(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 111063070 A
(43)申请公布日 2020.04.24

(21)申请号 201911365909.6

(22)申请日 2019.12.26

(71)申请人 捷德(中国)信息科技有限公司
地址 330096 江西省南昌市高新技术开发区火炬大街

(72)发明人 贺洪恩

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 朱颖 刘芳

(51)Int.Cl.
G07C 9/00(2020.01)

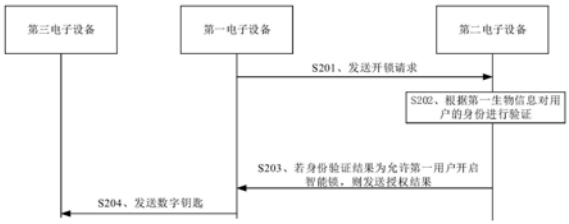
权利要求书2页 说明书14页 附图8页

(54)发明名称

数字钥匙的共享方法、验证方法、及设备

(57)摘要

本发明提供一种数字钥匙的共享方法、验证方法、及设备，该方法包括通过对第一用户的身份进行验证，确定是否允许第一用户开启智能锁，若允许第一用户开启智能锁，则向第一用户发送数字钥匙。相较于现有的去约定地方取回数字钥匙的方法，本方法无需去约定地方取，只需由第二电子设备确定用户身份后将数字钥匙发送给第一电子设备，并由第一电子设备将数字钥匙传输至第三电子设备，第一用户即可使用第三电子设备开启该智能锁。



CN 111063070 A

1.一种数字钥匙的共享方法,其特征在于,应用于第一电子设备,所述方法包括:

向第二电子设备发送开锁请求,所述开锁请求中包括需要开启智能锁的第一用户的第一生物信息;

接收所述第二电子设备返回的授权结果,所述授权结果中包括用于开启所述智能锁的数字钥匙;

向第三电子设备发送所述数字钥匙,所述第三电子设备用于开启所述智能锁。

2.根据权利要求1所述的方法,其特征在于,在所述接收所述第二电子设备生成的授权结果之前,还包括:

接收所述第二电子设备发送的第一获取请求;

根据所述第一获取请求,获取所述第一用户的第二生物信息;

向所述第二电子设备发送所述第二生物信息;

其中,所述第二生物信息用于所述第二电子设备生成所述数字钥匙。

3.根据权利要求2所述的方法,其特征在于,所述接收所述第二电子设备发送的第一获取请求之前,所述方法还包括:

接收所述第二电子设备发送的身份验证结果;所述身份验证结果用于指示是否允许所述第一用户开启所述智能锁。

4.根据权利要求1至3任一项所述的方法,其特征在于,在所述向第二电子设备发送开锁请求之前,还包括:

获取所述第一用户在当前时刻使用所述第一电子设备与第二用户进行通话时的第一语音;其中,所述第一语音用于生成所述开锁请求。

5.根据权利要求4所述的方法,其特征在于,所述第一用户的第一生物信息包括:加密语音,在所述获取所述第一用户在当前时刻使用所述第一电子设备与第二用户进行通话时的第一语音之后,还包括:

向第三电子设备发送所述第一语音;其中,所述第三电子设备使用本地存储的对称公钥对所述第一语音加密,生成加密语音;

接收所述第三电子设备返回的所述加密语音;其中,所述加密语音用于生成所述开锁请求。

6.根据权利要求5所述的方法,其特征在于,在所述接收所述第三电子设备返回的所述加密语音之前,还包括:

接收所述第二电子设备发送的第二获取请求;

根据所述第二获取请求,获取所述第一用户的第一预留信息;

向所述第二电子设备发送所述第一预留信息;

其中,第二电子设备向第四电子设备发送所述第一预留信息,所述第四电子设备使用所述第一预留信息生成所述对称公钥。

7.根据权利要求6所述的方法,其特征在于,在所述接收所述第三电子设备返回的所述加密语音之前,还包括:

向所述第二电子设备发送第三获取请求;其中,所述第三获取请求用于获取第二用户的第二预留信息;

接收所述第二电子设备发送的所述第二预留信息;

向所述第三电子设备发送所述第一预留信息和所述第二预留信息；

其中，所述第一预留信息和所述第二预留信息用于生成所述对称公钥。

8.一种数字钥匙的共享方法，其特征在于，应用于第二电子设备，所述方法包括：

接收第一电子设备发送的开锁请求，所述开锁请求中包括需要开启智能锁的第一用户的第一生物信息；

根据所述第一生物信息，对所述第一用户的身份进行验证；

若允许所述第一用户开启所述智能锁，则向所述第一电子设备发送授权结果，所述授权结果中包括用于开启所述智能锁的数字钥匙。

9.一种数字钥匙的共享方法，其特征在于，应用于第三电子设备，所述第三电子设备包括：安全芯片和第三近场通信NFC芯片；所述方法包括：

通过所述第三NFC芯片接收第一电子设备发送的数字钥匙，所述数字钥匙中包括用于开启智能锁的开锁信息；

将所述数字钥匙存储至所述安全芯片。

10.一种数字钥匙的验证方法，其特征在于，应用于智能锁，所述方法包括：

接收第三电子设备输入的数字钥匙，所述数字钥匙中包括用于开启所述智能锁的开锁信息及第一用户的第二生物信息；

通过传感器获取当前需要开启所述智能锁的第一用户的第二生物信息；

若所述数字钥匙中的第二生物信息与通过传感器获取到的第二生物信息匹配，则根据所述开锁信息控制开启所述智能锁。

11.一种电子设备，其特征在于，包括：第一无线网络通信芯片、第一近场通信NFC芯片、第一传感器及第一处理器，所述第一处理器用于执行权利要求1至7任一项所述的共享方法。

12.一种电子设备，其特征在于，包括：第二无线网络通信芯片、第二近场通信NFC芯片、第二传感器及第二处理器，所述第二处理器用于执行权利要求8所述的共享方法。

13.一种电子设备，其特征在于，包括：第三近场通信NFC芯片、第一安全芯片及第三处理器，所述第三处理器用于执行权利要求9所述的共享方法。

14.一种电子设备，其特征在于，包括：

第三传感器，用于获取用户的生物信息；

存储器，用于存储程序；

第四处理器，用于执行所述存储器存储的所述程序，当所述程序被执行时，所述第四处理器用于执行权利要求10中所述的验证方法。

数字钥匙的共享方法、验证方法、及设备

技术领域

[0001] 本发明涉及数据传输技术领域，尤其涉及一种数字钥匙的共享方法、验证方法、及设备。

背景技术

[0002] 智能锁是是一种使用数字钥匙的开启的电子设备，数字钥匙不同于传统的机械钥匙，常见形式有：近场通信(Near Field Communication，简称：NFC)芯片。当用户使用数字钥匙时，先需要拿到数字钥匙。

[0003] 然而，现有的共享方式是：若用户A要从用户B手中拿到数字钥匙，用户A与用户B先约定取该数字钥匙地方L1，由用户A或者其他人员去约定地方L1取回数字钥匙。但是，当约定地方L1距离数字钥匙所在地方L2比较远，或者约定地方L1距离用户A所在地方L3比较远，用户A将无法快速拿到该数字钥匙。

[0004] 由于现有的共享方法是通过用户或者其他人员去约定地方取回数字钥匙，导致用户无法快速拿到数字钥匙。

发明内容

[0005] 本发明提供一种数字钥匙的共享方法、验证方法、及设备，旨在解决现有共享方法通过用户或者其他人员去约定地方取回数字钥匙，造成用户无法快速拿到数字钥匙的技术问题。

[0006] 第一方面，本发明提供一种数字钥匙的共享方法，应用于第一电子设备，方法包括：向第二电子设备发送开锁请求，开锁请求中包括需要开启智能锁的第一用户的第一生物信息；接收第二电子设备返回的授权结果，授权结果中包括用于开启智能锁的数字钥匙；向第三电子设备发送数字钥匙。

[0007] 可选地，在接收第二电子设备生成的授权结果之前，还包括：接收第二电子设备发送的第一获取请求；根据第一获取请求，获取第一用户的第二生物信息；向第二电子设备发送第二生物信息；其中，第二生物信息用于第二电子设备生成数字钥匙。

[0008] 可选地，接收第二电子设备发送的第一获取请求之前，方法还包括：接收第二电子设备发送的身份验证结果；身份验证结果用于指示是否允许第一用户开启智能锁。

[0009] 可选地，第一用户的第一生物信息包括：第一语音，在向第二电子设备发送开锁请求之前，还包括：获取第一用户在当前时刻使用第一电子设备与第二用户进行通话时的第一语音；其中，第一语音用于生成开锁请求。

[0010] 可选地，第一用户的第一生物信息包括：加密语音，在获取第一用户在当前时刻使用第一电子设备与第二用户进行通话时的第一语音之后，还包括：向第三电子设备发送第一语音；其中，第三电子设备使用本地存储的对称公钥对第一语音加密，生成加密语音；接收第三电子设备返回的加密语音；其中，加密语音用于生成开锁请求。

[0011] 可选地，在接收第三电子设备返回的加密语音之前，还包括：接收第二电子设备发

送的第二获取请求;根据第二获取请求,获取第一用户的第一预留信息;向第二电子设备发送第一预留信息;其中,第二电子设备向第四电子设备发送第一预留信息,第四电子设备使用第一预留信息生成对称公钥。

