(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109951513 B
(45)授权公告日 2021.10.22

(21)申请号 201910027000.3
(22)申请日 2019.01.11
(65)同一申请的已公布的文献号
申请公布号 CN 109951513 A
(43)申请公布日 2019.06.28
(73)专利权人 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 杨羽成
(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 29/08(2006.01)
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)
G06N 10/00(2019.01)

(56)对比文件
CN 109150519 A,2019.01.04
CN 109104276 A,2018.12.28
CN 106961327 A,2017.07.18
CN 106357396 A,2017.01.25
CN 103475464 A,2013.12.25
CN 109150835 A,2019.01.04
US 2014331050 A1,2014.11.06
US 2018205541 A1,2018.07.19

审查员 胡诗婷

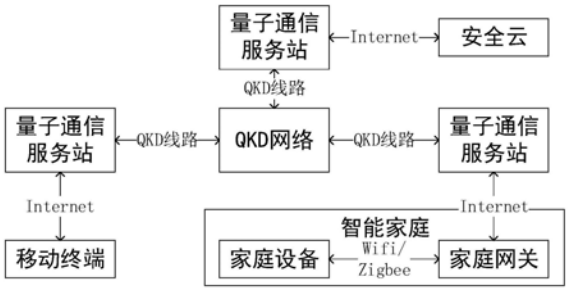
权利要求书2页 说明书11页 附图3页

(54)发明名称

基于量子密钥卡的抗量子计算智能家庭量子云存储方法和系统

(57)摘要

本发明涉及基于量子密钥卡的抗量子计算智能家庭量子云存储方法和系统，各智能家庭组件以及量子通信服务站和安全云分别配有量子密钥卡，各量子密钥卡中存储有私钥、非对称密钥池、以及公钥指针随机数，所述移动终端、所述家庭网关、所述安全云的量子密钥卡内还存储有第三对称密钥池，且所有的对称密钥池还同时存储在所述量子通信服务站的量子密钥卡内；所述智能家庭组件与安全云通信存取文件时，所述文件利用双方的量子密钥卡采用非对称算法对文件进行签名和验证；所述智能家庭组件与量子通信服务站之间，以及量子通信服务站与安全云之间转发文件时，利用相应的对称密钥池生成密钥，采用对称算法进行加密通信。



CN 109951513 B

1.基于量子密钥卡的抗量子计算智能家庭量子云存储方法，其特征在于，包括智能家庭组件经由量子通信服务站向安全云存取文件，其中所述智能家庭组件包括家庭网关和移动终端，各智能家庭组件以及量子通信服务站和安全云分别配有量子密钥卡，各量子密钥卡中存储有私钥、非对称密钥池、以及公钥指针随机数，其中非对称密钥池存储有各方的公钥，通过公钥指针随机数可结合非对称密钥池获取与任一方私钥相应的公钥；

所述移动终端的量子密钥卡内还存储有第一对称密钥池，所述家庭网关的量子密钥卡内还存储有第二对称密钥池，所述安全云的量子密钥卡内还存储有第三对称密钥池，且所有的对称密钥池还同时存储在所述量子通信服务站的量子密钥卡内；

所述智能家庭组件与安全云通信存取文件时，所述文件利用双方的量子密钥卡采用非对称算法对文件进行签名和验证；

所述智能家庭组件与量子通信服务站之间，以及量子通信服务站与安全云之间转发文件时，利用相应的对称密钥池生成密钥，采用对称算法进行加密通信；

所述智能家庭组件向安全云通信存储文件时，在智能家庭组件处包括：

利用私钥对文件进行签名得到文件签名；

生成利用真随机数R_M并利用真随机数R_M从对称密钥池中提取密钥K_M；

利用密钥K_M加密文件和文件签名得到文件密文，然后将文件密文连同真随机数R_M发送至量子通信服务站；

所述智能家庭组件和安全云与同一量子通信服务站直接通信，在所述量子通信服务站包括：

接收来自所述智能家庭组件的文件密文以及真随机数R_M；

利用真随机数R_M从与智能家庭组件相应的对称密钥池中提取密钥K_M；

利用密钥K_M解密文件密文得到文件和文件签名；

利用私钥对解密得到的文件和文件签名再次签名得到二次签名；

生成利用真随机数Rss并利用真随机数Rss从第三对称密钥池中提取密钥Kss；

利用密钥Kss加密所述文件、所述文件签名以及所述二次签名得到文件密文，然后将文件密文连同真随机数Rss发送至所述安全云；

在所述安全云包括：

接收来自与安全云直接通信的量子通信服务站的文件密文以及真随机数Rss；

利用真随机数Rss从第三对称密钥池中提取密钥Kss；

利用密钥Kss解密文件密文得到所述文件、所述文件签名以及所述二次签名；

利用与安全云直接通信的量子通信服务站的公钥指针随机数结合非对称密钥池得到量子通信服务站的公钥；

利用所述量子通信服务站的公钥对所述二次签名进行验证；

利用与智能家庭组件相应的公钥指针随机数结合非对称密钥池得到智能家庭组件的公钥；

利用所述智能家庭组件的公钥对所述文件签名进行验证；

验证通过后加密存储。

2.如权利要求1所述的基于量子密钥卡的抗量子计算智能家庭量子云存储方法，其特征在于，所述智能家庭组件与量子通信服务站Q_M直接通信，所述安全云与量子通信服务站

Qss直接通信;在所述量子通信服务站Q_M包括:

接收来自所述智能家庭组件的文件密文以及真随机数R_M;

利用真随机数R_M从与智能家庭组件相应的对称密钥池中提取密钥K_M;

利用密钥K_M解密文件密文得到文件和文件签名;

对所述真随机数R_M以及文件和文件签名进行站间签名以及站间加密的方式直至发送至量子通信服务站Qss;

在所述量子通信服务站Qss包括:

采用站间验证以及站间解密的方式得到文件和文件签名;

利用私钥对解密得到的文件和文件签名再次签名得到二次签名;

生成利用真随机数Rss并利用真随机数Rss从第三对称密钥池中提取密钥Kss;

利用密钥Kss加密所述文件、所述文件签名以及所述二次签名得到文件密文,然后将文件密文连同真随机数Rss发送至所述安全云。

3.如权利要求1所述的基于量子密钥卡的抗量子计算智能家庭量子云存储方法,其特征在于,所述智能家庭组件还包括家庭设备,所述家庭设备经由所述家庭网关向安全云存取文件;所述家庭设备向所述家庭网关发送文件时包括:

对文件进行签名;

利用量子密钥卡生成真随机数形式的密钥K;

