(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106549754 A
(43)申请公布日 2017.03.29

(21)申请号 201611053417.X

(22)申请日 2016.11.24

(71)申请人 北京爱接力科技发展有限公司
地址 100026 北京市朝阳区光华路4号东方梅地亚C座1505

(72)发明人 赵微 许楠 张勇

(74)专利代理机构 北京鼎佳达知识产权代理事务所(普通合伙) 11348
代理人 王伟锋 刘铁生

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 12/28(2006.01)

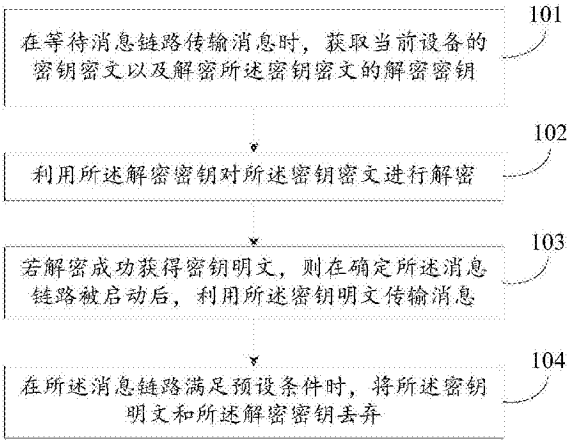
权利要求书2页 说明书10页 附图6页

(54)发明名称

管理密钥的方法和装置

(57)摘要

本发明公开了一种管理密钥的方法和装置，涉及数据安全技术领域，能够提高密钥明文的安全性。本发明的方法主要包括：在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥，其中，所述密钥密文为对所述当前设备加密和/或解密消息时所使用的密钥明文进行加密后的文件；利用所述解密密钥对所述密钥密文进行解密；若解密成功获得密钥明文，则在确定所述消息链路被启动后，利用所述密钥明文传输消息；在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃。本发明主要适用于加密传输数据的场景中。



CN 106549754 A

1.一种管理密钥的方法，其特征在于，所述方法包括：

在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥，其中，所述密钥密文为对所述当前设备加密和/或解密消息时所使用的密钥明文进行加密后的文件；

利用所述解密密钥对所述密钥密文进行解密；

若解密成功获得密钥明文，则在确定所述消息链路被启动后，利用所述密钥明文传输消息；

在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃。

2.根据权利要求1所述的方法，其特征在于，所述获取解密所述密钥密文的解密密钥包括：

当前设备为源设备时，接收输入的解密所述密钥密文的解密密钥；

当前设备为中继设备或者目标设备时，接收所述消息链路上与所述当前设备相邻的前一设备发送的解密密钥。

3.根据权利要求2所述的方法，其特征在于，若所述当前设备为源设备或者中继设备，则在解密成功获得密钥明文后，所述方法还包括：

根据所述当前设备的解密密钥，确定所述消息链路上与所述当前设备相邻的下一设备的解密密钥；

将确定的解密密钥发送给所述下一设备，以便所述下一设备利用所述确定的解密密钥对所述下一设备的密钥密文进行解密。

4.根据权利要求3所述的方法，其特征在于，所述根据所述当前设备的解密密钥，确定所述消息链路上与所述当前设备相邻的下一设备的解密密钥包括：

将所述当前设备的解密密钥确定为所述下一设备的解密密钥；

或者，根据预设算法对所述当前设备的解密密钥进行运算，并将运算结果确定为所述下一设备的解密密钥。

5.根据权利要求4所述的方法，其特征在于，所述根据预设算法对所述当前设备的解密密钥进行运算，并将运算结果确定为所述下一设备的解密密钥包括：

为所述当前设备的解密密钥添加预先存储的、用于设置所述下一设备的解密密钥的数据；

计算添加数据后的解密密钥的哈希值；

将所述哈希值确定为所述下一设备的解密密钥。

6.根据权利要求1至5中任一项所述的方法，其特征在于，所述在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃包括：

当将本次传输的消息传输至目标设备时，将所述当前设备的密钥明文和解密密钥丢弃；

或者，当所述目标设备接收到的消息个数达到预设个数阈值时，将所述当前设备的密钥明文和解密密钥丢弃；

或者，当所述消息链路发生中断时，将所述当前设备的密钥明文和解密密钥丢弃。

7.根据权利要求1至5中任一项所述的方法，其特征在于，所述确定所述消息链路被启动包括：

在确定所述消息链路上的所有设备获得对应的密钥明文后，确定所述消息链路被启动。

8.根据权利要求1至5中任一项所述的方法，其特征在于，所述方法还包括：

在所述消息链路上的各个设备都生成传输消息所使用的密钥明文后，获取加密所述当前设备的密钥明文的加密密钥；

利用所述加密密钥对所述当前设备的密钥明文进行加密，获得所述密钥明文对应的密钥密文；

将所述当前设备的密钥明文进行丢弃。

9.根据权利要求8所述的方法，其特征在于，所述获取加密所述当前设备的密钥明文的加密密钥包括：

当前设备为源设备时，接收输入的加密所述当前设备的密钥明文的加密密钥；

当前设备为中继设备或者目标设备时，接收所述消息链路上与所述当前设备相邻的前一设备发送的加密密钥。

10.一种管理密钥的装置，其特征在于，所述装置包括：

获取单元，用于在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥，其中，所述密钥密文为对所述当前设备加密和/或解密消息时所使用的密钥明文进行加密后的文件；

解密单元，用于利用所述获取单元获取的所述解密密钥对所述密钥密文进行解密；

确定单元，用于在所述解密单元解密成功获得密钥明文的情况下，确定所述消息链路是否被启动；

传输单元，用于在所述确定单元确定所述消息链路被启动后，利用所述密钥明文传输消息；

丢弃单元，用于在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃。

管理密钥的方法和装置

技术领域

[0001] 本发明涉及数据安全技术领域，尤其涉及一种管理密钥的方法和装置。

背景技术

[0002] 随着互联网技术的发展，越来越多的智能家居设备融入人们的生活，例如智能门锁、监控摄像头、智能电饭煲等。人们可以直接利用手机、电脑等用户设备来远程控制这些智能家居设备，十分方便。