[0012] 可选地,在接收第三电子设备返回的加密语音之前,还包括:向第二电子设备发送第三获取请求;其中,第三获取请求用于获取第二用户的第二预留信息;接收第二电子设备发送的第二预留信息;向第三电子设备发送第二预留信息和第一预留信息;其中,第一预留信息和第二预留信息用于生成对称公钥。

[0013] 可选地,第一电子设备包括:第一NFC芯片,在向第二电子设备发送开锁请求之前,还包括:通过第一NFC芯片获取从第三电子设备返回的第一加密标识;向第二电子设备发送第一加密标识;其中,第一加密标识用于生成开锁请求。

[0014] 可选地,数字钥匙还包括:有效期限。

[0015] 第二方面,本发明提供一种数字钥匙的共享方法,应用于第二电子设备,方法包括:接收第一电子设备发送的开锁请求,开锁请求中包括需要开启智能锁的第一用户的第一生物信息;根据第一生物信息,对第一用户的身份进行验证;若允许第一用户开启智能锁,则向第一电子设备发送授权结果,授权结果中包括用于开启智能锁的数字钥匙。

[0016] 可选地,向第一电子设备发送授权结果之前,方法还包括:向第一电子设备发送第一获取请求,其中,第一获取请求用于获取第一用户的第二生物信息;接收第一电子设备发送的第二生物信息;根据第二生物信息以及本地存储的开启智能锁的开锁信息生成数字钥匙。

[0017] 可选地,向第一电子设备发送第一获取请求之前,方法还包括:向第一电子设备发送身份验证结果,身份验证结果用于指示是否允许第一用户开启智能锁。

[0018] 可选地,第一生物信息包括:第一用户的第一语音;根据第一生物信息,对第一用户的身份进行验证,具体包括:获取第二用户在当前使用第二电子设备与第一用户进行通话时的第二语音;对第二语音与第一语音进行匹配处理。

[0019] 可选地,第一生物信息包括:第一用户的加密语音;在确定第二语音与第一语音是否匹配之前,还包括:向第四电子设备发送加密语音,其中,第四电子设备使用对称公钥对加密语音进行解密生成第一语音;接收第四电子设备返回的第一语音。

[0020] 可选地,在接收第四电子设备返回的第一语音之前,还包括:接收第一电子设备发送的第三获取请求;根据第三获取请求,获取第二用户的第二预留信息;向第一电子设备发送第二预留信息;其中,第二预留信息用于第一电子设备生成对称公钥。

[0021] 可选地,在使用对称公钥对加密语音进行解密,获得第一语音之前,还包括:向第一电子设备发送第二获取请求;第二获取请求用于获取第一用户的第一预留信息;接收第一电子设备发送的第一预留信息;向第四电子设备发送第二预留信息和第一预留信息;其中,第一预留信息和第二预留信息用于生成对称公钥。

[0022] 可选地,开锁请求还包括:第一加密标识;在若允许第一用户开启智能锁,则向第一电子设备发送授权结果之前,还包括:接收第一电子设备返回的第一加密标识;将第一加密标识发送至第四电子设备,其中,第四电子设备使用本地存储的第一私钥对第一加密标识进行解密生成第三标识,并根据本地存储的第二公钥对第三标识进行加密生成第二加密标识;接收第四电子设备返回的第二加密标识;将第二加密标识发送至服务器;接收服务器

返回的设备验证结果，若设备验证结果为允许第三电子设备开启智能锁。

[0023] 可选地，在根据第二生物信息以及本地存储的开启智能锁的开锁信息生成数字钥匙之后，还包括：在数字钥匙中添加有效期限。

[0024] 第三方面，本发明提供一种数字钥匙的共享方法，应用于第三电子设备，第三电子设备包括：第一安全芯片和第三近场通信NFC芯片；方法包括：通过第三NFC芯片接收第一电子设备发送的数字钥匙，数字钥匙中包括用于开启智能锁的开锁信息；将数字钥匙存储至安全芯片。

[0025] 可选地，在通过第三NFC芯片接收第一电子设备发送的数字钥匙之前，还包括：第三电子设备接收第一电子设备返回的第一预留信息和第二预留信息；第三电子设备根据第一预留信息和第二预留信息生成对称公钥。

[0026] 可选地，在通过第三NFC芯片接收第一电子设备发送的数字钥匙之前，还包括：第三电子设备接收第一电子设备发送的第一语音；使用对称公钥对第一语音进行加密处理生成加密语音；向第一电子设备发送加密语音。

[0027] 可选地，在通过第三NFC芯片接收第一电子设备发送的数字钥匙之前，还包括：第三电子设备获取第三电子设备的第三标识；使用第一公钥对第三标识进行加密处理生成第一加密标识；向第一电子设备发送第一加密标识。

[0028] 第四方面，本发明提供一种数字钥匙的验证方法，应用于智能锁，方法包括：接收第一电子设备输入的数字钥匙，数字钥匙中包括用于开启智能锁的开锁信息以及第一用户的第二生物信息；通过传感器获取当前需要开启智能锁的第一用户的第二生物信息；若数字钥匙中的第一第二生物信息与通过传感器获取到的第二生物信息匹配，则根据开锁信息控制开启智能锁。

[0029] 可选地，开锁信息控制开启智能锁，具体包括：

[0030] 若开锁信息与存储在本地的预留开锁信息匹配，则开启智能锁。

[0031] 可选地，预留开锁信息包括：至少一个用户、用户的指纹数据、及用户的钥匙标识。

[0032] 可选地，数字钥匙中还包括：有效期限，在根据开锁信息控制开启智能锁之前，还包括：判断数字钥匙的使用期限达到有效期限，若未达到。

[0033] 可选地，在若数字钥匙中的第一第二生物信息与通过传感器获取到的第二生物信息匹配，则根据开锁信息控制开启智能锁之前，还包括：

[0034] 获取第三电子设备的第三标识；

[0035] 根据第三标识和智能锁中记录数据确定第三电子设备的使用次数；

[0036] 若使用次数小于预设数量。

[0037] 第五方面，本发明提供一种电子设备，包括：第一无线网络通信芯片、第一近场通信NFC芯片、第一传感器及第一处理器，第一处理器用于执行第一方面及可选方案所涉及的共享方法。

[0038] 第六方面，本发明提供一种电子设备，包括：第二无线网络通信芯片、第二近场通信NFC芯片、第二传感器及第二处理器，第二处理器用于执行第二方面及可选方案所涉及的共享方法。

[0039] 第七方面，本发明提供一种电子设备，包括：第三近场通信NFC芯片、第一安全芯片及第三处理器，第三处理器用于执行第三方面及可选方案所涉及的共享方法。

[0040] 第八方面，本发明提供一种电子设备，包括：第三传感器，用于获取用户的生物信息；存储器，用于存储程序；第四处理器，用于执行存储器存储的程序，当程序被执行时，第四处理器用于执行第四方面及可选方案所涉及的验证方法。

[0041] 本发明提供的数字钥匙的共享方法、验证方法及设备，在数字钥匙的共享方法中，先确定是否允许第一用户开启智能锁，具体为第一电子设备向第二电子设备发送第一用户的第一生物信息，使第二电子设备根据该第一生物信息验证第一用户的身份，若允许第一用户开启智能锁，则向第一用户发送数字钥匙。相较于现有的去约定地方取回数字钥匙的方法，本方法无需去约定地方取，只需由第二电子设备确定用户身份后将数字钥匙发送给第一电子设备，即可实现更快速的共享数字钥匙。

附图说明

[0042] 图1为本发明提供的数字钥匙的共享系统的结构示意图；

[0043] 图2为本发明根据一示例性实施例示出的数字钥匙的共享方法的流程示意图；

[0044] 图3为本发明根据另一示例性实施例示出的数字钥匙的共享方法的流程示意图；

[0045] 图4为本发明根据再一示例性实施例示出的共享方法中初始化的流程示意图；

[0046] 图5为本发明根据再一示例性实施例示出的共享方法中验证过程的流程示意图；

[0047] 图6为本发明根据再一示例性实施例示出的验证方法中流程示意图；

[0048] 图7为本发明根据再一示例性实施例示出的验证方法中流程示意图；

[0049] 图8为本发明根据再一示例性实施例示出的共享装置的机构示意图；

[0050] 图9为本发明根据再一示例性实施例示出的共享装置的机构示意图；

[0051] 图10为本发明根据再一示例性实施例示出的共享装置的机构示意图；

[0052] 图11为本发明根据再一示例性实施例示出的验证装置的机构示意图。

具体实施方式

[0053] 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中的附图，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做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。

[0054] 现有的数字钥匙的共享方法，通过双方约定地点，由使用者或者其他人员去约定地方取回数字钥匙，实现数字钥匙的共享，现有的共享方法由于需要到约定地方取回数字钥匙，无法快速拿到数字钥匙。

[0055] 本发明的发明构思是：第一用户向第二用户请求开启智能锁的数字钥匙，先对第一用户的身份进行验证，若允许第一用户开启智能锁，则向第一用户发送数字钥匙。其中，在对第一用户进行身份验证时，使用两个电子设备进行通话过程的语音作为验证内容，并用第一用户和第二用户的预留信息生成对称公钥，对语音进行加密，以提高身份验证过程的安全性。在生成数字钥匙的过程中，获取第一用户的生物信息，联合智能锁的开锁信息共同生成数字钥匙，提高数字钥匙的安全性。本申请不仅可以实现让用户快速拿到数字钥匙，还可保证钥匙共享的安全性。

