(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114071461 B
(45)授权公告日 2023.11.03

(21)申请号 202111342028.X
(22)申请日 2021.11.12
(65)同一申请的已公布的文献号
申请公布号 CN 114071461 A
(43)申请公布日 2022.02.18
(73)专利权人 江苏亨通问天量子信息研究院有限公司
地址 215200 江苏省苏州市吴江经济技术开发区交通北路168号
(72)发明人 王成金 赵良圆 曹凌云 程万里 曹子建 沈明 杜佳静 韦峥 梁洪源
(74)专利代理机构 苏州市中南伟业知识产权代理事务所(普通合伙) 32257
专利代理师 李柏柏
(51)Int.Cl.
H04W 12/0431(2021.01)
H04W 12/0433(2021.01)
H04W 12/06(2021.01)
H04W 12/069(2021.01)
H04L 9/08(2006.01)

(56)对比文件
CN 110572265 A,2019.12.13
CN 112367124 A,2021.02.12
WO 2020223319 A1,2020.11.05
WO 2021147660 A1,2021.07.29
CN 105471584 A,2016.04.06
CN 109756877 A,2019.05.14
CN 110557253 A,2019.12.10
CN 110650009 A,2020.01.03
CN 110690962 A,2020.01.14
CN 110808834 A,2020.02.18
CN 112865966 A,2021.05.28
CN 112995990 A,2021.06.18
CN 113596062 A,2021.11.02
WO 2020260751 A1,2020.12.30
WO 2021090027 A1,2021.05.14
WO 2021104448 A1,2021.06.03 (续)

审查员 陈君

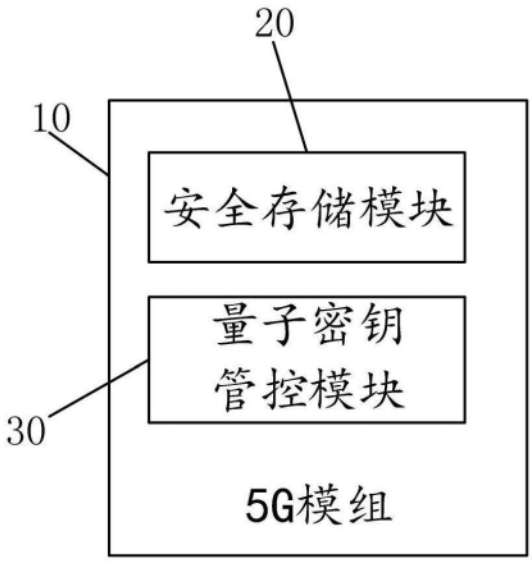
权利要求书2页 说明书6页 附图2页

(54)发明名称

基于量子密钥加密的5G通信模组

(57)摘要

本发明涉及一种基于量子密钥加密的5G通信模组，包括5G模组、安全存储模块和量子密钥管控模块，5G模组设置有安全存储模块和量子密钥管控模块，安全存储模块与量子密钥管控模块通信，用于利用量子证书完成5G模组的身份认证以及量子密钥分发，使用分发的量子密钥完成5G业务数据加密传输。本发明在5G模组上增加安全存储模块和量子密钥管控模块，利用量子密钥解决5G模组设备的身份认证和传输加密问题，既可以防止密钥泄露风险，又能够降低密钥维护成本，而且还能够抵抗量子计算和量子算法的攻击，能够为使用5G的物联网提供安全的无线网络通讯。



CN 114071461 B

[转续页]

[接上页]

(56)对比文件

李古月;俞佳宝;胡爱群.基于设备与信道特征的物理层安全方法.密码学报.2020,(第02期),全文.

王健全;马彰超;李新中;孙雷;胡昌玮.量子保密通信网络架构及移动化应用方案.电信科学.2018,(第09期),全文.

Jin Cao.Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System.IEEE Internet of Things Journal.2019,全文.