[0003] 然而，由于这些智能家居设备存在于网络当中，所以也存在着网络风险。因此，为了保证手机、电脑等用户设备通过中继设备向智能家居设备传输的消息不被泄露，从而避免智能家居设备发生危险，现有技术中采用加密消息的方式防止消息传输过程中被泄露，采用签名的方式确保消息发送方身份的正确性。由此可知，从用户设备到智能家居设备的整个消息链路上，每个设备上都需要存储密钥。但是，发明人在实现上述发明的过程中发现，将密钥明文直接存储在硬盘中，很容易被他人窃取，从而使得智能家居设备发生危险。

发明内容

[0004] 鉴于上述技术问题，本发明提出了一种管理密钥的方法和装置，能够提高密钥明文的安全性。

[0005] 一方面，本发明提供了一种管理密钥的方法，所述方法包括：

[0006] 在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥，其中，所述密钥密文为对所述当前设备加密和/或解密消息时所使用的密钥明文进行加密后的文件；

[0007] 利用所述解密密钥对所述密钥密文进行解密；

[0008] 若解密成功获得密钥明文，则在确定所述消息链路被启动后，利用所述密钥明文传输消息；

[0009] 在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃。

[0010] 另一方面，本发明提供了一种管理密钥的装置，所述装置包括：

[0011] 获取单元，用于在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥，其中，所述密钥密文为对所述当前设备加密和/或解密消息时所使用的密钥明文进行加密后的文件；

[0012] 解密单元，用于利用所述获取单元获取的所述解密密钥对所述密钥密文进行解密；

[0013] 确定单元，用于在所述解密单元解密成功获得密钥明文的情况下，确定所述消息链路是否被启动；

[0014] 传输单元，用于在所述确定单元确定所述消息链路被启动后，利用所述密钥明文传输消息；

[0015] 丢弃单元，用于在所述消息链路满足预设条件时，将所述密钥明文和所述解密密

钥丢弃。

[0016] 借由上述技术方案，本发明提供的管理密钥的方法和装置，能够在消息链路未启动时，在消息链路上的各个设备中只存储传输消息时所需密钥的密钥密文，而不存储密钥明文；当等待消息链路传输消息时，消息链路上的各个设备可以获取各自所需的解密密钥，然后利用解密密钥对本地存储的密钥密文进行解密获得密钥明文，并且在确定消息链路被启动后，开始利用密钥明文来传输消息；在消息开始传输后，若消息链路满足预设条件(例如消息链路上某两个设备之间的连接中断)，则将密钥明文和解密密钥丢弃。由此可知，与现有技术直接存储密钥明文相比，本发明只将密钥密文进行永久存储，而将密钥明文只进行短暂存储，从而降低了密钥明文外泄的几率，进而提高了密钥明文的安全性。

[0017] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0018] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0019] 图1示出了本发明实施例提供的一种管理密钥的方法的流程图；

[0020] 图2示出了本发明实施例提供的另一种管理密钥的方法的流程图；

[0021] 图3示出了本发明实施例提供的一种加密密钥明文的方法示意图；

[0022] 图4示出了本发明实施例提供的一种解密密钥密文的方法示意图；

[0023] 图5示出了本发明实施例提供的一种管理密钥的装置的组成框图；

[0024] 图6示出了本发明实施例提供的另一种管理密钥的装置的组成框图。

具体实施方式

[0025] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0026] 本发明实施例提供一种管理密钥的方法，如图1所示，该方法主要包括：

[0027] 101、在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥。

[0028] 其中，密钥密文，可以是对当前设备加密和/或解密消息时所使用的密钥明文进行加密后的文件。

[0029] 在实际应用中，当使用对称加密技术对传输的消息进行加密时，每个设备可以具有一个加密密钥；当使用非对称加密技术对传输的消息进行加密时，每个设备可以具有一个公私钥对；当需要对传输的消息进行签名或者验签时，每个设备还可以具有一个公私钥对。由于公钥是对外公开、私钥是设备私有的，所以需要加密的密钥明文可以包括利用对称加密技术加密或解密消息时所使用的密钥、利用非对称加密技术加密或/解密消息时所使

用的私钥以及利用非对称加密技术对消息签名或者验签时所使用的私钥。由此可知，需要加密的密钥明文包括至少一个。当密钥明文为多个时，可以分别对不同的密钥明文进行加密，获得多个密钥密文，也可以对多个密钥明文一起进行加密，获得一个密钥密文。

[0030] 需要补充的是，在对密钥明文进行加密时，所采用的加密技术可以是对称加密技术，所以当前设备在对自己的密钥明文进行加密时所使用的加密密钥与后续对密钥密文进行解密时所需的解密密钥是相同的。

[0031] 当未启动消息链路传输消息时，消息链路上的各个设备可以仅存储密钥密文，而不存储密钥明文，并且可以将密钥密文存储至硬盘中进行永久存储。当需要消息链路传输消息时，消息链路上的各个设备可以获取本地存储的密钥密文以及获取解密该密钥密文所需的解密密钥，以便利用解密密钥对密钥密文进行解密获得密钥明文。

[0032] 102、利用所述解密密钥对所述密钥密文进行解密。

[0033] 具体地，若解密不成功，可以输出显示解密失败的提示信息，以使得用户获知解密密钥错误。若解密成功，则执行步骤103。

[0034] 103、若解密成功获得密钥明文，则在确定所述消息链路被启动后，利用所述密钥明文传输消息。

[0035] 其中，在确定所述消息链路上的所有设备获得对应的密钥明文后，当前设备可以确定所述消息链路被启动，此时可以等待消息链路上与所述当前设备相邻的前一设备发送加密以及签名的消息，并在接收到消息后，可以利用当前设备获得的密钥明文中用于解密消息的解密密钥(如果选用对称加密技术则该解密密钥指与前一设备约定的密钥，如果选用非对称加密技术则该解密密钥指当前设备的用于解密消息的私钥)对接收到的消息进行解密，利用前一设备的签名公钥对前一设备发送的签名进行验签，若确认发送的消息无误，则继续利用密钥明文中后一设备的加密密钥(如果选用对称加密技术则该加密密钥指与后一设备约定的密钥，如果选用非对称加密技术则该加密密钥指后一设备的用于加密消息的公钥)进行加密、利用当前设备的签名私钥进行签名操作，以便将加密、签名后的消息发送给消息链路上与所述当前设备相邻的下一设备，直至将消息传输至目标设备。