利用密钥K加密文件和文件签名得到密文,并使用家庭网关的公钥加密密钥K;

将加密的密钥K以及密文发送至家庭网关;

家庭网关经解密和验证后,将得到的文件发送给安全云。

4.如权利要求1所述的基于量子密钥卡的抗量子计算智能家庭量子云存储方法,其特征在于,所述智能家庭组件从安全云下载文件时,包括:

经由量子通信服务站向安全云发送下载请求;

安全云相应该下载请求并提取相应文件;

将文件进行签名并加密后发送至量子通信服务站;

量子通信服务站解密后对得到的文件以及文件签名进行二次签名并加密后发送给智能家庭组件;

智能家庭组件相应解密并验证。

5.如权利要求1所述的基于量子密钥卡的抗量子计算智能家庭量子云存储方法,其特征在于,各方通信时还发送相应的身份标识,接收方可利用该身份标识在量子密钥卡中按需获得与身份标识相应的公钥指针随机数。

6.如权利要求5所述的基于量子密钥卡的抗量子计算智能家庭量子云存储方法,其特征在于,所述安全云中存储有合法用户列表,安全云依照所述身份标识验证对方身份。

基于量子密钥卡的抗量子计算智能家庭量子云存储方法和系统

技术领域

[0001] 本发明涉及智能家庭设备技术领域，尤其一种基于量子密钥卡的抗量子计算智能家庭通信方法。

背景技术

[0002] 随着信息化技术和社会经济的不断发展，人们的生活水平得到了不断的提高，生活节奏也逐渐加快，居民们通过手机等终端可方便快捷地享受到智能、舒适、高效与安全的家居生活。随着家庭智能化设备的逐渐增加，人们对家庭设备的智能化操作提出了更高的要求。一般智能家庭设备通信方法中使用非对称密钥加密来保证数据的安全性，非对称密钥加密需要使用不同的密钥来分别完成加密和解密操作，一个公开发布，即公钥，另一个由用户自己秘密保存，即私钥。信息发送者用公钥去加密，而信息接收者用私钥去解密；或者信息发送者用私钥去加密，而信息接收者用公钥去解密。

[0003] 目前传统的通信加密和传输安全，都是依赖于复杂的数学算法。即由于目前计算机的计算能力所限，来不及在需求所在的时间段内计算出结果，因此可以说现在的数字密码体系是安全的。但是这种安全性现状已经越来越受到量子计算机的威胁。例如，针对经典密码学中的非对称密钥算法，存在专用的量子计算机算法(shor算法等)进行破解。在计算能力强大的量子计算机面前，即便是再高级的保密通信，只要是通过当前的通信手段，都会面临被破译和窃听的可能。因此，建立实际可用的整套量子通信网络方案已经是迫在眉睫的刚需。

[0004] 正如大多数人所了解的，量子计算机在密码破解上有着巨大潜力。当今主流的非对称(公钥)加密算法，如RSA加密算法，大多数都是基于大整数的因式分解或者有限域上的离散对数的计算这两个数学难题。他们的破解难度也就依赖于解决这些问题的效率。传统计算机上，要求解这两个数学难题，花费时间为指数时间(即破解时间随着公钥长度的增长以指数级增长)，这在实际应用中是无法接受的。而为量子计算机量身定做的秀尔算法可以在多项式时间内(即破解时间随着公钥长度的增长以k次方的速度增长，其中k为与公钥长度无关的常数)进行整数因式分解或者离散对数计算，从而为RSA、离散对数加密算法的破解提供可能。

[0005] 现有技术存在的问题：

[0006] (1)现有技术中，家庭网关没有可靠的防护措施。家庭网关是智能家庭的中心网元，而且有Internet上网能力，很有可能被感染病毒木马，从而被窃取信息；或者被攻击导致瘫痪，从而导致整个智能家庭方案的瘫痪。

[0007] (2)现有技术中，移动终端密钥存储于移动终端存储器中，暴露于移动终端的病毒木马的威胁之下，可以被恶意软件或恶意操作窃取。

[0008] (3)由于量子计算机能快速通过公钥得到对应的私钥，因此现有的建立在公私钥基础之上的智能家庭通信方法容易被量子计算机破解。

[0009] (4)现有技术中，基于公私钥的数字签名的输入和输出均可被敌方所知，在量子计算机存在的情况下，可能被推导出私钥，导致建立在公私钥基础之上的智能家庭通信系统被量子计算机破解。

[0010] (5)现有技术中，云存储上的文件如不使用数字签名，将没有抗抵赖的效果，如果出现不合法文件，将难以追查来源。即使使用数字签名，也存在因私钥被盗导致的非法签名。

[0011] (6)现有技术中，可能存在非合法用户使用云，导致安全问题。

[0012] (7)云存储密钥如没有硬件保护，不够安全。

[0013] (8)上传云存储一般使用公钥体制的SSL协议协商会话密钥，该过程会被量子计算机破解。

发明内容

[0014] 本发明提供一种基于量子密钥卡的抗量子计算智能家庭量子云存储方法，包括智能家庭组件经由量子通信服务站向安全云存取文件，其中所述智能家庭组件包括家庭网关和移动终端，各智能家庭组件以及量子通信服务站和安全云分别配有量子密钥卡，各量子密钥卡中存储有私钥、非对称密钥池、以及公钥指针随机数，其中非对称密钥池存储有各方的公钥，通过公钥指针随机数可结合非对称密钥池获取与任一方私钥相应的公钥；

[0015] 所述移动终端的量子密钥卡内还存储有第一对称密钥池，所述家庭网关的量子密钥卡内还存储有第二对称密钥池，所述安全云的量子密钥卡内还存储有第三对称密钥池，且所有的对称密钥池还同时存储在所述量子通信服务站的量子密钥卡内；

