(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 116016417 A
(43)申请公布日 2023.04.25

(21)申请号 202310005900.4

(22)申请日 2023.01.04

(71)申请人 深圳市中达为科技有限公司
地址 518000 广东省深圳市南山区南头街道南联社区北环大道11008号豪方天际广场写字楼3301

(72)发明人 彭莎莎 祝鹏 陈琰 汪红刚 李钊

(74)专利代理机构 深圳市正威知识产权代理事务所(特殊普通合伙) 44643
专利代理师 周军

(51)Int.Cl.
H04L 51/42(2022.01)
H04L 9/08(2006.01)

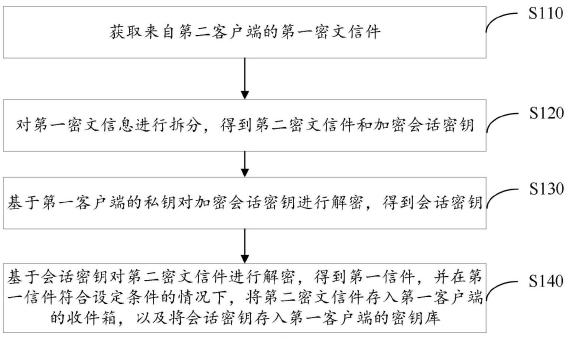
权利要求书2页 说明书9页 附图5页

(54)发明名称

信件处理方法、装置、电子设备及存储介质

(57)摘要

本公开实施例提供无需人工干预的邮箱公钥认证和上传方法。公钥交换服务是加密通信的关键，本实例解决的是在普通用户免操作的情况下认证并上传公钥的问题。认证和公钥上传是由邮箱客户端1和云服务2合作完成完成。邮箱客户端1先发送认证请求去云服务2，云服务2会发送验证邮件到客户邮箱，邮箱客户端1读取客户邮箱中认证邮件，通过认证邮件中的内容完成公钥的上传服务。



CN 116016417 A

1.一种密钥处理方法,其特征在于,应用于第一客户端,所述方法包括:

在用户在第一客户端上登录其用户帐号的情况下,向密钥服务器发送密钥对注册请求,以使所述密钥服务器向所述用户帐号对应的用户邮箱发送验证邮件;

从所述用户邮箱中获取所述验证邮件;

将所述验证邮件中的验证信息发送给所述密钥服务器,以使所述密钥密服务器根据其发送的验证邮件中的验证信息与从所述第一客户端接收到的验证信息进行比对,以确定是否返回认证成功信息给所述第一客户端;

在接收到所述密钥服务器返回的认证成功信息的情况下,将所述第一客户端的公钥上传至所述密钥服务器。

2.根据权利要求1所述的方法,其特征在于,还包括:

利用随机密码器生成所述第一客户端的密钥对,所述密钥对包括所述第一客户端的私钥和公钥;

在所述第一客户端中存储所述第一客户端的私钥和公钥。

3.根据权利要求1所述的方法,其特征在于,还包括:

响应于针对所述第一客户端的密钥更新请求,显示信息验证窗口;

基于向所述信息验证窗口输入的用户信息,确定所述密钥更新请求是否合法;

在确定所述密钥更新请求合法的情况下,利用所述随机密码器生成所述第一客户端的新密钥对,所述新密钥对包括所述第一客户端的新私钥和新公钥;

将所述第一客户端存储的私钥更新为所述第一客户端的新私钥;

向所述密钥服务器发送所述第一客户端的新公钥,以更新所述密钥服务器中的所述第一客户端的公钥。

4.根据权利要求3所述的方法,其特征在于,还包括:

在接收到所述第二客户端的新公钥的情况下,基于所述第二客户端的新公钥,对所述第一客户端中的属于所述第二客户端的公钥进行更新;其中,所述第二客户端的公钥用于加密所述第一客户端向所述第二客户端发送的邮件。

5.根据权利要求1所述的方法,其特征在于,还包括:

响应于向第二客户端发送第一信件的邮件发送请求,生成会话密钥,并从所述密钥服务器中获取第二客户端的公钥;

基于所述会话密钥对所述第一信件进行加密,得到第一密文信件;

基于所述第二客户端的公钥对所述会话密钥进行加密,得到加密会话密钥;

对所述第一密文信件和所述加密会话密钥进行拼接,得到第二密文信件;

向所述第二客户端发送所述第二密文信件。

6.一种密钥处理装置,其特征在于,应用于第一客户端,所述装置包括:

注册请求发送模块,用于在用户在第一客户端上登录其用户帐号的情况下,向密钥服务器发送密钥对注册请求,以使所述密钥服务器向所述用户帐号对应的用户邮箱发送验证邮件;

验证邮件获取模块,用于从所述用户邮箱中获取所述验证邮件;

验证信息发送模块,用于将所述验证邮件中的验证信息发送给所述密钥服务器,以使所述密钥密服务器根据其发送的验证邮件中的验证信息与从所述第一客户端接收到的验

证信息进行比对，以确定是否返回认证成功信息给所述第一客户端；

公钥上传模块，用于在接收到所述密钥服务器返回的认证成功信息的情况下，将所述第一客户端的公钥上传至所述密钥服务器。

7.根据权利要求6所述的装置，其特征在于，还包括：

密钥对生成模块，用于利用随机密码器生成所述第一客户端的密钥对，所述密钥对包括所述第一客户端的私钥和公钥；

密钥对存储模块，用于在所述第一客户端中存储所述第一客户端的私钥和公钥。

8.根据权利要求6所述的装置，其特征在于，还包括：

窗口显示模块，用于响应于针对所述第一客户端的密钥更新请求，显示信息验证窗口；

合法性确定模块，用于基于向所述信息验证窗口输入的用户信息，确定所述密钥更新请求是否合法；

密钥对生成模块，用于在确定所述密钥更新请求合法的情况下，利用所述随机密码器生成所述第一客户端的新密钥对，所述新密钥对包括所述第一客户端的新私钥和新公钥；

密钥对更新模块，用于将所述第一客户端存储的私钥更新为所述第一客户端的新私钥；

第一公钥更新模块，用于向所述密钥服务器发送所述第一客户端的新公钥，以更新所述密钥服务器中的所述第一客户端的公钥。

9.根据权利要求8所述的装置，其特征在于，还包括：

第二公钥更新模块，用于在接收到所述第二客户端的新公钥的情况下，基于所述第二客户端的新公钥，对所述第一客户端中的属于所述第二客户端的公钥进行更新；其中，所述第二客户端的公钥用于加密所述第一客户端向所述第二客户端发送的邮件。