[0056] 本发明可应用于智能汽车、住宅等使用智能锁的场景。在智能汽车应用场景，若车

主的朋友需要使用车或者授权代驾使用，车主在任何位置均可通过本方法共享数字钥。

[0057] 图1为本发明提供的数字钥匙的共享系统的结构示意图。如图1所示，本发明提供的共享系统100包括：第一电子设备110、第二电子设备120、第三电子设备130、及第四电子设备140。第一用户使用第一电子设备110与第二电子设备120通信，实现第一用户与第二用户通信。第二用户可使用第四电子设备140直接开启智能锁。

[0058] 第一电子设备110包括第一NFC芯片、第一传感器和第一无线网通信芯片。第二电子设备120包括第二NFC芯片、第二传感器和第二无线网通信芯片。第三电子设备130包括第三NFC芯片和第一安全芯片。第四电子设备140包括第四NFC芯片和第二安全芯片。

[0059] 第一电子设备110和第二电子设备120之间通过第一无线网通信芯片和第二无线网通信芯片进行通信，第一电子设备110与第三电子设备130之间通过第一NFC芯片和第三NFC芯片进行通信，第二电子设备120与第四电子设备140之间通过第二NFC芯片和第四NFC芯片进行通信。

[0060] 在本实施例中，第一电子设备和第三电子设备分为第一用户所持有的终端设备和钥匙卡，第二电子设备和第四电子设备分别为第二用户所持有的终端设备和钥匙卡。

[0061] 为了使第一用户使用所持有的第三电子设备开启该智能锁，第一用户所持有的第一电子设备110向第二用户所持有的第二电子设备120发送开锁请求，其中，开锁请求中包括第一用户的第一生物信息和第三电子设备130的第三标识，第二电子设备120将开锁请求的中第一生物信息和第三标识通过第二NFC芯片发送给第二用户所持有的第四电子设备140，由第四电子设备140中第二安全芯片进行解密，第四电子设备140将解密后的第一生物信息和第三标识通过四NFC芯片发送给第二电子设备120，第二电子设备120根据第一生物信息确定是否授权第一用户开启智能锁，并根据第三标识确定是否允许第三电子设备130开启智能锁，若允许第一用户使用第三电子设备130开启智能锁，则向第一电子设备110发送数字钥匙，第一电子设备110将数字钥匙通过第一NFC芯片存入第三电子设备130的第一安全芯片中。

[0062] 图2为本发明根据一示例性实施例示出的数字钥匙的共享方法的流程示意图。如图2所示，本发明提供的一种数字钥匙的共享方法，方法包括如下步骤：

[0063] S201、第一电子设备向第二电子设备发送开锁请求。

[0064] 更具体地，第一电子设备为第一用户所持有的终端设备，第二电子设备为第二用户所持有的终端设备。第一用户所持有的终端设备向第二用户所持有的终端设备发送开锁请求，开锁请求中包括第一用户的第一生物信息，其中，第一用户的第一生物信息为可识别第一用户身份的信息，用于识别第一用户的身份。第一生物信息可为：虹膜、指纹、声音等信息。

[0065] S202、第二电子设备根据第一生物信息对用户的身份进行验证。

[0066] 更具体地，第二用户所持有的终端设备将存储在本地的生物信息与接收的第一生物信息进行比较，若二者相同，则允许第一用户开启智能锁，若二者不相同，则不允许第一用户开启智能锁。

[0067] S203、若身份验证结果为允许第一用户开启智能锁，则第二电子设备向第一电子设备发送授权结果。

[0068] 更具体地，确定允许第一用户开启智能锁，第二用户所持有的终端设备向第一用

户所持有的终端设备发送授权结果，授权结果中包括数字钥匙，该数字钥匙用于开启智能锁。

[0069] S204、第一电子设备向第三电子设备发送数字钥匙。

[0070] 更具体地，第三电子设备为第一用户持有的钥匙卡，第一用户所持有的终端设备从授权结果中提取出数字钥匙，通过NFC传输向第一用户持有的钥匙卡传输数字钥匙，第一用户使用钥匙卡开启智能锁。

[0071] 在本实施例中，第一电子设备和第二电子设备不限定为终端设备，第三电子设备不限定为钥匙卡，可以为其他设备。

[0072] 在本实施例中，第一用户向第二用户请求开启智能锁的数字钥匙，第二电子设备先对第一用户的身份进行验证，若允许第一用户开启智能锁，则向第一电子设备发送数字钥匙。相较于现有的方法，本方案无需到约定地方取回数字钥匙，可快速取到数字钥匙。

[0073] 图3为本发明根据另一示例性实施例示出的数字钥匙的共享方法的流程示意图。如图3所示，本发明提供的共享方法包括如下步骤：

[0074] S301、第一电子设备向第二电子设备发送开锁请求。

[0075] 更具体地，第一电子设备为第一用户所持有的终端设备，第二电子设备为第二用户所持有的终端设备。第一用户所持有的终端设备向第二用户所持有的终端设备发送开锁请求。

[0076] S302、第二电子设备根据第一生物信息对用户的身份进行验证生成身份验证结果。

[0077] S303、第二电子设备向第一电子设备发送身份验证结果。

[0078] S304、若身份验证结果允许第一用户开启智能锁，则第二电子设备向第一电子设备发送第一获取请求。

[0079] 更具体地，第一获取请求用于获取第一用户的第二生物信息，该第二生物信息用于生成数字钥匙，将第二生物信息添加到数字钥匙中，可防止未被授权的用户使用该数字钥匙开启智能锁，提高数字钥匙共享的可靠性。其中，第二生物信息用于识别第一用户的身份，第二生物信息可以为：虹膜、声音、指纹等信息。

[0080] S305、第一电子设备根据第一获取请求获第二生物信息。

[0081] 更具体地，在接收到第一获取请求之后，使用第二电子设备中设置的第二传感器采集第一用户的第二生物信息。

[0082] S306、第一电子设备向第二电子设备发送第二生物信息。

[0083] S307、第二电子设备根据第二生物信息及本地存储的开启智能锁的开锁信息生成数字钥匙。

[0084] 更具体地，开锁信息为开启智能锁的信息，第二用户可使用所持有的第四电子设备开启该智能锁，因此，开锁信息包括：第四电子设6备的标识和第二用户的第二生物信息。第二电子设备通过NFC传输获取第四电子设备的标识，并通过第二传感器采集第二用户的第二生物信息，并将上述标识和第二生物信息存储在本地。第二电子设备对第二生物信息及开锁信息进行处理，生成数字钥匙。

[0085] 在本实施例中，对第二生物信息及开锁信息使用哈希操作生成数字钥匙。也可采用其它算法获得数字钥匙，此处不做限制。

[0086] S308、第二电子设备获取数字钥匙的有效期限。

[0087] 更具体地，第二电子设备获取第二用户输入的有效期限，有效期限为数字钥匙的有效期限，用于限制数字钥匙的使用期限。例如：有效期限为24小时，以第一电子设备接收到授权结果的时刻为计时初始时刻，计时时长达到24小时后，该数字钥匙失效。

[0088] S309、第二电子设备根据有效期限和数字钥匙生成授权结果。

[0089] S310、第二电子设备向第一电子设备发送授权结果。

[0090] S311、第一电子设备将数字钥匙发送至第三电子设备。

[0091] 更具体地，第三电子设备为第一用户持有的钥匙卡，将第一用户持有的第一电子设备与第三电子设备贴合，使第一电子设备通过NFC传输向第三电子设备发送数字钥匙。

[0092] S312、第三电子设备将数字钥匙存储在第一安全芯片中。

[0093] 更具体地，第一安全芯片可防止数据被盗用，将数字钥匙存储在第一安全芯片中，可以提高数字钥匙的可靠性。

[0094] 在本实施例中，数字钥匙由第一用户的第二生物信息与开锁信息生成，可防止数字钥匙被未授权的用户拿到后使用该数字钥匙开启智能锁，并设置数字钥匙的使用期限，提高钥匙共享的可靠性。

[0095] 本发明根据再一示例性实施例示出的共享方法包括初始化过程和验证过程。其中，图4为本发明根据再一示例性实施例示出的共享方法中初始化的流程示意图。如图4所示，初始化具体包括如下步骤：

[0096] S401、第二电子设备向第一电子设备发送第二获取请求。

[0097] 更具体地，第一电子设备为第一用户所持有的终端设备，第二电子设备为第二用户所持有的终端设备。第二用户所持有的终端设备向第一用户所持有的终端设备发送第二获取请求。第二获取请求用于获取第一用户的第一预留信息。其中，第一预留信息存储在第一电子设备中。第一预留信息用于生成对称公钥。

[0098] 在本实施例中，第一预留信息包括第一用户的生物信息和获取该生物信息的时刻。其中，生物信息包括：虹膜、指纹、声音等信息。预留信息也可为其他信息，此处不做限定。

[0099] S402、第一电子设备根据第二获取请求获取第一预留信息。

[0100] 更具体地，第一预留信息为第一用户的生物信息和获取该生物信息的时刻。第一电子设备使用第一传感器采集第一用户的生物信息，并记录下采集该生物信息的时刻。

[0101] S403、第一电子设备分别向第二电子设备和第三电子设备发送第一预留信息。

[0102] 更具体地，第三电子设备为第一用户所持有的钥匙卡，第一电子设备通过无线网络通信发送第一预留信息给第二电子设备。将第一电子设备与第三电子设备贴合，使第一电子设备通过NFC传输向第三电子设备发送第一预留信息。