[0016] 所述智能家庭组件与安全云通信存取文件时，所述文件利用双方的量子密钥卡采用非对称算法对文件进行签名和验证；

[0017] 所述智能家庭组件与量子通信服务站之间，以及量子通信服务站与安全云之间转发文件时，利用相应的对称密钥池生成密钥，采用对称算法进行加密通信。

[0018] 可选的，所述智能家庭组件向安全云通信存储文件时，在智能家庭组件处包括：

[0019] 利用私钥对文件进行签名得到文件签名；

[0020] 生成利用真随机数R_M并利用真随机数R_M从对称密钥池中提取密钥K_M；

[0021] 利用密钥K_M加密文件和文件签名得到文件密文，然后将文件密文连同真随机数R_M发送至量子通信服务站。

[0022] 可选的，所述智能家庭组件和安全云与同一量子通信服务站直接通信，在所述量子通信服务站包括：

[0023] 接收来自所述智能家庭组件的文件密文以及真随机数R_M；

[0024] 利用真随机数R_M从与智能家庭组件相应的对称密钥池中提取密钥K_M；

[0025] 利用密钥K_M解密文件密文得到文件和文件签名；

[0026] 利用私钥对解密得到的文件和文件签名再次签名得到二次签名；

[0027] 生成利用真随机数Rss并利用真随机数Rss从第三对称密钥池中提取密钥Kss；

[0028] 利用密钥Kss加密所述文件、所述文件签名以及所述二次签名得到文件密文，然后将文件密文连同真随机数Rss发送至所述安全云。

[0029] 可选的，所述智能家庭组件与量子通信服务站Q_M直接通信，所述安全云与量子通

信服务站Qss直接通信;在所述量子通信服务站Q_M包括:

[0030] 接收来自所述智能家庭组件的文件密文以及真随机数R_M;

[0031] 利用真随机数R_M从与智能家庭组件相应的对称密钥池中提取密钥K_M;

[0032] 利用密钥K_M解密文件密文得到文件和文件签名;

[0033] 对所述真随机数R_M以及文件和文件签名进行站间签名以及站间加密的方式直至发送至量子通信服务站Qss;

[0034] 在所述量子通信服务站Qss包括:

[0035] 采用站间验证以及站间解密的方式得到文件和文件签名;

[0036] 利用私钥对解密得到的文件和文件签名再次签名得到二次签名;

[0037] 生成利用真随机数Rss并利用真随机数Rss从第三对称密钥池中提取密钥Kss;

[0038] 利用密钥Kss加密所述文件、所述文件签名以及所述二次签名得到文件密文,然后将文件密文连同真随机数Rss发送至所述安全云。

[0039] 可选的,在所述安全云包括:

[0040] 接收来自与安全云直接通信的量子通信服务站的文件密文以及真随机数Rss;

[0041] 利用真随机数Rss从第三对称密钥池中提取密钥Kss;

[0042] 利用密钥Kss解密文件密文得到所述文件、所述文件签名以及所述二次签名;

[0043] 利用与安全云直接通信的量子通信服务站的公钥指针随机数结合非对称密钥池得到量子通信服务站的公钥;

[0044] 利用所述量子通信服务站的公钥对所述二次签名进行验证;

[0045] 利用与智能家庭组件相应的公钥指针随机数结合非对称密钥池得到智能家庭组件的公钥;

[0046] 利用所述智能家庭组件的公钥对所述文件签名进行验证;

[0047] 验证通过后加密存储。

[0048] 可选的,所述智能家庭组件还包括家庭设备,所述家庭设备经由所述家庭网关向安全云存取文件;所述家庭设备向所述家庭网关发送文件时包括:

[0049] 对文件进行签名;

[0050] 利用量子密钥卡生成真随机数形式的密钥K;

[0051] 利用密钥K加密文件和文件签名得到密文,并使用家庭网关的公钥加密密钥K;

[0052] 将加密的密钥K以及密文发送至家庭网关;

[0053] 家庭网关经解密和验证后,将得到的文件发送给安全云。

[0054] 可选的,所述智能家庭组件从安全云下载文件时,包括:

[0055] 经由量子通信服务站向安全云发送下载请求;

[0056] 安全云相应该下载请求并提取相应文件;

[0057] 将文件进行签名并加密后发送至量子通信服务站;

[0058] 量子通信服务站解密后对得到的文件以及文件签名进行二次签名并加密后发送给智能家庭组件;

[0059] 智能家庭组件相应解密并验证。

[0060] 可选的,各方通信时还发送相应的身份标识,接收方可利用该身份标识在量子密钥卡中按需获得与身份标识相应的公钥指针随机数。

[0061] 可选的，所述安全云中存储有合法用户列表，安全云依照所述身份标识验证对方身份。

[0062] 本发明还提供一种基于量子密钥卡的抗量子计算智能家庭量子云存储系统，包括智能家庭组件经由量子通信服务站向安全云存取文件，其中所述智能家庭组件包括家庭网关和移动终端，各智能家庭组件以及量子通信服务站和安全云分别配有量子密钥卡，各量子密钥卡中存储有私钥、非对称密钥池、以及公钥指针随机数，其中非对称密钥池存储有各方的公钥，通过公钥指针随机数可结合非对称密钥池获取与任一方私钥相应的公钥；

[0063] 所述移动终端的量子密钥卡内还存储有第一对称密钥池，所述家庭网关的量子密钥卡内还存储有第二对称密钥池，所述安全云的量子密钥卡内还存储有第三对称密钥池，且所有的对称密钥池还同时存储在所述量子通信服务站的量子密钥卡内；

[0064] 所述智能家庭组件与安全云通信存取文件时，所述文件利用双方的量子密钥卡采用非对称算法对文件进行签名和验证；

[0065] 所述智能家庭组件与量子通信服务站之间，以及量子通信服务站与安全云之间转发文件时，利用相应的对称密钥池生成密钥，采用对称算法进行加密通信。

[0066] 本发明量子密钥卡是结合了密码学技术、硬件安全隔离技术、量子物理学技术(搭载量子随机数发生器的情况下)的身份认证和加解密产品。量子密钥卡的内嵌芯片和操作系统可以提供密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，量子密钥卡成为私钥和密钥池的安全载体。每一个量子密钥卡可以有硬件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。总之，量子密钥卡使得密钥等绝密信息不以明文形式出现在主机的磁盘及内存中，从而能有效保证绝密信息的安全。

[0067] 智能家庭成员中的移动终端和家庭网关均配备有量子密钥卡，量子通信服务站和安全云也配备有量子密钥卡，使用量子密钥卡存储密钥。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。同时，各所述智能家庭成员利用所公开的抗量子计算公钥结合所述非对称密钥池提取所需智能家庭成员的公钥，且智能家庭成员的公钥存储在量子密钥卡内，保证量子计算机无法得到用户公钥，进而无法得到对应的私钥，因此降低被量子计算机破解风险。另外，为上传至安全云的每一个文件添加数字签名，且基于公私钥的数字签名被随机数密钥进一步加密，形成加密的数字签名。即使在量子计算机存在的情况下，也难以被推导出私钥。因此该方案不容易被量子计算机破解。对每条消息均加入数字签名，可以明确每条消息的真实来源，提高智能家庭系统的安全性。还在安全云上存储有合法用户列表，可防止非合法用户使用安全云。