1.一种基于量子密钥加密的5G通信模组,其特征在于,包括5G模组、安全存储模块和量子密钥管控模块,所述5G模组设置有所述安全存储模块和所述量子密钥管控模块,所述安全存储模块与所述量子密钥管控模块通信,用于利用量子证书完成所述5G模组的身份认证以及量子密钥分发,使用分发的量子密钥完成5G业务数据加密传输;

所述安全存储模块与所述量子密钥管控模块用于完成5G模组身份认证的通信方法包括:

利用所述量子密钥管控模块存储量子密钥;基于所述量子密钥生成所述5G模组的量子证书以及物联网服务器的量子证书并分别导入至5G模组以及所述物联网服务器;所述物联网服务器和所述5G模组利用自身的量子证书的密钥加密信息分别得到物联网服务器标识和5G模组标识,并利用所述物联网服务器标识和5G模组标识分别完成所述物联网服务器和所述5G模组的身份认证;

在完成所述物联网服务器和所述5G模组的身份认证后需要完成所述量子密钥管控模块的身份认证;

利用所述物联网服务器标识完成所述物联网服务器的身份认证包括:

所述物联网服务器将所述物联网服务器标识发送到所述量子密钥管控模块,所述量子密钥管控模块将其解密后得到解密信息,并将所述解密信息与所述物联网服务器的注册信息进行内容对比,内容一致则物联网服务器认证成功;

利用所述5G模组标识完成所述5G模组的身份认证包括:

所述5G模组将所述5G模组标识发送到所述量子密钥管控模块,所述量子密钥管控模块将其解密后得到解密信息,并将所述解密信息与所述5G模组的注册信息进行内容对比,内容一致则5G模组认证成功;

利用量子证书完成所述5G模组的量子密钥分发的方法包括:

所述5G模组与所述量子密钥管控模块协商量子密钥分发的第一会话密钥,同时所述物联网服务器与所述量子密钥管控模块协商量子密钥分发的第二会话密钥;所述5G模组和所述物联网服务器分别使用对应的第一会话密钥和第二会话密钥与所述量子密钥管控模块通信,用于获取通信两端对称的量子密钥分别分发给通信两端;所述物联网服务器通过量子密钥加密后的所述5G模组与物联网终端进行通信;

所述5G模组的量子密钥分发方法包括:

所述5G模组生成加密请求信息,并将所述加密请求信息发送给所述量子密钥管控模块,所述量子密钥管控模块解密所述加密请求信息后判断所述5G模组是否有效,若判断结果为否,则结束该次加密请求,若判断结果为是,则继续判断是否能够查询到与所述5G模组对应的物联网服务器信息,若判断结果为否,则结束该次加密请求,若判断结果为是,则所述量子密钥管控模块确定量子密钥并加密,之后向所述物联网服务器发送所述量子密钥,所述物联网服务器接收所述量子密钥并将所述量子密钥发送给所述5G模组。

2.根据权利要求1所述的基于量子密钥加密的5G通信模组,其特征在于:所述安全存储模块包括量子密钥存储单元,所述量子密钥存储单元连接所述量子密钥管控模块,所述量子密钥存储单元用于接收所述量子密钥管控模块产生的量子密钥并对其进行存储。

3.根据权利要求1所述的基于量子密钥加密的5G通信模组,其特征在于:所述安全存储模块包括量子证书存储单元,所述量子证书存储单元连接所述量子密钥管控模块,所述量

子证书存储单元用于接收所述量子密钥管控模块产生的量子证书并对其进行存储。

4.根据权利要求1所述的基于量子密钥加密的5G通信模组,其特征在于:所述5G模组与所述物联网服务器的对应关系预先存储在所述量子密钥管控模块中。

基于量子密钥加密的5G通信模组

技术领域

[0001] 本发明涉及5G通信技术领域，尤其是指一种基于量子密钥加密的5G通信模组。

背景技术

[0002] 5G是面向2020年以后移动通信需求而发展的新一代移动通信系统，5G具有超高的频谱利用率和能效，在传输速率和频谱资源利用率等方面较4G移动通信提高一个量级或更高，其无线覆盖性能、传输时延、系统安全和用户体验也将得到显著的提高。5G移动通信将与其他无线移动通信技术密切结合，构成新一代无所不在的移动信息网络，满足未来10年移动互联网流量增加1000倍的发展需求。5G移动通信系统的应用领域也将进一步扩展，对海量传感设备及机器与机器(M2M)通信的支撑能力将成为系统设计的重要指标之一。未来5G系统还须具备充分的灵活性，具有网络自感知、自调整等智能化能力，以应对未来移动信息社会难以预计的快速变化。5G时代不仅能给我们带来超高带宽、超低时延以及超大规模连接的用户体验，其丰富的垂直行业应用将为移动网络带来更多样化的业务需求，尤其是网络切片、能力开放两大创新功能的应用，将改变传统业务运营方式和作业模式，为各行业用户打造定制化的“行业专网”服务，可更好地满足业务差异化需求，进一步提升了企业对自身业务的自主可控能力和运营效率。