[0103] S404、第二电子设备向第四电子设备发送第一预留信息。

[0104] 更具体地，第四电子设备为第二用户所持有的钥匙卡，将第二电子设备与第四电子设备贴合，使第二电子设备通过NFC传输向第四电子设备发送第一预留信息。

[0105] S405、第一电子设备向第二电子设备发送第三获取请求。

[0106] 更具体地，第三获取请求用于获取第二用户的第二预留信息。其中，第二预留信息存储在第二电子设备中。第二预留信息用于生成对称公钥。在本实施例中，第二预留信息包

括第二用户的生物信息和获取该生物信息的时刻。其中，生物信息包括：虹膜、指纹、声音等信息。

[0107] S406、第二电子设备根据第三获取请求获取第二预留信息。

[0108] 更具体地，第二预留信息为第二用户的生物信息和获取该生物信息的时刻。第二电子设备使用第二传感器采集第二用户的生物信息，并记录下采集该生物信息的时刻。

[0109] S407、第二电子设备向第一电子设备和第四电子设备发送第二预留信息。

[0110] 更具体地，第二电子设备通过无线网络通信发送第二预留信息给第一电子设备。将第二电子设备与第四电子设备贴合，使第二电子设备通过NFC传输向第四电子设备发送第二预留信息。

[0111] S408、第一电子设备向第三电子设备发送第二预留信息。

[0112] 更具体地，将第一电子设备与第三电子设备贴合，使第一电子设备通过NFC传输向第三电子设备发送第二预留信息。

[0113] S409、第三电子设备使用预设算法对第一预留信息和第二预留信息进行处理生成对称公钥。

[0114] 更具体地，在第三电子设备和第四电子设备中预先存储相同的算法，该算法用于生成对称公钥。在本实施例中，用于生成对称公钥的算法的具体运算过程为：对第一预留信息进行哈希(HASH)操作，生成第一哈希值。对第二预留信息进行哈希操作，生成第二哈希值。对第一哈希值和第二哈希值进行运算，生成对称秘钥。

[0115] 例如：第一预留信息为张三的指纹信息和获取指纹信息的时间戳，对指纹信息和该时间戳进行哈希操作，得到第一哈希值。第二预留信息为李四的指纹信息和获取该指纹的时间戳，对指纹信息和时间戳进行哈希操作，得到第二哈希值。对第一哈希值和第二哈希值采用以下任意一种方式获得对称秘钥。具体为：从第一哈希值和第二哈希值中分别选取一段数据，将两段数据合并后作为对称秘钥。对第一哈希值和第二哈希值进行哈希操作，生成对称秘钥。将第一哈希值和第二哈希值相加，生成对称秘钥。将第一哈希值和第二哈希值相减，生成对称秘钥。取第二哈希值的一半或者取第一哈希值的一半作为对称秘钥。

[0116] S410、第四电子设备使用预设算法对第一预留信息和第二预留信息进行处理生成对称公钥。

[0117] 更具体地，第四电子设备使用相同的算法对第一预留信息和第二预留信息进行处理生成对称公钥，使得第四电子设备可使用该对称公钥对第三电子设备发送的加密数据进行解密处理。

[0118] 在本实施例中，第一非对称秘钥包括第一私钥和第一公钥，其中，第四电子设备中存储有第一私钥，第三电子设备中存储有第一公钥。第一电子设备和第三电子设备之间非对称公钥的初始化不再赘述。

[0119] 第二非对称秘钥包括第二公钥和第二私钥。其中，第四电子设备中存储有第二公钥，服务器中存储有第二私钥。第四电子设备和服务器之间非对称公钥的初始化不再赘述。

[0120] 图5为本发明根据再一示例性实施例示出的共享方法中验证过程的流程示意图。如图5所示，本发明提供的验证过程如下：

[0121] S501、第三电子设备使用第一公钥对第三标识加密生成第一加密标识。

[0122] 更具体地，第三电子设备为第一用户所持有的钥匙卡，第三标识为第三电子设备

的标识，第三电子设备获取自身的标识，并使用第一公钥对第三标识加密生成第一加密标识。

[0123] S502、第三电子设备接收第一电子设备发送的第一语音。

[0124] 更具体地，第一电子设备为第二用户所持有的终端设备，将第三电子设备与第一电子设备贴合，以便第三电子设备与第一电子设备之间进行NFC传输，第一语音为第一用户在当前时刻使用第一电子设备与第二用户通话过程中的语音，音内容可以为任意内容，第一电子设备将通话语音发送通过NFC传输发送给第三电子设备。

[0125] S503、第三电子设备使用对称公钥对第一语音进行加密生成加密语音。

[0126] S504、第三电子设备向第一电子设备发送第一加密标识和加密语音。

[0127] 更具体地，将第三电子设备与第一电子设备贴合，第三电子设备通过NFC传输向第一电子设备第一加密标识和加密语音。

[0128] S505、第一电子设备根据第一加密标识和加密语音生成开锁请求。

[0129] S506、第一电子设备向第二电子设备发送开锁请求。

[0130] 更具体地，第二电子设备为第二用户持有的终端设备。

[0131] S507、第二电子设备从开锁请求中提取加密语音和第一加密标识。

[0132] S508、第二电子设备向第四电子设备发送加密语音和第一加密标识。

[0133] 更具体地，第四电子设备为第二用户所持有的钥匙卡，将第二电子设备与第四电子设备贴合，使第二电子设备通过NFC传输向第四电子设备发送加密语音和第一加密标识。

[0134] S509、第四电子设备使用对称秘钥对加密语音进行解密。

[0135] S510、第四电子设备使用第一私钥对第一加密标识进行解密，并使用第二公钥对第三标识进行加密。

[0136] 更具体地，第一私钥和第一公钥为一对非对称秘钥，第一公钥存储在第三电子设备中，第一私钥存储在第四电子设备中，第三电子设备使用第一公钥对第三电子设备的第三标识进行加密，生成第一加密标识。第四电子设备在接收到第一加密标识后，使用第一私钥对第一加密标识进行解密，生成第三标识。第二公钥和第二私钥为一对非对称秘钥，第二公钥存储在第四电子设备中，第二私钥存储在服务器中，服务器为生产第三电子设备的产商所拥有，在服务器中存储有其生产的电子设备的标识，使用第二公钥对第三标识进行加密生成第二加密标识，将第二加密标识通过NFC传输发送至第二电子设备，再有第二电子设备通过无线网络发送至服务器，以对第三电子设备的合法性进行验证。

[0137] S511、第四电子设备向第二电子设备发送第一语音和第二加密标识。

[0138] 更具体地，将第二电子设备与第四电子设备贴合，使第四电子设备通过NFC传输向第二电子设备发送第一语音和第二加密标识。

[0139] S512、第二电子设备向服务器发送第二加密标识，并接收服务器返回的设备验证结果。

[0140] 更具体地，第二电子设备通过无线网络将第二加密标识发送给服务器，服务器使用第二私钥对第二加密标识进行解密，生成第三标识，并与存储在本地的标识信息进行比较，并生成设备验证结果。若在服务器中存储有第三电子设备的标识，则设备验证结果为授权第三电子设备开启智能锁，若在服务器中不存在第三电子设备的标识，则设备验证结果为不授权第三电子设备开启智能锁，最终实现验证第三电子设备的合法性。

[0141] S513、第二电子设备获取第二语音。

[0142] 更具体地，第二语音为第二用户在当前时刻使用第二电子设备与第一用户通话时的语音。由于第一用户使用第一电子设备与第二用户通话时，第一电子设备和第二电子设备均可获取该通话语音，则可以利用该通话语音验证第一用户的身份。

[0143] S514、第二电子设备将第二语音和第一语音进行比较，生成身份验证结果。

[0144] 更具体地，第二电子设备获取与第一电子设备通话过程中的第二语音，比较第二语音和第一电子设备发送的第一语音，生成身份验证结果，若第一语音和第二语音相同，则设备验证结果为授权第一用户开启智能锁，若第一语音和第二语音不相同，则设备验证结果为不授权第一用户开启智能锁。

[0145] S515、第二电子设备根据设备验证结果和身份验证结果确定验证结果。

[0146] 更具体地，若设备验证结果为授权第三电子设备开启智能锁，身份验证结果为授权第一用户开启智能锁，则验证结果为允许第一用户使用第三电子设备开启该智能锁，并向第一电子设备返回授权结果，授权结果中包含数字钥匙和有效期限。若设备验证结果和身份验证结果中任意一个为不授权，则不向第一电子设备返回授权结果。

[0147] 在本实施例中，对第三电子设备和第二用户进行双重验证，可提高数字钥匙共享的可靠性。

[0148] 图6为本发明根据再一示例性实施例示出的验证方法中流程示意图。如图6所示，本发明提供的数字钥匙的验证方法，应用于智能锁，方法包括：

[0149] S601、接收第三电子设备输入的数字钥匙。

[0150] 更具体地，数字钥匙中包括开锁信息及第一用户的第二生物信息。其中，开锁信息用于开启智能锁。

[0151] S602、通过传感器获取当前需要开启智能锁的第一用户的第三生物信息。

[0152] 更具体地，由智能锁中传感器采集第一用户的第三生物信息，第三生物信息用于与数字钥匙中第二生物信息进行比较，验证第一用户的身份。

[0153] S603、确定第二生物信息和第三生物信息是否匹配，若匹配，则进入S604否则，进入S605。

[0154] S604、根据开锁信息控制开启智能锁。

[0155] 更具体地，若第二生物信息和第三生物信息匹配，则第一用户的身份合法，也就是允许第一用户开启该智能锁。由于第二用户可使用第四电子设备开启智能锁，智能锁中存储有第二用户的生物信息和第四电子设备的标识信息，将开锁信息与存储在本地的预留开锁信息进行匹配，若开锁信息与预留开锁信息匹配，则开启智能锁。