10.根据权利要求9所述的装置，其特征在于，还包括：

密钥获取模块，用于响应于向第二客户端发送第一信件的邮件发送请求，生成会话密钥，并从所述密钥服务器中获取第二客户端的公钥；

信件加密模块，用于基于所述会话密钥对所述第一信件进行加密，得到第一密文信件；

密钥加密模块，用于基于所述第二客户端的公钥对所述会话密钥进行加密，得到加密会话密钥；

拼接模块，用于对所述第一密文信件和所述加密会话密钥进行拼接，得到第二密文信件；

密文信件发送模块，用于向所述第二客户端发送所述第二密文信件。

11.一种电子设备，包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行权利要求1-5中任一项所述的方法。

12.一种存储有计算机指令的非瞬时计算机可读存储介质，所述计算机指令用于使计算机执行权利要求1-5中任一项所述的方法。

信件处理方法、装置、电子设备及存储介质

技术领域

[0001] 本公开涉及人工智能技术领域，尤其涉及一种信件处理方法、装置、电子设备及存储介质。

背景技术

[0002] 随着互联网技术的发展，人们对网络信息的安全保护越来越重视。其中，邮件的安全传输是网络信息安全的一种。邮箱作为人们常见的通信工具，如果电子邮件被盗取，致使机密资源误入他人之手，这会对个人或者企业遭受经济或者其他方面的损失。因此，对于如何提高邮件的安全性，这是信息安全所要解决的一个技术问题。

发明内容

[0003] 本公开实施例提供一种信件处理方法、装置、电子设备及存储介质，以解决或缓解现有技术中的一项或更多项技术问题。

[0004] 作为本公开实施例的第一个方面，本公开实施例提供一种信件处理方法，包括：

[0005] 获取来自第二客户端的第一密文信件；

[0006] 对所述第一密文信息进行拆分，得到第二密文信件和加密会话密钥；

[0007] 基于所述第一客户端的私钥对所述加密会话密钥进行解密，得到会话密钥；

[0008] 基于所述会话密钥对所述第二密文信件进行解密，得到第一信件，并在所述第一信件符合设定条件的情况下，将所述第二密文信件存入所述第一客户端的收件箱，以及将所述会话密钥存入所述第一客户端的密钥库。

[0009] 作为本公开实施例的第二个方面，本公开实施例提供一种信件处理装置，包括：

[0010] 密文信件获取模块，用于获取来自第二客户端的第一密文信件；

[0011] 信件拆分模块，用于对所述第一密文信息进行拆分，得到第二密文信件和加密会话密钥；

[0012] 密钥解密模块，用于基于所述第一客户端的私钥对所述加密会话密钥进行解密，得到会话密钥；

[0013] 信件处理模块，用于基于所述会话密钥对所述第二密文信件进行解密，得到第一信件，并在所述第一信件符合设定条件的情况下，将所述第二密文信件存入所述第一客户端的收件箱，以及将所述会话密钥存入所述第一客户端的密钥库。

[0014] 作为本公开实施例的第三个方面，本公开实施例提供一种电子设备，包括：

[0015] 至少一个处理器；以及

[0016] 与所述至少一个处理器通信连接的存储器；其中，

[0017] 所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器能够执行本公开实施例提供的信件处理方法。

[0018] 作为本公开实施例的第四个方面，本公开实施例提供一种存储有计算机指令的非瞬时计算机可读存储介质，所述计算机指令用于使计算机执行本公开实施例提供的信息处

理方法。

[0019] 本公开实施例提供的技术方案，在接收密文信件时，先对密文信件中的加密会话密钥进行解密得到会话密钥，并利用会话密钥对密文信件进行解密，得到明文信件，然后判断明文信息是否符合设定的条件，如果符合，则认为该信件未被他人截取过，进而将其对应的密文信件存储在收件箱中，并将会话密钥存储在密钥库中。从而，当用户查看收件箱中的信件时，从密钥库中调取会话密钥对密文信件进行解密，得到明文信件。

[0020] 上述概述仅仅是为了说明书的目的，并不意图以任何方式进行限制。除上述描述的示意性的方面、实施方式和特征之外，通过参考附图和以下的详细描述，本公开进一步的方面、实施方式和特征将会是容易明白的。

附图说明

[0021] 在附图中，除非另外规定，否则贯穿多个附图相同的附图标记表示相同或相似的部件或元素。这些附图不一定是按照比例绘制的。应该理解，这些附图仅描绘了根据本公开的一些实施方式，而不应将其视为是对本公开范围的限制。

[0022] 图1是本公开一实施例的信件处理的流程图；

[0023] 图2是本公开另一实施例的信息处理方法的流程图；

[0024] 图3是本公开一实施例的密钥交换的示意图；

[0025] 图4是本公开一实施例的信件加密过程的流程图；

[0026] 图5是本公开一实施例的信件解密过程的流程图；

[0027] 图6是本公开一实施例的信件处理装置的结构框图；

[0028] 图7是本公开一实施例的电子设备的示意图。

具体实施方式

[0029] 在下文中，仅简单地描述了某些示例性实施例。正如本领域技术人员可认识到的那样，在不脱离本公开的精神或范围的情况下，可通过各种不同方式修改所描述的实施例。因此，附图和描述被认为本质上是示例性的而非限制性的。

[0030] 图1是本公开一实施例的信件处理方法的流程图。如图1所示，该信件处理方法可以应用于第一客户端，包括以下步骤：

[0031] S110，获取来自第二客户端的第一密文信件；

[0032] S120，对第一密文信息进行拆分，得到第二密文信件和加密会话密钥；

[0033] S130，基于第一客户端的私钥对加密会话密钥进行解密，得到会话密钥；

[0034] S140，基于会话密钥对第二密文信件进行解密，得到第一信件，并在第一信件符合设定条件的情况下，将第二密文信件存入第一客户端的收件箱，以及将会话密钥存入第一客户端的密钥库。

[0035] 在本示例中，在接收密文信件时，先对密文信件中的加密会话密钥进行解密得到会话密钥，并利用会话密钥对密文信件进行解密，得到明文信件，然后判断明文信息是否符合设定的条件，如果符合，则认为该信件未被他人截取过，进而将其对应的密文信件存储在收件箱中，并将会话密钥存储在密钥库中。从而，当用户查看收件箱中的信件时，从密钥库中调取会话密钥对密文信件进行解密，得到明文信件。

