(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 113285803 B
(45)授权公告日 2022.03.11

(21)申请号 202110706152.3
(22)申请日 2021.06.24
(65)同一申请的已公布的文献号
申请公布号 CN 113285803 A
(43)申请公布日 2021.08.20
(73)专利权人 中电信量子科技有限公司
地址 236000 安徽省合肥市高新区创新产业园一期A3-812
(72)发明人 刘驰 李杏桃 王建 黄伟胜 王丙磊 胡缙 程显赫
(74)专利代理机构 合肥市浩智运专利代理事务所(普通合伙) 34124
代理人 丁瑞瑞
(51)Int.Cl.
H04L 51/42(2022.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)

(56)对比文件
CN 109951381 A,2019.06.28
US 2018198799 A1,2018.07.12
US 2021083865 A1,2021.03.18
CN 108123795 A,2018.06.05

审查员 李文聪

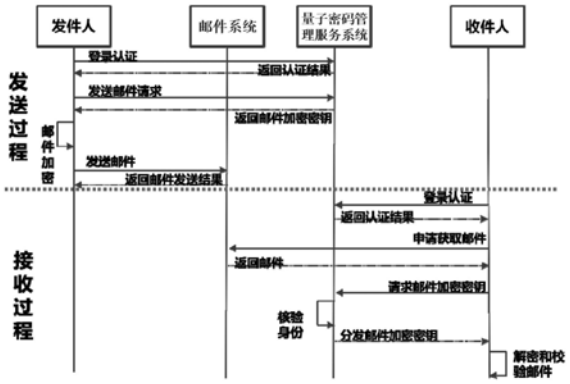
权利要求书3页 说明书16页 附图4页

(54)发明名称

一种基于量子安全密钥的邮件传输系统和传输方法

(57)摘要

本发明提供了一种基于量子安全密钥的邮件传输系统和传输方法,包括:邮箱系统;量子随机数发生器;量子交换密码机,预先存储有密钥;量子密钥充注机,与量子交换密码机的输出端连接;量子密码管理服务系统,用于提供邮件加密密钥以及身份认证功能;量子安全芯片,存储量子安全密钥,每个量子安全芯片内存储的密钥和量子交换密码机内预先存储的密钥是对称密钥,量子安全芯片中的安全密钥通过网络和量子密码管理服务系统进行对称实体认证;内置或者外接有量子安全芯片的邮件收发设备。采用上述技术方案,解决网络攻击日益严峻的环境对邮箱收发环境的威胁,防范未来量子计算机和量子算法带来的安全威胁,并且方案易于实现。



CN 113285803 B

1.一种基于量子安全密钥的邮件传输方法,采用基于量子安全密钥的邮件传输系统,该基于量子安全密钥的邮件传输系统包括:

邮箱系统,用于提供收发邮件的功能;

量子随机数发生器,用于生成量子密钥;

量子交换密码机,用于提供密钥服务,量子交换密码机内预先存储有密钥,并存储在该量子交换密码机内,与量子安全芯片内的密钥为对称密钥;

量子安全芯片,存储量子安全密钥,每个量子安全芯片内存储的密钥和量子交换密码机内预先存储的密钥是对称密钥;

邮件收发设备,用于邮件的收发;

其特征在于:量子交换密码机接收量子随机数发生器发出的量子密钥,该密钥为量子随机数生成器预生成的密钥;量子密钥充注机,与量子交换密码机的输出端连接,用于充注量子密钥;量子密码管理服务系统,通过网络分别与邮箱系统和量子安全芯片实现数据交互,量子密码管理服务系统直接连接量子密码交换机,用于提供邮件加密密钥以及身份认证功能;量子安全芯片中的安全密钥通过网络和量子密码管理服务系统进行对称实体认证;所述量子安全芯片内置或者外接于该邮件收发设备;

该传输的方法包括下述步骤:

S1、发送或接收邮件前,邮件收发设备通过量子密码管理服务系统进行身份验证,邮件收发设备读取量子安全芯片内预置的量子安全密钥和量子密码管理服务系统进行对称实体身份认证,最后返回认证结果;

S2、用户经过步骤S1登录认证完成后,需要收发邮件时,发件人需要使用量子安全芯片中预置的密钥向量子密码管理服务系统提出申请获取邮件加密密钥,量子密码管理服务系统将使用预置的与量子安全芯片中预置的密钥的对称密钥对邮件加密密钥进行加密后发送给收件人,邮件系统收到对邮件加密密钥进行加密的邮件后进行平台存储,收件人使用邮件收发设备内置量子安全密钥对邮件加密密钥进行解密,获取邮件加密密钥,并发送邮件。

2.如权利要求1所述的基于量子安全密钥的邮件传输方法,其特征在于:步骤S1中对称实体身份认证的具体过程为:

S11、用户在邮件收发设备上打开邮箱应用,输入账号密码进行邮箱应用的登录授权,登录邮箱;

S12、邮件收发设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T15843.2标准基于对称密钥进行实体认证,用户登录认证完后进入步骤S2。

3.如权利要求1或2所述的基于量子安全密钥的邮件传输方法,其特征在于:步骤S1中对称实体身份认证的具体过程为:

S12a、检测内置于邮件收发设备的量子安全芯片是否在量子密码管理服务系统登录有效期内,在有效期内的,直接进入步骤S2,不在有效期内的,其邮件收发设备通过内置的量子安全芯片和量子密码管理服务系统基于对称密钥进行实体认证;

S12b、用户登录认证过程完成,每次认证后量子密码管理服务系统的登录有效期为预先设置时间。

4.如权利要求1所述的基于量子安全密钥的邮件传输方法,其特征在于:步骤S1中对称

实体身份认证的具体过程为：

步骤S121、用户登录完成后邮件收发设备自动向量子安全芯片发送认证请求；

步骤S122、量子安全芯片返回量子密钥及该量子密钥所在的序列Z-1至邮件收发设备；

步骤S123、邮件收发设备发送认证请求以及量子安全芯片返回的量子密钥序列Z-1至量子密码管理服务系统；

步骤S124、量子密码管理服务系统通过量子密钥交换密码机查找所述量子密钥序列Z-1对应的密钥；

步骤S125、量子密钥交换密码机返回所述量子密钥序列Z-1对应的密钥，即对称密钥至量子密码管理服务系统；

步骤S126、量子密码管理服务系统采用约好的方案，用所述量子密钥序列Z-1对应的密钥加密发送给邮件收发设备，用于验证量子密码管理服务系统是本人；

步骤S127、邮件收发设备采用约好的方案，使用所述量子密钥序列Z-1对应的密钥加密发送给量子密码管理服务系统，用于验证邮件收发设备是本人；

步骤S128、双方通过均验证后，量子密码管理服务系统加密发送认证结果至邮件收发设备。

5.如权利要求1所述的基于量子安全密钥的邮件传输方法，其特征在于：步骤S2中发送加密过程为：

S211、发件人使用发送端邮件收发设备在本地编辑完成本地邮件；

S212、发送方邮件收发设备选取量子安全芯片内密码序列为Z的密钥B，将邮件号和密码序列Z一起发送给量子密码管理服务系统，申请获得邮件加密密钥；

S213、量子密码管理服务系统使用量子随机数生成器生成安全的随机的邮件加密密码M，量子密码管理服务系统通过量子交换密码机存放的量子安全密钥找到密码序列为Z的对称密钥B'，使用对称密钥B'对邮件加密密码M进行加密，产生加密后的邮件加密密码$M^{B'}$；

S214、量子密码管理服务系统将已使用对称密钥B'加密后的邮件加密密码$M^{B'}$发送至邮件发送方的邮件收发设备；

S215、发送方的邮件收发设备接收到加密后的邮件加密密码$M^{B'}$，使用和对称密钥B'对称的密钥B进行解密，得到邮件加密密码M；

S216:发送方将加密邮件使用哈希算法生成消息摘要γ；

S217:发送方的邮件收发设备使用邮件加密密码M对本地邮件和消息摘要γ一起加密成加密邮件包；

S218:发送方邮件收发设备将邮件号、收件人信息、收件人验证码β、消息摘要γ使用序列为Z+1的量子密钥对称C加密发送给量子密码管理服务系统；

S219:量子密码管理服务系统根据邮件号和步骤S1认证的发件人的信息生成发件人验证码α'；

S220:发送方邮件收发设备将加密后的邮件包、收发件人信息和邮件号一起发送至邮件系统，邮件系统收到加密后的邮件进行存储。

6.如权利要求4所述的基于量子安全密钥的邮件传输方法，其特征在于：步骤S2中接收解密过程为：

S221:接收方邮件收发设备从邮箱系统接收到加密后的邮件，加密后的邮件包括加密

后的邮件包、收发件人信息和邮件号；

S222:接收方邮件收发设备根据发件人信息和邮件号生成发件人验证码α”；

S223:接收方邮件收发设备选取量子安全芯片内密码序列为Z的密钥D,将邮件号、密码序列Z一起发送给量子密码管理服务系统,申请获得邮件加密密钥；

S224:量子密码管理服务系统通过邮件号搜索到邮件加密密码M、发件人验证码α’和邮件消息摘要γ；

S225:量子密码管理服务系统使用接收方邮件收发设备提供的收件人信息和邮件号生成收件人验证码β”,对比验证β”和存储在量子密码管理服务系统内部的收件人验证码β’是否一致；

S226:量子密码管理服务系统通过量子交换密码机存放的量子安全密钥找到密码序列为Z的对应密钥D’,使用密钥D’对邮件加密密码M和量子密码管理服务系统内存储的邮件消息摘要γ’、发件人验证码α’进行加密；

S227:量子密码管理服务系统将已使用密钥D’加密的邮件加密密码M和邮件消息摘要γ’、发件人验证码α’发送至接收方邮件收发设备；

S228:接收方邮件收发设备使用本地对称密钥D对已加密的邮件加密密码M进行解密,获得邮件加密密码M、发件人验证码α’和邮件消息摘要γ’,使用邮件加密密码M对加密邮件内容进行解密,获得邮件正文和随邮件正文一起被加密的邮件消息摘要γ”；

S229:接收方比对邮件消息摘要γ’、发件人验证码α’和从邮件包中解密出来的邮件消息摘要γ”、步骤S222生成的发件人验证码α”,如果不一致,说明加密邮件有被篡改可能,或者发件方不可信,如果一致,说明该邮件可信；