[0156] 智能锁中可存储多个用户的生物信息和电子设备的标识信息，以便多个用户可授权其他用户开启该智能锁。当该智能锁初始使用时，在智能锁中仅保存该智能锁的主人的生物信息和电子设备的标识，主人可使用该电子设备开启智能锁。主人可将其他用户和对应电子设备的标识添加至智能锁中，多个用户可授权其他人开启该智能锁。

[0157] S605、返回提示信息。

[0158] 更具地，提示信息用于提示用户开锁失败。

[0159] 在本实施例提供的验证方法中，通过验证第一用户的生物信息确定第一用户是否可开启该智能锁，再验证数字钥匙的开锁信息是否与本地存储的开锁信息是否匹配，即可

控制该智能锁，通过双重验证可提高验证结果可靠性。

[0160] 图7为本发明根据再一示例性实施例示出的验证方法中流程示意图。如图7所示，本发明提供的数字钥匙的验证方法，应用于智能锁，方法包括：

[0161] S701、接收第三电子设备输入的数字钥匙和第三电子设备的标识。

[0162] S702、根据第三电子设备的标识和智能锁中记录数据确定第三电子设备的开锁次数。

[0163] 更具体地，当第三电子设备开启一次智能锁，智能锁记录下第三电子设备开启次数，当第三电子设备再次开启智能锁时，则可通过记录数据确定第三电子设备的开启次数。

[0164] S703、若第三电子设备的开锁次数达到预设数量，则进入S708，否则，进入S704。

[0165] 更具体地，可设置预设数量为1次，仅允许第三电子设备开启该智能锁一次。可设置预设数量为多次，也就是允许第三电子设备多次开启该智能锁。

[0166] S704、通过传感器获取当前需要开启智能锁的第一用户的第三生物信息。

[0167] S705、确定第二生物信息和第三生物信息是否匹配，若匹配则进入S706，否则，进入S708。

[0168] S706、判断数字钥匙的使用时间是否满足有效期限，若满足，则进入S707，否则，进入S708。

[0169] 更具体地，若数字钥匙的使用时间在有效期限内，则可使用开锁信息开启该智能锁。

[0170] S707、根据开锁信息控制开启智能锁。

[0171] S708、返回提示信息。

[0172] 更具地，提示信息用于提示用户开锁失败。

[0173] 在本实施例提供的验证方法，通过判断数字钥匙的使用次数，可控制该数字钥匙开启智能锁的次数，进而提高验证方法的可靠性。

[0174] 图8为本发明根据再一示例性实施例示出的共享装置的机构示意图。如图8，本发明提供的共享装置应用于第一电子设备，装置800包括：发送模块801，用于向第二电子设备发送开锁请求，开锁请求中包括需要开启智能锁的第一用户的第一生物信息；接收模块802，用于接收第二电子设备返回的授权结果，授权结果中包括用于开启智能锁的数字钥匙；发送模块801还用于向第三电子设备发送数字钥匙。

[0175] 可选地，装置还包括：获取模块803；接收模块802还用于接收第二电子设备发送的第一获取请求；获取模块803，用于根据第一获取请求，获取第一用户的第二生物信息；发送模块801还用于向第二电子设备发送第二生物信息；其中，第二生物信息用于第二电子设备生成数字钥匙。

[0176] 可选地，接收模块802还用于接收第二电子设备发送的身份验证结果；身份验证结果用于指示是否允许第一用户开启智能锁。

[0177] 可选地，第一用户的第一生物信息包括：第一语音，获取模块803还用于获取第一用户在当前时刻使用第一电子设备与第二用户进行通话时的第一语音；其中，第一语音用于生成开锁请求。

[0178] 可选地，第一用户的第一生物信息包括：加密语音，发送模块801还用于向第三电子设备发送第一语音；其中，第三电子设备使用本地存储的对称公钥对第一语音加密，生成

加密语音;接收模块802还用于接收第三电子设备返回的加密语音;其中,加密语音用于生成开锁请求。

[0179] 可选地,接收模块802还用于接收第二电子设备发送的第二获取请求;获取模块803还用于根据第二获取请求,获取第一用户的第一预留信息;发送模块801还用于向第二电子设备发送第一预留信息;其中,第二电子设备向第四电子设备发送第一预留信息,第四电子设备使用第一预留信息生成对称公钥。

[0180] 可选地,发送模块801还用于向第二电子设备发送第三获取请求;其中,第三获取请求用于获取第二用户的第二预留信息;接收模块802还用于接收第二电子设备发送的第二预留信息;发送模块801还用于向第三电子设备发送第二预留信息和第一预留信息;其中,第一预留信息和第二预留信息用于生成对称公钥。

[0181] 可选地,第一电子设备包括:第一NFC芯片,获取模块803还用于通过第一NFC芯片获取从第三电子设备返回的第一加密标识;发送模块801还用于向第二电子设备发送第一加密标识;其中,第一加密标识用于生成开锁请求。

[0182] 可选地,数字钥匙还包括:有效期限。

[0183] 图9为本发明根据再一示例性实施例示出的共享装置的机构示意图。如图9,本发明提供的共享装置应用于第二电子设备,装置900包括:接收模块901,用于接收第一电子设备发送的开锁请求,开锁请求中包括需要开启智能锁的第一用户的第一生物信息;验证模块902,用于根据第一生物信息,对第一用户的身份进行验证;发送模块903,用于若允许第一用户开启智能锁,则向第一电子设备发送授权结果,授权结果中包括用于开启智能锁的数字钥匙。

[0184] 可选地,发送模块903还用于向第一电子设备发送第一获取请求,其中,第一获取请求用于获取第一用户的第二生物信息;接收模块901还用于接收第一电子设备发送的第二生物信息;生成模块904,用于根据第二生物信息以及本地存储的开启智能锁的开锁信息生成数字钥匙。

[0185] 可选地,发送模块903还用于向第一电子设备发送身份验证结果,身份验证结果用于指示是否允许第一用户开启智能锁。

[0186] 可选地,第一生物信息包括:第一用户的第一语音;验证模块902具体用于:获取第二用户在当前使用第二电子设备与第一用户进行通话时的第二语音;对第二语音与第一语音进行匹配处理。

[0187] 可选地,第一生物信息包括:第一用户的加密语音;发送模块903还用于向第四电子设备发送加密语音,其中,第四电子设备使用对称公钥对加密语音进行解密生成第一语音;接收模块901还用于接收第四电子设备返回的第一语音。

[0188] 可选地,装置还包括获取模块905;接收模块901还用于接收第一电子设备发送的第三获取请求;获取模块905用于根据第三获取请求,获取第二用户的第二预留信息;发送模块903还用于向第一电子设备发送第二预留信息;其中,第二预留信息用于第一电子设备生成对称公钥。

[0189] 可选地,发送模块903还用于向第一电子设备发送第二获取请求;第二获取请求用于获取第一用户的第一预留信息;接收模块901还用于接收第一电子设备发送的第一预留信息;发送模块903还用于向第四电子设备发送第二预留信息和第一预留信息;其中,第一

预留信息和第二预留信息用于生成对称公钥。

[0190] 可选地，开锁请求还包括：第一加密标识；接收模块901还用于接收第一电子设备返回的第一加密标识；发送模块903还用于将第一加密标识发送至第四电子设备，其中，第四电子设备使用本地存储的第一私钥对第一加密标识进行解密生成第三标识，并根据本地存储的第二公钥对第三标识进行加密生成第二加密标识；接收模块901还用于接收第四电子设备返回的第二加密标识；发送模块903还用于向服务器发送第二加密标识；接收模块901还用于接收服务器返回的设备验证结果，若设备验证结果为允许第三电子设备开启智能锁。

[0191] 可选地，生成模块904还用于在数字钥匙中添加有效期限。

[0192] 图10为本发明根据再一示例性实施例示出的共享装置的机构示意图。如图10所示，本发明提供一种数字钥匙的共享装置，应用于第三电子设备，第三电子设备包括：第一安全芯片和第三近场通信NFC芯片；装置包括：接收模块1001，用于通过第三NFC芯片接收第一电子设备发送的数字钥匙，数字钥匙中包括用于开启智能锁的开锁信息；存储模块1002，用于将数字钥匙存储至安全芯片。

[0193] 可选地，装置还包括生成模块；接收模块1001还用于第三电子设备接收第一电子设备返回的第一预留信息和第二预留信息；生成模块1003第三电子设备根据第一预留信息和第二预留信息生成对称公钥。

[0194] 可选地，还包括：加密模块1004和发送模块1005；接收模块1001还用于第三电子设备接收第一电子设备发送的第一语音；加密模块1004用于使用对称公钥对第一语音进行加密处理生成加密语音；发送模块1005还用于向第一电子设备发送加密语音。

[0195] 可选地，还包括获取模块1006，获取模块1006用于第三电子设备获取第三电子设备的第三标识；加密模块1004还用于使用第一公钥对第三标识进行加密处理生成第一加密标识；发送模块1006向第一电子设备发送第一加密标识。