[0036] 示例性地，第一客户端在接收到第一密文信件时，即可执行上述步骤S120至S140。在这过程中，用户是无感的，不影响用户写信发信之类。

[0037] 示例性地，用户可以在第一客户端点击收信按扭，从而执行上述步骤S110至S140。

[0038] 示例性地，第一客户端可以是安装在一个终端设备上的邮件应用程序，第二客户端可以安装在另一个终端设备上的邮件应用程序。终端设备可以是手机、电脑、平板等。邮件应用程序可以是yahoo、gmail、outlook、homtmail等。

[0039] 示例性地，会话密钥是第二客户端生成的，其可以根据第一信件中的一些信息，例如，根据摘要、标题或者正文件中的某些段落生成会话密钥。会话密钥也可以是利用随机密码器随机生成。

[0040] 示例性地，在第一客户端与第二客户端建立加密信件的协议时，第一客户端生成密钥对，在本地存储私钥，并将公钥上传给密钥服务器。密钥服务器将公钥发送给第二客户端，第二客户端存储第一客户端的公钥。进而，在第二客户端利用会话密钥对第一信件进行加密时，利用第一客户端的公钥对会话密钥进行加密，并添加在加密后的信件中。从而，即使信件被盗取，由于其没有第一客户端的私钥，无法对会话密钥进行解密，进而无法对信件进行解密，提高信件的安全性。

[0041] 示例性地，由于加密会话密钥是通过第一客户端的公钥对会话密钥加密得到的，进而，利用第一客户端的私钥对加密会话密钥进行解密可以得到会话密钥。

[0042] 示例性地，由于第二密文信件是通过会话密钥对第一信件加密而得到的，因此，利用会话密钥对第二密文信件进行解密可以得到第一信件。

[0043] 在本示例性中，对解密得到的第一信件进行校验，以确定其是否被篡改。如果其不符合设定条件，则说明其被篡改，丢弃该信件。与此同时，可以向第二客户端发送一个拒信的通知，以使第二客户端将第一信件重新加密并重新发送。如果其符合设定条件，则说明其未被篡改，则可以将该信件投入收件箱当中。

[0044] 在本示例中，为了避免其他人看到用户的信件，可以将未解密的第二密文信件投入收件箱当中，并将信件的解密密钥，也就上述会话密钥存入密钥库。这样，当用户查看信件时，可以从密钥中提取密钥来对信件进行解密。

[0045] 示例性地，上述方法可以包括：

[0046] 响应于针对收件箱中的第二密文信件的查看请求，从密钥库中提取第二密文信件对应的会话密钥；

[0047] 基于会话密钥对第二密文信件进行解密，得到第一信件；

[0048] 在显示界面中展示第一信件。

[0049] 在本示例中，响应于针对第二密文信件的查看请求，如果当前时间距离用户上一次查看任意一个信件的时长大于设定阈值时，则退出登录并提供登录窗口给用户重新登录，待用户重新登录之后，此时即验证了用户是这个收件箱的合法用户，可以从从密钥库中提取第二密文信件对应的会话密钥来对第二密文信件进行解密并展示信件。

[0050] 如果当前时间距离用户上一次查看任意一个信件的时长小于设定阈值时，则保持当前的登录状态，直接从密钥库中提取第二密文信件对应的会话密钥来对第二密文信件进行解密并展示信件。

[0051] 在一些实施例中，第二客户端可以对解密的第一信件进行验证，其是否为假信件

或者被篡改过的信件。

[0052] 示例性地，在上述步骤S140中，上述基于会话密钥对第二密文信件进行解密，得到第一信件，并在第一信件符合设定条件的情况下，将第一密文信件存入第一客户端的收件箱，可以包括：

[0053] 基于会话密钥对第二密文信件进行解密，得到第二信件；

[0054] 对第二信件进行拆分，得到加密标记信息和第一信件；

[0055] 基于第二客户端的公钥对加密标记信息进行解密，得到标记信息，并在标记信息满足设定条件下，将第二密文信件存入第一客户端的收件箱，并将会话密钥存入第一客户端的密钥库。

[0056] 在本示例中，利用会话密钥对密文信件进行解密，得到第二信件，利用第一客户端的公钥对第二信件中的加密标记信息进行解密，得到标记信件，在标记信件满足设条件下，将第二密文信件存储到第二客户端的收件箱。这样可以避免假信件或者被篡改过的信件收入到收件箱。

[0057] 示例性地，在标记信息不满足设定条件下，将第二密文信件丢弃，并通知第一客户端该信件被拒收。这样，第一客户端在收到拒收信息时，可以重新发送信件。

[0058] 在本示例中，加密标记信息是由第二客户端利用其私钥对标记信息加密而成的，因此，利用第二客户端的公钥对加密标记信息进行解密可以得到标记信息。

[0059] 在一些实施例中，第二客户端在对标记信息进行加密之前，可以利用预定的算法对标记信息进行加密，因此，在判断标记信息是否符合设定条件时，也需要利用该算法进行判断。

[0060] 示例性地，上述基于第二客户端的公钥对加密标记信息进行解密，得到标记信息，并在标记信息满足设定条件下，将第二密文信件存入第一客户端的收件箱，并将会话密钥存入第一客户端的密钥库，可以包括：

[0061] 基于第二客户端的公钥对加密标记信息进行解密，得到第一标记；

[0062] 基于第一算法，对第一信件中的标记信息进行处理，得到第二标记；

[0063] 在第一标记和第二标记相同的情况下，将第二密文信件存入第一客户端的收件箱，并将会话密钥存入第一客户端的密钥库。

[0064] 在本示例中，可以进一步提高标记信息是否被篡改的识别准确率。

[0065] 示例性地，第一算法可以是MD5算法。

[0066] 在一些实施例中，标记信息为邮件摘要、标题、邮件正文中的指定段落或签名。

[0067] 在一些实施例中，在上述步骤S140中，也可以将第一密文信件添加到收件箱，在查看信件时，则需要对第一密文信件进行拆分得到第二密文信件和加密会话密钥，并对加密会话密钥进行解密，然后再利用解密得到的会话密钥对第二密文信件进行解密，得到明文的第一信件并对第一信件进行展示。

[0068] 以上述对信件收进信件并在查看信件时如何对信件进行解密的具体过程。以下将以第二客户端为例，举例描述如何在发信时对信件进行加密的过程。

[0069] 图2是本公开另一实施例的信件处理方法的流程图。如图2所示，该信件处理方法可以应用于第二客户端，包括如下步骤：

[0070] S110，响应于向第一客户端发送第一信件的邮件发送请求，基于会话密钥对第一

信件进行加密，得到第二密文信件；

[0071] S120，基于第一客户端的公钥对会话密钥进行加密，得到加密会话密钥；

[0072] S130，对第二密文信件和加密会话密钥进行拼接，得到第一密文信件；

[0073] S140，向第一客户端发送第一密文信件。

[0074] 示例性地，第一信件为明文信件，用户将第一信件写好，并点击发送按钮，此时，邮件系统收到邮件发送请求，执行上述步骤S110至S140，对第一信件进行加密后发送。

