(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110611905 B
(45)授权公告日 2023.11.21

(21)申请号 201910735944.6
(22)申请日 2019.08.09
(65)同一申请的已公布的文献号
申请公布号 CN 110611905 A
(43)申请公布日 2019.12.24
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 李付生 李德永 王英超 李娟
(74)专利代理机构 深圳中一联合知识产权代理有限公司 44414
专利代理师 李艳丽
(51)Int.Cl.
H04W 4/80(2018.01)
H04W 12/03(2021.01)
H04W 12/06(2021.01)
H04W 48/08(2009.01)
H04W 12/69(2021.01)
H04W 12/55(2021.01)

(56)对比文件
CN 105101339 A,2015.11.25
CN 106131828 A,2016.11.16
US 2017078839 A1,2017.03.16
US 8844012 B1,2014.09.23
CN 104104414 A,2014.10.15
CN 108616847 A,2018.10.02
CN 104780204 A,2015.07.15
US 2014220894 A1,2014.08.07

审查员 刘丽

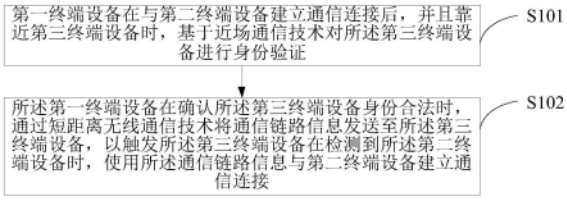
权利要求书2页 说明书31页 附图7页

(54)发明名称

信息共享方法、终端设备、存储介质及计算机程序产品

(57)摘要

本申请适用于通信技术领域,提供了一种信息共享方法、终端设备、存储介质及计算机程序产品,该信息共享方法包括:在第一终端设备与第二终端设备建立通信连接之后,将第一终端设备靠近第三终端设备时,第一终端设备通过近场通信NFC对第三终端设备进行身份验证;第一终端设备在确认第三终端设备身份合法时,通过短距离无线通信技术将通信链路信息发送给第三终端设备,以便第三终端设备在接收到通信链路信息后,并且检测到第二终端设备时,使用该通信链路信息与第二终端设备建立通信连接。上述方案,将第一终端设备靠近第三终端设备时即可方便快捷地建立通信连接并实现信息共享,可简化第三终端设备与第二终端设备建立通信连接的操作步骤。



CN 110611905 B

1.一种信息共享方法,其特征在于,包括:

第一终端设备与第二终端设备建立通信连接;

所述第一终端设备检测到第三终端设备时,通过近场通信NFC对所述第三终端设备进行身份验证,包括:所述第一终端设备在与所述第二终端设备建立通信连接后,并且靠近第三终端设备时,通过NFC向所述第三终端设备发送身份认证通知消息;所述第一终端设备获取所述第三终端设备在接收到所述身份认证通知消息时通过NFC返回的第一身份信息;其中,所述第一身份信息包括所述第三终端设备的第一设备标识、公钥属性凭据的第一版本号以及由所述第三终端设备生成的第一随机数;所述第一终端设备从身份数据库中查找与所述第一设备标识匹配的设备标识;当查找到所述匹配的设备标识,且所述第一版本号小于或等于预存的公钥属性凭据的第二版本号时,从所述身份数据库中获取所述第三终端设备的公钥;当未查找到所述匹配的设备标识,且所述第一版本号大于预存的公钥属性凭据的第二版本号,向所述第三终端设备请求获取所述第三终端设备的公钥;当未查找到所述匹配的设备标识,且所述第一版本号小于预存的公钥属性凭据的第二版本号时,判定所述第三终端设备身份不合法;所述第一终端设备基于自身的私钥和所述第三终端设备的公钥计算第一共享密钥,并生成第二随机数;所述第一终端设备基于所述第一共享密钥、所述第一终端设备的第二设备标识、所述第一随机数以及所述第二随机数,计算第一身份特征值;所述第一终端设备通过近场通信向所述第三终端设备发送所述第一身份特征值、所述第一终端设备的第二设备标识、公钥属性凭据的第二版本号以及所述第二随机数;所述第一终端设备接收所述第三终端设备返回的第二身份特征值;其中,所述第二身份特征值由所述第三终端设备在计算出第二共享密钥时,基于所述第二共享密钥、所述第二设备标识、所述第一随机数以及所述第二随机数计算得到,所述第二共享密钥基于所述第三终端设备的私钥以及所述第一终端设备的公钥计算得到;所述第一终端设备在确认所述第一身份特征值与所述第二身份特征值相同时,判定所述第三终端设备身份合法;其中,通过比较公钥属性凭据的第一版本号以及第二版本号,来确认第三终端设备是否被撤销可信资格;