[0196] 图11为本发明根据再一示例性实施例示出的验证装置的机构示意图。如图11所示，本发明提供一种数字钥匙的验证装置，应用于智能锁，装置1100包括：接收模块1101，用于接收第一电子设备输入的数字钥匙，数字钥匙中包括用于开启智能锁的开锁信息以及第一用户的第二生物信息；获取模块1102，通过传感器获取当前需要开启智能锁的第一用户的第二生物信息；控制模块1103，用于若数字钥匙中的第一第二生物信息与通过传感器获取到的第二生物信息匹配，则根据开锁信息控制开启智能锁。

[0197] 可选地，控制模块1103具体用于：

[0198] 若开锁信息与存储在本地的预留开锁信息匹配，则开启智能锁。

[0199] 可选地，预留开锁信息包括：至少一个用户、用户的指纹数据、及用户的钥匙标识。

[0200] 可选地，数字钥匙中还包括：有效期限，在根据开锁信息控制开启智能锁之前，还包括：判断数字钥匙的使用期限达到有效期限，若未达到。

[0201] 可选地，获取模块1102还用于：

[0202] 获取第三电子设备的第三标识；

[0203] 根据第三标识和智能锁中记录数据确定第三电子设备的使用次数；

[0204] 若使用次数小于预设数量。

[0205] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽

管参照前述各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，或者对其中部分或者全部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范围。

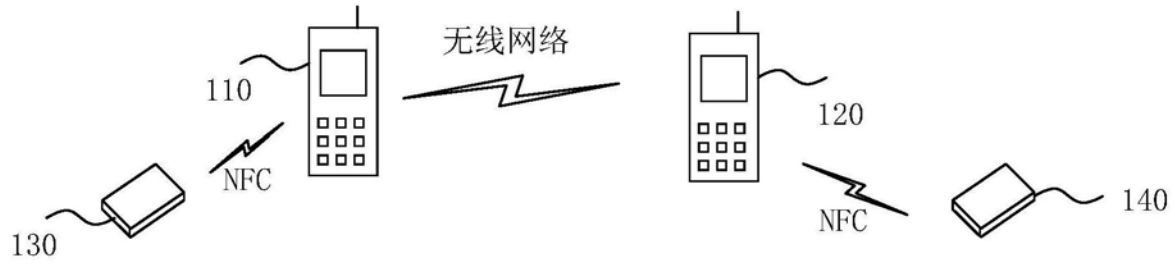

无线网络
110
120
NFC
NFC
130
140

图1

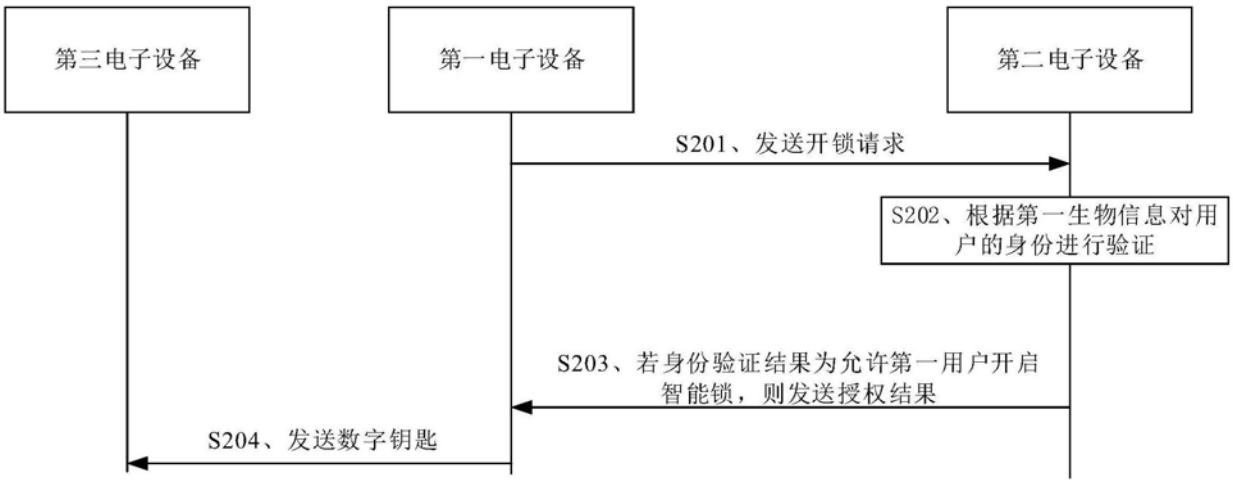

第三电子设备
第一电子设备
第二电子设备
S201、发送开锁请求
S202、根据第一生物信息对用户的身份进行验证
S203、若身份验证结果为允许第一用户开启智能锁，则发送授权结果
S204、发送数字钥匙

图2

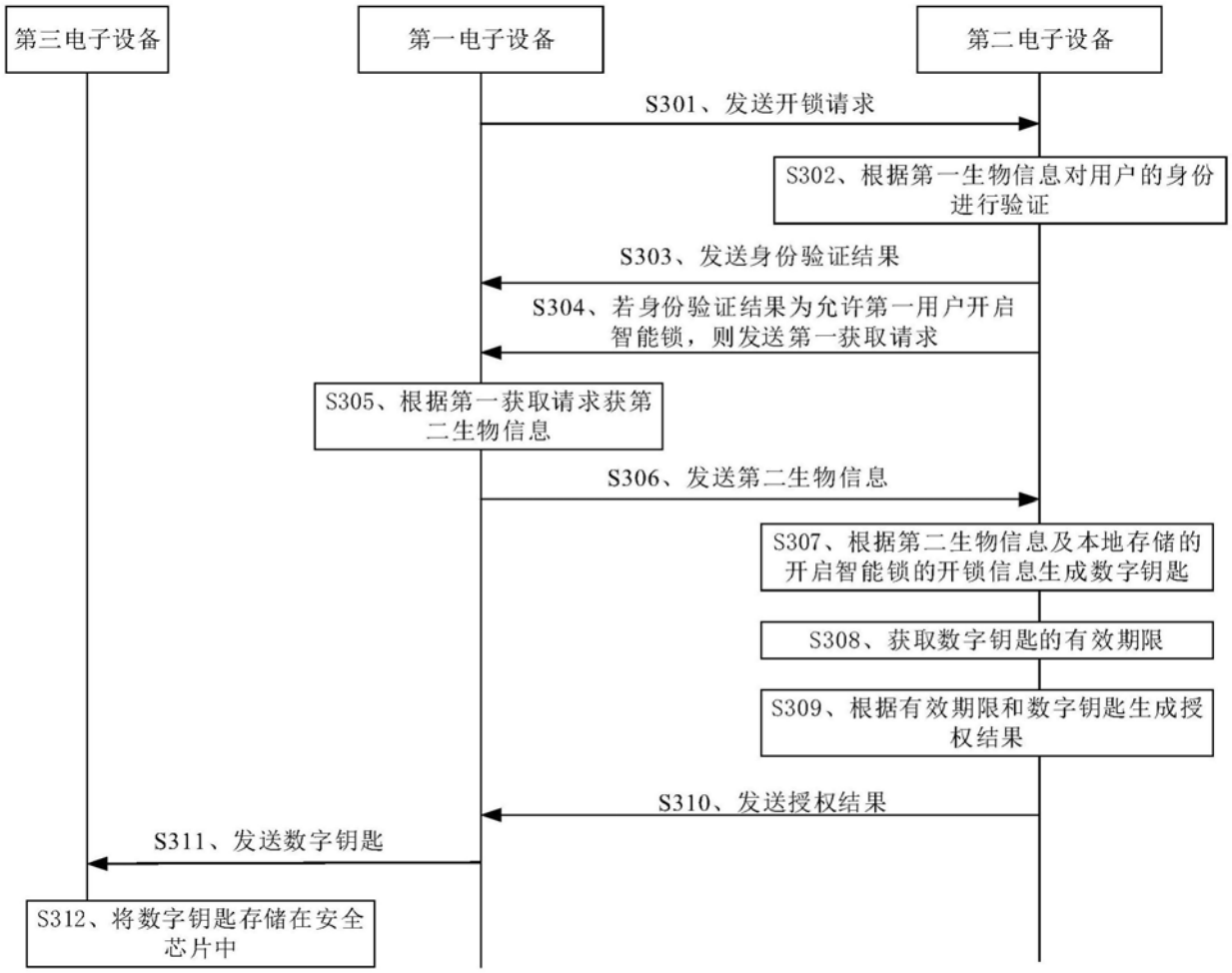

第三电子设备
第一电子设备
第二电子设备
S301、发送开锁请求
S302、根据第一生物信息对用户的身份进行验证
S303、发送身份验证结果
S304、若身份验证结果为允许第一用户开启智能锁，则发送第一获取请求
S305、根据第一获取请求获第二生物信息
S306、发送第二生物信息
S307、根据第二生物信息及本地存储的开启智能锁的开锁信息生成数字钥匙
S308、获取数字钥匙的有效期限
S309、根据有效期限和数字钥匙生成授权结果
S310、发送授权结果
S311、发送数字钥匙
S312、将数字钥匙存储在安全芯片中