[0003] 5G应用有较高的开发难度、过长的开发周期和多样化的行业需求，制约着5G在行业规模应用发展。5G模组的诞生将加速工业互联网的普及，有助于推动制造业的高质量发展。5G模组可适应各种应用场景，简化终端产品设计，对现存的技术层面的不确定性及终端需求的多样性有关键意义，对促进产业加速成熟，推动5G落地商用具有关键作用。

[0004] 由于人们对通信网络的性能和安全需求不断提高，5G通信技术发展迅猛并得到了前所未有的关注。然而5G依然面临一些安全挑战，5G无线网络进行通信时，庞大的数据流在网络中含有大量隐私和敏感信息，为确保隐私不被泄漏，有必要将5G和密码学知识相结合，在安全研究方面，3GPP、5GPPP、NGMN、ITU-2020推进组、爱立信、诺基亚和华为也发布了各自的5G安全需求白皮书，但当前提出的安全方案是基于传统数字证书认证与密钥协商算法，其安全性依赖密钥交换过程的安全性和加解密算法的安全性，其中，密钥分发过程主要依赖于公钥密码，其安全性主要基于质数分解、离散对数、椭圆曲线等数学困难问题的计算复杂度，主要存在下面几个问题：1)对称密钥密码体制存在的最主要问题是由于加密和解密双方都要使用相同的密钥，容易产生发送者或接收者单方面密钥泄露问题；2)对称密钥在有n方参与的通信中，若n方都采用同一对称密钥，一旦密钥被破解，整个密码体系就会崩溃；若采用不同的对称密钥则需要n(n-1)个密钥，密钥数与参与通信的人数的平方数成正比，密钥的管理几乎不可能；3)密钥分发是加密体系中最薄弱的环节，如果加长密钥更新的周期，则给他人破译密钥提供了机会。

[0005] 量子保密通信是指利用量子比特作为信息载体来传输信息的通信技术，它是利用量子力学基本原理和量子纠缠现象达到传递信息、传输数据的一种先进通信技术。量子保密通信技术提供了迄今为止唯一高度安全的通信保密方式，突破了传统信息技术的安全保

密和信息容量极限。如果将量子保密通信技术与5G无线通信技术相结合，其可以在享受5G高带宽低延迟的同时，又可保障传输数据的安全不被破坏者窃取，从而保障物联网设备及应用系统的正常运行，因此将量子保密通信技术与5G无线通信技术相结合具有重要的意义。

发明内容

[0006] 为此，本发明所要解决的技术问题在于克服现有技术存在的问题，提出一种基于量子密钥加密的5G通信模组，在5G模组上增加安全存储模块和量子密钥管控模块，利用量子密钥加密完成5G模组设备身份认证，在通过密钥分发服务向互相通信的5G模组设备和通信的物联网服务器设备分发量子密钥，利用量子密钥解决5G模组设备的身份认证和传输加密问题，既可以防止密钥泄露风险，又能够降低密钥维护成本，而且还能够抵抗量子计算和量子算法的攻击，从而保证5G通信的数据安全性，能够为使用5G的物联网提供安全的无线网络通讯。

[0007] 为解决上述技术问题，本发明提供一种基于量子密钥加密的5G通信模组，包括5G模组、安全存储模块和量子密钥管控模块，所述5G模组设置有所述安全存储模块和所述量子密钥管控模块，所述安全存储模块与所述量子密钥管控模块通信，用于利用量子证书完成所述5G模组的身份认证以及量子密钥分发，使用分发的量子密钥完成5G业务数据加密传输。

[0008] 在本发明的一个实施例中，所述安全存储模块包括量子密钥存储单元，所述量子密钥存储单元连接所述量子密钥管控模块，所述量子密钥存储单元用于接收所述量子密钥管控模块产生的量子密钥并对其进行存储。

[0009] 在本发明的一个实施例中，所述安全存储模块包括量子证书存储单元，所述量子证书存储单元连接所述量子密钥管控模块，所述量子证书存储单元用于接收所述量子密钥管控模块产生的量子证书并对其进行存储。

