1包括认证工具11以及加解密模块12。所述量子随机数发生器21用于产生量子随机数；所述认证工具11用于与所述加密服务器2建立连接，获取并基于量子随机数生成的量子密钥；所述加解密模块12用于通过量子密钥对数据进行加密或解密。

[0059] 其中，量子随机数发生器21的随机性保障源自于量子物理原理，相比伪随机数发生器和传统的噪声源随机数发生相比，量子随机数发生器21的随机性来源更加清晰，并可采用物理熵理论严格证明其随机性，具有更高的安全性。

[0060] 在具体应用场景下，量子随机数发生器21可以为已有的量子随机数发生器21，例如，QRNG-PHF100系列量子随机数发生器，量子随机数产生的过程依据已有的方案设计即可，例如，依据QRNG-PHF100系列量子随机数发生器的产品规格书进行设计。在实际使用过程中，量子随机数发生器21按照预设的速率生产真随机的量子随机数，供整个密钥系统作为加密的密钥使用。同时，加密服务器2可以根据业务流量大小进行调节，量子密钥的更新频率，使量子密钥的使用更合理，减少不必要的密钥浪费。

[0061] 关于加密终端1的具体结构请参照图1、图2以及相关的文字描述。

[0062] 实施例3：

[0063] 本实施例还提供了一种数据传输系统，上述实施例2的密钥系统适用于本实施例的数据传输系统，采用上述实施例2的密钥系统对数据传输系统进行加密和解密，可以加强数据传输的安全性。而且，可以在不改变已部署的设备网络架构基础上，添加加密终端1，用户无感知，不影响用户使用习惯，用户体验性佳。

[0064] 如图4所示，本实施例的数据传输系统包括至少一个上述实施例1的数据采集终端3、至少一个加密终端1、加密服务器2以及数据采集服务器4，所述数据采集终端3与所述加密终端1连接，所述加密终端1与所述加密服务器2连接，所述加密服务器2与所述数据采集服务器4连接。其中，加密终端1设置在数据采集终端3和传输网络(Inernet)之间，加密服务器2设置在传输网络(Inernet)和数据采集服务器4之间。

[0065] 所述加密终端1用于对所述数据采集终端3获取到的数据进行加密或者解密，所述加密服务器2用于对所述加密终端1所发送的经过加密或者解密的数据，进行解密或者加密，加密终端1和加密服务器2相互配合完成对传输数据的加密和解密。所述数据采集服务器4用于存储所述数据采集终端3所采集到的数据。

[0066] 其中，数据采集终端3将采集到的数据发送至数据采集服务器4，数据采集终端3可以为向数据采集服务器4进行数据交互的网络结构中的客户机，数据采集终端3的数目不做具体限定，可以依据实际情况而定。

[0067] 其中，加密终端1的数目不做具体限定，依据需要进行加密或者解密的数据流而定。在可选的实施例中，加密终端1与数据采集终端3一一对应。

[0068] 关于加密终端1以及加密服务器2的具体结构，以及二者相互配合进行加密解密的过程，在此不再赘述，请详见图1、图2、图3以及相关的文字描述。

[0069] 本领域的技术人员容易理解，以上所述仅为本实用新型的较佳实施例而已，并不用以限制本实用新型，凡在本实用新型的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本实用新型的保护范围之内。