所述第一终端设备在确认所述第三终端设备身份合法时,通过短距离无线通信技术将通信链路信息发送至所述第三终端设备,所述通信链路信息用于所述第三终端设备和所述第二终端设备之间建立通信连接或门禁授权;

所述第三终端设备的蜂窝移动网络和无线局域网均处于关闭状态,所述短距离无线通信技术为NFC或蓝牙通信;

所述通信链路信息包括无线网的接入信息、NFC门禁识别信息中的至少一种。

2.如权利要求1所述的信息共享方法,其特征在于,所述第一终端设备在确认所述第三终端设备身份合法时,通过短距离无线通信技术将通信链路信息发送至所述第三终端设备,包括:

所述第一终端设备在确认所述第三终端设备身份合法时,生成会话密钥,并通过短距离无线通信技术将所述会话密钥发送至所述第三终端设备;

所述第一终端设备采用所述会话密钥对所述通信链路信息进行加密,并通过所述短距离无线通信技术将加密数据发送至所述第三终端设备。

3.一种终端设备,包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序,其特征在于,所述处理器执行所述计算机程序时实现如权利要求1或2

所述的信息共享方法。

4.一种计算机可读存储介质,所述计算机可读存储介质存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现如权利要求1或2所述的信息共享方法。

信息共享方法、终端设备、存储介质及计算机程序产品

技术领域

[0001] 本申请属于通信技术领域，尤其涉及一种信息共享方法、终端设备、存储介质及计算机程序产品。

背景技术

[0002] 随着科学技术的发展，人们在日常生活中使用的电子设备的种类越来越多，例如，手机、可穿戴设备、平板电脑、笔记本电脑、蓝牙耳机以及路由器等。电子设备之间可以互相连接或配对。

[0003] 在一应用场景中，当用户需要将至少两个终端设备与同一个蓝牙耳机配对时，用户分别通过每个终端设备的交互界面，触发终端设备搜索蓝牙设备，用户从搜索到的设备列表中选择待配对的蓝牙设备，从而使终端设备与蓝牙耳机建立通信连接。例如，当用户需要将手机、平板电脑均与同一个蓝牙耳机配对时，用户需要通过手机的交互界面控制手机与蓝牙耳机进行配对，并通过平板电脑的交互界面控制平板电脑与蓝牙耳机进行配对。

[0004] 然而，这种建立至少两个终端设备与同一个蓝牙耳机之间的通信连接的方法，需要用户在每个终端设备上重复进行配对连接操作，操作较繁琐，导致配对效率较低。

发明内容

[0005] 本申请实施例提供了信息共享方法、终端设备、存储介质及计算机程序产品，可以解决现有技术中，当用户需要将至少两个终端设备与另一个终端设备连接或配对时，需要用户在每个终端设备上重复进行配对或连接操作，操作较繁琐，导致操作效率较低的问题。

[0006] 第一方面，本申请实施例提供了一种信息共享方法，包括：第一终端设备与第二终端设备建立通信连接；第一终端设备检测到第三终端设备时，通过近场通信NFC对所述第三终端设备进行身份验证；所述第一终端设备在确认第三终端设备身份合法时，通过短距离无线通信技术将通信链路信息发送至所述第三终端设备，所述通信链路信息用于所述第三终端设备和所述第二终端设备之间建立通信连接。

[0007] 可选地，短距离无线通信技术可以为NFC、蓝牙通信或无线保真(Wireless-Fidelity,WIFI)。

[0008] 可选地，所述第一终端设备在确认所述第三终端设备身份合法时，可以通过文字或语音消息等方式提示用户。第一终端设备与第三终端设备建立通信连接后，第三终端设备也可以向第一终端设备发送需要共享的信息。

[0009] 第一终端设备以及第三终端设备属于同一用户账号下的可信设备，用户账号用于标识用户账号的拥有者的身份信息，用户账号可以是预先注册的华为账号。可信设备是指该用户账号的拥有者信任的用户设备，可信设备之间具有信息分享权限。第一终端设备以及第三终端设备预先已通过登录该用户账号，同步所有可信设备的身份信息。即，第一终端设备以及第三终端设备内预先存储有所有可信设备的身份信息。