S230:收件方获得解密后的可信邮件。

7.如权利要求1所述的一种基于量子安全密钥的邮件传输方法,其特征在于:量子安全芯片是SIM卡或U盘。

8.如权利要求1所述的一种基于量子安全密钥的邮件传输方法,其特征在于:量子安全芯片中的安全密钥为预先内置,量子安全芯片发卡的时候通过量子密钥充注机提前充注好,使用的量子安全芯片都有预置量子密码,每个量子安全芯片有自己的编号,每支量子密钥有自己的序列号,提供量子安全芯片的编号和量子密钥序列号,能在量子交换密码机内找到对应的密钥。

9.如权利要求1所述的一种基于量子安全密钥的邮件传输方法,其特征在于:所述邮件收发设备包括:手机、固定设备,邮箱用户与量子安全芯片预先绑定,一个邮箱用户绑定一个量子安全芯片。

一种基于量子安全密钥的邮件传输系统和传输方法

技术领域

[0001] 本申请属于安全应用类产品领域,特别涉及一种基于量子密钥的安全邮箱身份认证和邮件加密的系统及方法。

背景技术

[0002] 目前,网络攻击日益严峻的环境对邮箱收发环境构成威胁,其中包括:邮件收发方实体的身份认证问题,邮件传输、存储过程中邮件内容被窃取的问题,邮件传输过程中可能存在的收发件人篡改和邮件信息篡改问题。

[0003] 申请日:2019.09.24,申请号:CN201910904251.5的专利申请公开了一种基于量子数字签名的邮件系统及收发方法,为了保证发送信息的真实性,在信息发送前往往会通过特定的签名算法(如Hash算法)来进行消息的签名。将计算得出的签名信息附在消息后面一起发送给服务器,之后接收端在获取消息的内容进行相同的计算,并将计算的结果同发送端后面携带的签名信息进行比较。如果两者相同说明消息内容没有被篡改过,否则说明消息有可能遭到篡改。该申请中的系统采用三层结构:物理层、密钥层、应用层;物理层为密钥产生终端,负责实时产生用来进行签名的密钥串;密钥层用来存储物理层产生的密钥串,并在需要的时候向上层应用层提供所需要的密钥;应用层是邮件系统收发的软件部分,通过从密钥层中提取物理层生成的密钥来对所需要发送的信息进行加密。邮件收发方法包括量子密钥分发阶段、邮件签名阶段、签名验证阶段。该发明同算法签名相比,通过量子数字签名加密之后的邮件的安全性得到了更为有力的保障。但是该方法舍去了复杂的签名密码算法,使用量子数字签名的方式,依据量子力学原理提升了邮件的真实性和不可否认性,但是没有对邮件加密安全性本身进行提升。同时该方法需要在应用层的终端之间对量子密钥进行交换,且没有详细叙述量子密钥的交换过程,在交换的过程中密钥存在暴露风险。

[0004] 申请日:2019.04.24申请号:CN201910331987.8的专利申请公开了一种基于量子密钥公共云服务平台的邮件安全传输方法,涉及量子保密通信技术领域,包括步骤:量子密钥公共云服务平台从量子密钥分发QKD设备获取量子密钥并存储;待进行邮件传输的客户端A和客户端B之间协商生成配对验证码;所述客户端A和客户端B向量子密钥公共云服务平台发送下载量子密钥的请求消息;量子密钥公共云服务平台接收中客户端A和客户端B所发送的下载量子密钥的请求消息,并匹配验证码,配对成功则分发量子密钥,进入下一步,配对失败则提示配对错误;客户端A对邮件加密并发送给公共邮件服务器,客户端B从公共邮件服务器接收已加密的邮件并解密。本发明实现了电子邮件加密信息在网络中传输的绝对安全性。该专利采用JAVA中的random方法生成伪随机数,即其随机数由伪随机数生成器生成。且该方法将量子密钥生成量子密钥压缩包,由收发件方进行下载解压获取量子密钥,压缩下发过程安全性不可信。另外,客户端AB两方都发送验证码,平台进行比对,有极高的安全风险,可被中间人攻击。

[0005] 未来量子计算机和量子算法也可能带来安全威胁,其中包括:基于大因数分解难题的公钥密码算法被破译问题,量子计算机带来的安全威胁以及量子算法对已有密码体系

的威胁。

[0006] 并且现有邮件传输系统还需要第三方的大量参与,这样会提高人力成本。

发明内容

[0007] 本发明所要解决的技术问题在于如何解决网络攻击日益严峻的环境对邮箱收发环境的威胁。

[0008] 本发明通过以下技术手段实现解决上述技术问题的:一种基于量子安全密钥的邮件传输系统,包括:

[0009] 邮箱系统,用于提供收发邮件的功能;

[0010] 量子随机数发生器,用于生成量子密钥;

[0011] 量子交换密码机,接收量子随机数发生器发出的量子密钥,用于提供密钥服务,量子交换密码机内预先存储有密钥,该密钥为量子随机数生成器预生成的密钥,并存储在该量子交换密码机内,与量子安全芯片内的密钥为对称密钥;

[0012] 量子密钥充注机,与量子交换密码机的输出端连接,用于充注量子密钥;

[0013] 量子密码管理服务系统,通过网络分别与邮箱系统和量子安全芯片实现数据交互,量子密码管理服务系统直接连接量子密码交换机,用于提供邮件加密密钥以及身份认证功能;

[0014] 量子安全芯片,存储量子安全密钥,每个量子安全芯片内存储的密钥和量子交换密码机内预先存储的密钥是对称密钥,量子安全芯片中的安全密钥通过网络和量子密码管理服务系统进行对称实体认证;

[0015] 邮件收发设备,用于邮件的收发,所述量子安全芯片内置或者外接于该邮件收发设备。

[0016] 采用上述技术方案,解决网络攻击日益严峻的环境对邮箱收发环境的威胁,具体为解决邮件收发方实体的身份认证问题:使用量子安全芯片内置的量子对称密钥进行身份认证,一次认证一份密钥。

[0017] 采用上述技术方案,防范未来量子计算机和量子算法带来的安全威胁,具体为防范基于大因数分解难题的公钥密码算法被破译问题:使用量子对称密钥,无法通过大因数分解来破译;

[0018] 并且该技术方案易于实现,量子安全芯片是可行的存在的技术,基于量子对称密钥的安全认证也是可以实现的技术。

[0019] 作为优化的技术方案,量子安全芯片是SIM卡或U盘。

[0020] 作为优化的技术方案,量子安全芯片中的安全密钥为预先内置,量子安全芯片发卡的时候通过量子密钥充注机提前充注好,使用的量子安全芯片都有预置量子密码,每个量子安全芯片有自己的编号,每支量子密钥有自己的序列号,提供量子安全芯片的编号和量子密钥序列号,能在量子交换密码机内找到对应的密钥。

[0021] 作为优化的技术方案,所述邮件收发设备包括:手机、固定设备,邮箱用户与量子安全芯片预先绑定,一个邮箱用户绑定一个量子安全芯片。

[0022] 本发明还提供了一种采用上述任一方案所述的基于量子安全密钥的邮件传输系统进行邮件传输的方法,包括下述步骤:

[0023] S1、发送或接收邮件前，邮件收发设备通过量子密码管理服务系统进行身份验证，邮件收发设备读取量子安全芯片内预置的量子安全密钥和量子密码管理服务系统进行对称实体身份认证，最后返回认证结果；

[0024] S2、用户经过步骤S1登录认证完成后，需要收发邮件时，发件人需要使用量子安全芯片中预置的密钥向量子密码管理服务系统提出申请获取邮件加密密钥，量子密码管理服务系统将使用预置的与量子安全芯片中预置的密钥的对称密钥对邮件加密密钥进行加密后发送给收件人，邮件系统收到对邮件加密密钥进行加密的邮件后进行平台存储，收件人使用邮件收发设备内置量子安全密钥对邮件加密密钥进行解密，获取邮件加密密钥，并发送邮件。

[0025] 作为优化的技术方案，步骤S1中对称实体身份认证的具体过程为：

[0026] S11、用户在邮件收发设备上打开邮箱应用，输入账号密码进行邮箱应用的登录授权，登录邮箱；

[0027] S12、邮件收发设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T15843.2标准基于对称密钥进行实体认证，用户登录认证完后进入步骤S2。

[0028] 7.如权利要求5或6所述的基于量子安全密钥的邮件传输系统进行邮件传输的方法，其特征在于：步骤S1中对称实体身份认证的具体过程为：

[0029] S12a、检测内置于邮件收发设备的量子安全芯片是否在量子密码管理服务系统登录有效期内，在有效期内的，直接进入步骤S2，不在有效期内的，其邮件收发设备通过内置的量子安全芯片和量子密码管理服务系统基于对称密钥进行实体认证；

[0030] S12b、用户登录认证过程完成，每次认证后量子密码管理服务系统的登录有效期为预先设置时间。

[0031] 作为优化的技术方案，步骤S1中对称实体身份认证的具体过程为：

[0032] 步骤S121、用户登录完成后邮件收发设备自动向量子安全芯片发送认证请求；

[0033] 步骤S122、量子安全芯片返回量子密钥及该量子密钥所在的序列Z-1至邮件收发设备；

[0034] 步骤S123、邮件收发设备发送认证请求以及量子安全芯片返回的量子密钥序列Z-1至量子密码管理服务系统；

[0035] 步骤S124、量子密码管理服务系统通过量子密钥交换密码机查找所述量子密钥序列Z-1对应的密钥；

[0036] 步骤S125、量子密钥交换密码机返回所述量子密钥序列Z-1对应的密钥，即对称密钥至量子密码管理服务系统；

[0037] 步骤S126、量子密码管理服务系统采用约好的方案，用所述量子密钥序列Z-1对应的密钥加密发送给邮件收发设备，用于验证量子密码管理服务系统是本人；

[0038] 步骤S127、邮件收发设备采用约好的方案，使用所述量子密钥序列Z-1对应的密钥加密发送给量子密码管理服务系统，用于验证邮件收发设备是本人；

[0039] 步骤S128、双方通过均验证后，量子密码管理服务系统加密发送认证结果至邮件收发设备。

[0040] 作为优化的技术方案，步骤S2中发送加密过程为：

[0041] S211、发件人使用发送端邮件收发设备在本地编辑完成本地邮件；

[0042] S212、发送方邮件收发设备选取量子安全芯片内密码序列为Z的密钥B，将邮件号和密码序列Z一起发送给量子密码管理服务系统，申请获得邮件加密密钥；

[0043] S213、量子密码管理服务系统使用量子随机数生成器生成安全的随机的邮件加密密码M，量子密码管理服务系统通过量子交换密码机存放的量子安全密钥找到密码序列为Z的对称密钥B'，使用对称密钥B'对邮件加密密码M进行加密，产生加密后的邮件加密密码$M^{B'}$；