附图说明

[0068] 图1为本发明实施例提供的智能家庭组网图；

[0069] 图2为量子密钥卡密钥区的结构示意图；

[0070] 图中(a)部分示意了家庭网关量子密钥卡的结构；

[0071] 图中(b)部分示意了家庭设备量子密钥卡的结构；

[0072] 图中(c)部分示意了量子通信服务站量子密钥卡的结构。

[0073] 图3为本发明实施例提供的公钥存储方式流程图；

[0074] 图4为本发明实施例提供的公钥读取方式流程图；

[0075] 图5为本发明实施例提供的生成密钥的流程图；

[0076] 图6为移动终端与量子通信服务站之间消息的结构图；

[0077] 图7为家庭设备向家庭网关发送的请求的消息结构图；

[0078] 图8为家庭网关向家庭设备发送的消息结构图。

具体实施方式

[0079] 量子通信技术是基于量子物理学建立起来的新兴安全通信技术。我国的量子通信技术已经进入了实用化的阶段，其应用前景和战略意义也引起了地方政府和重要行业对其产业发展的广泛关注。除建立量子通信干线以外，一些规模化城域量子通信网络也已经建设成功并运行。基于城域量子通信网络，量子通信技术也有了初步的应用，可实现高保密性的视频语音通信等应用。量子通信干线和量子通信城域网等量子通信网络，组成量子通信网络，其本质是量子密钥分发(QKD)。因此以QKD技术为基础建立起来的量子通信网络可称为QKD网络。

[0080] 虽然目前量子城域网已经可以允许用户接入并享有量子网络的高安全特性，但是目前用户接入量子网络的部分仍然是整个量子通信网络中的软肋。一方面量子密钥分发后的密钥安全到达用户手中是一个很大的问题，存在被窃取或篡改的风险；另一方面，同一台量子密钥分发设备所能连接的用户数有限，无法同时连接大量用户。因此需要在用户接入量子网络的部分，采用量子通信服务站的方式，解决上述问题：

[0081] (1)量子通信服务站作为类似运营商的角色，一方面与QKD网络建立合作关系，实现安全连接的保证，从而保证量子密钥可以安全分发到量子通信服务站；另一方面，量子通信服务站为用户颁发量子密钥卡，将量子随机数密钥颁发给用户，同时自身保存用户所拥有的密钥，可实现量子通信服务站与用户之间的安全通信。

[0082] (2)量子通信服务站可以搭建为集群服务器的模式，可以同时接入大量用户。

[0083] 在智能家庭量子通信方案中，移动终端、家庭网关均为量子通信服务站的用户，量子通信服务站为其分别颁发量子密钥卡。

[0084] 本实施例中，智能家庭成员都有匹配的量子密钥卡，量子密钥卡的颁发方为量子密钥卡的主管方，一般为智能家庭本身，或者智能家庭的管理部门例如小区物业，量子密钥卡的被颁发方为量子密钥卡的主管方所管理的成员，一般为智能家庭的家庭成员、维护人员及访客。

[0085] 量子密钥卡中带有用于存储公钥的非对称密钥池。非对称密钥池拥有本组织所有采用公私钥体制的用户的公钥，并且每个公钥与该公钥对应的ID一一对应。包括家庭网关、家庭设备、移动终端的公钥。

[0086] 公钥的存储方式如图3所示，具体步骤如下：对某个用户随机取公钥指针随机数rk(即公钥的存储位置参数)，结合特定的公钥指针函数frkp得到公钥指针rkp并从相应的非对称密钥池中的对应位置存入该用户的公钥krk。读取密钥方式如图4所示，方式与存储密

钥方式相同。公布公钥指针随机数rk作为抗量子计算公钥。

[0087] 智能家庭结构如图1所示，家庭网关(S)具有路由功能，是连接所有家庭设备的管理中心。可通过Wifi或Internet与移动终端相连。本文假设其ID为SID。为方便信息接收方处理，SID包含其公钥指针随机数，还可用于指定量子通信服务站中的Q密钥池。家庭网关量子密钥卡位于家庭网关内部，一般体现为密钥板卡的形式。具体结构如图2(a)部分所示，卡内除了包括非对称密钥池、公钥指针随机数和私钥，还包括Q密钥池，Q密钥池来自量子通信服务站，且其密钥均为私有密钥，每个成员均不同。Q密钥池不仅存储于该成员的量子密钥卡中，还存储于该成员匹配的量子通信服务站的量子密钥卡中。

[0088] 家庭设备(C)包括监控摄像头、猫眼、门锁、智能开关、影音服务器、监控服务器等。本文假设其ID为CID。为方便信息接收方处理，CID包含其公钥指针随机数。家庭设备使用C量子密钥卡，具体结构如图2(b)部分所示。与家庭网关量子密钥卡的区别在于无用于与量子通信服务站联系的Q密钥池。

[0089] 移动终端(M)包括家庭主人的手机、平板电脑等。可通过Wifi或Internet接入家庭网关并控制家庭设备。本文假设其ID为MID。为方便信息接收方处理，MID包含其公钥指针随机数，还可用于指定量子通信服务站中的Q密钥池。移动终端使用移动终端量子密钥卡，其内部存储密钥区与家庭网关相同。不同的是该量子密钥卡一般体现为SDKEY或UKEY或手机主板芯片等便携形式。

[0090] 安全云(SS)指公有云或者智能家庭私有云，用于存储智能家庭的加密数据，例如视频、图像、文本及其他类型的数据。该云的安全性由量子密钥卡保证，不会将数据的密钥暴露于云的管理者，因此用户存储的各类数据无需担心其安全性。本文假设其ID为SSID。为方便信息接收方处理，SSID包含其公钥指针随机数，还可用于指定量子通信服务站中的Q密钥池。安全云使用安全云量子密钥卡，其内部存储密钥区与家庭网关相同。不同的是安全云量子密钥卡还存储有合法用户列表，该用户列表由用户登记形成，列表成员用公钥指针随机数的方式表示，且该用户列表可由量子密钥卡管理员进行更改维护。

[0091] 量子通信服务站包括量子服务中心，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通信服务站通信连接，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；还包括量子密钥分发设备，主要用于通过QKD方式实现站间量子密钥的共享。量子通信服务站使用Q量子密钥卡，内部结构如图2(c)部分所示。其中，Q量子密钥卡中的非对称密钥池与智能家庭系统是同一个。除了非对称密钥池，Q量子密钥卡还保存有合法服务站列表，该用户列表由量子通信服务站运维人员登记形成，列表成员用公钥指针随机数的方式表示，且该服务站列表可由量子密钥卡管理员进行更改维护。Q量子密钥卡包括多个Q密钥池，分别对应该量子通信服务中匹配的各个家庭网关或移动终端。本文假设与M对应的量子通信服务站的ID为QID_M，同理与S对应的量子通信服务站的ID即为QID_S。为方便信息接收方处理，QID包含其公钥指针随机数，还可用于指定与匹配的家庭网关或移动终端对应的Q密钥池。