[0036] 需要说明的是，当解密成功获得密钥明文后，可以将密钥明文存储至内存中，也可以将其存储至其他存储空间。

[0037] 104、在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃。

[0038] 在消息链路满足预设条件时，可以仅将密钥明文丢弃，也可以将密钥明文和解密密钥密文的解密密钥一起丢弃。其中，由于若将解密密钥永久存储，则可能会发生解密密钥外泄，导致密钥密文被解开的现象，所以将密钥明文与解密密文一起丢弃与仅丢弃密钥明文相比，将密钥明文与解密密文一起丢弃可以进一步保证密钥明文的安全。

[0039] 具体的，预设条件可以包括但不限于以下几种情况：

[0040] (1)当将本次需要传输的消息传输至目标设备时，将所述当前设备的密钥明文和解密密钥丢弃。也就是说，每传输一条消息，都需要重新对密钥密文进行解密获得密钥明文。

[0041] (2)当所述目标设备接收到的消息个数达到预设个数阈值时，将所述当前设备的密钥明文和解密密钥丢弃。

[0042] 具体地，虽然每发一条消息对密钥密文进行一次解密，可以防止密钥明文外泄，但

是却会大大影响传输消息的效率，因此为了综合考虑，可以在将消息成功传输至目标设备的消息个数达到预设个数阈值时，才将密钥明文和解密密钥丢弃。

[0043] (3)当所述消息链路发生中断时，将所述当前设备的密钥明文和解密密钥丢弃。

[0044] 当消息链路上的某个连接发生中断致使整个消息链路无法继续传输消息(例如某个设备断电)时，每个设备可以将其各自的密钥明文和解密密钥丢弃，当消息链路再次连通且需要传输消息时，再通过解密密钥密文的方式获取密钥明文进行消息传输操作。

[0045] 本发明实施例提供的管理密钥的方法，能够在消息链路未启动时，在消息链路上的各个设备中只存储传输消息时所需密钥的密钥密文，而不存储密钥明文；当等待消息链路传输消息时，消息链路上的各个设备可以获取各自所需的解密密钥，然后利用解密密钥对本地存储的密钥密文进行解密获得密钥明文，并且在确定消息链路被启动后，开始利用密钥明文来传输消息；在消息开始传输后，若消息链路满足预设条件(例如消息链路上某两个设备之间的连接中断)，则将密钥明文和解密密钥丢弃。由此可知，与现有技术直接存储密钥明文相比，本发明只将密钥密文进行永久存储，而将密钥明文只进行短暂存储，从而降低了密钥明文外泄的几率，进而提高了密钥明文的安全性。

[0046] 进一步的，依据图1所示的方法，本发明的另一个实施例还提供一种管理密钥的方法，如图2所示，该方法主要包括：

[0047] 201、在所述消息链路上的各个设备都生成传输消息所使用的密钥明文后，获取加密所述当前设备的密钥明文的加密密钥。

[0048] 在实际应用中，可以采用顺序加密的方式实现各个设备对自身密钥明文的加密，也可以采用其他方式进行加密。

[0049] 其中，顺序加密为：从第二个设备起，每个设备所需的加密密钥都是由相邻的前一设备发送的，而第一个设备的加密密钥是由用户输入的。即当所述当前设备为源设备时，接收用户输入的加密所述当前设备的密钥明文所需的加密密钥；当所述当前设备为中继设备或者目标设备时，接收所述消息链路上与所述当前设备相邻的前一设备发送的加密密钥。其中，用户输入加密密钥的方式为数字、手势或者指纹等。

[0050] 由于源设备与中继设备都需要向与其相邻的下一设备发送加密密钥，所以当前设备为源设备或者中继设备时，在对当前设备的密钥明文进行加密后，可以根据当前设备的加密密钥确定消息链路上与该当前设备相邻的下一设备的加密密钥，然后将确定的加密密钥发送给该下一设备。

[0051] 其中，根据当前设备的加密密钥确定消息链路上与该当前设备相邻的下一设备的加密密钥的具体实现方式包括但不限于以下两种：

[0052] (1)直接将所述当前设备的加密密钥确定为所述下一设备的加密密钥，即每个设备所使用的加密密钥相同。

[0053] (2)根据预设算法对所述当前设备的加密密钥进行运算，并将运算结果确定为所述下一设备的加密密钥。

[0054] 在实际应用中，可以采用多种运算方式对当前设备的加密密钥进行运算，获得下一设备的加密密钥。例如，可以先为所述当前设备的加密密钥添加预先存储的、用于设置所述下一设备的加密密钥所需的数据，然后计算添加数据后的加密密钥的哈希值，最后将所述哈希值确定为所述下一设备的加密密钥。其中，在当前设备的加密密钥上添加数据时，可

以在当前设备的加密密钥的任一位置进行添加。

[0055] 需要说明的是，第二种确定下一设备的加密密钥的方式，可以使得各个设备的加密密钥都不相同，从而即使某一个加密密钥(由于采用对称加密技术，所以解密密钥与加密密钥相同)泄露，也不会导致其他加密密钥泄露，由此能够进一步提高密钥明文的安全性。

[0056] 202、利用所述加密密钥对所述当前设备的密钥明文进行加密，获得所述密钥明文对应的密钥密文。

[0057] 当密钥明文有多个时，可以利用不同的加密密钥分别对不同的密钥明文进行加密获得不同的密钥密文，也可以利用一个加密密钥分别对不同的密钥明文进行加密获得不同的密钥密文，也可以利用一个加密密钥对所有的密钥明文一块加密获得一个密钥密文。

[0058] 203、将所述当前设备的密钥明文进行丢弃。

[0059] 在获得密钥密文后，可以将密钥明文丢弃，以便在需要将密钥密文进行解密时，再获得密钥明文。

[0060] 204、在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥。

[0061] 与顺序加密相对应的，在对密钥密文进行解密时，可以采用顺序解密的方式使得各个设备依次获得其所需的解密密钥。

[0062] 具体的，当所述当前设备为源设备时，接收输入的解密所述密钥密文所需的解密密钥；当所述当前设备为中继设备或者目标设备时，接收所述消息链路上与所述当前设备相邻的前一设备发送的解密密钥。

[0063] 由于源设备与中继设备都需要向与其相邻的下一设备发送解密密钥，所以当前设备为源设备或者中继设备时，在当前设备解密成功获得密钥明文后，可以根据所述当前设备的解密密钥，确定所述消息链路上与所述当前设备相邻的下一设备的解密密钥，并将确定的解密密钥发送给所述下一设备，以便所述下一设备利用所述确定的解密密钥对所述下一设备的密钥密文进行解密。