图3

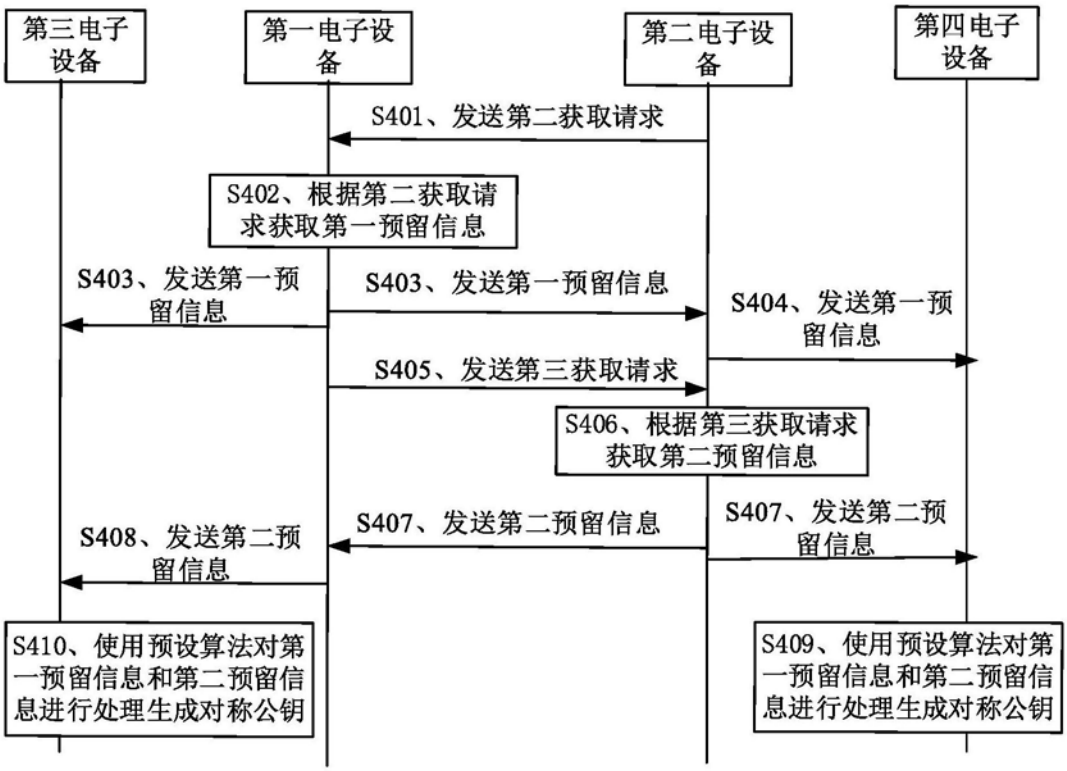

第三电子设备
第一电子设备
第二电子设备
第四电子设备
S401、发送第二获取请求
S402、根据第二获取请求获取第一预留信息
S403、发送第一预留信息
S403、发送第一预留信息
S404、发送第一预留信息
S405、发送第三获取请求
S406、根据第三获取请求获取第二预留信息
S408、发送第二预留信息
S407、发送第二预留信息
S407、发送第二预留信息
S410、使用预设算法对第一预留信息和第二预留信息进行处理生成对称公钥
S409、使用预设算法对第一预留信息和第二预留信息进行处理生成对称公钥

图4

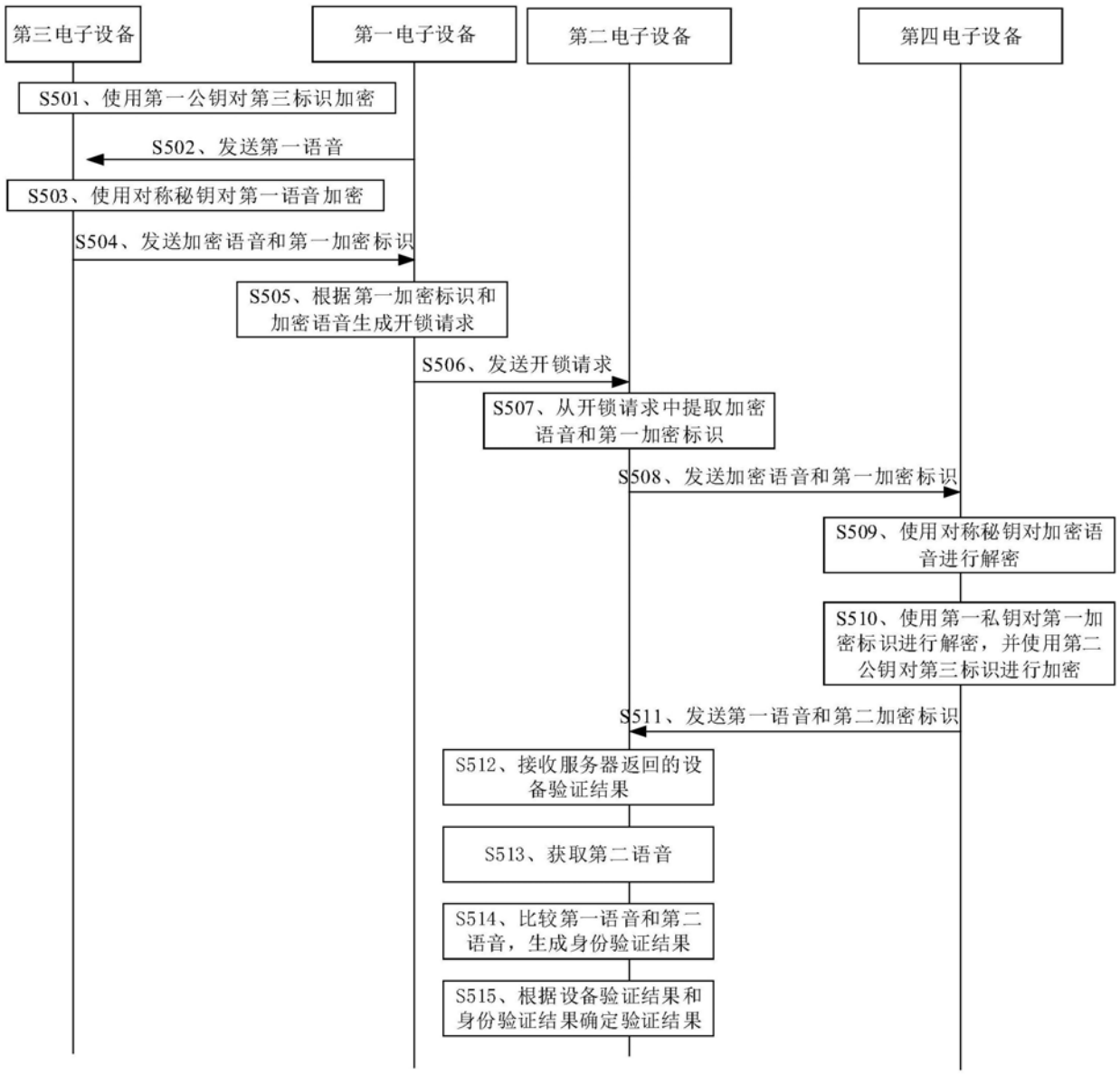

第三电子设备
第一电子设备
第二电子设备
第四电子设备
S501、使用第一公钥对第三标识加密
S502、发送第一语音
S503、使用对称秘钥对第一语音加密
S504、发送加密语音和第一加密标识
S505、根据第一加密标识和加密语音生成开锁请求
S506、发送开锁请求
S507、从开锁请求中提取加密语音和第一加密标识
S508、发送加密语音和第一加密标识
S509、使用对称秘钥对加密语音进行解密
S510、使用第一私钥对第一加密标识进行解密，并使用第二公钥对第三标识进行加密
S511、发送第一语音和第二加密标识
S512、接收服务器返回的设备验证结果
S513、获取第二语音
S514、比较第一语音和第二语音，生成身份验证结果
S515、根据设备验证结果和身份验证结果确定验证结果