[0075] 在这过程中，用户是无感加密信件的，只需要点击发送按钮，邮件系统即可针对第一信件进行加密并发送。

[0076] 示例性地，第一客户端可以是安装在一个终端设备上的邮件应用程序，第二客户端可以安装在另一个终端设备上的邮件应用程序。终端设备可以是手机、电脑、平板等。邮件应用程序可以是yahoo、gmail、outlook、homtmail等。

[0077] 示例性地，会话密钥是第二客户端生成的，其可以根据第一信件的一些信息来生成，例如，根据摘要、标题或者正文中的某些段落生成会话密钥。会话密钥也可以是利用随机密码器随机生成的。

[0078] 在一些实施例中，在上述步骤S110中，响应向第一客户端发送第一信件的邮件发送请求，显示加密复选框，在该加密复选框为选择加密的情况下，基于会话密钥对第一信件进行加密，得到第二密文信件。此外，在该加密复选框为不选择加密的情况下，向第一客户端发送第一信件。

[0079] 在一些实施例中，在利用会话密钥对信件进行加密之前，可以利用第二客户端的私钥对从信件中提取的标记信息进行加密再添加到信件一起被会话密钥加密，从而即使信件被盗取了，并提供假信件给第一客户端，可以通过加密的标记信息来确定该信件是否为假信件。

[0080] 示例性地，在上述步骤S110中，响应于向第一客户端发送第一信件的邮件发送请求，基于会话密钥对第一信件进行加密，得到第二密文信件，包括：

[0081] 响应于向第一客户端发送第一信件的邮件发送请求，基于第二客户端的私钥，对第一信件中的标记信息进行加密，得到加密标记信息；

[0082] 对加密标记信息和第一信件进行拼接，得到第二信件；

[0083] 基于会话密钥对第二信件进行加密，得到第二密文信件。

[0084] 在本示例中，基于第二客户端的私钥从明文信件提取标记信息进行加密，并利用会话密钥对拼接在一起的加密标记信息与原明文信件进行加密，这样，即使密文信件被破解后发送给一个假信件给第一客户端，第一客户端可以通过加密的标记信息来确定该信件是否为假信件，以决定是否丢弃该假信件。

[0085] 在一些实施例中，可以利用预定的算法对标记信息进行处理之后再进行加密，这样可以更准确地发现信件是否被篡改。

[0086] 示例性地，上述基于第二客户端的私钥，对第一信件中的标记信息进行加密，得到加密标记信息，包括：

[0087] 基于第一算法，对第一信件中的标记信息进行处理，得到第一标记；

[0088] 基于第二客户端的私钥，对第一标记进行加密，得到加密标记信息。

[0089] 在本示例中，可以利用预定的算法对标记信息进行处理之后再进行加密，这样可

以更准确地发现信件是否被篡改。

[0090] 示例性地,第一算法可以是MD5(Message-DigestAlgorithm,信息摘要算法)算法。

[0091] 示例性地,标记信息可以为邮件摘要、标题、邮件正文中的指定段落或签名等。

[0092] 在一些实施例中,在将加密标记信息与第一信件拼接得到第二信件之后,可以对第二信件进行压缩后再加密,或者也可以加密后压缩。

[0093] 示例性地,基于会话密钥对第二信件进行加密,得到第一密文信件,包括:

[0094] 对第二信件进行压缩;

[0095] 基于会话密钥对压缩后的第二信件进行加密,得到第一密文信件。

[0096] 在一些实施例中,可以设置密钥服务器用于交换任意两个相互授权的客户端之间的公钥,这样可以利用双方的密钥对进行加密或解密。

[0097] 在一些实施例中,可以在邮件应用程序中提供密钥管理的功能,例如,利用密钥管理的功能生成会话密钥、第二客户端的密钥对、将第二客户端的公钥上传密钥服务器、从密钥服务器中获取其他客户端的公钥等。

[0098] 示例性地,上述方法还可以包括:

[0099] 响应于针对第一客户端的授权设置请求,向密钥服务器发送密钥分发指令,其中,密钥分发指令用于指示密钥服务器向第二客户端分发第一客户端的公钥,并向第一客户端分发第二客户端的公钥;

[0100] 在接收到第一客户端的公钥的情况下,存储第一客户端的公钥。

[0101] 在本示例中,第二客户端可以从密钥服务器中获取其他客户端的公钥,也可以让密钥服务器将第二客户端的公钥分发给其他客户端。

[0102] 在一些实施例中,上述方法还可以包括:

[0103] 在检测到邮件发送请求,且第一客户端为未授权客户端的情况下,提示第一客户端为未授权客户端;

[0104] 响应于针对第一客户端的授权设置请求,向密钥服务器发送密钥分发指令,其中,密钥分发指令用于指示密钥服务器向第二客户端分发第一客户端的公钥,并向第一客户端分发第二客户端的公钥;

[0105] 在接收到第一客户端的公钥的情况下,响应邮件发送请求。

[0106] 在本示例中,在检测上述步骤S110中的邮件发送请求时,但第一客户端为未授权客户端,即本地未存储有第一客户端的公钥,此时,向用户进行提示是否要将第一客户端确定为授权客户端,即需要对信件进行加密传输的客户端。从而,在确定第一客户端为授权客户端时,可以从密钥服务器中获取第一客户端的公钥,并存储于第二客户端的密钥库。

[0107] 在一些实施例中,可以通过密钥注册来生成密钥并上传到密钥服务器中存府。

[0108] 示例性地,响应于针对第二客户端的密钥注册请求,利用随机密码器生成第二客户端的密钥对,密钥对包括第二客户端的私钥和公钥;在第二客户端中存储第二客户端的私钥;向密钥服务器发送第二客户端的公钥,以在密钥服务器存储第二客户端的公钥。

[0109] 在本示例中,可以在第二客户端登录时,即进行密钥注册请求。

[0110] 在一些实施例中,还可以对第二客户端的密钥对进行更新。

[0111] 示例性地,上述方法还可以包括:

[0112] 响应于针对第二客户端的密钥更新请求,显示信息验证窗口;