[0064] 与根据当前设备的加密密钥确定下一设备的加密密钥相对应的(确定加密密钥的方法与确定解密密钥的方法相同)，根据当前设备的解密密钥确定下一设备的解密密钥的具体实现方式包括但不限于以下两种：

[0065] (1)将所述当前设备的解密密钥确定为所述下一设备的解密密钥。

[0066] (2)根据预设算法对所述当前设备的解密密钥进行运算，并将运算结果确定为所述下一设备的解密密钥。

[0067] 其中，与获取加密密钥相对应的，获取解密密钥采用的运算方式可以为：为所述当前设备的解密密钥添加预先存储的、用于设置所述下一设备的解密密钥所需的数据；计算添加数据后的解密密钥的哈希值；将所述哈希值确定为所述下一设备的解密密钥。

[0068] 205、利用所述解密密钥对所述密钥密文进行解密。

[0069] 206、若解密成功获得密钥明文，则在确定所述消息链路被启动后，利用所述密钥明文传输消息。

[0070] 207、在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃。

[0071] 本发明实施例提供的管理密钥的方法，除了只有在需要使用密钥明文时，才对密钥密文进行解密获取密钥明文，从而降低了密钥明文外泄的几率外，在获取加密密钥以及

解密密钥时，通过采用顺序加密解密的方式，使得当前设备所需的加密密钥以及解密密钥均只有与其相邻的前一设备来确定，而其他设备发送的加密密钥或者解密密钥均不采纳，从而防止他人通过发送错误的加密密钥对密钥明文进行加密，或者防止他人通过发送正确的解密密钥来获取密钥明文，由此进一步提高了密钥明文的安全。

[0072] 下面以用户设备通过中继设备(包括用户设备的应用软件对应的服务器以及智能家居设备对应的服务器)控制智能家居设备，且所采用的加密解密方式为顺序方式为例，对上述密钥管理方法进行介绍：

[0073] (一)加密过程(如图3所示)

[0074] 当用户设备、中继设备以及智能家居设备都生成发送消息所需的密钥后，用户可以通过用户设备上的应用软件输入加密密钥1；当用户设备获得加密密钥1后，可以利用加密密钥1对密钥明文1进行加密获得密钥密文1，并根据加密密钥1确定加密密钥2，将加密密钥2发送给中继设备，将加密密钥1以及密钥明文1丢弃；中继设备接收到用户设备发送的加密密钥2后，可以利用加密密钥2对密钥明文2进行加密获得密钥密文2，并根据加密密钥2确定加密密钥3，将加密密钥3发送给智能家居设备，将加密密钥2以及密钥明文2丢弃；智能家居设备接收到中继设备发送的加密密钥3后，可以利用加密密钥3对密钥明文3进行加密获得密钥密文3，将加密密钥3以及密钥明文3丢弃。

[0075] (二)解密过程(如图4所示)

[0076] 当需要启动由用户设备、中继设备以及智能家居设备构成的消息链路传输消息时，用户可以通过用户设备上的应用软件输入解密密钥1；当用户设备获得解密密钥1后，可以利用解密密钥1对密钥密文1进行解密获得密钥明文1，并根据解密密钥1确定解密密钥2，将解密密钥2发送给中继设备；中继设备接收到用户设备发送的解密密钥2后，可以利用解密密钥2对密钥密文2进行解密获得密钥明文2，并根据解密密钥2确定解密密钥3，将解密密钥3发送给智能家居设备；智能家居设备接收到中继设备发送的解密密钥3后，可以利用解密密钥3对密钥密文3进行解密获得密钥明文3。当用户设备确定智能家居设备获得密钥明文后，用户可以通过用户设备上的应用软件向中继设备发送消息，由中继设备转发消息至智能家居设备，从而实现用户设备对智能家居设备的控制。在开启消息传输功能后，在消息链路满足预设条件时，用户设备、中继设备以及智能家居设备可以将各自的密钥明文和解密密钥丢弃，以便下次需要启动消息链路传输消息时，再重新解密密钥密文。

[0077] 需要说明的是，当在对密钥明文进行加密时所采用的加密技术是对称加密技术时，图4中用户输入的解密密钥1必须与图3中用户输入的加密密钥1相同，用户设备才能成功解密获得密钥明文1；同理，当解密密钥2与加密密钥2相同时，中继设备才能成功解密获得密钥明文2，当解密密钥3与加密密钥3相同时，智能家居设备才能成功解密获得密钥明文3。

[0078] 进一步的，依据上述方法实施例，本发明的另一个实施例还提供一种管理密钥的装置，如图5所示，所述装置主要包括：获取单元31、解密单元32、确定单元33、传输单元34以及丢弃单元35。其中，

[0079] 获取单元31，用于在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥，其中，所述密钥密文为对所述当前设备加密和/或解密消息时所使用的密钥明文进行加密后的文件；

[0080] 其中，当密钥明文为多个时，可以分别对不同的密钥明文进行加密，获得多个密钥密文，也可以对多个密钥明文一起进行加密，获得一个密钥密文。

[0081] 解密单元32，用于利用所述获取单元31获取的所述解密密钥对所述密钥密文进行解密；

[0082] 确定单元33，用于在所述解密单元32解密成功获得密钥明文的情况下，确定所述消息链路是否被启动；

[0083] 需要说明的是，当解密成功获得密钥明文后，可以将密钥明文存储至内存中，也可以将其存储至其他存储空间。此外，当解密失败时，可以输出显示解密失败的提示信息，以使得用户获知解密密钥错误。

[0084] 传输单元34，用于在所述确定单元33确定所述消息链路被启动后，利用所述密钥明文传输消息；

[0085] 丢弃单元35，用于在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃。

[0086] 可选的，如图6所示，所述获取单元31包括：

[0087] 第一接收模块311，用于当前设备为源设备时，接收输入的解密所述密钥密文的解密密钥；当所述当前设备为中继设备或者目标设备时，接收所述消息链路上与所述当前设备相邻的前一设备发送的解密密钥。