图5

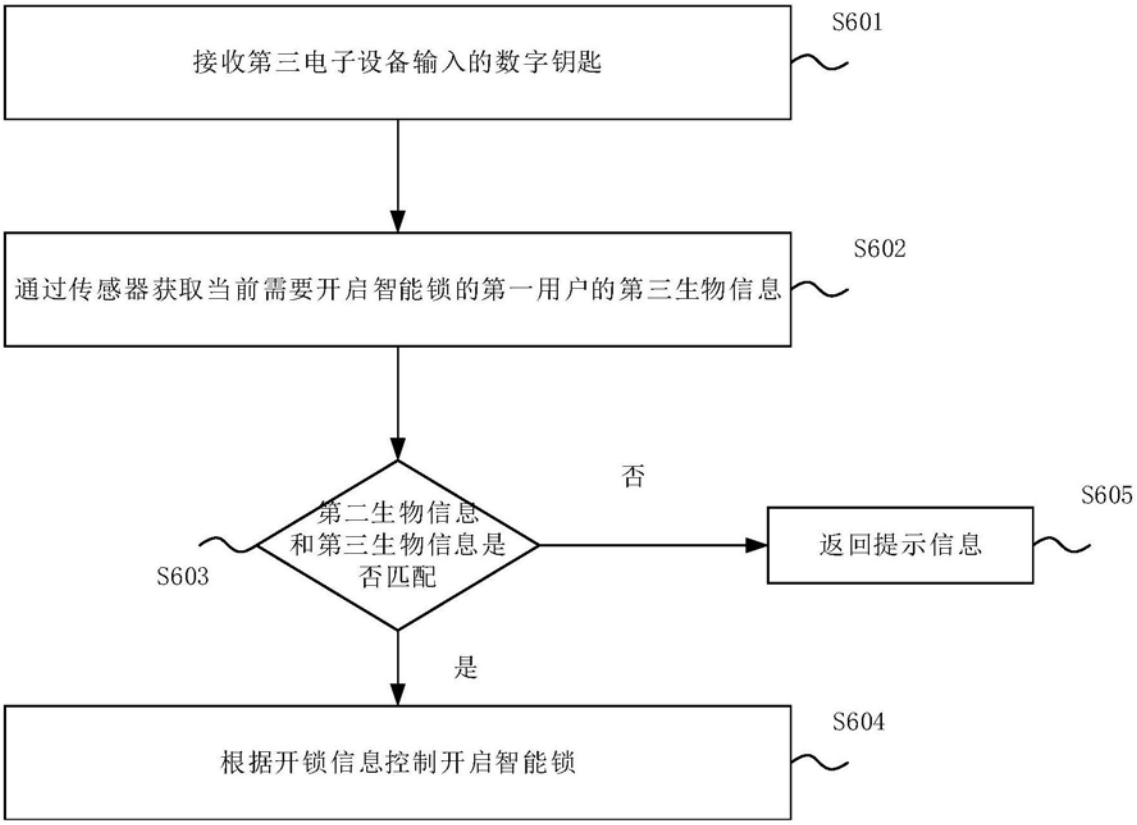

接收第三电子设备输入的数字钥匙
S601
通过传感器获取当前需要开启智能锁的第一用户的第三生物信息
S602
第二生物信息和第三生物信息是否匹配
S603
否
返回提示信息
S605
是
根据开锁信息控制开启智能锁
S604

图6

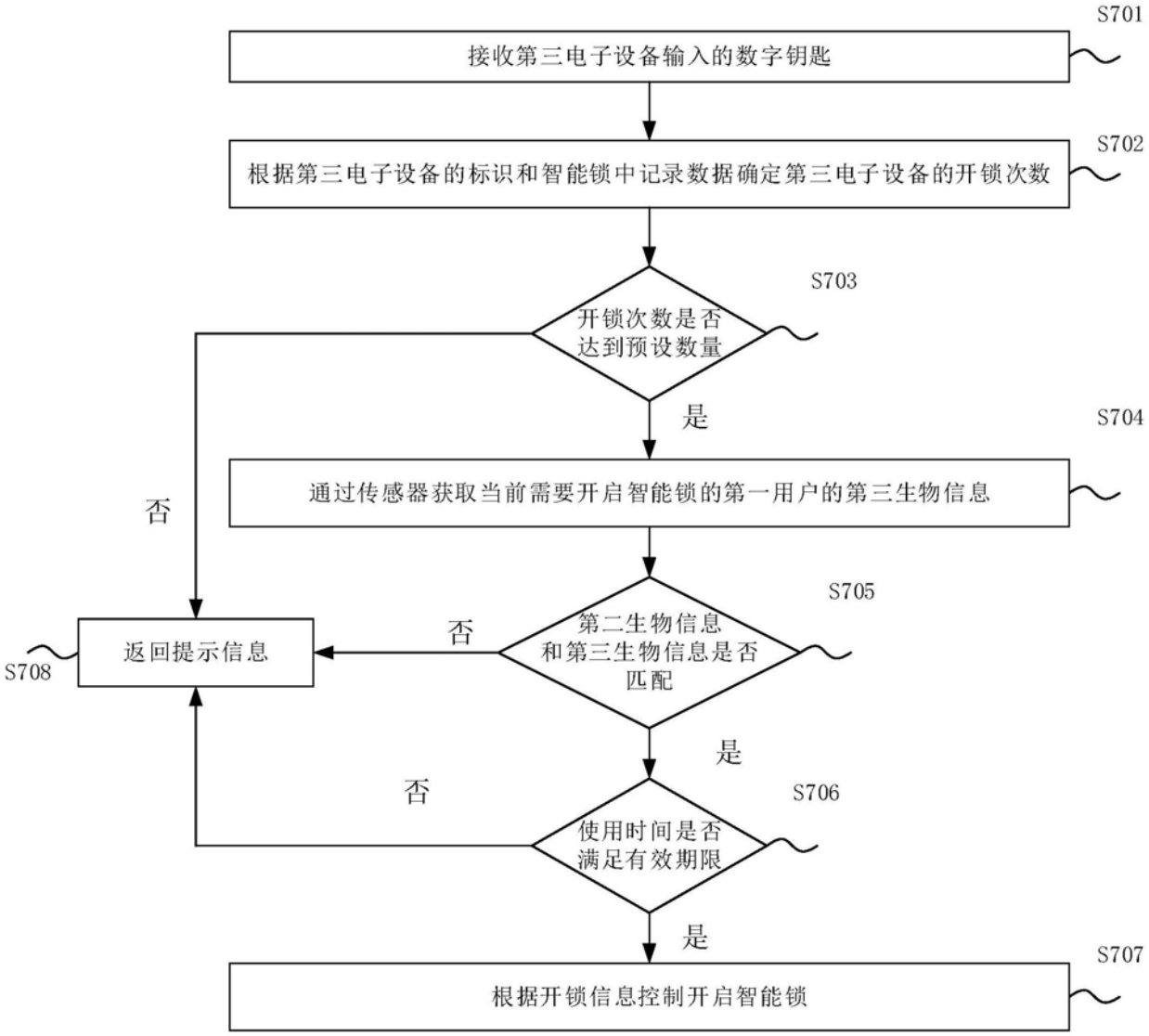

S701
接收第三电子设备输入的数字钥匙
S702
根据第三电子设备的标识和智能锁中记录数据确定第三电子设备的开锁次数
S703
开锁次数是否达到预设数量
是
否
S704
通过传感器获取当前需要开启智能锁的第一用户的第三生物信息
S705
第二生物信息和第三生物信息是否匹配
否
是
S708
返回提示信息
否
S706
使用时间是否满足有效期限
是
S707
根据开锁信息控制开启智能锁

图7

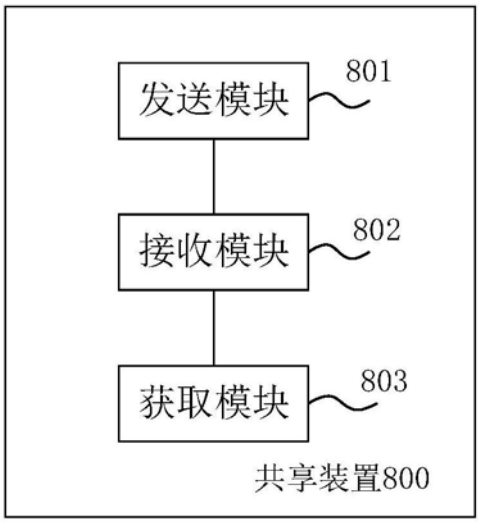

发送模块
801
接收模块
802
获取模块
803
共享装置800

图8

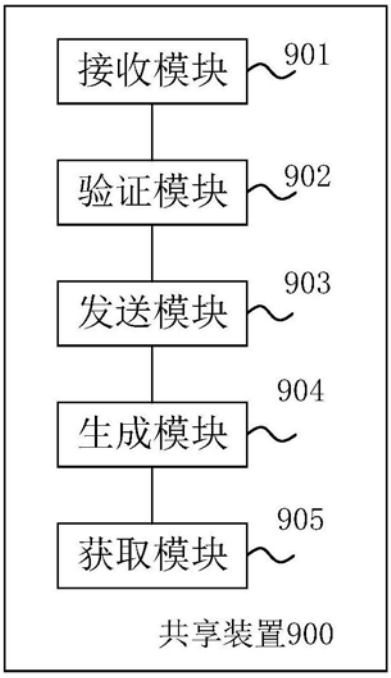

接收模块
901
验证模块
902
发送模块
903
生成模块
904
获取模块
905
共享装置900

图9

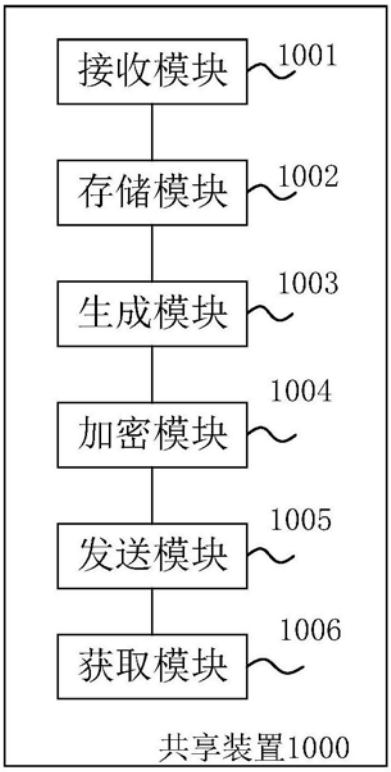

接收模块
1001
存储模块
1002
生成模块
1003
加密模块
1004
发送模块
1005
获取模块
1006
共享装置1000

图10

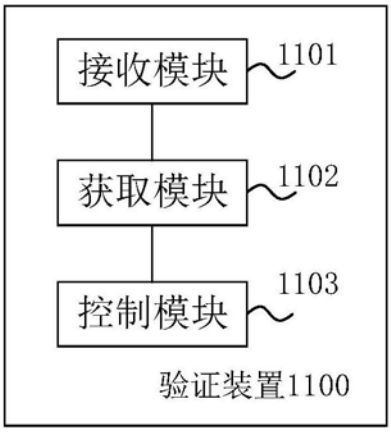

接收模块
1101
获取模块
1102
控制模块
1103
验证装置1100

图11