[0044] S214、量子密码管理服务系统将已使用对称密钥B'加密后的邮件加密密码$M^{B'}$发送至邮件发送方的邮件收发设备；

[0045] S215、发送方的邮件收发设备接收到加密后的邮件加密密码$M^{B'}$，使用和对称密钥B'对称的密钥B进行解密，得到邮件加密密码M；

[0046] S216:发送方将加密邮件使用哈希算法生成消息摘要γ；

[0047] S217:发送方的邮件收发设备使用邮件加密密码M对本地邮件和消息摘要γ一起加密成加密邮件包；

[0048] S218:发送方邮件收发设备将邮件号、收件人信息、收件人验证码β、消息摘要γ使用序列为Z+1的量子密钥对称C加密发送给量子密码管理服务系统；

[0049] S219:量子密码管理服务系统根据邮件号和步骤S1认证的发件人的信息生成发件人验证码α'；

[0050] S220:发送方邮件收发设备将加密后的邮件包、收发件人信息和邮件号一起发送至邮件系统，邮件系统收到加密后的邮件进行存储。

[0051] 作为优化的技术方案，步骤S2中接收解密过程为：

[0052] S221:接收方邮件收发设备从邮箱系统接收到加密后的邮件，加密后的邮件包括加密后的邮件包、收发件人信息和邮件号；

[0053] S222:接收方邮件收发设备根据发件人信息和邮件号生成发件人验证码α"；

[0054] S223:接收方邮件收发设备选取量子安全芯片内密码序列为Z的密钥D，将邮件号、密码序列Z一起发送给量子密码管理服务系统，申请获得邮件加密密钥；

[0055] S224:量子密码管理服务系统通过邮件号搜索到邮件加密密码M、发件人验证码α'和邮件消息摘要γ；

[0056] S225:量子密码管理服务系统使用接收方邮件收发设备提供的收件人信息和邮件号生成收件人验证码β"，对比验证β"和存储在量子密码管理服务系统内部的收件人验证码β'是否一致；

[0057] S226:量子密码管理服务系统通过量子交换密码机存放的量子安全密钥找到密码序列为Z的对应密钥D'，使用密钥D'对邮件加密密码M和量子密码管理服务系统内存储的邮件消息摘要γ'、发件人验证码α'进行加密；

[0058] S227:量子密码管理服务系统将已使用密钥D'加密的邮件加密密码M和邮件消息摘要γ'、发件人验证码α'发送至接收方邮件收发设备；

[0059] S228:接收方邮件收发设备使用本地对称密钥D对已加密的邮件加密密码M进行解密，获得邮件加密密码M、发件人验证码α'和邮件消息摘要γ'，使用邮件加密密码M对加密邮件内容进行解密，获得邮件正文和随邮件正文一起被加密的邮件消息摘要γ"；

[0060] S229:接收方比对邮件消息摘要γ'、发件人验证码α'和从邮件包中解密出来的邮

件消息摘要γ”、步骤S222生成的发件人验证码α”，如果不一致，说明加密邮件有被篡改可能，或者发件方不可信，如果一致，说明该邮件可信；

[0061] S230：收件方获得解密后的可信邮件。

[0062] 本发明的优点在于：

[0063] 1、本发明使用量子密码管理服务系统来进行身份认证和分发邮件加密密码，增加了安全性。

[0064] (1)解决网络攻击日益严峻的环境对邮箱收发环境的威胁：

[0065] ①解决邮件收发方实体的身份认证问题：使用量子安全芯片内置的量子对称密钥进行身份认证，一次认证一份密钥。

[0066] ②解决邮件传输、存储过程中邮件内容被窃取的问题：邮件以密文传输，以密文存储，加密密钥为量子密码管理服务系统生成的通过量子密码技术安全下发的量子真随机密钥。即使邮件被截取，攻击者只能得到密文，无法得到信息。

[0067] ③解决邮件传输过程中可能存在的收发件人篡改和邮件内容篡改问题：量子密码管理服务系统可对收发件人进行验证码认证，确保收发件人真实。实体间使用哈希算法(如国密SM3)对邮件内容进行消息摘要，并使用邮件加密密码通过一次一密的方式进行加密传输存储，在解密邮件后进行核对，规避内容篡改风险。

[0068] (2)防范未来量子计算机和量子算法带来的安全威胁；

[0069] ①防范基于大因数分解难题的公钥密码算法被破译问题：使用量子对称密钥，无法通过大因数分解来破译；

[0070] ②防范未来出现的量子计算机带来的安全威胁：使用量子安全密码进行加密传输，传输过程理论上是完全安全可信的；

[0071] ③防范未来可能出现的量子算法对已有密码体系的威胁：使用量子安全密码进行加密传输，量子安全密钥是通过量子随机数生成器生成的真随机数，无法通过算法来破译。

[0072] (3)无需数字证书的第三方颁发和认证；

[0073] ①提供无证书的认证方式，减少第三方的参与：使用基于对称密码的实体认证协议进行使用者双方的实体认证，无需颁发证书的第三方。减少过程的参与方，减少三方协议风险。

[0074] 2、易于实现、通用性强、延展性好

[0075] (1)开发技术易于实现

[0076] 量子安全芯片是可行的存在的技术，基于量子对称密钥的安全认证也是可以实现的技术，用于加密邮件的邮件加密密码可以使用量子随机数生成，技术成熟，安全性高。

[0077] (2)通用性强、延展性好

[0078] 本发明对邮箱系统自身进行改造的地方极少，主要是通过增加量子密钥服务系统的方式对安全性进行提升，通用性强。本发明可以集成到量子安全服务平台上，对外提供功能接口，延展性好。

[0079] 3、经济效益

[0080] (1)网络安全能力得到显著提升

[0081] 本发明可以针对现有的攻击方式以及未来可能有的量子计算威胁进行防御，可极大减少因信息泄露带来的经济损失。

[0082] (2)邮箱安全服务升级

[0083] 本发明可以极大增强邮件的安全性,提供更加优质安全的邮件通信服务。如对已有3W用户(10元/月)的邮件系统进行改造,改造前收入收益30W元/月,改造后服务升级月租为15元/月,改造后收入收益为45W/月。

[0084] (3)改造成本低

[0085] 本发明可以在现有系统上进行改造,平台侧几乎无改造量,应用端进行对接即可,改造成本低。

附图说明

[0086] 图1是本发明实施例基于量子安全密钥对邮箱进行认证和加密的系统架构图;

[0087] 图2是本发明实施例基于量子安全密钥对邮箱进行认证和加密的系统工作时序图;

[0088] 图3是本发明实施例中的登录认证流程图;

[0089] 图4是本发明实施例中的身份认证具体流程图;

[0090] 图5是本发明实施例中的发送加密流程图;

[0091] 图6是本发明实施例中的量子密钥管理服务系统的存储流程图;

[0092] 图7是本发明实施例中的邮件系统的存储流程图;

[0093] 图8是本发明实施例中的接收解密流程图。

具体实施方式

[0094] 为使本发明实施例的目的、技术方案和优点更加清楚,下面将结合本发明实施例,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0095] 实施例一基于量子安全密钥的邮件传输方法

[0096] 如图1所示,该实施例公开一种基于量子安全密钥的邮件的传输方法,使用基于量子安全密钥的邮件的传输系统,该系统包括:

[0097] 邮箱系统,用于提供收发邮件的功能;

[0098] 量子随机数发生器,用于生成量子密钥;

[0099] 量子交换密码机,接收量子随机数发生器发出的量子密钥,用于提供密钥服务,量子交换密码机内预先存储有密钥,该密钥为量子随机数生成器预生成的密钥,并存储在该量子交换密码机内,与量子安全芯片内的密钥为对称密钥;

[0100] 量子密钥充注机,与量子交换密码机的输出端连接,用于充注量子密钥;

[0101] 量子密码管理服务系统,通过网络分别与邮箱系统和量子安全芯片实现数据交互,量子密码管理服务系统直接连接量子密码交换机,用于提供邮件加密密钥以及身份认证功能;

[0102] 量子安全芯片,存储量子安全密钥,量子安全芯片中的安全密钥通过网络和量子密码管理服务系统进行对称实体认证,量子安全芯片可以是SIM卡或U盘等形式,量子安全芯片中的安全密钥为预先内置,量子安全芯片发卡的时候就通过量子密钥充注机提前充注

好,使用的量子安全芯片都有预置量子密码,即原理为:量子安全芯片在使用前初始化(预充注密码),量子安全芯片通过量子密码充注机被充注量子安全密钥,每个量子安全芯片被充注的密钥和量子交换密码机内预置的密钥是对称密钥(即一一对应的密钥)。每个量子安全芯片有自己的编号,每支量子密钥有自己的序列号,只要提供量子安全芯片的编号和量子密钥序列号,就能在量子交换密码机内找到对应的密钥;

[0103] 邮件收发设备,用于邮件的收发,所述量子安全芯片内置或者外接于该邮件收发设备,所述邮件收发设备包括:手机、固定设备如电脑等,邮箱用户需要与量子安全芯片预先绑定,只有绑定邮箱用户可以使用内置该量子安全芯片的邮件收发设备发送邮件,理论上一个量子安全芯片可以绑定多个邮箱用户,或者一个邮箱用户可以与多个量子安全芯片进行绑定。但是出于安全性考虑,优选的,一个邮箱用户绑定一个量子安全芯片,即,同一个邮箱用户更换邮件收发设备后不可使用,或同一台邮件收发设备更换邮件用户后不可使用。

[0104] 如图2所示,基于量子安全密钥的邮件的传输方法包括下述步骤:

[0105] S1、发送或接收邮件前,邮件收发设备通过量子密码管理服务系统进行身份验证,邮件收发设备读取量子安全芯片内预置的量子安全密钥和量子密码管理服务系统进行对称实体身份认证,最后返回认证结果。

[0106] 所述对称实体身份认证可使用邮件收发设备的邮箱程序开启后,自动调用量子安全芯片,完成基于量子安全密钥的对称密钥的身份认证。

[0107] 如图3所示,对称实体身份认证的具体过程为:

[0108] S11、用户在邮件收发设备上打开邮箱应用,输入账号密码进行邮箱应用的登录授权,登录邮箱;

[0109] S12、邮件收发设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T15843.2标准基于对称密钥进行实体认证,用户登录认证完后进入步骤S2;