[0088] 其中，用户输入加密密钥的方式为数字、手势或者指纹等。

[0089] 可选的，所述确定单元33还用于当前设备为源设备或者中继设备时，在解密成功获得密钥明文后，根据所述当前设备的解密密钥，确定所述消息链路上与所述当前设备相邻的下一设备的解密密钥；

[0090] 如图6所示，所述装置还包括：

[0091] 发送单元36，用于将所述确定单元33确定的解密密钥发送给所述下一设备，以便所述下一设备利用所述确定的解密密钥对所述下一设备的密钥密文进行解密。

[0092] 可选的，如图6所示，所述确定单元33包括：

[0093] 第一确定模块331，用于将所述当前设备的解密密钥确定为所述下一设备的解密密钥；

[0094] 第二确定模块332，用于根据预设算法对所述当前设备的解密密钥进行运算，并将运算结果确定为所述下一设备的解密密钥。

[0095] 可选的，如图6所示，所述第二确定模块332包括：

[0096] 添加子模块3321，用于为所述当前设备的解密密钥添加预先存储的、用于设置所述下一设备的解密密钥的数据；

[0097] 其中，在当前设备的加密密钥上添加数据时，可以在当前设备的加密密钥的任一位置进行添加。

[0098] 计算子模块3322，用于计算所述添加子模块3321添加数据后的解密密钥的哈希值；

[0099] 确定子模块3323，用于将所述计算子模块3322获得的所述哈希值确定为所述下一设备的解密密钥。

[0100] 可选的，如图6所示，所述丢弃单元35包括：

[0101] 第一丢弃模块351，用于当将本次传输的消息传输至目标设备时，将所述当前设备的密钥明文和解密密钥丢弃；

[0102] 第二丢弃模块352，用于当所述目标设备接收到的消息个数达到预设个数阈值时，将所述当前设备的密钥明文和解密密钥丢弃；

[0103] 第三丢弃模块353，用于当所述消息链路发生中断时，将所述当前设备的密钥明文和解密密钥丢弃。

[0104] 可选的，所述确定单元33用于在确定所述消息链路上的所有设备获得对应的密钥明文后，确定所述消息链路被启动。

[0105] 可选的，所述获取单元31还用于在所述消息链路上的各个设备都生成传输消息所使用的密钥明文后，获取加密所述当前设备的密钥明文的加密密钥；

[0106] 如图6所示，所述装置还包括：

[0107] 加密单元37，用于利用所述获取单元31获取的所述加密密钥对所述当前设备的密钥明文进行加密，获得所述密钥明文对应的密钥密文；

[0108] 所述丢弃单元35还用于将所述当前设备的密钥明文进行丢弃。

[0109] 可选的，如图6所示，所述获取单元31包括：

[0110] 第二接收模块312，用于当前设备为源设备时，接收输入的加密所述当前设备的密钥明文的加密密钥；当前设备为中继设备或者目标设备时，接收所述消息链路上与所述当前设备相邻的前一设备发送的加密密钥。

[0111] 本发明实施例提供的管理密钥的装置，能够在消息链路未启动时，在消息链路上的各个设备中只存储传输消息时所需密钥的密钥密文，而不存储密钥明文；当等待消息链路传输消息时，消息链路上的各个设备可以获取各自所需的解密密钥，然后利用解密密钥对本地存储的密钥密文进行解密获得密钥明文，并且在确定消息链路被启动后，开始利用密钥明文来传输消息；在消息开始传输后，若消息链路满足预设条件(例如消息链路上某两个设备之间的连接中断)，则将密钥明文和解密密钥丢弃。由此可知，与现有技术直接存储密钥明文相比，本发明只将密钥密文进行永久存储，而将密钥明文只进行短暂存储，从而降低了密钥明文外泄的几率，进而提高了密钥明文的安全性。此外，在获取加密密钥以及解密密钥时，通过采用顺序加密解密的方式，使得当前设备所需的加密密钥以及解密密钥均只有与其相邻的前一设备来确定，而其他设备发送的加密密钥或者解密密钥均不采纳，从而防止他人通过发送错误的加密密钥对密钥明文进行加密，或者防止他人通过发送正确的解密密钥来获取密钥明文，由此进一步提高了密钥明文的安全。

[0112] 该装置实施例与前述方法实施例对应，为便于阅读，本装置实施例不再对前述方法实施例中的细节内容进行逐一赘述，但应当明确，本实施例中的装置能够对应实现前述方法实施例中的全部内容。

[0113] 所述管理密钥的装置包括处理器和存储器，上述获取单元、解密单元、确定单元、传输单元和丢弃单元等均作为程序单元存储在存储器中，由处理器执行存储在存储器中的上述程序单元来实现相应的功能。

[0114] 处理器中包含内核，由内核去存储器中调取相应的程序单元。内核可以设置一个或以上，通过调整内核参数来提高密钥明文的安全性。

[0115] 存储器可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/

或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)，存储器包括至少一个存储芯片。

[0116] 本申请还提供了一种计算机程序产品，当在数据处理设备上执行时，适于执行初始化有如下方法步骤的程序代码：

[0117] 在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥，其中，所述密钥密文为对所述当前设备加密和/或解密消息时所使用的密钥明文进行加密后的文件；

[0118] 利用所述解密密钥对所述密钥密文进行解密；

[0119] 若解密成功获得密钥明文，则在确定所述消息链路被启动后，利用所述密钥明文传输消息；

[0120] 在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃。

[0121] 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。

[0122] 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。

[0123] 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。

[0124] 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。

[0125] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0126] 存储器可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。存储器是计算机可读介质的示例。

[0127] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除

可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0128] 以上仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