[0092] 实施例1

[0093] 本实施例为智能家庭成员上传文件至安全云，智能家庭成员上传文件至安全云分为以下三种情况：移动终端M上传文件至安全云，家庭网关S上传文件至安全云，家庭设备C上传文件至安全云。

[0094] 情况1:移动终端上传文件至安全云。如图1所示,移动终端通过量子通信服务站向安全云上传文件。

[0095] 步骤1.1.1:移动终端将文件发送至量子通信服务站。

[0096] 移动终端M根据匹配的量子密钥卡中的真随机数发生器生成真随机数R_M(以下简称R_M,其它同理省去汉字部分作为简称)。R_M结合特定的密钥生成算法f得到指针P_M。P_M指向M的Q密钥池中的某一部分,可以在该密钥池中提取出相应的密钥K_M。使用该密钥加密文件F和文件签名MS得到密文,然后将密文连同真随机数R_M以及MID一起发送至移动终端匹配的量子通信服务站Q_M,消息结构如图6所示,可表示为$\{MID||R_M||\{F||S_M\}K_M\}$。此处文件签名$S_M$即移动终端M对原文件进行数字签名算法得到文件签名$S_M$。

[0097] 步骤1.1.2:量子通信服务站之间传输信息。

[0098] 量子通信服务站Q_M收到来自移动终端M的加密消息和R_M以及MID后,使用R_M结合特定的密钥生成算法f得到指针P_M,通过P_M在由MID指定的与移动终端M匹配的Q密钥池中提取出相应的密钥K_M。

[0099] 量子通信服务站Q_M使用K_M对密文进行解密得到文件F和文件签名S_M。Q_M用MID取出M的公钥,方法见图4;用M的公钥对S_M进行签名验证,如验证失败则停止处理;如验证成功则继续后续流程。使用Q_M的私钥对MID、原文件F和S_M进行数字签名算法得到文件签名S_{QM}。组合成新消息,可表示为$\{MID||F||S_M||S_{QM}\}$。

[0100] 将消息传递到与安全云SS匹配的量子通信服务站Q_{SS}处。量子通信服务站Q_M与量子通信服务站Q_{SS}利用各自的量子密钥分发设备实现站间量子密钥的共享,使得明文形式的消息全文在量子通信服务站Q_M加密后发送至量子通信服务站Q_{SS},再经解密恢复出明文形式的消息全文。此处传递的消息全文内容包括QID_M以及被QKD密钥加密的$\{MID||F||S_M||S_{QM}\}$。

[0101] 量子通信服务站Q_M与量子通信服务站Q_{SS}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通信服务站(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。中转过程中,其他网络节点通过QID_M获得Q_M的公钥指针随机数并进一步得到Q_M的公钥,查看Q_M的公钥指针随机数是否属于本服务站的合法服务站列表,如不属于则停止处理;如属于则继续后续流程。用Q_M的公钥对S_{QM}进行数字签名验证,如验证失败则停止处理;如验证成功则继续后续流程。S_{QM}验证通过信任该文件后本量子通信服务站制作自己的文件签名,即使用自己的私钥对MID、原文件和S_M进行数字签名算法得到文件签名。使用QKD密钥加密消息全文。将自己的ID附加在加密的消息全文之前,传递给下一个网络节点。

[0102] 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。

[0103] 步骤1.1.3:量子通信服务站上传文件至安全云。

[0104] 量子通信服务站Q_{SS}收到消息后,通过QID_M获得Q_M的公钥指针随机数并进一步得到Q_M的公钥,具体过程如图4所示。查看Q_M的公钥指针随机数是否属于本服务站的合法服务站列表,如不属于则停止处理;如属于则继续后续流程。用Q_M的公钥对S_{QM}进行数字签名验证,如验证失败则停止处理;如验证成功则继续后续流程。

[0105] S_{QM}验证通过信任该文件后本量子通信服务站制作自己的文件签名,即使用自己的私钥对MID、原文件和S_M进行数字签名算法得到文件签名S_{QSS}。

[0106] 量子通信服务站Q_{SS}根据匹配的量子密钥卡中的真随机数发生器生成真随机数R_{SS},R_{SS}结合特定的密钥生成算法f得到指针P_{SS},P_{SS}指向由SSID指定的与安全云SS匹配的Q密钥池中的某一部分,可以在该密钥池中提取出相应的密钥K_{SS}。使用该密钥加密消息得到密文,可表示为$QID_{SS}||R_{SS}||\{MID||F||S_M||S_{QSS}\}K_{SS}$,传递给下一个网络节点即SS。

[0107] 步骤1.1.4:安全云收到文件并进行存储。

[0108] 安全云SS接受来自Q_{SS}的消息后,将R_{SS}结合特定的密钥生成算法f得到指针P_{SS},通过P_{SS}在Q密钥池中提取出相应的密钥K_{SS}。使用K_{SS}解密密文得到$\{MID||F||S_M||S_{QSS}\}$。SS用QID_{SS}取出Q_{SS}的公钥,方法见图4;用Q_{SS}的公钥对S_{QSS}进行签名验证,如验证失败则停止处理;如验证成功则继续后续流程。SS对MID进行验证,若存在于合法用户列表中,则通过验证。通过验证后通过MID获得M的公钥指针随机数并进一步得到M的公钥,具体过程如图4所示。使用M的公钥对文件进行数字签名验证,验证通过则信任该消息。

[0109] 对消息验证通过后,安全云根据匹配的量子密钥卡中的真随机数发生器生成文件密钥,使用该密钥加密文件及其签名,并使用量子密钥卡中的安全密钥加密文件密钥,将MID、加密的文件密钥和加密的文件及其签名存储到云存储空间中。

[0110] 特别的,当移动终端与安全云匹配的量子通信服务站为同一个时,移动终端M向安全云上传文件的流程具体步骤描述如下:

[0111] 步骤1.2.1.移动终端加密文件。

[0112] 移动终端M将根据匹配的量子密钥卡中的真随机数发生器生成真随机数R_M。R_M结合特定的密钥生成算法f得到指针P_M。P_M指向M的Q密钥池中的某一部分,可以在该密钥池中提取出相应的密钥K_M。使用该密钥加密文件F和文件签名S_M得到密文,然后将密文连同真随机数R_M以及MID一起发送至移动终端匹配的量子通信服务站Q,消息结构如图6所示,可表示为$\{MID||R_M||\{F||S_M\}K_M\}$。此处文件签名$S_M$即移动终端M对原文件进行数字签名算法得到文件签名$S_M$。

[0113] 步骤1.2.2:上传文件至安全云。

[0114] 量子通信服务站Q收到来自移动终端M的加密消息和R_M以及MID后,使用R_M结合特定的密钥生成算法f得到指针P_M,通过P_M在由MID指定的与移动终端M匹配的Q密钥池中提取出相应的密钥K_M。

[0115] 量子通信服务站Q使用K_M对密文进行解密得到文件F和文件签名S_M。通过MID取出M的公钥,方法见图4;用M的公钥对S_M进行签名验证,如验证失败则停止处理;如验证成功则继续后续流程。验证通过信任该文件后量子通信服务站Q制作自己的文件签名,即使用自己的私钥对MID、原文件和S_M进行数字签名算法得到文件签名S_Q。

[0116] 量子通信服务站Q根据匹配的量子密钥卡中的真随机数发生器生成真随机数R_{SS},R_{SS}结合特定的密钥生成算法f得到指针P_{SS},P_{SS}指向由SSID指定的与安全云SS匹配的Q密钥池中的某一部分,可以在该密钥池中提取出相应的密钥K_{SS}。使用该密钥加密消息得到密文,可表示为$QID||R_{SS}||\{MID||F||S_M||S_Q\}K_{SS}$,传递给下一个网络节点即SS。

[0117] 步骤1.2.3:安全云收到文件并进行存储。

[0118] 安全云SS接受来自Q的消息后,将R_{SS}结合特定的密钥生成算法f得到指针P_{SS},通过P_{SS}在Q密钥池中提取出相应的密钥K_{SS}。使用K_{SS}解密密文得到$\{MID||F||S_M||S_Q\}$。SS用QID取出Q的公钥,方法见图4;用Q的公钥对S_Q进行签名验证,如验证失败则停止处理;如验证成功

则继续后续流程。SS对MID进行验证，若存在于合法用户列表中，则通过验证。通过验证后通过MID获得M的公钥指针随机数并进一步得到M的公钥，具体过程如图4所示。使用M的公钥对文件进行数字签名验证。结果一致则信任该消息。

[0119] 对消息验证通过后，安全云根据匹配的量子密钥卡中的真随机数发生器生成文件密钥，使用该密钥加密文件及其签名，并使用量子密钥卡中的安全密钥加密文件密钥，将MID、加密的文件密钥和加密的文件及其签名存储到云存储空间中。

[0120] 情况2：家庭网关上传文件至安全云。具体过程与移动终端上传文件至安全云的过程相同。

[0121] 情况3：家庭设备借助家庭网关上传文件至安全云。如图1所示，家庭设备通过家庭网关向安全云上传文件。

[0122] 步骤1.3.1：家庭设备将文件发送至家庭网关。

[0123] 家庭设备C根据匹配的量子密钥卡中的真随机数发生器生成密钥K，使用该密钥加密文件F和文件签名S_C，并使用S的公钥加密密钥K。将CID、加密的密钥K、以及密文发送至家庭网关S。此处密文即使用密钥K加密文件F和文件签名S_C，此处签名即家庭设备C对原文件进行数字签名算法得到文件签名S_C。消息结构如图7所示，可表示为$\{CID||\{K\}PK_S||\{F||S_C\}K\}$。

[0124] 步骤1.3.2：家庭网关将文件上传至安全云。

[0125] 安全网关S收到来自家庭设备C的消息后，对CID进行验证，若存在于合法用户列表中，则通过验证。通过验证后使用自己的私钥解密得到密钥K，使用K解密请求得到文件和签名。通过CID取得C的公钥，方法见图4。使用C的公钥对文件进行数字签名验证，结果一致则信任该消息。

[0126] 完成验证后对文件制作安全网关的签名，将文件和签名通过量子通信服务站上传至安全云SS，具体步骤与情况1中描述相同。

[0127] 步骤1.3.3：安全云收到文件并进行存储。

[0128] 具体步骤与情况1中步骤1.1.4描述相同。

[0129] 实施例2

[0130] 本实施例为智能家庭成员从安全云处下载文件，智能家庭成员从安全云下载文件分为以下三种情况：移动终端M从安全云下载文件，家庭网关S从安全云下载文件和家庭设备C从安全云下载文件。

[0131] 情况1：移动终端从安全云下载文件。

[0132] 步骤2.1.1：移动终端向安全云发送下载文件请求。

[0133] 移动终端向安全云发送的下载文件请求通过量子通信服务站进行中转，请求包括移动终端的MID。

[0134] 步骤2.1.2：量子通信服务站获取并传输文件。

[0135] 安全云SS收到下载文件的请求后，对MID进行验证，若存在于合法用户列表中，则通过验证。通过验证后安全云SS提取相应加密文件并使用文件密钥对其进行解密。

[0136] 安全云SS根据匹配的量子密钥卡中的真随机数发生器生成真随机数R_{SS}，R_{SS}结合特定的密钥生成算法f得到指针P_{SS}，P_{SS}指向安全云SS的Q密钥池中的某一部分，可以在该密钥池中提取出相应的密钥K_{SS}。安全云使用密钥K_{SS}加密文件F和签名S_{SS}得到密文，然后将密

文连同真随机数R_{SS}以及SSID一起发送至量子通信服务站Q_{SS}，消息结构可表示为{SSID||R_{SS}||{F||S_{SS}}K_{SS}}。此处文件签名S_{SS}即安全云SS对原文件进行数字签名算法得到文件签名S_{SS}。

[0137] 与安全云SS匹配的量子通信服务站Q_{SS}从安全云SS处获取加密的文件F和签名S_{SS}，通过R_{SS}得到K_{SS}后进行解密得到文件，通过SSID得到SS的公钥后对S_{SS}进行签名验证，如验证失败则停止处理；如验证成功则继续后续流程。使用Q_{SS}的私钥对SSID、原文件F和S_{SS}进行数字签名算法得到文件签名S_{QSS}。组合成新消息，可表示为{SSID||F||S_{SS}||S_{QSS}}。