[0110] 实际操作中,每次登录都重新进行实体认证的话,实体认证过程复杂耗时长,用户体验差,所以作为优选的方案,设置登陆有效期,在登陆有效期内多次登录均不需要进行实体认证,具体步骤为:

[0111] S12a、检测内置于邮件收发设备的量子安全芯片是否在量子密码管理服务系统登录有效期内,在有效期内的,直接进入步骤S2,不在有效期内的,其邮件收发设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T 15843.2标准基于对称密钥进行实体认证;

[0112] S12b、用户登录认证过程完成,每次认证后量子密码管理服务系统的登录有效期可以设置为一个月。

[0113] 上述步骤S12a中,如果邮件收发设备内置的量子安全芯片和邮件用户进行了一一绑定,也可检测该邮件用户是否在有效期内。

[0114] 参阅图4,上述邮件收发设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T 15843.2标准基于对称密钥进行实体认证的具体步骤如下:

[0115] 步骤S121、用户登录完成后邮件收发设备自动向量子安全芯片发送认证请求;

[0116] 步骤S122、量子安全芯片返回量子密钥及该量子密钥所在的序列Z-1至邮件收发设备;

[0117] 步骤S123、邮件收发设备发送认证请求以及量子安全芯片返回的量子密钥序列Z-1至量子密码管理服务系统；

[0118] 步骤S124、量子密码管理服务系统通过量子密钥交换密码机查找所述量子密钥序列Z-1对应的密钥；

[0119] 步骤S125、量子密钥交换密码机返回所述量子密钥序列Z-1对应的密钥，即对称密钥至量子密码管理服务系统；

[0120] 步骤S126、量子密码管理服务系统采用某种约好的方案如时间戳和设备物理地址，用所述量子密钥序列Z-1对应的密钥加密发送给邮件收发设备，用于验证量子密码管理服务系统是本人；

[0121] 步骤S127、邮件收发设备采用某种约好的方案如时间戳和设备物理地址，使用所述量子密钥序列Z-1对应的密钥加密发送给量子密码管理服务系统，用于验证邮件收发设备是本人，并不是别人截取信息后重新发送的申请；

[0122] 步骤S128、双方通过均验证后，量子密码管理服务系统加密发送认证结果至邮件收发设备。

[0123] 使用量子安全芯片预置的量子对称密钥进行身份认证，量子对称密钥是通过量子密钥充注机在发量子安全芯片时初始进行充注预置的，一次认证一份密钥，从而解决邮件收发实体的身份认证问题，并且无需颁发证书的第三方。减少过程的参与方，减少三方协议风险；

[0124] S2、用户经过步骤S1登录认证完成后，需要收发邮件时，发件人需要使用量子安全芯片中预置的密钥向量子密码管理服务系统提出申请获取邮件加密密钥，量子密码管理服务系统将使用预置的与量子安全芯片中预置的密钥的对称密钥对邮件加密密钥进行加密后发送给收件人，邮件系统收到对邮件加密密钥进行加密的邮件后进行平台存储，收件人使用邮件收发设备内置量子安全密钥可对邮件加密密钥进行解密，获取邮件加密密钥，并发送邮件。

[0125] 具体地说，如图5至7所示，发送加密过程为：

[0126] S211、发件人使用发送端邮件收发设备在本地编辑完成本地邮件；

[0127] S212、假定本次发送邮件为认证后的第一次邮件发送，则发送方邮件收发设备选取量子安全芯片内密码序列为Z的密钥B，将邮件号和密码序列Z一起发送给量子密码管理服务系统，申请获得邮件加密密钥，这里作为一个可选的规则，所有量子安全芯片内的密钥按照密钥顺序使用，如认证时使用的序列为Z-1的密钥，则本次选取序列为Z的密钥，下次选取的密钥的序列为Z+1，使用后的密钥舍弃，当然，也可以是其他的顺序，如果本次发送邮件为非认证后的第一次邮件发送，则使用相应次序的密码序列的密钥即可；

[0128] S213、量子密码管理服务系统使用量子随机数生成器生成安全的随机的邮件加密密码M，量子密码管理服务系统通过量子交换密码机存放的量子安全密钥找到密码序列为Z的对称密钥B'，使用对称密钥B'对邮件加密密码M进行加密，产生加密后的邮件加密密码$M^{B'}$；

[0129] S214、量子密码管理服务系统将已使用对称密钥B'加密后的邮件加密密码$M^{B'}$发送至邮件发送方的邮件收发设备；

[0130] S215、发送方的邮件收发设备接收到加密后的邮件加密密码$M^{B'}$，使用和对称密钥

B’对称的密钥B进行解密，得到邮件加密密码M；

[0131] S216:发送方将加密邮件使用哈希算法生成消息摘要γ，规避内容篡改风险；

[0132] S217:发送方的邮件收发设备使用邮件加密密码M对本地邮件和消息摘要γ一起加密成加密邮件包，使用邮件加密密码M进行加密传输存储，进一步规避内容篡改风险；

[0133] S218:发送方邮件收发设备将邮件号、收件人信息、收件人验证码β、消息摘要γ使用序列为Z+1的量子密钥对称C加密发送给量子密码管理服务系统，如图5所示，量子密码管理服务系统存储发收件人和邮件的对应关系，存储在量子密码管理服务系统内的收件人验证码表示为β’，收件人验证码是为了防止收件人信息在明文传输过程中被篡改(收件人信息必须明文传输)，收件人验证码是由收件人信息和邮件号通过哈希算法生成，并发送给量子密码管理服务系统，在验证收件人身份时，量子密码服务管理系统可使收件人信息(请求收件的收件人)和邮件号使用同样算法再次生成收件人验证码，并于先前存储的验证码进行比较，从而核实收件人的身份，β和β’的关系为，β’是β存储在量子密码管理服务系统后改名，其本质相同，这里及下面提到的收件人信息和发件人信息，预先设定的是收/发件人的账号，但是收/发件人账号和邮件收发设备为对应绑定的关系，所以也可以是邮件收发设备的信息；

[0134] S219:量子密码管理服务系统根据邮件号和步骤S1认证的发件人的信息生成发件人验证码α’；

[0135] S220:发送方邮件收发设备将加密后的邮件包、收发件人信息和邮件号一起发送至邮件系统，邮件系统收到加密后的邮件进行存储，邮件系统可以接收非加密邮件也可以接收加密邮件，如图5所示，邮件系统存储加密后的邮件包、收发件人信息和邮件号。

[0136] 邮件以密文传输，以密文存储，加密密钥为量子密码管理服务系统生成的量子真随机密钥。即使邮件被截取，攻击者只能得到密文，无法得到信息。

[0137] 从上述邮件发送过程可知，整个邮件发送过程总共会消耗三支密钥。①用来身份认证；②用来获取邮件加密密钥；③用来将邮件信息安全的送给量子密码管理服务系统。

[0138] 如图8所示，接收解密过程为：

[0139] 用户使用接收方邮件收发设备登陆邮箱并完成身份认证后，点击收取邮件，收取他人发送的加密邮件，并触发密钥获取流程。如果接收方邮件收发设备已经经过步骤S1的身份认证流程，则这里可以直接点击收取邮件，如果没有，则需要按照步骤S11-S13完成身份认证，量子密码管理服务系统使用接收方邮件收发设备在量子交换密码机内存放的密钥将本封邮件的加密下发至接收方邮件收发设备，接收方邮件收发设备在本地进行解密读取。

[0140] 具体步骤为：

[0141] S221:接收方邮件收发设备从邮箱系统接收到加密后的邮件，加密后的邮件包括加密后的邮件包、收发件人信息和邮件号；

[0142] S222:接收方邮件收发设备根据发件人信息和邮件号生成发件人验证码α”；

[0143] S223:接收方邮件收发设备选取量子安全芯片内密码序列为Z的密钥D，将邮件号、密码序列Z一起发送给量子密码管理服务系统，申请获得邮件加密密钥；

[0144] S224:量子密码管理服务系统通过邮件号搜索到邮件加密密码M、发件人验证码α’和邮件消息摘要γ；

[0145] S225:量子密码管理服务系统使用接收方邮件收发设备提供的收件人信息和邮件号生成收件人验证码β”,对比验证β”和存储在量子密码管理服务系统内部的收件人验证码β’是否一致;

[0146] S226:量子密码管理服务系统通过量子交换密码机存放的量子安全密钥找到密码序列为Z的对应密钥D’,使用密钥D’对邮件加密密码M和量子密码管理服务系统内存储的邮件消息摘要γ’、发件人验证码α’进行加密,为了方便辨别,存储在量子密码管理服务系统内的数值均记为’,该邮件消息摘要γ’对应上述邮件消息摘要γ;

[0147] S227:量子密码管理服务系统将已使用密钥D’加密的邮件加密密码M和邮件消息摘要γ’、发件人验证码α’发送至接收方邮件收发设备;

[0148] S228:接收方邮件收发设备使用本地对称密钥D对已加密的邮件加密密码M进行解密,获得邮件加密密码M、发件人验证码α’和邮件消息摘要γ’。使用邮件加密密码M对加密邮件内容进行解密,获得邮件正文和随邮件正文一起被加密的邮件消息摘要γ”;

[0149] S229:接收方比对邮件消息摘要γ’、发件人验证码α’和从邮件包中解密出来的邮件消息摘要γ”、步骤S222生成的发件人验证码α”。如果不一致,说明加密邮件有被篡改可能,或者发件方不可信。如果一致,说明该邮件可信;

[0150] S230:收件方获得解密后的可信邮件。

[0151] 采用上述验证码的验证方式:

[0152] 1、无须发送方和接收方两方都发送验证码,只需要根据发件人信息和邮件号重新生成发件人验证码与之前存储的发件人验证码进行比对,对发件人进行验证,防止他人伪造发件人信息;或根据收件人信息和邮件号重新生成收件人验证码与之前存储的收件人验证码进行比对,对收件人进行验证,防止无权限用户获取邮件信息;对邮件内容进行验证,防止邮件内容被篡改;从而可对发件人、收件人和邮件本身进行验证,防止邮件和身份伪造。