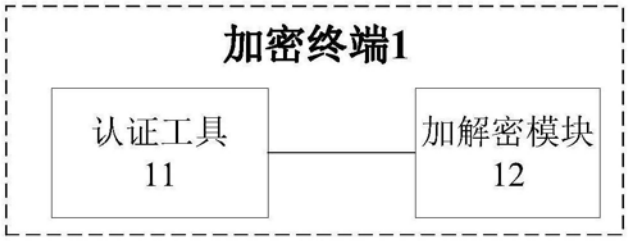
加密终端1
认证工具
11
加解密模块
12

图1

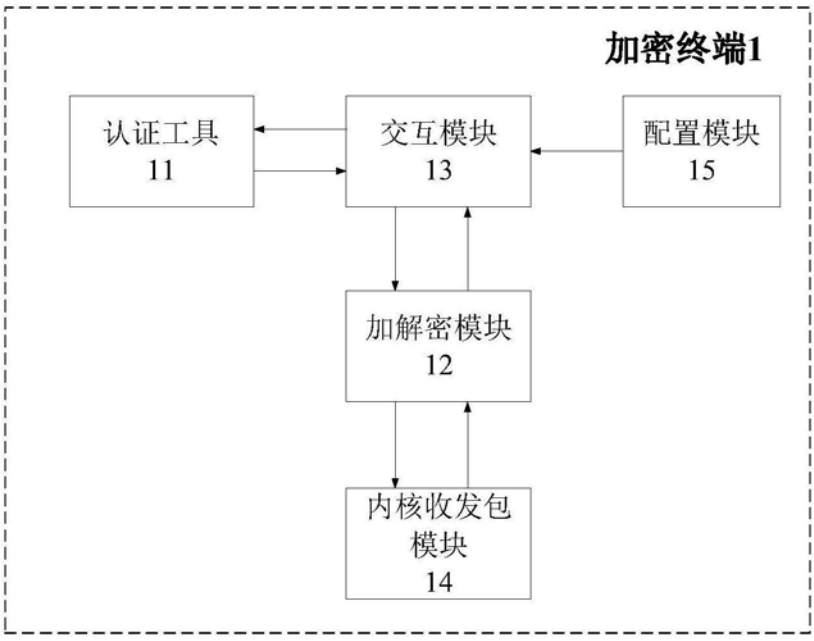
加密终端1
认证工具
11
交互模块
13
配置模块
15
加解密模块
12
内核收发包
模块
14

图2

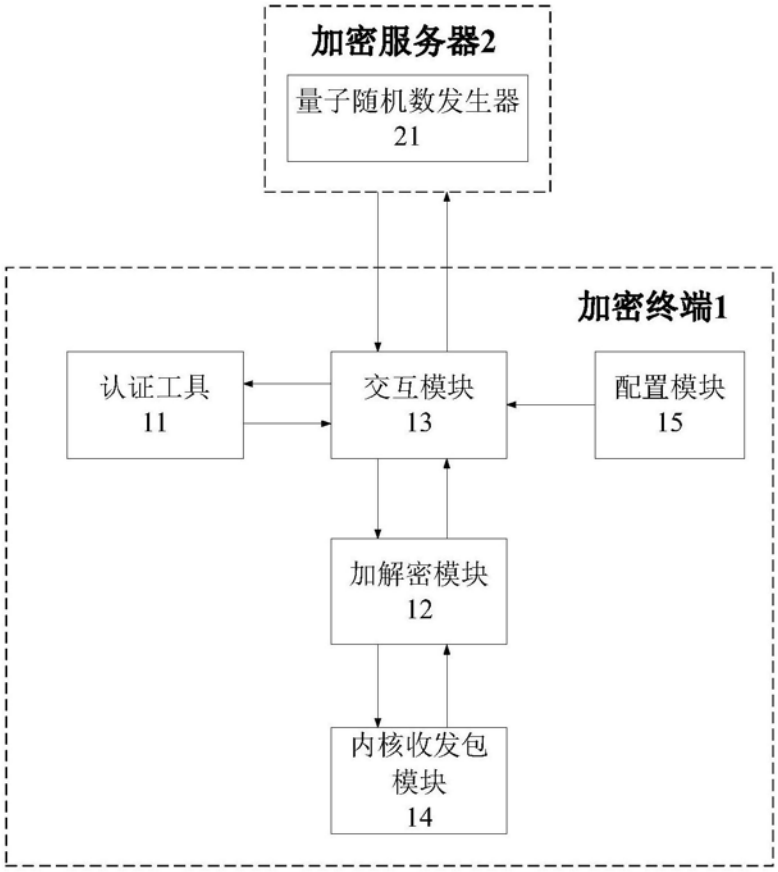
加密服务器2
量子随机数发生器
21
加密终端1
认证工具
11
交互模块
13
配置模块
15
加解密模块
12
内核收发包
模块
14

图3

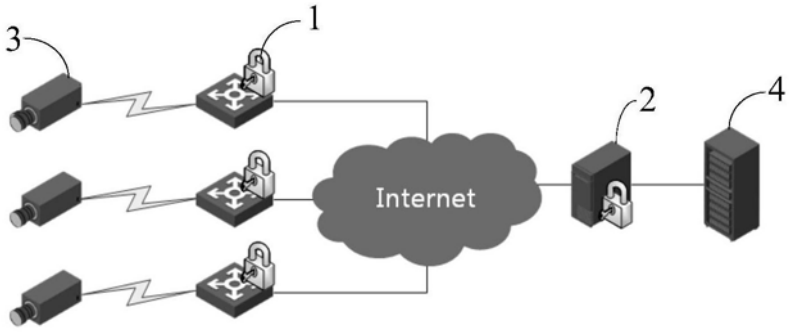
3
1
2
4
Internet

图4