[0010] 在本发明的一个实施例中，所述安全存储模块与所述量子密钥管控模块用于完成5G模组身份认证的通信方法包括：

[0011] 利用所述量子密钥管控模块存储量子密钥；基于所述量子密钥生成所述5G模组的量子证书以及物联网服务器的量子证书并分别导入至5G模组以及所述物联网服务器；所述物联网服务器和所述5G模组利用自身的量子证书的密钥加密信息分别得到物联网服务器标识和5G模组标识，并利用所述物联网服务器标识和5G模组标识分别完成所述物联网服务器和所述5G模组的身份认证。

[0012] 在本发明的一个实施例中，在完成所述物联网服务器和所述5G模组的身份认证后需要完成所述量子密钥管控模块的身份认证。

[0013] 在本发明的一个实施例中，利用所述物联网服务器标识完成所述物联网服务器的身份认证包括：

[0014] 所述物联网服务器将所述物联网服务器标识发送到所述量子密钥管控模块，所述量子密钥管控模块将其解密后得到解密信息，并将所述解密信息与所述物联网服务器的注册信息进行内容对比，内容一致则物联网服务器认证成功。

[0015] 在本发明的一个实施例中，利用所述5G模组标识完成所述5G模组的身份认证包

括：

[0016] 所述5G模组将所述5G模组标识发送到所述量子密钥管控模块，所述量子密钥管控模块将其解密后得到解密信息，并将所述解密信息与所述5G模组的注册信息进行内容对比，内容一致则5G模组认证成功。

[0017] 在本发明的一个实施例中，利用量子证书完成所述5G模组的量子密钥分发的方法包括：

[0018] 所述5G模组与所述量子密钥管控模块协商量子密钥分发的第一会话密钥，同时所述物联网服务器与所述量子密钥管控模块协商量子密钥分发的第二会话密钥；所述5G模组和所述物联网服务器分别使用对应的第一会话密钥和第二会话密钥与所述量子密钥管控模块通信，用于获取通信两端对称的量子密钥分别分发给通信两端；所述物联网服务器通过量子密钥加密后的所述5G模组与物联网终端进行通信。

[0019] 在本发明的一个实施例中，所述5G模组的量子密钥分发方法包括：

[0020] 所述5G模组生成加密请求信息，并将所述加密请求信息发送给所述量子密钥管控模块，所述量子密钥管控模块解密所述加密请求信息后判断所述5G模组是否有效，若判断结果为否，则结束该次加密请求，若判断结果为是，则继续判断是否能够查询到与所述5G模组对应的物联网服务器信息，若判断结果为否，则结束该次加密请求，若判断结果为是，则所述量子密钥管控模块确定量子密钥并加密，之后向所述物联网服务器发送所述量子密钥，所述物联网服务器接收所述量子密钥并将所述量子密钥发送给所述5G模组。

[0021] 在本发明的一个实施例中，所述5G模组与所述物联网服务器的对应关系预先存储在所述量子密钥管控模块中。

[0022] 本发明的上述技术方案相比现有技术具有以下优点：

[0023] 本发明在5G模组上增加安全存储模块和量子密钥管控模块，利用量子密钥加密完成5G模组设备身份认证，在通过密钥分发服务向互相通信的5G模组设备和通信的物联网服务器设备分发量子密钥，利用量子密钥解决5G模组设备的身份认证和传输加密问题，既可以防止密钥泄露风险，又能够降低密钥维护成本，而且还能够抵抗量子计算和量子算法的攻击，从而保证5G通信的数据安全性，能够为使用5G的物联网提供安全的无线网络通讯。