[0138] 将消息传递到与移动终端M匹配的量子通信服务站Q_M处。通过站间信息传输将新消息发送至与移动终端M匹配的量子通信服务站Q_M。如果移动终端M和安全云SS匹配的是同一个量子通信服务站的话，则不需要通过站间信息传输。具体过程中的签名与验签步骤与实施例1中所描述的站间信息传输过程一致。量子通信服务站Q_M得到并信任消息后，根据匹配的量子密钥卡中的真随机数发生器生成真随机数R_M，R_M结合特定的密钥生成算法f得到指针P_M，P_M指向由MID指定的与移动终端M匹配的Q密钥池中的某一部分，可以在该密钥池中提取出相应的密钥K_M。使用该密钥加密消息得到密文，可表示为QID_M||R_M||{SSID||F||S_{SS}||S_{QM}}K_M，传递给下一个网络节点即移动终端M。

[0139] 步骤2.1.3：移动终端获取文件。

[0140] 移动终端M从量子通信服务站Q_M获得消息后，将R_M结合特定的密钥生成算法f得到指针P_M，通过P_M在Q密钥池中提取出相应的密钥K_M。使用K_M解密文件密文得到{SSID||F||S_{SS}||S_{QM}}。M用QID_M取出Q_M的公钥，方法见图4；用Q_M的公钥对S_{QM}进行签名验证，如验证失败则停止处理；如验证成功则继续后续流程。通过SSID获得SS的公钥指针随机数并进一步得到SS的公钥，具体过程如图4所示。使用SS的公钥对文件进行数字签名验证，验证通过则信任该消息。验证签名后获得文件。

[0141] 情况2：家庭网关从安全云下载文件。具体过程与移动终端从安全云下载文件的过程相同。

[0142] 情况3：家庭设备借助家庭网关从安全云下载文件。

[0143] 步骤2.3.1：家庭设备向家庭网关发送请求。

[0144] 家庭设备C根据匹配的量子密钥卡中的真随机数发生器生成密钥K_1，使用该密钥加密请求request，并使用S的公钥加密密钥K_1。将CID、加密的密钥K_1以及请求密文发送至家庭网关S，消息结构可表示为{CID||{K_1}PK_S||{request||S_C}K_1}。此处请求密文即使用密钥K_1加密请求和签名，此处签名即家庭设备C对原请求进行数字签名算法得到该签名。消息结构如图7所示。

[0145] 步骤2.3.2：家庭网关处理请求并应答。

[0146] 安全网关S收到来自家庭设备C的请求后，对CID进行验证，若存在于合法用户列表中，则通过验证。通过验证后安全网关S使用自己的私钥解密得到密钥K_1，使用K_1解密请求密文得到请求和签名。使用C的公钥解密签名后对签名进行验证，验证通过则信任该请求。

[0147] 完成验证后安全网关S通过量子通信服务站从安全云SS处获取加密的文件F和文件签名S_C。具体过程见实施例2情况1。对文件签名进行验证后将文件发送给家庭设备C。家庭网关S根据匹配的量子密钥卡中的真随机数发生器生成随机数K_2，使用该密钥加密文件，并使用C的公钥加密密钥K_2，将SID、加密的密钥K_2、加密的文件F和签名S_S发送至家庭设备C，消息结构可表示为{SID||{K_2}PK_C||{F||S_S}K_2}。此处签名S_S即家庭网关S对原文件进行数字

签名算法得到该签名。消息结构如图8所示。

[0148] 步骤2.3.3:家庭设备得到文件。

[0149] 家庭设备C收到了来自家庭网关S的应答后,使用自己的私钥解密得到密钥K_2,使用K_2解密应答密文得到文件和签名。使用S的公钥对S_S进行签名验证,如验证失败则停止处理;如验证成功则继续后续流程。验证成功后,获得文件。

[0150] 以上所述实施例的各技术特征可以进行任意的组合,为使描述简洁,未对上述实施例中的各个技术特征所有可能的组合都进行描述,然而,只要这些技术特征的组合不存在矛盾,都应当认为是本说明书记载的范围。

[0151] 以上所述实施例仅表达了本发明的几种实施方式,其描述较为具体和详细,但并不能因此而理解为对发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干变形和改进,这些都属于本发明的保护范围。因此,本发明专利的保护范围应以所附权利要求为准。

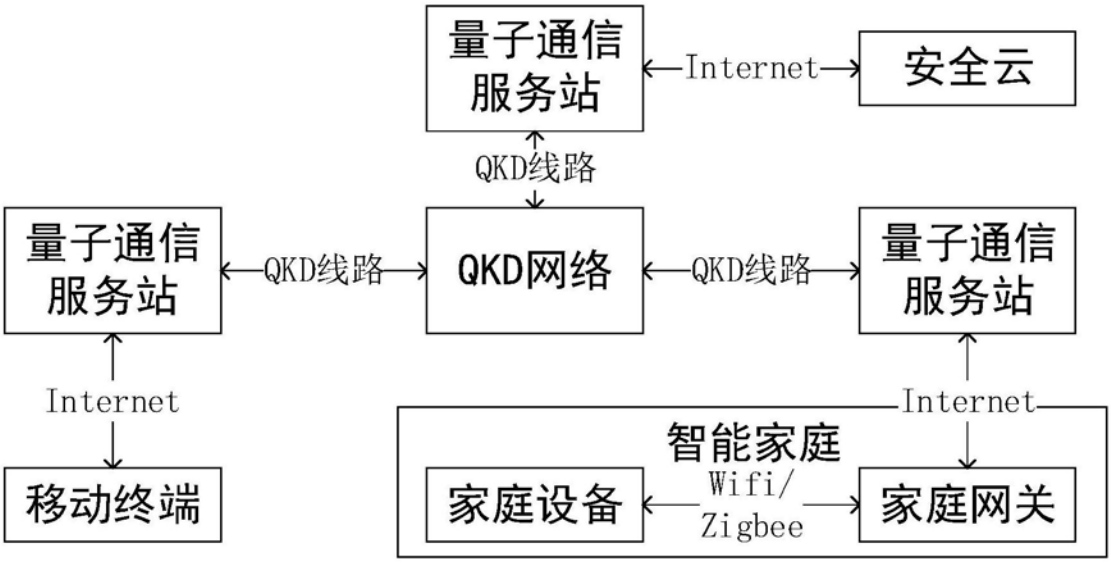

量子通信
服务站
Internet
安全云
QKD线路
量子通信
服务站
QKD线路
QKD网络
QKD线路
量子通信
服务站
Internet
Internet
智能家庭
移动终端
家庭设备
Wifi/
Zigbee
家庭网关