[0153] 2、同时验证码的验证方式均为加密传输,传输过程安全,避免了验证码被中间人攻击的风险,更加保障了邮件收发的安全性。

[0154] 3、平台侧的验证码为根据信息生成,可防止中间人攻击风险。

[0155] 4、证码由平台和收发件方自行生成,无需对邮箱系统进行改造适配,所以该验证方法的适用性高。

[0156] 实施例二基于量子安全密钥的发送邮件的加密方法,应用于邮件发送设备

[0157] 该实施例公开一种基于量子安全密钥的发送邮件的加密方法,应用于邮件发送设备。

[0158] 邮件发送设备,用于邮件的发送,内置或者外接有量子安全芯片。

[0159] 量子安全芯片,存储量子安全密钥,量子安全芯片中的安全密钥通过网络和量子密码管理服务系统进行对称实体认证,量子安全芯片可以是SIM卡或U盘等形式,量子安全芯片中的安全密钥为预先内置,量子安全芯片发卡的时候就通过量子密钥充注机提前充注好,使用的量子安全芯片都有预置量子密码,即原理为:量子安全芯片在使用前初始化(预充注密码),量子安全芯片通过量子密码充注机被充注量子安全密钥,每个量子安全芯片被充注的密钥和量子交换密码机内预置的密钥是对称密钥(即一一对应的密钥)。每个量子安全芯片有自己的编号,每支量子密钥有自己的序列号,只要提供量子安全芯片的编号和量

子密钥序列号，就能在量子交换密码机内找到对应的密钥；

[0160] 所述邮件发送设备包括：手机、固定设备如电脑等，邮箱用户需要与量子安全芯片预先绑定，只有绑定邮箱用户可以使用内置该量子安全芯片的邮件发送设备发送邮件，理论上一个量子安全芯片可以绑定多个邮箱用户，或者一个邮箱用户可以与多个量子安全芯片进行绑定。但是出于安全性考虑，优选的，一个邮箱用户绑定一个量子安全芯片，即，同一个邮箱用户更换邮件发送设备后不可使用，或同一台邮件发送设备更换邮件用户后不可使用。

[0161] 基于量子安全密钥的发送邮件的加密方法，应用于邮件发送设备，包括下述步骤：

[0162] S1’、发送邮件前，邮件发送设备通过量子密码管理服务系统进行身份验证，邮件发送设备读取量子安全芯片内预置的量子安全密钥和量子密码管理服务系统进行对称实体身份认证，最后返回认证结果。

[0163] 所述对称实体身份认证可使用邮件发送设备的邮箱程序开启后，自动调用量子安全芯片，完成基于量子安全密钥的对称密钥的身份认证。

[0164] 对称实体身份认证的具体过程为：

[0165] S11’、用户在邮件发送设备上打开邮箱应用，输入账号密码进行邮箱应用的登录授权，登录邮箱；

[0166] S12’、邮件发送设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T15843.2标准基于对称密钥进行实体认证，用户登录认证完后进入步骤S2’；

[0167] 实际操作中，每次登录都重新进行实体认证的话，实体认证过程复杂耗时长，用户体验差，所以作为优选的方案，设置登陆有效期，在登陆有效期内多次登录均不需要进行实体认证，具体步骤为：

[0168] S12’a、检测内置于邮件发送设备的量子安全芯片是否在量子密码管理服务系统登录有效期内，在有效期内的，直接进入步骤S2，不在有效期内的，其邮件发送设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T 15843.2标准基于对称密钥进行实体认证；

[0169] S12’b、用户登录认证过程完成，每次认证后量子密码管理服务系统的登录有效期可以设置为一个月。

[0170] 上述步骤S12’a中，如果邮件发送设备内置的量子安全芯片和邮件用户进行了一一绑定，也可检测该邮件用户是否在有效期内。

[0171] 上述邮件发送设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T15843.2标准基于对称密钥进行实体认证的具体步骤如下：

[0172] 步骤S121’、用户登录完成后邮件发送设备自动向量子安全芯片发送认证请求；

[0173] 步骤S122’、量子安全芯片返回量子密钥及该量子密钥所在的序列Z-1至邮件发送设备；

[0174] 步骤S123’、邮件发送设备发送认证请求以及量子安全芯片返回的量子密钥序列Z-1至量子密码管理服务系统；

[0175] 步骤S124’、邮件发送设备接收量子密码管理服务系统发送过来的用所述量子密钥序列Z-1对应的密钥加密的某种约好的方案，如时间戳和设备物理地址，用于验证量子密码管理服务系统是本人；

[0176] 步骤S125’、邮件发送设备采用某种约好的方案如时间戳和设备物理地址，使用所述量子密钥序列Z-1对应的密钥加密发送给量子密码管理服务系统，量子密码管理服务系统用于验证邮件发送设备是本人，并不是别人截取信息后重新发送的申请；

[0177] 步骤S126’、双方通过均验证后，邮件发送设备收到量子密码管理服务系统加密发送认证结果。

[0178] 使用量子安全芯片预置的量子对称密钥进行身份认证，量子对称密钥是通过量子密钥充注机在发量子安全芯片时初始进行充注预置的，一次认证一份密钥，从而解决邮件发送实体的身份认证问题，并且无需颁发证书的第三方。减少过程的参与方，减少三方协议风险；

[0179] S2’、用户经过步骤S1登录认证完成后，需要发送邮件时，发件人需要使用量子安全芯片中预置的密钥向量子密码管理服务系统提出申请获取邮件加密密钥，并发送邮件。

[0180] 具体地说，发送加密过程为：

[0181] S211’、发件人使用邮件发送设备在本地编辑完成本地邮件；

[0182] S212’、假定本次发送邮件为认证后的第一次邮件发送，则邮件发送设备选取量子安全芯片内密码序列为Z的密钥B，将邮件号和密码序列Z一起发送给量子密码管理服务系统，申请获得邮件加密密钥，这里作为一个可选的规则，所有量子安全芯片内的密钥按照密钥顺序使用，如认证时使用的序列为Z-1的密钥，则本次选取序列为Z的密钥，下次选取的密钥的序列为Z+1，使用后的密钥舍弃，当然，也可以是其他的顺序，如果本次发送邮件为非认证后的第一次邮件发送，则使用相应次序的密码序列的密钥即可；

[0183] S213’、邮件发送设备收到量子密码管理服务系统返回的使用对称密钥B’加密后的邮件加密密码$M^{B'}$；

[0184] S215’、邮件发送设备接收到加密后的邮件加密密码$M^{B'}$后，使用和对称密钥B’对称的密钥B进行解密，得到邮件加密密码M；

[0185] S216’:发送方将加密邮件使用哈希算法生成消息摘要γ，规避内容篡改风险；

[0186] S217’:邮件发送设备使用邮件加密密码M对本地邮件和消息摘要γ一起加密成加密邮件包，使用邮件加密密码M进行加密传输存储，进一步规避内容篡改风险；

[0187] S218’:邮件发送设备将邮件号、收件人信息、收件人验证码β、消息摘要γ使用序列为Z+1的量子密钥对称C加密发送给量子密码管理服务系统，量子密码管理服务系统存储发收件人和邮件的对应关系，存储在量子密码管理服务系统内的收件人验证码表示为β’，收件人验证码是为了防止收件人信息在明文传输过程中被篡改(收件人信息必须明文传输)，收件人验证码是由收件人信息和邮件号通过哈希算法生成，并发送给量子密码管理服务系统，在验证收件人身份时，量子密码服务管理系统可使收件人信息(请求收件的收件人)和邮件号使用同样算法再次生成收件人验证码，并于先前存储的验证码进行比较，从而核实收件人的身份，β和β’的关系为，β’是β存储在量子密码管理服务系统后改名，其本质相同，这里及下面提到的收件人信息和发件人信息，预先设定的是收/发件人的账号，但是收/发件人账号和邮件发送设备为对应绑定的关系，所以也可以是邮件发送设备的信息；

[0188] S219’:邮件发送设备将加密后的邮件包、收发件人信息和邮件号一起发送至邮件系统，邮件系统收到加密后的邮件进行存储，邮件系统可以接收非加密邮件也可以接收加密邮件，邮件系统存储加密后的邮件包、收发件人信息和邮件号。

[0189] 邮件以密文传输，以密文存储，加密密钥为量子密码管理服务系统生成的量子真随机密钥。即使邮件被截取，攻击者只能得到密文，无法得到信息。

[0190] 从上述邮件发送过程可知，整个邮件发送过程总共会消耗三支密钥。①用来身份认证；②用来获取邮件加密密钥；③用来将邮件信息安全的送给量子密码管理服务系统。

[0191] 上面所述的量子密码管理服务系统，通过网络分别与邮箱系统和量子安全芯片实现数据交互，用于提供邮件加密密钥以及身份认证功能。

[0192] 实施例三基于量子安全密钥的接收邮件的解密方法，应用于邮件接收设备

[0193] 该实施例公开一种基于量子安全密钥的接收邮件的解密方法，应用于邮件接收设备。

[0194] 邮件接收设备，用于邮件的接收，内置或者外接有量子安全芯片。

[0195] 量子安全芯片，存储量子安全密钥，量子安全芯片中的安全密钥通过网络和量子密码管理服务系统进行对称实体认证，量子安全芯片可以是SIM卡或U盘等形式，量子安全芯片中的安全密钥为预先内置，量子安全芯片发卡的时候就通过量子密钥充注机提前充注好，使用的量子安全芯片都有预置量子密码，即原理为：量子安全芯片在使用前初始化(预充注密码)，量子安全芯片通过量子密码充注机被充注量子安全密钥，每个量子安全芯片被充注的密钥和量子交换密码机内预置的密钥是对称密钥(即一一对应的密钥)。每个量子安全芯片有自己的编号，每支量子密钥有自己的序列号，只要提供量子安全芯片的编号和量子密钥序列号，就能在量子交换密码机内找到对应的密钥；

[0196] 所述邮件接收设备包括：手机、固定设备如电脑等，邮箱用户需要与量子安全芯片预先绑定，只有绑定邮箱用户可以使用内置该量子安全芯片的邮件接收设备接收邮件，理论上一个量子安全芯片可以绑定多个邮箱用户，或者一个邮箱用户可以与多个量子安全芯片进行绑定。但是出于安全性考虑，优选的，一个邮箱用户绑定一个量子安全芯片，即，同一个邮箱用户更换邮件接收设备后不可使用，或同一台邮件接收设备更换邮件用户后不可使用。

[0197] 基于量子安全密钥的接收邮件的解密方法，应用于邮件接收设备，包括下述步骤：

[0198] S1”、接收邮件前，邮件接收设备通过量子密码管理服务系统进行身份验证，邮件接收设备读取量子安全芯片内预置的量子安全密钥和量子密码管理服务系统进行对称实体身份认证，最后返回认证结果。