附图说明

[0024] 为了使本发明的内容更容易被清楚的理解，下面根据本发明的具体实施例并结合附图，对本发明作进一步详细的说明。

[0025] 图1是本发明基于量子密钥加密的5G通信模组的硬件结构示意图。

[0026] 图2是本发明基于量子密钥加密的5G通信模组中的安全存储模块的硬件结构示意图。

[0027] 图3是本发明实现5G模组身份认证的通信方法的流程示意图。

[0028] 图4是本发明利用量子证书完成所述5G模组的量子密钥分发的方法的流程示意图。

[0029] 其中，附图标记说明如下：10、5G模组；20、安全存储模块；21、量子密钥存储单元；22、量子证书存储单元；30、量子密钥管控模块。

具体实施方式

[0030] 下面结合附图和具体实施例对本发明作进一步说明，以使本领域的技术人员可以更好地理解本发明并能予以实施，但所举实施例不作为对本发明的限定。

[0031] 请参阅图1至图4所示，本发明实施例提供一种基于量子密钥加密的5G通信模组，包括5G模组10、安全存储模块20和量子密钥管控模块30，所述5G模组10设置有所述安全存储模块20和所述量子密钥管控模块30，所述安全存储模块20与所述量子密钥管控模块30通信，用于利用量子证书完成所述5G模组10的身份认证以及量子密钥分发，使用分发的量子密钥完成5G业务数据加密传输。

[0032] 其中，本发明公开描述的5G模组10可以是现有技术的5G模组10，该5G模组10具备本身的所有功能。

[0033] 在本发明公开的基于量子密钥加密的5G通信模组中，在5G模组10中增加安全存储模块20和量子密钥管控模块30，其中所述安全存储模块20和所述量子密钥管控模块30通信，通过安全存储模块20提供硬件级的安全数据存储。

[0034] 在本发明公开的基于量子密钥加密的5G通信模组中，所述5G模组10初始化时在安全存储模块20中导入量子证书，在所述量子密钥管控模块30中植入密钥分发程序，当5G模组10上电后启动密钥分发程序，密钥分发程序从安全存储模块20获取到量子证书通过网络模块与量子密钥管控模块30连接，利用量子证书的密钥与量子密钥管控模块30完成认证，获取量子密钥并存储于安全存储模块20。

[0035] 在本发明公开的基于量子密钥加密的5G通信模组中，在5G模组10通信时，密钥分发程序利用安全存储模块20的量子密钥加密通信过程中发出的数据，另一方面在接收到数据时密钥分发程序在安全存储模块20找到对应量子密钥完成接收数据的解密工作。

[0036] 在本发明公开的基于量子密钥加密的5G通信模组中，所述安全存储模块20包括量子密钥存储单元21，所述量子密钥存储单元21连接所述量子密钥管控模块30，所述量子密钥存储单元21用于接收所述量子密钥管控模块30产生的量子密钥并对其进行存储。

[0037] 在本发明公开的基于量子密钥加密的5G通信模组中，所述安全存储模块20包括量子证书存储单元22，所述量子证书存储单元22连接所述量子密钥管控模块30，所述量子证书存储单元22用于接收所述量子密钥管控模块30产生的量子证书并对其进行存储。

[0038] 在本发明公开的基于量子密钥加密的5G通信模组中，请参阅图3所示，所述安全存储模块20与所述量子密钥管控模块30用于完成5G模组10身份认证的通信方法包括以下步骤：

[0039] S101：利用所述量子密钥管控模块30存储量子密钥；

[0040] S102：基于所述量子密钥生成所述5G模组10的量子证书以及物联网服务器的量子证书并分别导入至5G模组10以及所述物联网服务器；

[0041] S103：所述物联网服务器和所述5G模组10利用自身的量子证书的密钥加密信息分别得到物联网服务器标识和5G模组10标识，并利用所述物联网服务器标识和5G模组10标识分别完成所述物联网服务器和所述5G模组10的身份认证。

[0042] 在本发明公开的基于量子密钥加密的5G通信模组中，在步骤S101中，利用所述量子密钥管控模块30存储量子密钥包括：所述量子密钥管控模块30可以与量子随机数发生器或量子芯片相连，其中所述量子随机数发生器或量子芯片产生量子密钥并发送至所述量子

密钥管控模块30，所述量子密钥管控模块30接收所述量子密钥并将所述量子密钥进行存储，例如所述量子密钥管控模块30包括密钥池，利用所述密钥池可以存储所述量子密钥。

[0043] 在本发明公开的基于量子密钥加密的5G通信模组中，在步骤S102中，上述的量子证书包含初始的量子密钥，把生成的5G模组10的量子证书以及物联网服务器的量子证书分别导入至5G模组10以及所述物联网服务器中，其通过量子数字证书供身份认证识别以及置换新量子密钥使用。