[0113] 基于向信息验证窗口输入的用户信息，确定密钥更新请求是否合法；

[0114] 在确定密钥更新请求合法的情况下，利用随机密码器生成第二客户端的新密钥对，新密钥对包括第二客户端的新私钥和新公钥；

[0115] 将第二客户端存储的私钥更新为第二客户端的新私钥；

[0116] 向密钥服务器发送第二客户端的新公钥，以更新密钥服务器中的第二客户端的公钥。

[0117] 示例性地，上述方法还可以包括：

[0118] 在接收到第一客户端的新公钥的情况下，基于第一客户端的新公钥，对第二客户端中的属于第一客户端的公钥进行更新。

[0119] 如图3所示，在本公开实施例中，密钥交换的通道是独立于邮件传输的通道。第一客户端与第二客户端之间通过密钥服务器交换双方的公钥，密钥服务器用于存储所有册注的客户端的公钥以及向相应的客户端发送相应的公钥。而邮件的传输则是通过邮件服务器或者邮件传输通道进行传输的，这与密钥服务器是不相关的。

[0120] 如图4和图5所示，以下将以第一客户端为Alice，第二客户端为Bob，讲述其加密和解密的一个应用示例。

[0121] 图6是本公开一实施例的信件处理装置的结构框图。如图6所示，该信件处理装置应用于第一客户端，包括：

[0122] 密文信件获取模块610，用于获取来自第二客户端的第一密文信件；

[0123] 信件拆分模块620，用于对所述第一密文信息进行拆分，得到第二密文信件和加密会话密钥；

[0124] 密钥解密模块630，用于基于所述第一客户端的私钥对所述加密会话密钥进行解密，得到会话密钥；

[0125] 信件处理模块640，用于基于所述会话密钥对所述第二密文信件进行解密，得到第一信件，并在所述第一信件符合设定条件的情况下，将所述第二密文信件存入所述第一客户端的收件箱，以及将所述会话密钥存入所述第一客户端的密钥库。

[0126] 在一些实施例中，所述装置还包括：

[0127] 密钥提取模块，用于响应于针对所述收件箱中的第二密文信件的查看请求，从所述密钥库中提取所述第二密文信件对应的会话密钥；

[0128] 信件解密模块，用于基于所述会话密钥对所述第二密文信件进行解密，得到第一信件；

[0129] 信件展示模块，用于在显示界面中展示所述第一信件。

[0130] 在一些实施例中，所述信件处理模块包括：

[0131] 信件解密单元，用于基于所述会话密钥对所述第二密文信件进行解密，得到第二信件；

[0132] 信件拆分单元，用于对所述第二信件进行拆分，得到加密标记信息和第一信件；

[0133] 信件处理单元，用于基于所述第二客户端的公钥对所述加密标记信息进行解密，得到标记信息，并在所述标记信息满足设定条件下，将所述第二密文信件存入所述第一客户端的收件箱，并将所述会话密钥存入所述第一客户端的密钥库。

[0134] 在一些实施例中，所述信件处理单元具体用于：

[0135] 基于所述第二客户端的公钥对所述加密标记信息进行解密，得到第一标记；

[0136] 基于第一算法，对所述第一信件中的标记信息进行处理，得到第二标记；

[0137] 在所述第一标记和所述第二标记相同的情况下，将所述第二密文信件存入所述第一客户端的收件箱，并将所述会话密钥存入所述第一客户端的密钥库。

[0138] 本公开实施例各装置中的各单元、模块或子模块的功能可以参见上述方法实施例中的对应描述，在此不再赘述。

[0139] 根据本公开的实施例，本公开还提供了一种电子设备、一种可读存储介质和一种计算机程序产品。

[0140] 图7示出了可以用来实施本公开的实施例的示例电子设备800的示意性框图。电子设备旨在表示各种形式的数字计算机，诸如，膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备还可以表示各种形式的移动装置，诸如，个人数字处理、蜂窝电话、智能电话、可穿戴设备和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅仅作为示例，并且不意在限制本文中描述的和/或要求的本公开的实现。

[0141] 如图7所示，电子设备800包括计算单元801，其可以根据存储在只读存储器(ROM)802中的计算机程序或者从存储单元808加载到随机访问存储器(RAM)803中的计算机程序来执行各种适当的动作和处理。在RAM803中，还可存储电子设备800操作所需的各种程序和数据。计算单元801、ROM802以及RAM803通过总线804彼此相连。输入输出(I/O)接口805也连接至总线804。

[0142] 电子设备800中的多个部件连接至I/O接口805，包括：输入单元806，例如键盘、鼠标等；输出单元807，例如各种类型的显示器、扬声器等；存储单元808，例如磁盘、光盘等；以及通信单元809，例如网卡、调制解调器、无线通信收发机等。通信单元809允许电子设备800通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

[0143] 计算单元801可以是各种具有处理和计算能力的通用和/或专用处理组件。计算单元801的一些示例包括但不限于中央处理单元(CPU)、图形处理单元(GPU)、各种专用的人工智能(AI)计算芯片、各种运行机器学习模型算法的计算单元、数字信号处理器(DSP)、以及任何适当的处理器、控制器、微控制器等。计算单元801执行上文所描述的各个方法和处理，例如音频与文本组合方法。例如，在一些实施例中，音频与文本组合方法可被实现为计算机软件程序，其被有形地包含于机器可读介质，例如存储单元808。在一些实施例中，计算机程序的部分或者全部可以经由ROM102和/或通信单元809而被载入和/或安装到电子设备800上。当计算机程序加载到RAM803并由计算单元801执行时，可以执行上文描述的音频与文本组合方法的一个或多个步骤。备选地，在其他实施例中，计算单元801可以通过其他任何适当的方式(例如，借助于固件)而被配置为执行音频与文本组合方法。

[0144] 本文中以上描述的系统和技术的各种实施方式可以在数字电子电路系统、集成电路系统、场可编程门阵列(FPGA)、专用集成电路(ASIC)、专用标准产品(ASSP)、芯片上系统的系统(SOC)、复杂可编程逻辑设备(CPLD)、计算机硬件、固件、软件、和/或它们的组合中实现。这些各种实施方式可以包括：实施在一个或者多个计算机程序中，该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释，该可编程处理器可以是专用或者通用可编程处理器，可以从存储系统、至少一个输入装置、和至少一个输出

装置接收数据和指令，并且将数据和指令传输至该存储系统、该至少一个输入装置、和该至少一个输出装置。

[0145] 用于实施本公开的方法的程序代码可以采用一个或多个编程语言的任何组合来编写。这些程序代码可以提供给通用计算机、专用计算机或其他可编程氛围灯调节装置的处理器或控制器，使得程序代码当由处理器或控制器执行时使流程图和/或框图中所规定的功能/操作被实施。程序代码可以完全在机器上执行、部分地在机器上执行，作为独立软件包部分地在机器上执行且部分地在远程机器上执行或完全在远程机器或服务器上执行。