[0199] 所述对称实体身份认证可使用邮件接收设备的邮箱程序开启后，自动调用量子安全芯片，完成基于量子安全密钥的对称密钥的身份认证。

[0200] 对称实体身份认证的具体过程为：

[0201] S11”、用户在邮件接收设备上打开邮箱应用，输入账号密码进行邮箱应用的登录授权，登录邮箱；

[0202] S12”、邮件接收设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T15843.2标准基于对称密钥进行实体认证，用户登录认证完后进入步骤S2”；

[0203] 实际操作中，每次登录都重新进行实体认证的话，实体认证过程复杂耗时长，用户体验差，所以作为优选的方案，设置登陆有效期，在登陆有效期内多次登录均不需要进行实体认证，具体步骤为：

[0204] S12”a、检测内置于邮件接收设备的量子安全芯片是否在量子密码管理服务系统

登录有效期内，在有效期内的，直接进入步骤S2”，不在有效期内的，其邮件接收设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T 15843.2标准基于对称密钥进行实体认证；

[0205] S12”b、用户登录认证过程完成，每次认证后量子密码管理服务系统的登录有效期可以设置为一个月。

[0206] 上述步骤S12”a中，如果邮件接收设备内置的量子安全芯片和邮件用户进行了一一绑定，也可检测该邮件用户是否在有效期内。

[0207] 上述邮件接收设备通过内置的量子安全芯片和量子密码管理服务系统使用GB/T15843.2标准基于对称密钥进行实体认证的具体步骤如下：

[0208] 步骤S121”、用户登录完成后邮件接收设备自动向量子安全芯片发送认证请求；

[0209] 步骤S122”、量子安全芯片返回量子密钥及该量子密钥所在的序列Z-1至邮件接收设备；

[0210] 步骤S123”、邮件接收设备发送认证请求以及量子安全芯片返回的量子密钥序列Z-1至量子密码管理服务系统；

[0211] 步骤S124”、邮件接收设备接收量子密码管理服务系统发送过来的用所述量子密钥序列Z-1对应的密钥加密的某种约好的方案，如时间戳和设备物理地址，用于验证量子密码管理服务系统是本人；

[0212] 步骤S125”、邮件接收设备采用某种约好的方案如时间戳和设备物理地址，使用所述量子密钥序列Z-1对应的密钥加密发送给量子密码管理服务系统，用于验证邮件接收设备是本人，并不是别人截取信息后重新发送的申请；

[0213] 步骤S126”、双方通过均验证后，量子密码管理服务系统加密发送认证结果至邮件接收设备。

[0214] 使用量子安全芯片预置的量子对称密钥进行身份认证，量子对称密钥是通过量子密钥充注机在发量子安全芯片时初始进行充注预置的，一次认证一份密钥，从而解决邮件收发实体的身份认证问题，并且无需颁发证书的第三方。减少过程的参与方，减少三方协议风险；

[0215] S2”、用户经过步骤S1”登录认证完成后，需要接收邮件时，收件人需要使用量子安全芯片中预置的密钥向量子密码管理服务系统提出申请获取邮件加密密钥。

[0216] 具体地说，接收解密过程为：

[0217] 收件人使用邮件接收设备登陆邮箱并完成身份认证后，点击收取邮件，收取他人发送的加密邮件，并触发密钥获取流程，邮件接收设备收到密钥后在本地进行解密读取。

[0218] 具体步骤为：

[0219] S221”：邮件接收设备从邮箱系统接收到加密后的邮件，加密后的邮件包括加密后的邮件包、收发件人信息和邮件号；

[0220] S222”：邮件接收设备根据发件人信息和邮件号生成发件人验证码α”；

[0221] S223”：邮件接收设备选取量子安全芯片内密码序列为Z的密钥D，将邮件号、密码序列Z一起发送给量子密码管理服务系统，申请获得邮件加密密钥；

[0222] S224”：邮件接收设备接收量子密码管理服务系统使用密钥D的对称密钥D’加密的邮件加密密码M和邮件消息摘要γ’、发件人验证码α’；

[0223] S225”:邮件接收设备使用本地对称密钥D对已加密的邮件加密密码M进行解密,获得邮件加密密码M、发件人验证码α’和邮件消息摘要γ’。使用邮件加密密码M对加密邮件内容进行解密,获得邮件正文和随邮件正文一起被加密的邮件消息摘要γ”;

[0224] S226”:收件人比对邮件消息摘要γ’、发件人验证码α’和从邮件包中解密出来的邮件消息摘要γ”、步骤S222”生成的发件人验证码α”。如果不一致,说明加密邮件有被篡改可能,或者发件人不可信。如果一致,说明该邮件可信;

[0225] S230”:收件方获得解密后的可信邮件。

[0226] 实施例四基于量子安全密钥的邮件传输过程中防篡改的方法

[0227] 针对基于量子安全密钥的邮件传输过程中邮件内容有可能被篡改的问题,本实施例提供了一种防篡改的方法,主要是通过验证码的比对来验证邮件是否被篡改,具体包括邮件发送时的验证码生成以及邮件接收时的验证码生成和比对。

[0228] 邮件发送时的验证码生成:

[0229] 步骤1:发送方邮件收发设备将邮件号、收件人信息、收件人验证码β、消息摘要γ使用序列为Z+1的量子密钥对称C加密发送给量子密码管理服务系统,量子密码管理服务系统存储发收件人和邮件的对应关系,存储在量子密码管理服务系统内的收件人验证码表示为β’,收件人验证码是为了防止收件人信息在明文传输过程中被篡改(收件人信息必须明文传输),收件人验证码是由收件人信息和邮件号通过哈希算法生成,并发送给量子密码管理服务系统,在验证收件人身份时,量子密码服务管理系统可使收件人信息(请求收件的收件人)和邮件号使用同样算法再次生成收件人验证码,并于先前存储的验证码进行比较,从而核实收件人的身份,β和β’的关系为,β’是β存储在量子密码管理服务系统后改名,其本质相同,这里及下面提到的收件人信息和发件人信息,预先设定的是收/发件人的账号,但是收/发件人账号和邮件收发设备为对应绑定的关系,所以也可以是邮件收发设备的信息;

[0230] 步骤2:量子密码管理服务系统根据邮件号和步骤S1认证的发件人的信息生成发件人验证码α’;

[0231] 邮件接收时的验证码生成和比对:

[0232] 步骤3:接收方邮件收发设备根据发件人信息和邮件号生成发件人验证码α”;

[0233] 步骤4:量子密码管理服务系统使用接收方邮件收发设备提供的收件人信息和邮件号生成收件人验证码β”,对比验证β”和存储在量子密码管理服务系统内部的收件人验证码β’是否一致;

[0234] 步骤5:量子密码管理服务系统使用密钥对邮件加密密码和量子密码管理服务系统内存储的邮件消息摘要γ’、发件人验证码α’进行加密,为了方便辨别,存储在量子密码管理服务系统内的数值均记为’;

[0235] 步骤6:量子密码管理服务系统将已使用密钥加密的邮件加密密码和邮件消息摘要γ’、发件人验证码α’发送至接收方邮件收发设备;

[0236] 步骤7:接收方邮件收发设备使用本地对称密钥对已加密的邮件加密密码进行解密,获得邮件加密密码、发件人验证码α’和邮件消息摘要γ’。使用邮件加密密码M对加密邮件内容进行解密,获得邮件正文和随邮件正文一起被加密的邮件消息摘要γ”;

[0237] 步骤8:接收方比对邮件验证码γ’、发件人验证码α’和从邮件包中解密出来的邮件消息摘要γ”、步骤3生成的发件人验证码α”。如果不一致,说明加密邮件有被篡改可能,

或者发件方不可信。如果一致，说明该邮件可信。

[0238] 采用上述验证码的验证方式：

[0239] 1、无须发送方和接收方两方都发送验证码，只需要根据发件人信息和邮件号重新生成发件人验证码与之前存储的发件人验证码进行比对，对发件人进行验证，防止他人伪造发件人信息；或根据收件人信息和邮件号重新生成收件人验证码与之前存储的收件人验证码进行比对，对收件人进行验证，防止无权限用户获取邮件信息；对邮件内容进行验证，防止邮件内容被篡改；从而可对发件人、收件人和邮件本身进行验证，防止邮件和身份伪造。

[0240] 2、同时验证码的验证方式均为加密传输，传输过程安全，避免了验证码被中间人攻击的风险，更加保障了邮件收发的安全性。

[0241] 3、平台侧的验证码为根据信息生成，可防止中间人攻击风险。

[0242] 4、证码由平台和收发件方自行生成，无需对邮箱系统进行改造适配，所以该验证方法的适用性高。

[0243] 以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

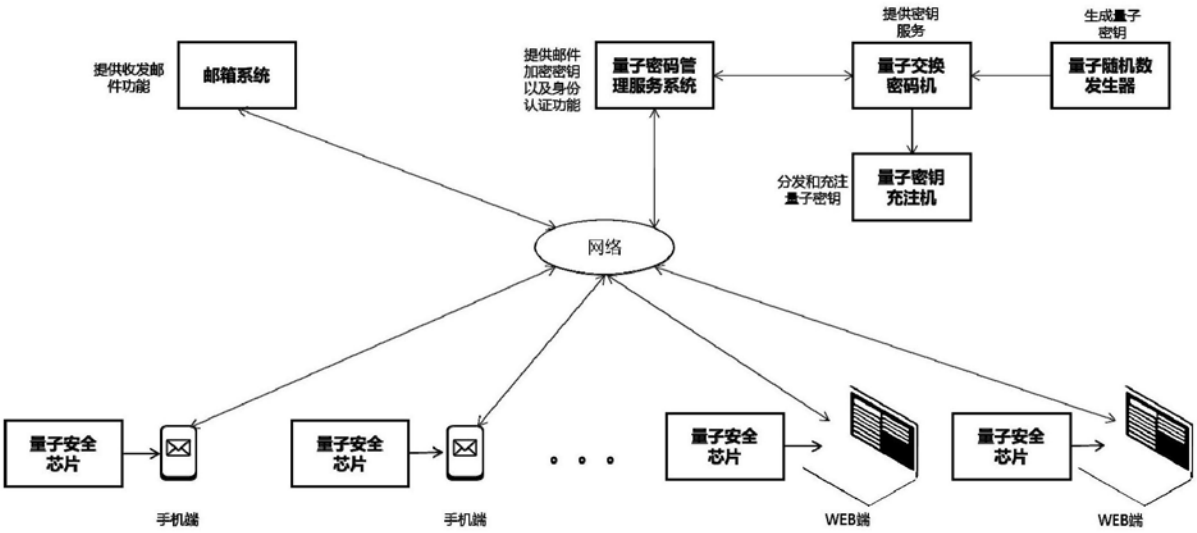

提供收发邮件功能
邮箱系统
提供邮件加密密钥以及身份认证功能
量子密码管理服务系统
提供密钥服务
量子交换密码机
生成量子密钥
量子随机数发生器
分发和充注量子密钥
量子密钥充注机
网络
量子安全芯片
手机端
量子安全芯片
手机端
量子安全芯片
WEB端
量子安全芯片
WEB端