[0044] 在本发明公开的基于量子密钥加密的5G通信模组中，在步骤S103中，利用所述物联网服务器标识完成所述物联网服务器的身份认证包括：所述物联网服务器将所述物联网服务器标识发送到所述量子密钥管控模块30，所述量子密钥管控模块30将其解密后得到解密信息，并将所述解密信息与所述物联网服务器的注册信息进行内容对比，内容一致则物联网服务器认证成功。

[0045] 在本发明公开的基于量子密钥加密的5G通信模组中，在步骤S103中，利用所述5G模组10标识完成所述5G模组10的身份认证包括：所述5G模组10将所述5G模组10标识发送到所述量子密钥管控模块30，所述量子密钥管控模块30将其解密后得到解密信息，并将所述解密信息与所述5G模组10的注册信息进行内容对比，内容一致则5G模组10认证成功。

[0046] 在本发明公开的基于量子密钥加密的5G通信模组中，在步骤S103中，在完成所述物联网服务器和所述5G模组10的身份认证后需要完成所述量子密钥管控模块30的身份认证。具体的，所述量子密钥管控模块30利用密钥加密自身信息得到量子密钥管控模块30标识，将所述量子密钥管控模块30标识发送到物联网服务器，物联网服务器通过量子证书的密钥解密并对比所述量子密钥管控模块30的信息，对比成功完成双向身份认证；以及所述量子密钥管控模块30利用密钥加密自身信息得到量子密钥管控模块30标识，将所述量子密钥管控模块30标识发送到所述5G模组10，所述5G模组10通过量子证书的密钥解密并对比所述量子密钥管控模块30的信息，对比成功完成双向身份认证。

[0047] 在本发明公开的基于量子密钥加密的5G通信模组中，请参阅图4所示，利用量子证书完成所述5G模组10的量子密钥分发的方法包括以下步骤：

[0048] S201：所述5G模组10与所述量子密钥管控模块30协商量子密钥分发的第一会话密钥，同时所述物联网服务器与所述量子密钥管控模块30协商量子密钥分发的第二会话密钥；

[0049] S202：所述5G模组10和所述物联网服务器分别使用对应的第一会话密钥和第二会话密钥与所述量子密钥管控模块30通信，用于获取通信两端对称的量子密钥分别分发给通信两端；

[0050] S203：所述物联网服务器通过量子密钥加密后的所述5G模组10与物联网终端进行通信。

[0051] 在本发明公开的基于量子密钥加密的5G通信模组中，在步骤S202中，所述5G模组10的量子密钥分发方法包括以下步骤：

[0052] S301：所述5G模组10生成加密请求信息，并将所述加密请求信息发送给所述量子密钥管控模块30；

[0053] S302：所述量子密钥管控模块30解密所述加密请求信息后判断所述5G模组10是否有效，若判断结果为否，则结束该次加密请求，若判断结果为是，则继续判断是否能够查询

到与所述5G模组10对应的物联网服务器信息，若判断结果为否，则结束该次加密请求，若判断结果为是，则所述量子密钥管控模块30确定量子密钥并加密；

[0054] S303：向所述物联网服务器发送所述量子密钥，所述物联网服务器接收所述量子密钥并将所述量子密钥发送给所述5G模组10。

[0055] 在本发明公开的基于量子密钥加密的5G通信模组中，上述5G模组10与所述物联网服务器的对应关系预先存储在所述量子密钥管控模块30中。

[0056] 在本发明公开的基于量子密钥加密的5G通信模组中，本发明在5G模组10上增加安全存储模块20和量子密钥管控模块30，利用量子密钥加密完成5G模组10设备身份认证，在通过密钥分发服务向互相通信的5G模组10设备和通信的物联网服务器设备分发量子密钥，利用量子密钥解决5G模组10设备的身份认证和传输加密问题，既可以防止密钥泄露风险，又能够降低密钥维护成本，而且还能够抵抗量子计算和量子算法的攻击，从而保证5G通信的数据安全性，能够为使用5G的物联网提供安全的无线网络通讯。

[0057] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0058] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0059] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0060] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0061] 显然，上述实施例仅仅是为清楚地说明所作的举例，并非对实施方式的限定。对于所属领域的普通技术人员来说，在上述说明的基础上还可以做出其它不同形式变化或变动。这里无需也无法对所有的实施方式予以穷举。而由此所引申出的显而易见的变化或变动仍处于本发明创造的保护范围之中。