[0146] 在本公开的上下文中，机器可读介质可以是有形的介质，其可以包含或存储以供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合地使用的程序。机器可读介质可以是机器可读信号介质或机器可读储存介质。机器可读介质可以包括但不限于电子的、磁性的、光学的、电磁的、红外的、或半导体系统、装置或设备，或者上述内容的任何合适组合。机器可读存储介质的更具体示例会包括基于一个或多个线的电气连接、便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或快闪存储器)、光纤、便捷式紧凑盘只读存储器(CD-ROM)、光学储存设备、磁储存设备、或上述内容的任何合适组合。

[0147] 为了提供与用户的交互，可以在计算机上实施此处描述的系统和技术，该计算机具有：用于向用户显示信息的显示装置(例如，CRT(阴极射线管)或者LCD(液晶显示器)监视器)；以及键盘和指向装置(例如，鼠标或者轨迹球)，用户可以通过该键盘和该指向装置来将输入提供给计算机。其它种类的装置还可以用于提供与用户的交互；例如，提供给用户的反馈可以是任何形式的传感反馈(例如，视觉反馈、听觉反馈、或者触觉反馈)；并且可以用任何形式(包括声输入、语音输入、或者触觉输入来接收来自用户的输入。

[0148] 可以将此处描述的系统和技术实施在包括后台部件的计算系统(例如，作为数据服务器)、或者包括中间件部件的计算系统(例如，应用服务器)、或者包括前端部件的计算系统(例如，具有图形用户界面或者网络浏览器的用户计算机，用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术的实施方式交互)、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信(例如，通信网络)来将系统的部件相互连接。通信网络的示例包括：局域网(LAN)、广域网(WAN)和互联网。

[0149] 计算机系统可以包括客户端和服务器。客户端和服务器一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务器的关系。服务器可以是云服务器，也可以为分布式系统的服务器，或者是结合了区块链的服务器。

[0150] 应该理解，可以使用上面所示的各种形式的流程，重新排序、增加或删除步骤。例如，本公开中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行，只要能够实现本公开公开的技术方案所期望的结果，本文在此不进行限制。

[0151] 上述具体实施方式，并不构成对本公开保护范围的限制。本领域技术人员应该明白的是，根据设计要求和其他因素，可以进行各种修改、组合、子组合和替代。任何在本公开的精神和原则之内所作的修改、等同替换和改进等，均应包含在本公开保护范围之内。

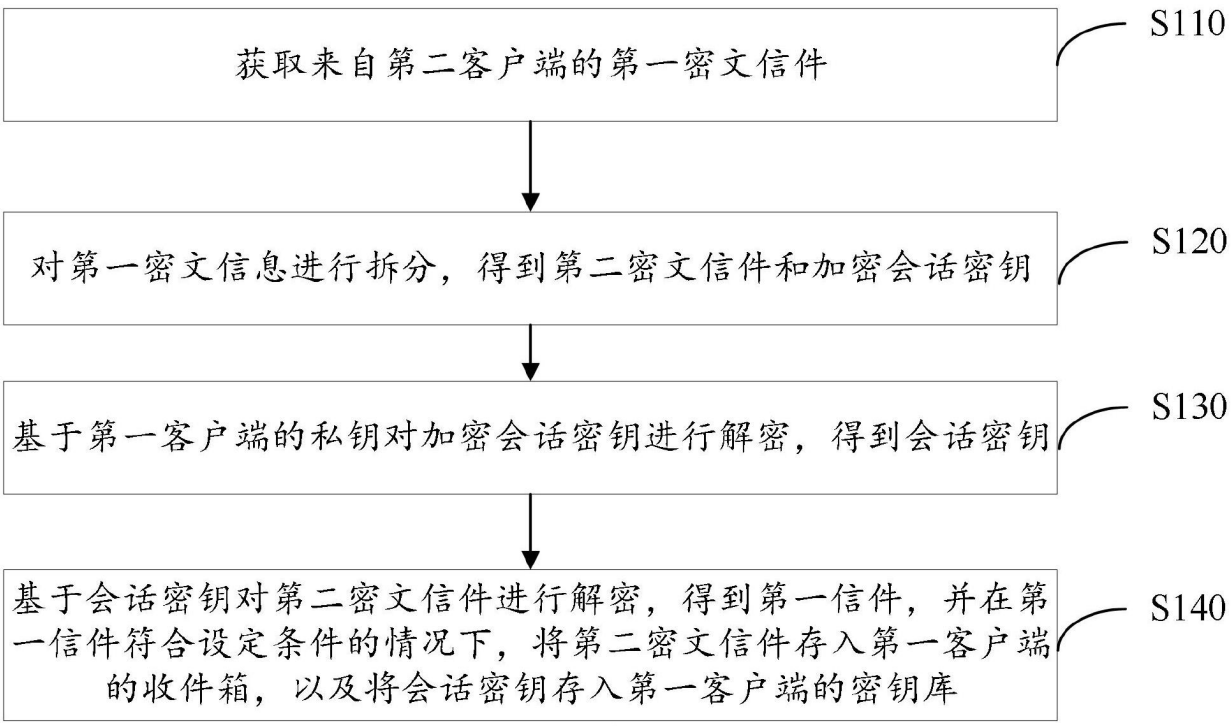

获取来自第二客户端的第一密文信件
S110
对第一密文信息进行拆分，得到第二密文信件和加密会话密钥
S120
基于第一客户端的私钥对加密会话密钥进行解密，得到会话密钥
S130
基于会话密钥对第二密文信件进行解密，得到第一信件，并在第一信件符合设定条件的情况下，将第二密文信件存入第一客户端的收件箱，以及将会话密钥存入第一客户端的密钥库
S140