图1

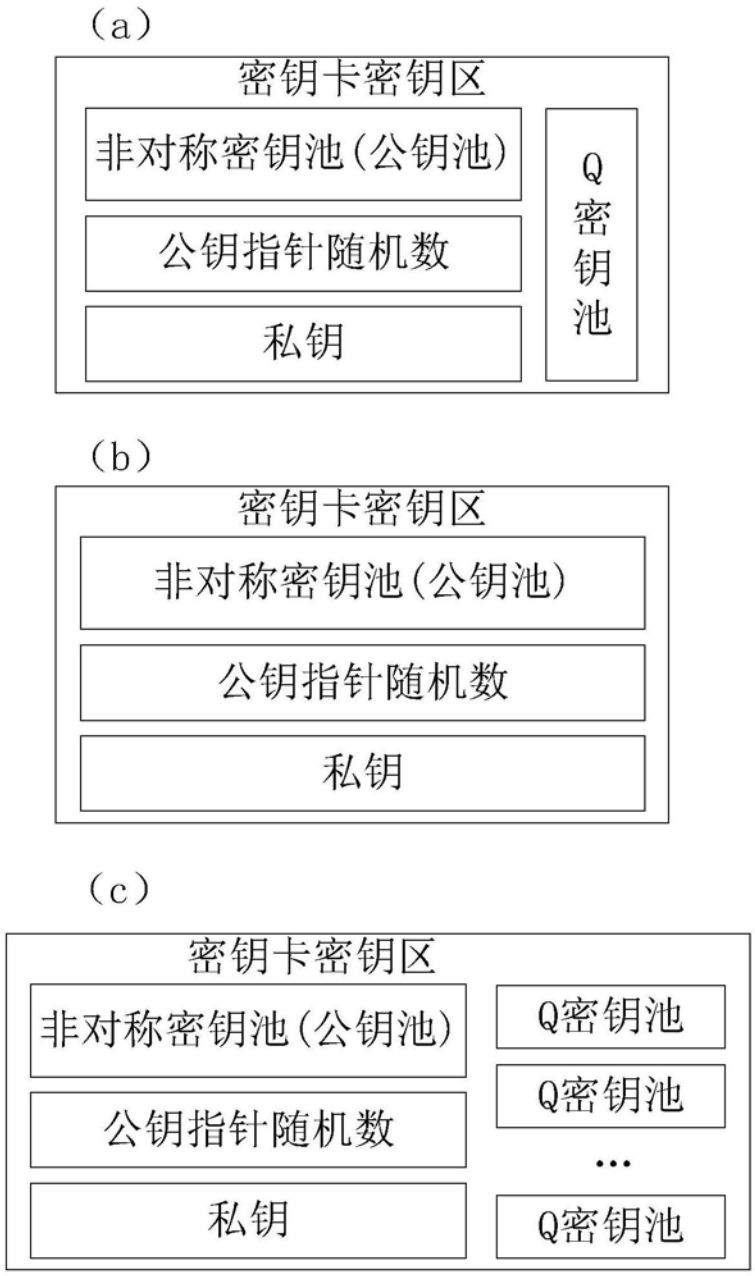

(a)
密钥卡密钥区
非对称密钥池(公钥池)
公钥指针随机数
私钥
Q密钥池
(b)
密钥卡密钥区
非对称密钥池(公钥池)
公钥指针随机数
私钥
(c)
密钥卡密钥区
非对称密钥池(公钥池)
公钥指针随机数
私钥
Q密钥池
Q密钥池
...
Q密钥池

图2

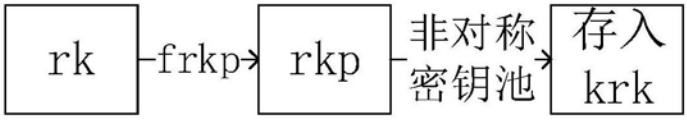

rk
frkp
rkp
非对称密钥池
存入krk

图3

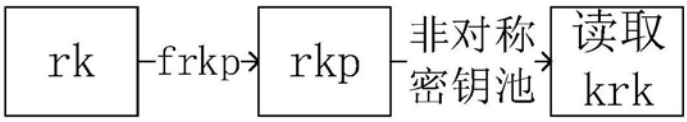

rk
frkp
rkp
非对称
密钥池
读取
krk

图4

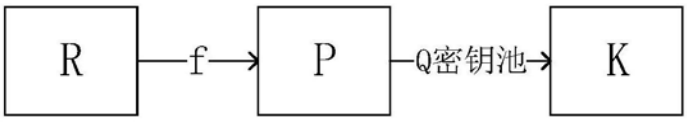

R
f
P
Q密钥池
K

图5

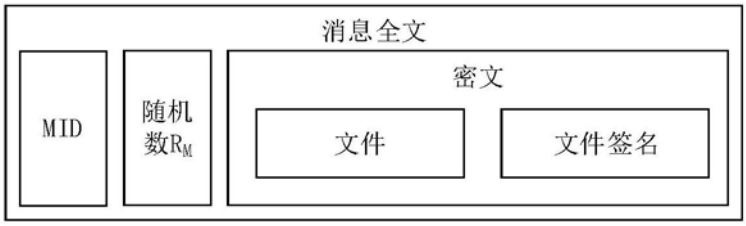

消息全文
MID
随机数R_M
密文
文件
文件签名

图6

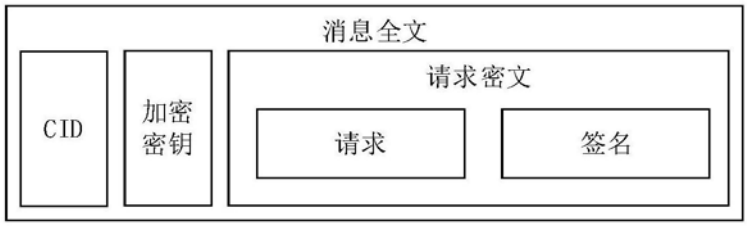

消息全文
CID
加密密钥
请求密文
请求
签名

图7

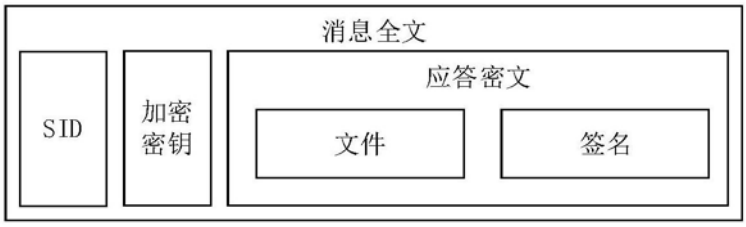

消息全文
SID
加密密钥
应答密文
文件
签名

图8