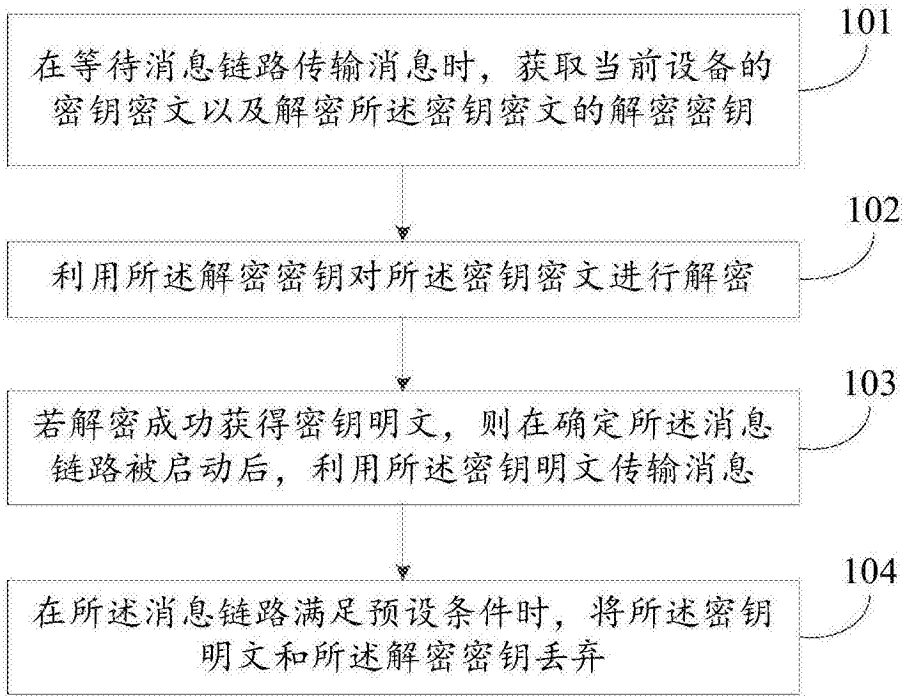

101
在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥
102
利用所述解密密钥对所述密钥密文进行解密
103
若解密成功获得密钥明文，则在确定所述消息链路被启动后，利用所述密钥明文传输消息
104
在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃

图1

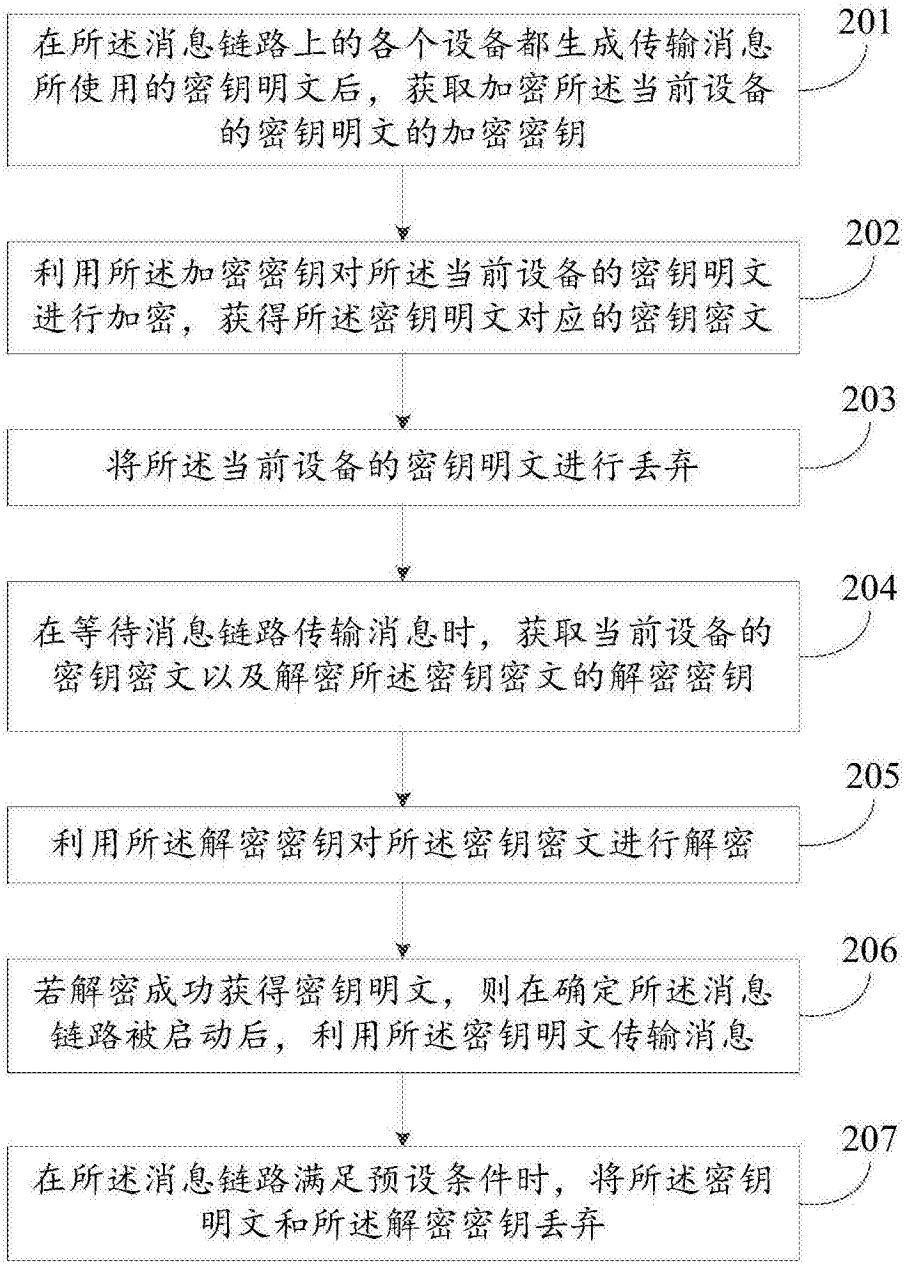

201
在所述消息链路上的各个设备都生成传输消息所使用的密钥明文后，获取加密所述当前设备的密钥明文的加密密钥
202
利用所述加密密钥对所述当前设备的密钥明文进行加密，获得所述密钥明文对应的密钥密文
203
将所述当前设备的密钥明文进行丢弃
204
在等待消息链路传输消息时，获取当前设备的密钥密文以及解密所述密钥密文的解密密钥
205
利用所述解密密钥对所述密钥密文进行解密
206
若解密成功获得密钥明文，则在确定所述消息链路被启动后，利用所述密钥明文传输消息
207
在所述消息链路满足预设条件时，将所述密钥明文和所述解密密钥丢弃