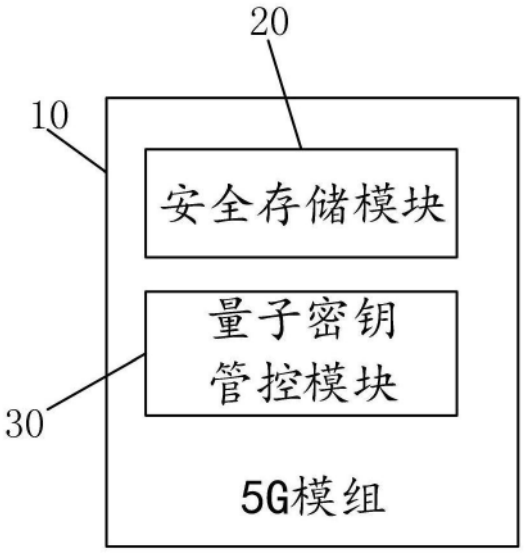

20
10
安全存储模块
量子密钥
管控模块
30
5G模组

图1

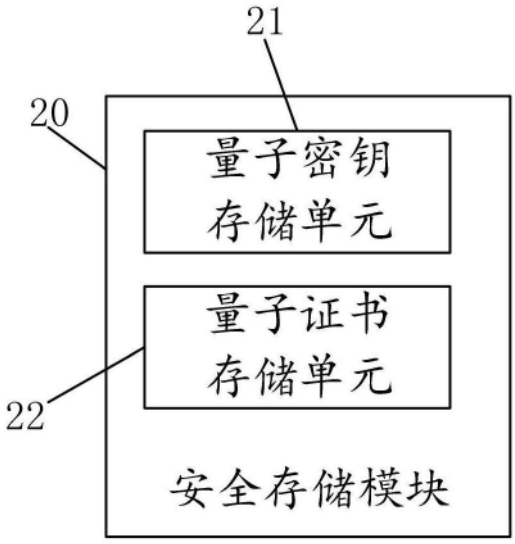

21
20
量子密钥
存储单元
量子证书
存储单元
22
安全存储模块

图2

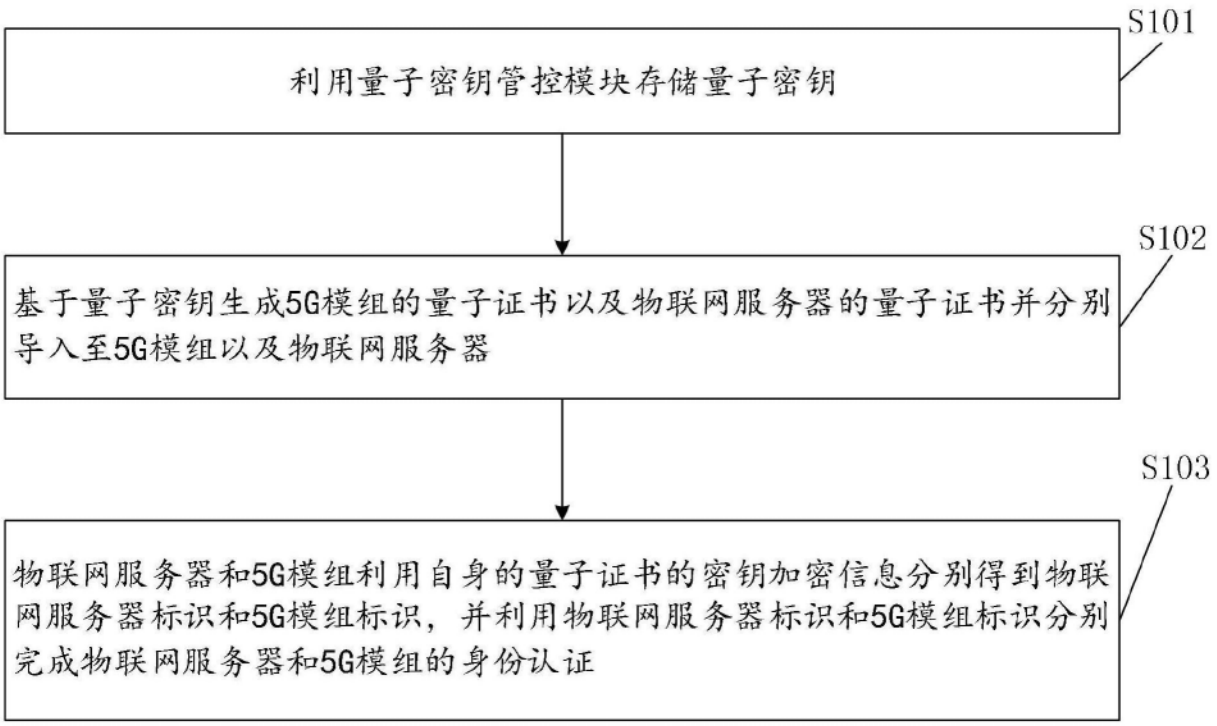

S101
利用量子密钥管控模块存储量子密钥
S102
基于量子密钥生成5G模组的量子证书以及物联网服务器的量子证书并分别导入至5G模组以及物联网服务器
S103