图1

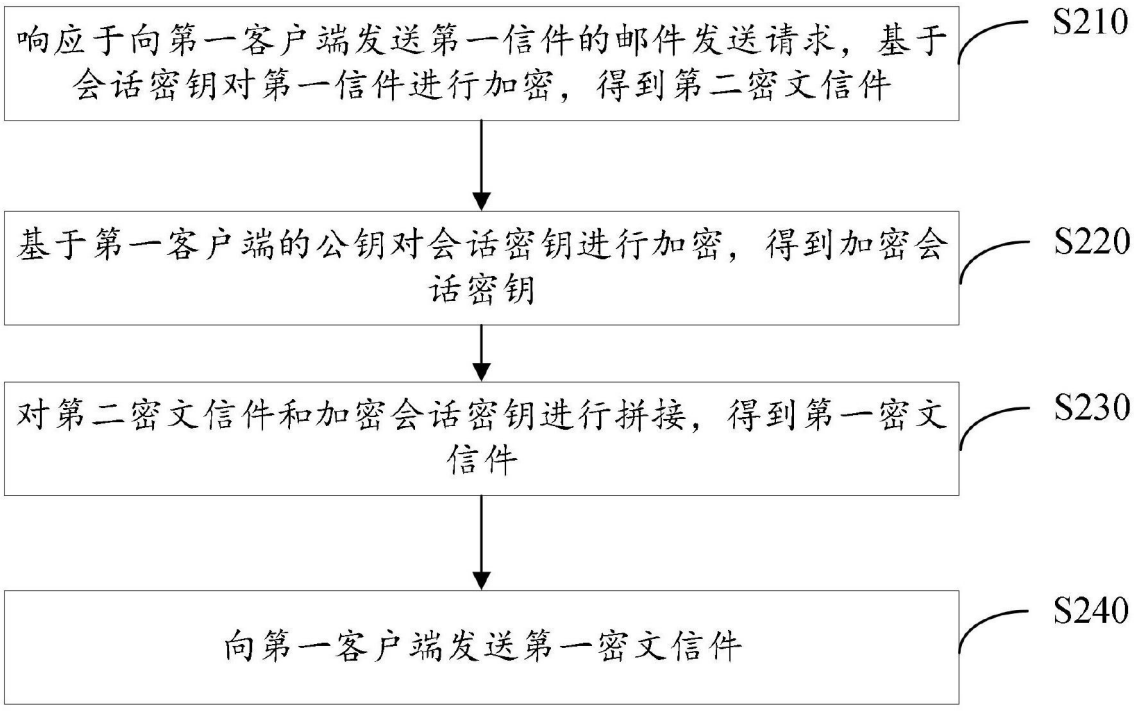

响应于向第一客户端发送第一信件的邮件发送请求，基于会话密钥对第一信件进行加密，得到第二密文信件
S210
基于第一客户端的公钥对会话密钥进行加密，得到加密会话密钥
S220
对第二密文信件和加密会话密钥进行拼接，得到第一密文信件
S230
向第一客户端发送第一密文信件
S240

图2

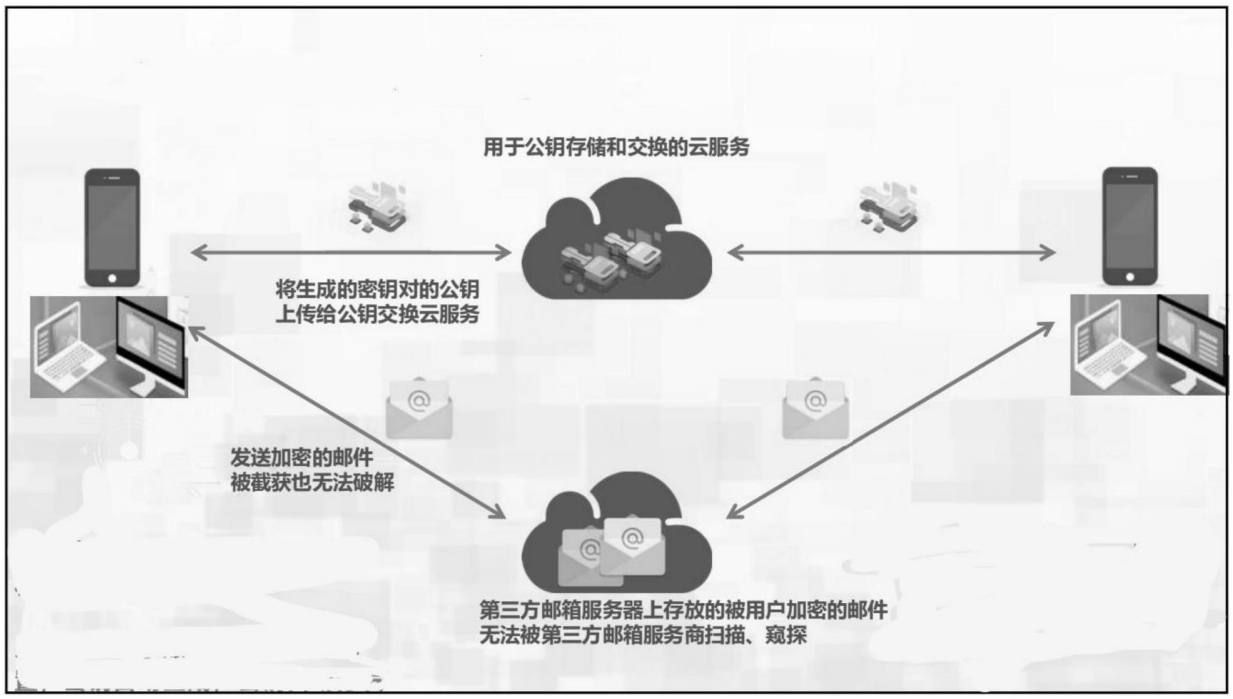
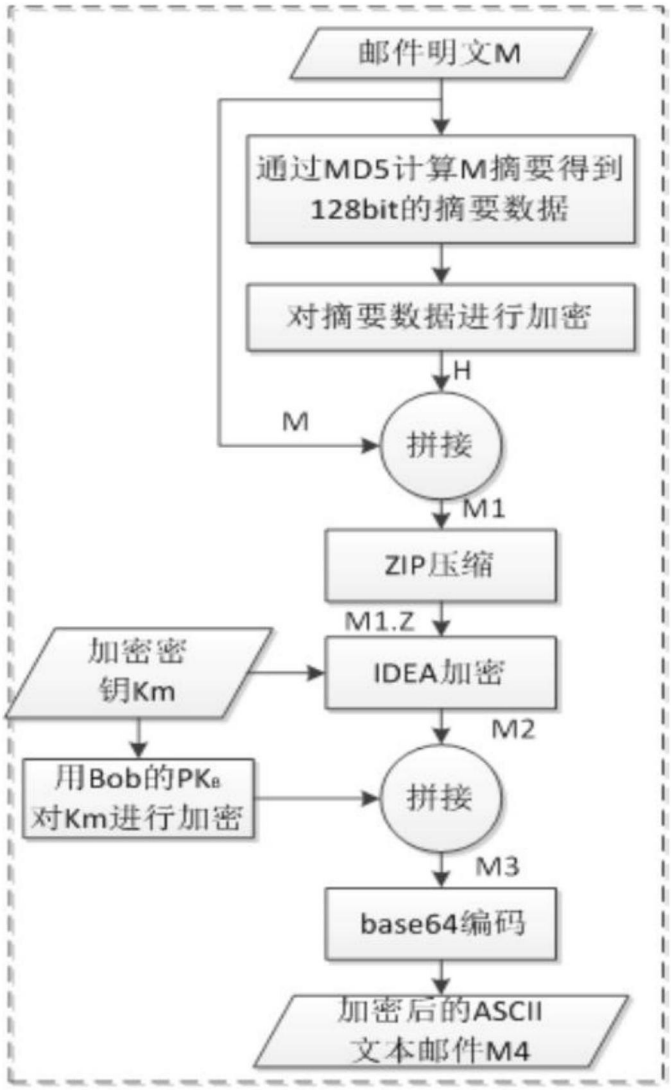
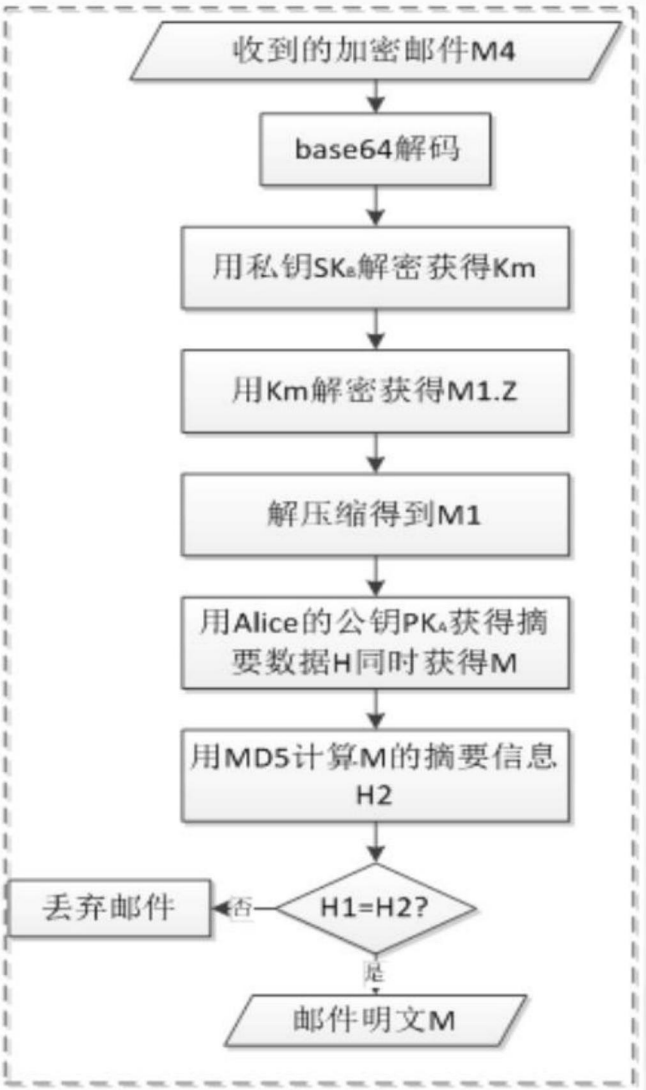