图2

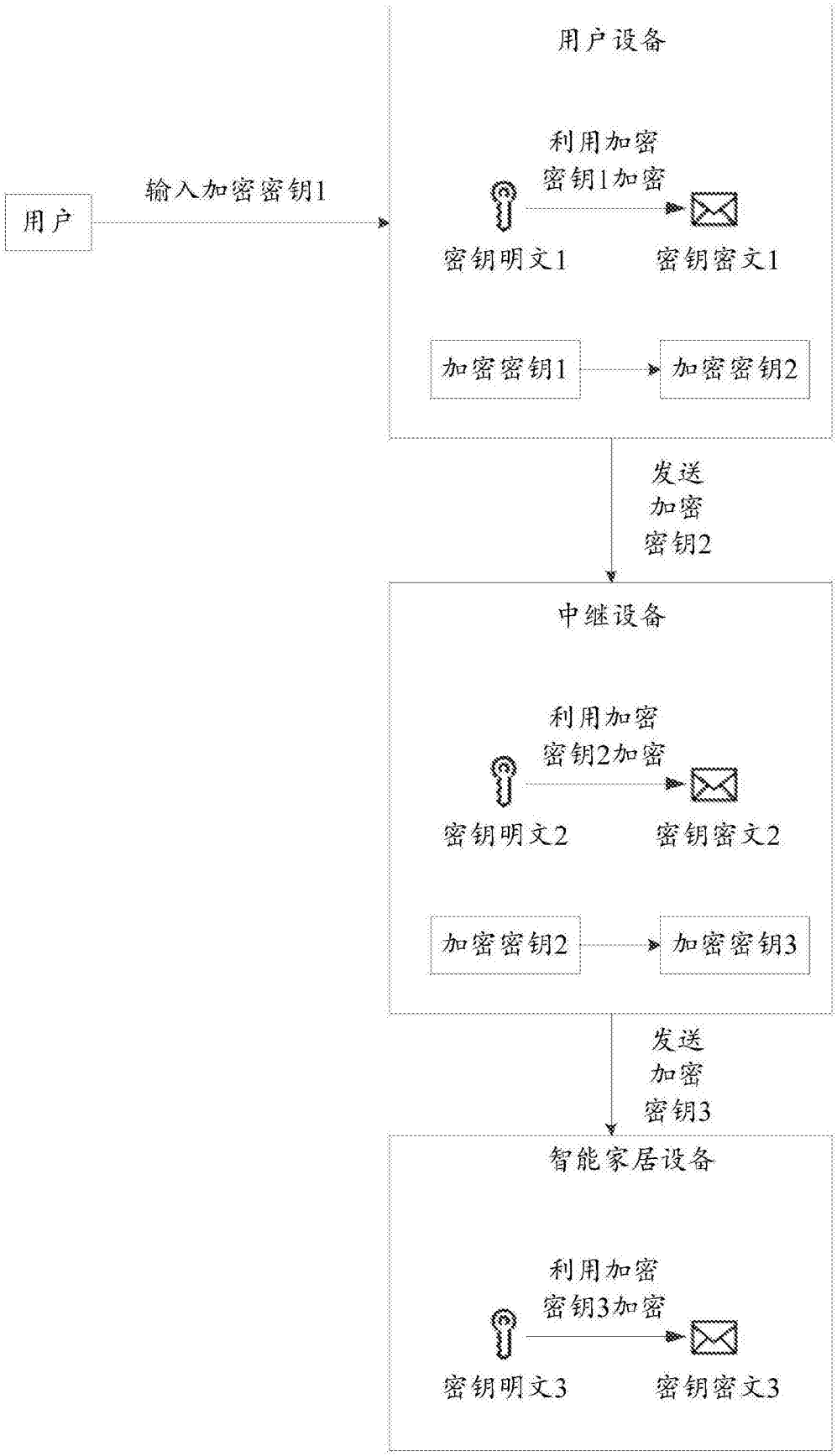

用户设备
利用加密
密钥1加密
用户
输入加密密钥1
密钥明文1
密钥密文1
加密密钥1
加密密钥2
发送
加密
密钥2
中继设备
利用加密
密钥2加密
密钥明文2
密钥密文2
加密密钥2
加密密钥3
发送
加密
密钥3
智能家居设备
利用加密
密钥3加密
密钥明文3
密钥密文3