图1

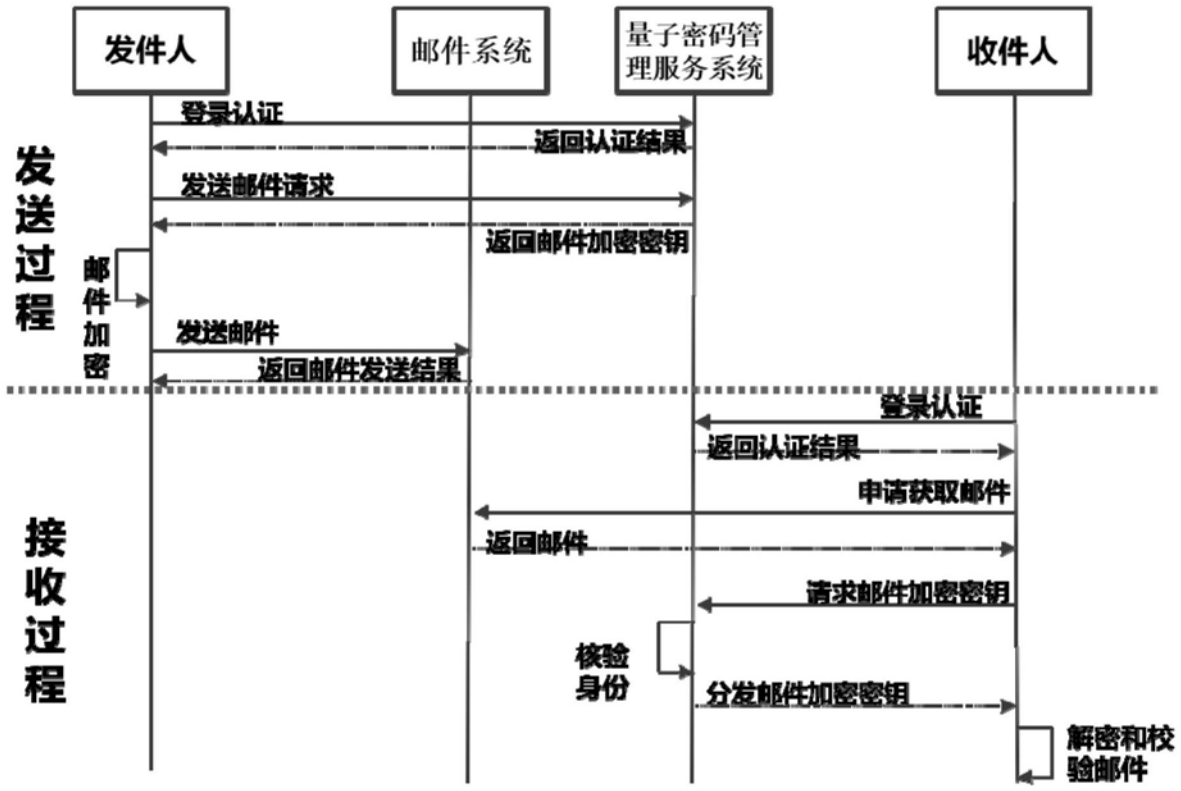

发件人
邮件系统
量子密码管理服务系统
收件人
发送过程
登录认证
返回认证结果
发送邮件请求
返回邮件加密密钥
邮件加密
发送邮件
返回邮件发送结果
接收过程
登录认证
返回认证结果
申请获取邮件
返回邮件
请求邮件加密密钥
核验身份
分发邮件加密密钥
解密和校验邮件

图2

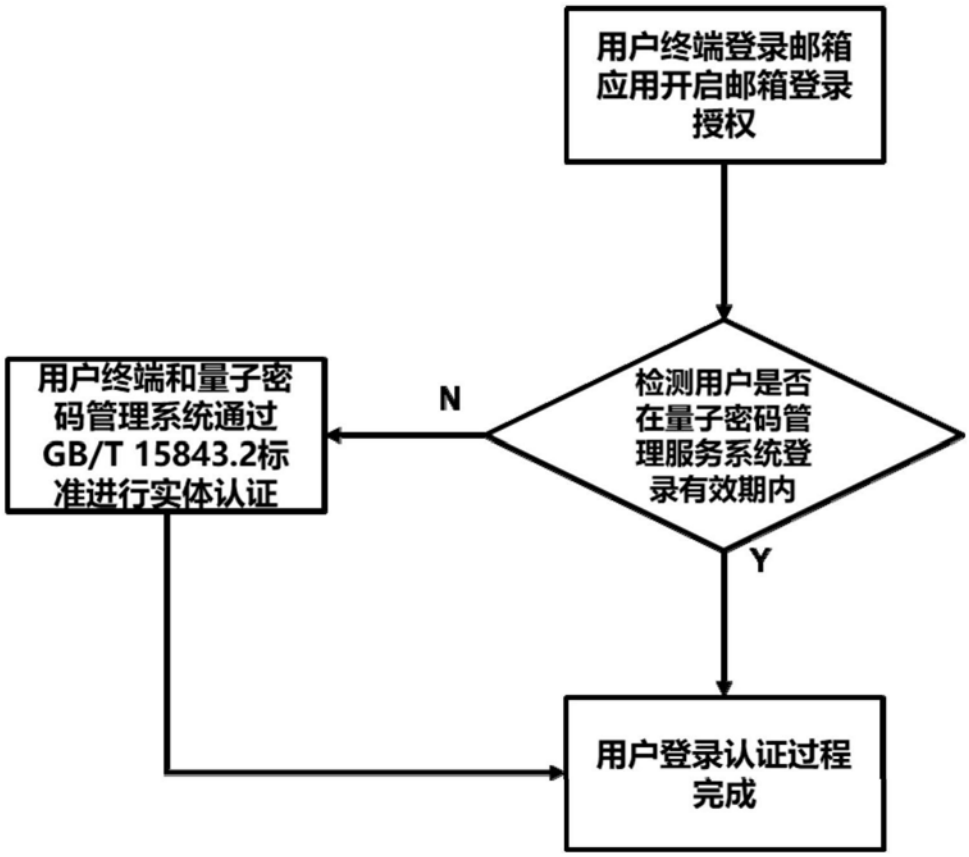

用户终端登录邮箱应用开启邮箱登录授权
检测用户是否在量子密码管理服务系统登录有效期内
N
Y
用户终端和量子密码管理系统通过GB/T 15843.2标准进行实体认证
用户登录认证过程完成

图3

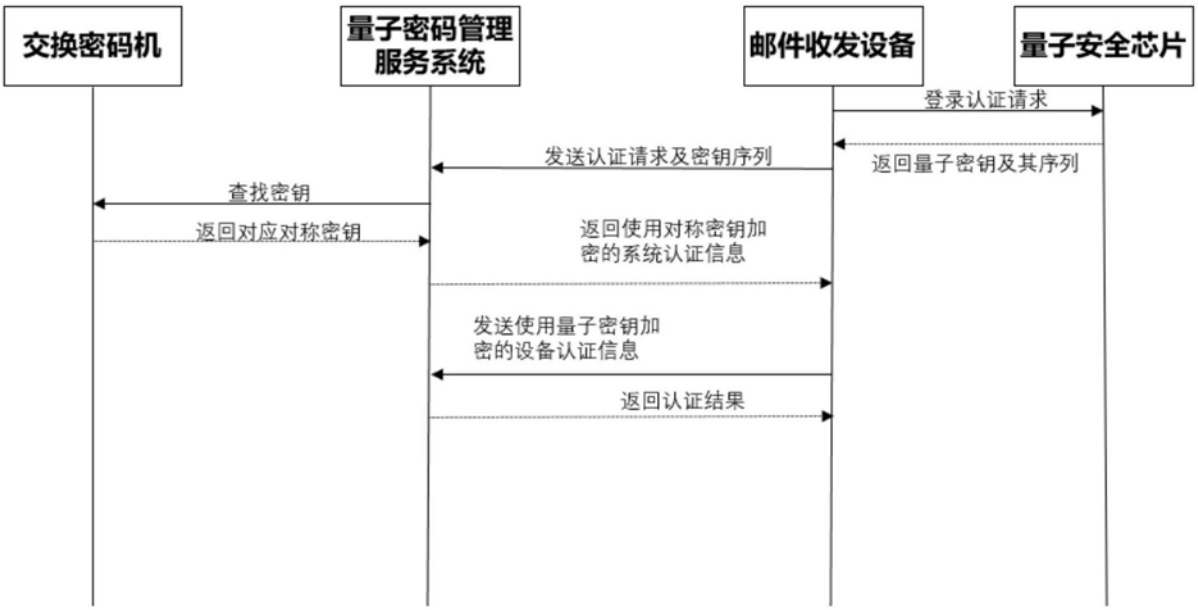

交换密码机
量子密码管理服务系统
邮件收发设备
量子安全芯片
登录认证请求
返回量子密钥及其序列
发送认证请求及密钥序列
查找密钥
返回对应对称密钥
返回使用对称密钥加密的系统认证信息
发送使用量子密钥加密的设备认证信息
返回认证结果