用于公钥存储和交换的云服务
将生成的密钥对的公钥
上传给公钥交换云服务
发送加密的邮件
被截获也无法破解
第三方邮箱服务器上存放的被用户加密的邮件
无法被第三方邮箱服务商扫描、窥探

图3



a. Alice发送邮件给Bob的加密处理

图4



b. Bob接收Alice邮件后的解密处理

图5

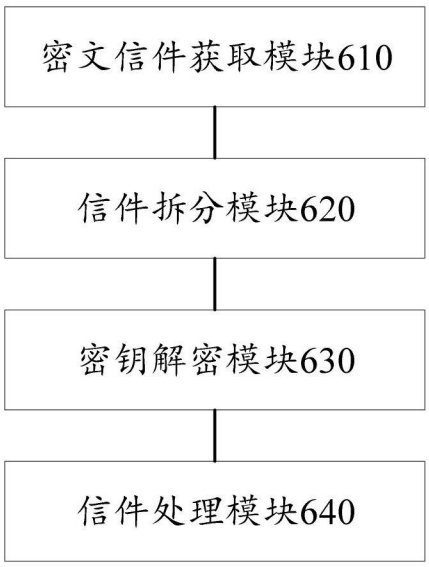

密文信件获取模块610
信件拆分模块620
密钥解密模块630
信件处理模块640

图6

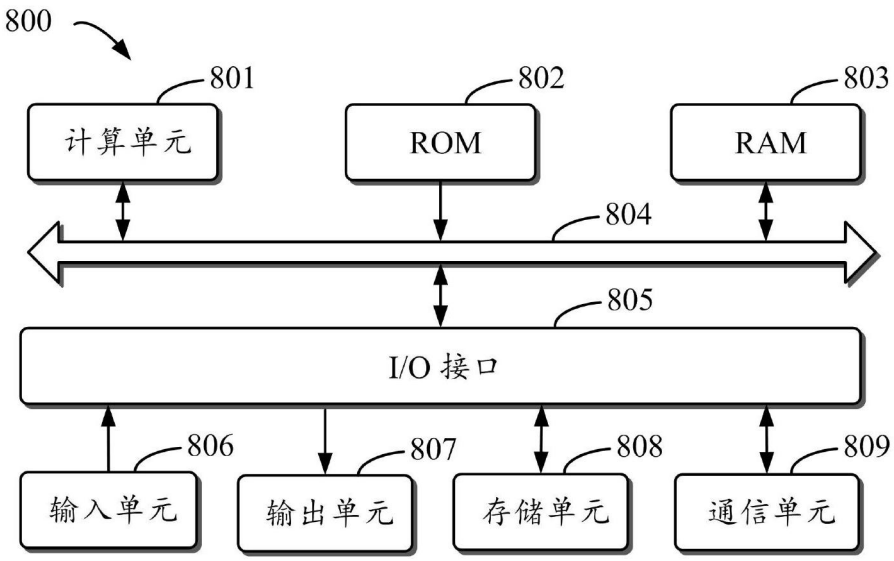

800
801
计算单元
802
ROM
803
RAM
804
805
I/O 接口
806
输入单元
807
输出单元
808
存储单元
809
通信单元

图7