物联网服务器和5G模组利用自身的量子证书的密钥加密信息分别得到物联网服务器标识和5G模组标识，并利用物联网服务器标识和5G模组标识分别完成物联网服务器和5G模组的身份认证

图3

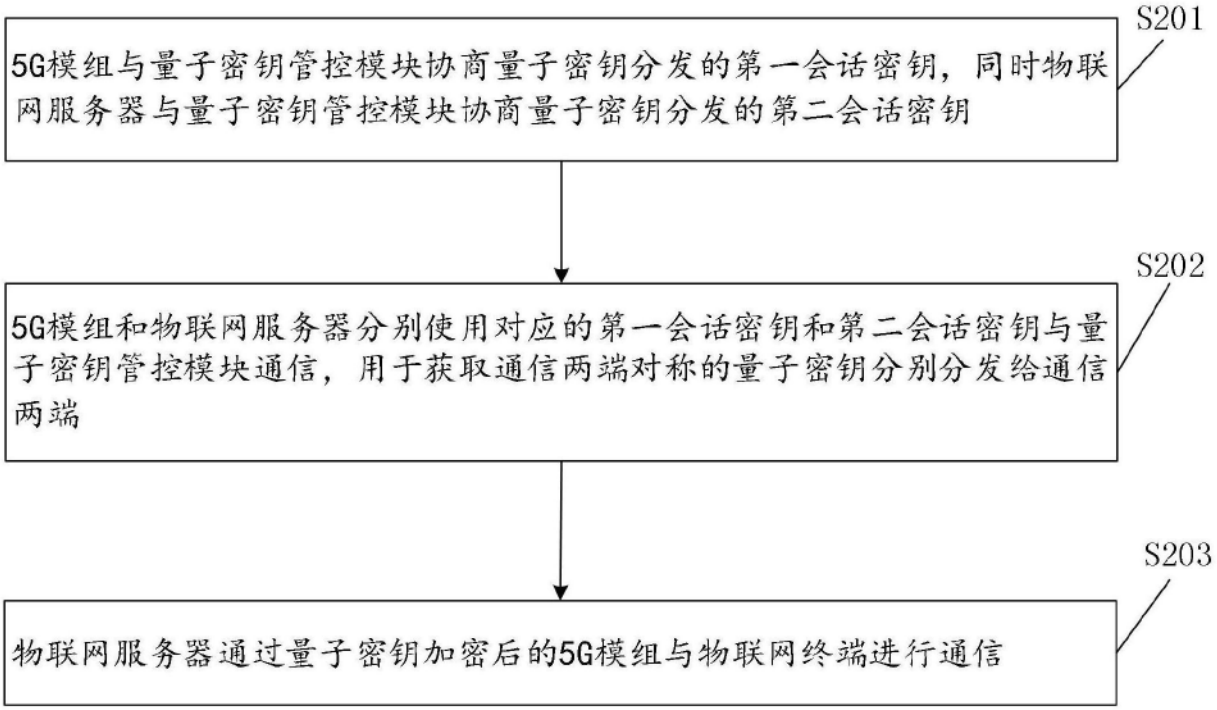

S201
5G模组与量子密钥管控模块协商量子密钥分发的第一会话密钥，同时物联网服务器与量子密钥管控模块协商量子密钥分发的第二会话密钥
S202
5G模组和物联网服务器分别使用对应的第一会话密钥和第二会话密钥与量子密钥管控模块通信，用于获取通信两端对称的量子密钥分别分发给通信两端
S203
物联网服务器通过量子密钥加密后的5G模组与物联网终端进行通信

图4