图4

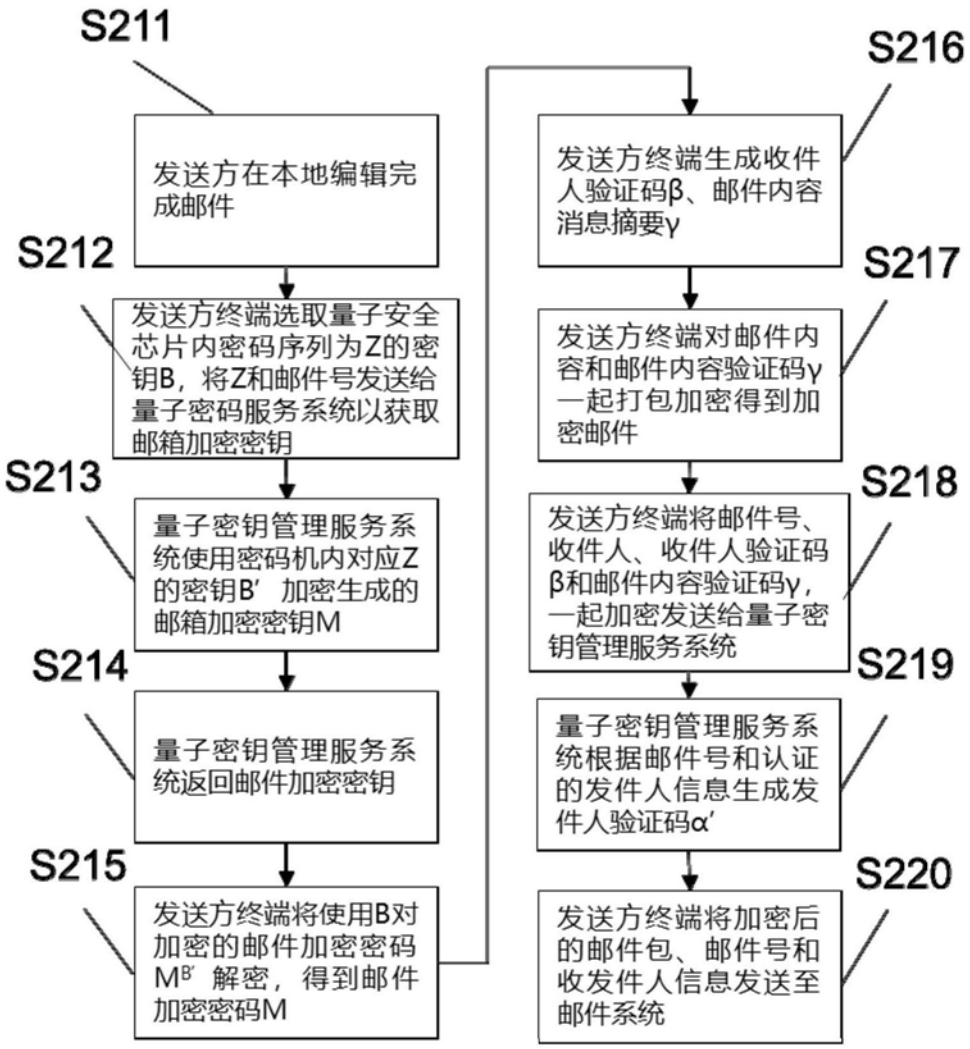

S211
发送方在本地编辑完成邮件
S212
发送方终端选取量子安全芯片内密码序列为Z的密钥B，将Z和邮件号发送给量子密码服务系统以获取邮箱加密密钥
S213
量子密钥管理服务系统使用密码机内对应Z的密钥B′ 加密生成的邮箱加密密钥M
S214
量子密钥管理服务系统返回邮件加密密钥
S215
发送方终端将使用B对加密的邮件加密密码 $M^{B'}$ 解密，得到邮件加密密码M
S216
发送方终端生成收件人验证码β、邮件内容消息摘要γ
S217
发送方终端对邮件内容和邮件内容验证码γ一起打包加密得到加密邮件
S218
发送方终端将邮件号、收件人、收件人验证码β和邮件内容验证码γ，一起加密发送给量子密钥管理服务系统
S219
量子密钥管理服务系统根据邮件号和认证的发件人信息生成发件人验证码α′
S220
发送方终端将加密后的邮件包、邮件号和收发件人信息发送至邮件系统

图5

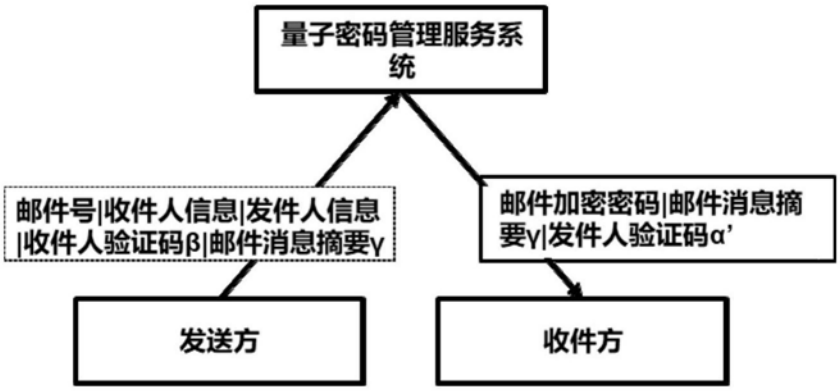

量子密码管理服务系统
邮件号|收件人信息|发件人信息|收件人验证码β|邮件消息摘要γ
邮件加密密码|邮件消息摘要γ|发件人验证码α'
发送方
收件方

图6

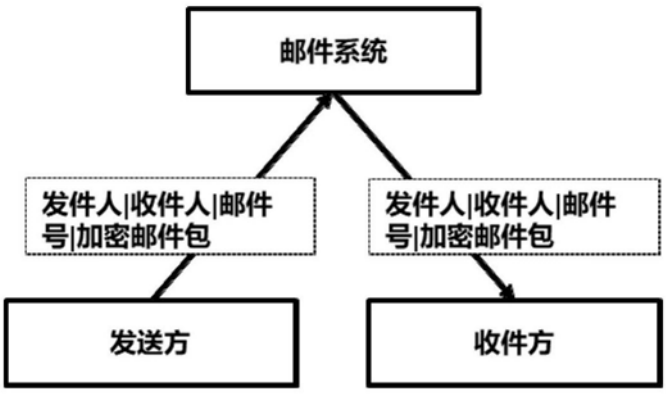

邮件系统
发件人|收件人|邮件号|加密邮件包
发件人|收件人|邮件号|加密邮件包
发送方
收件方

图7

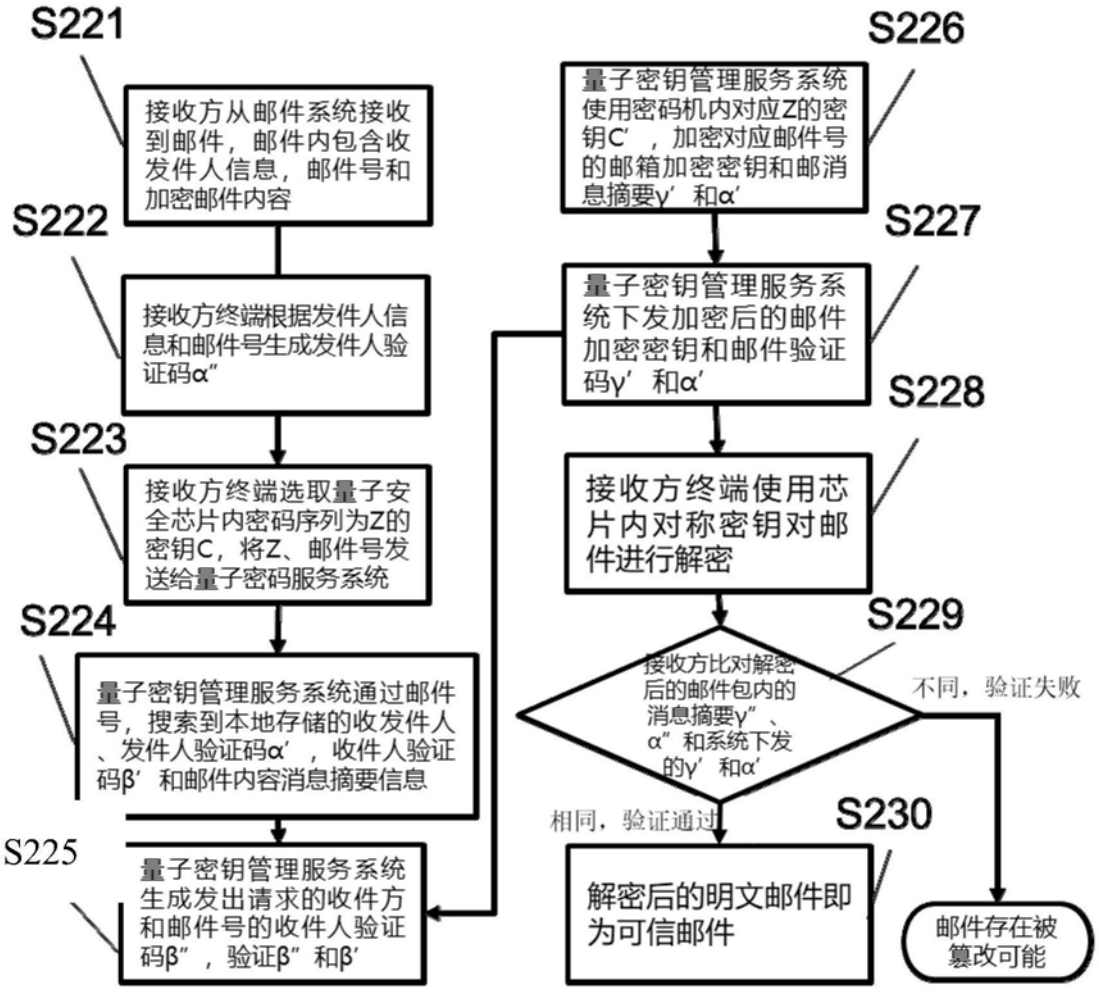

S221
接收方从邮件系统接收到邮件，邮件内包含收发件人信息，邮件号和加密邮件内容
S222
接收方终端根据发件人信息和邮件号生成发件人验证码α″
S223
接收方终端选取量子安全芯片内密码序列为Z的密钥C，将Z、邮件号发送给量子密码服务系统
S224
量子密钥管理服务系统通过邮件号，搜索到本地存储的收发件人、发件人验证码α′，收件人验证码β′和邮件内容消息摘要信息
S225
量子密钥管理服务系统生成发出请求的收件方和邮件号的收件人验证码β″，验证β″和β′
S226
量子密钥管理服务系统使用密码机内对应Z的密钥C′，加密对应邮件号的邮箱加密密钥和邮消息摘要γ′和α′
S227
量子密钥管理服务系统下发加密后的邮件加密密钥和邮件验证码γ′和α′
S228
接收方终端使用芯片内对称密钥对邮件进行解密
S229
接收方比对解密后的邮件包内的消息摘要γ″、α″和系统下发的γ′和α′
不同，验证失败
相同，验证通过
S230
解密后的明文邮件即为可信邮件
邮件存在被篡改可能

图8