图3

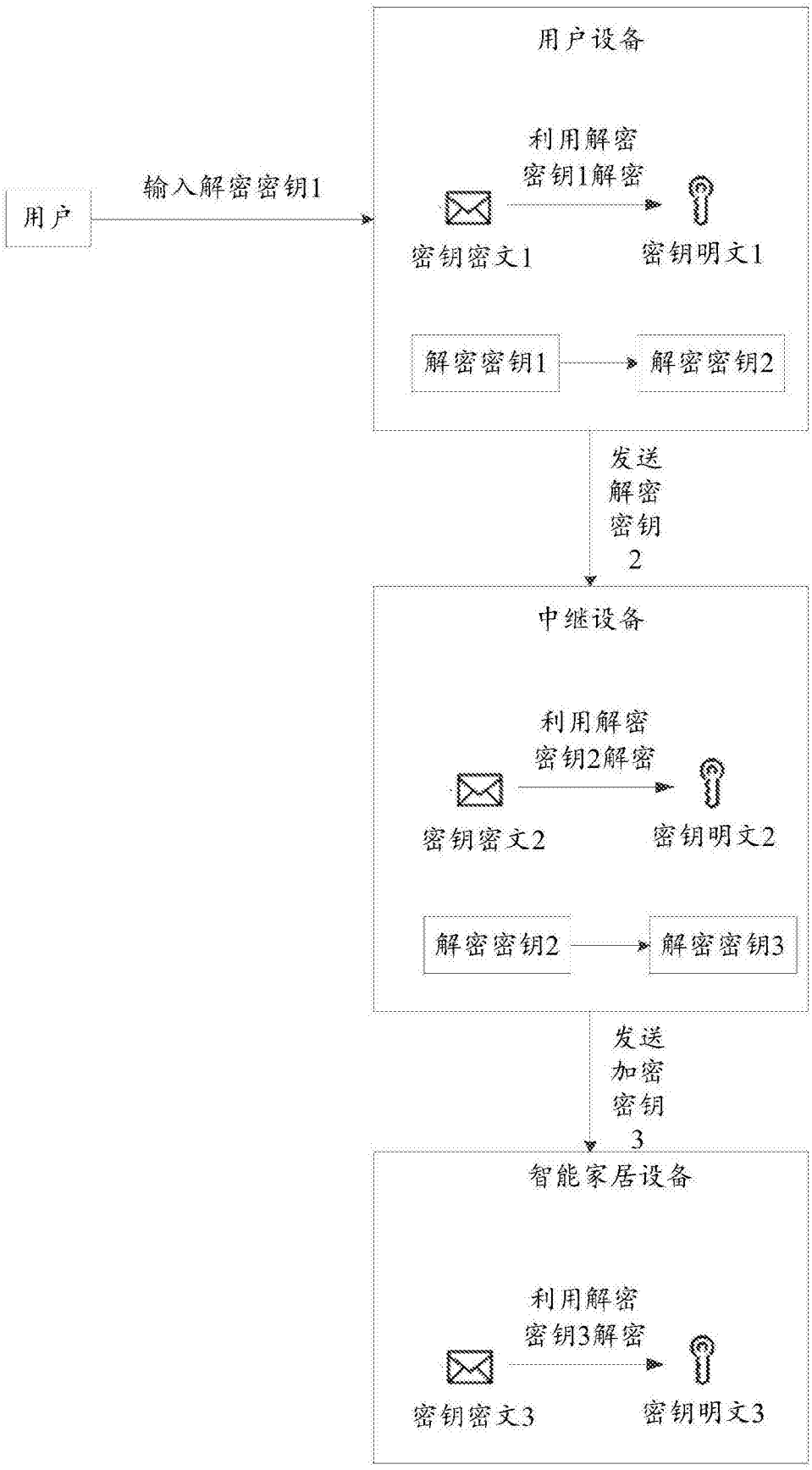

用户设备
利用解密
密钥1解密
用户
输入解密密钥1
密钥密文1
密钥明文1
解密密钥1
解密密钥2
发送
解密
密钥
2
中继设备
利用解密
密钥2解密
密钥密文2
密钥明文2
解密密钥2
解密密钥3
发送
加密
密钥
3
智能家居设备
利用解密
密钥3解密
密钥密文3
密钥明文3

图4

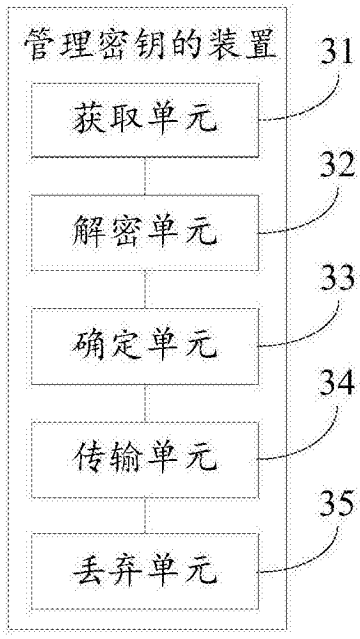


图5

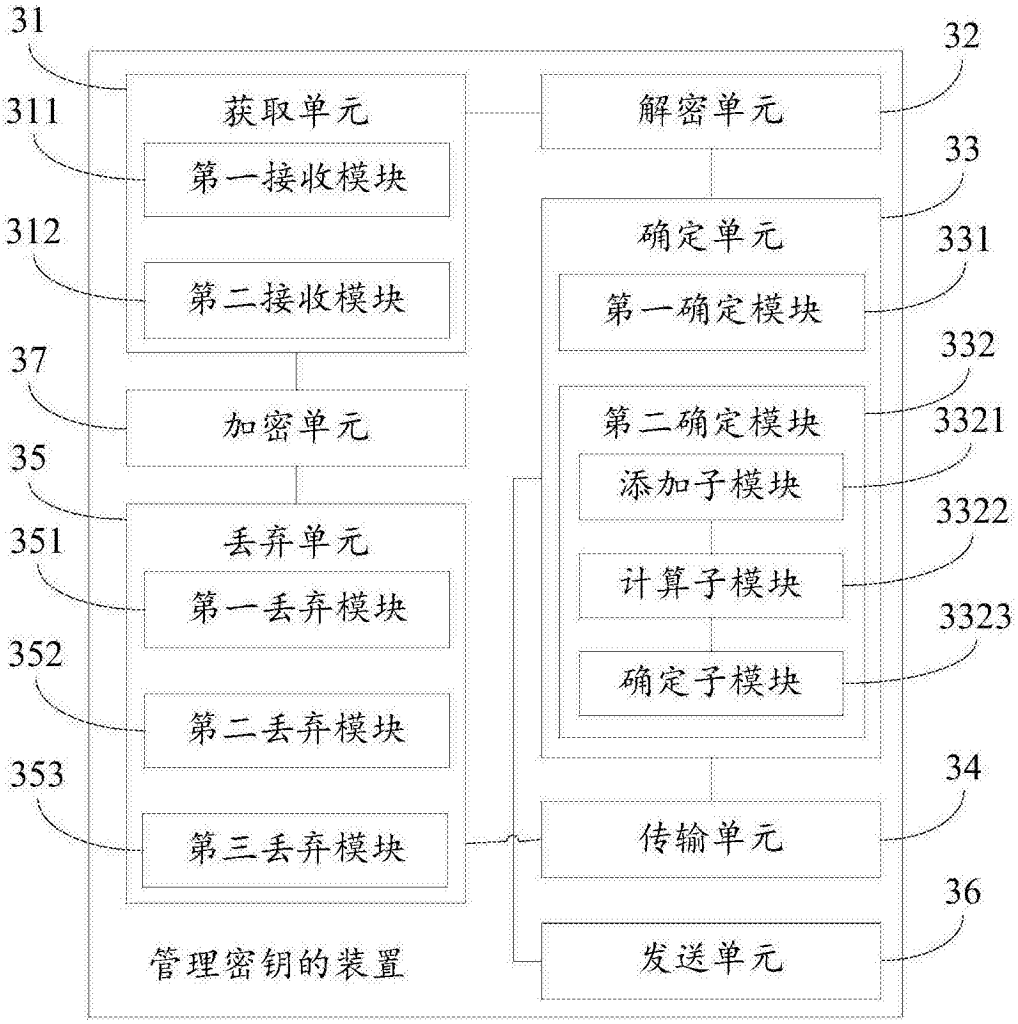

31
32
获取单元
解密单元
311
第一接收模块
33
312
确定单元
331
第二接收模块
第一确定模块
37
332
加密单元
第二确定模块
3321
35
添加子模块
3322
丢弃单元
351
计算子模块
第一丢弃模块
3323
352
确定子模块
第二丢弃模块
353
34
第三丢弃模块
传输单元
36
管理密钥的装置
发送单元

图6