[0010] 上述方案，在第一终端设备与第二终端设备建立通信连接之后，将第一终端设备

靠近第三终端设备时，即可方便快捷地使第一终端设备与第三终端设备建立通信连接，进而共享通信链路信息，以使得第三终端设备在检测到第二终端设备时，使用该通信链路信息与第二终端设备建立通信连接。既不需要其他设备参与数据交互，也不需要用户操控第三终端设备即可让第三终端设备与第二终端设备建立通信连接，可简化第三终端设备与第二终端设备建立通信连接的操作步骤，进而提高建立至少三个终端设备之间的通信连接的效率。

[0011] 结合第一方面，在第一方面的第一种可能的实现方式中，所述第三终端设备的蜂窝移动网络和无线局域网均处于关闭状态，短距离无线通信技术为NFC或蓝牙通信。

[0012] 其中，第三终端设备的蜂窝移动网络和无线局域网均处于关闭状态是指：第三终端设备未启用蜂窝移动网络和无线局域网，或者当前无法通过蜂窝移动网络或无线局域网接入互联网。

[0013] 本方案，由于第一终端设备与第三终端设备可以通过NFC或蓝牙通信共享信息，即使第三终端设备无法通过蜂窝移动网络或无线局域网接入互联网，第一终端设备也可与第三终端设备共享信息，使用场景不受互联网的限制，应用更广泛。

[0014] 结合第一方面，在第一方面的第二种可能的实现方式中，所述第二终端设备为预先与所述第一终端设备完成配对的终端设备，所述通信链路信息包括蓝牙配对信息，第三终端设备在接收到蓝牙配对信息后，并且检测到第二终端设备时，使用接收到的蓝牙配对信息与第二终端设备进行配对。

[0015] 结合第一方面，在第一方面或第一方面的第二种实现方式，在第一方面的第三种可能的实现方式中，所述通信链路信息包括无线网的接入信息和/或NFC门禁识别信息。

[0016] 其中，无线网的接入信息用于连接路由器、接入点或个人热点。接入信息可以是服务集标识(Service Set Identifier，SSID)和接入密码。此时，第三终端可以在进入任一SSID对应的无线网的信号覆盖范围时，通过无线网的接入信息，接入第一终端设备当前接入的无线网或曾接入过的无线网。

[0017] NFC门禁识别信息用于标识授权信息，例如NFC门禁授权信息，此时第三终端设备可作为NFC门禁卡与第二终端设备进行通信，从而实现开门等功能。

[0018] 结合第一方面，在第一方面的第四种可能的实现方式中，所述第一终端设备检测到第三终端设备时，通过近场通信NFC对所述第三终端设备进行身份验证，包括：所述第一终端设备与第二终端设备建立通信连接后，并且靠近第三终端设备时，通过NFC向所述第三终端设备发送身份认证通知消息；所述第一终端设备获取所述第三终端设备在接收到所述身份认证通知消息时通过NFC返回的第一身份信息；所述第一终端设备基于所述第一身份信息以及预存的第二身份信息，对所述第三终端设备进行身份验证。

[0019] 结合第一方面的第四种可能的实现方式，在第一方面的第五种可能的实现方式中，所述第一身份信息包括所述第三终端设备的第一设备标识以及第一公钥；所述第一终端设备基于所述第一身份信息以及预存的第二身份信息，对所述第三终端设备进行身份验证，包括：所述第一终端设备基于所述第一设备标识从身份数据库中获取所述第三终端设备对应的预存的公钥，并基于所述第一公钥和所述预存的公钥对所述第三终端设备进行身份验证；其中，当所述第一公钥和所述预存的公钥相同时，判定所述第三终端设备身份合法。

[0020] 结合第一方面的第四种可能的实现方式，在第一方面的第六种可能的实现方式中，所述第一身份信息包括所述第三终端设备的第一设备标识、公钥属性凭据的第一版本号以及由所述第三终端设备生成的第一随机数；所述第一终端设备基于所述第一身份信息以及预存的第二身份信息，对所述第三终端设备进行身份验证，包括：所述第一终端设备基于所述第一设备标识以及所述第一版本号，获取所述第三终端设备的第一公钥；所述第一终端设备基于自身的私钥和所述第一公钥计算第一共享密钥，并生成第二随机数；所述第一终端设备基于所述第一共享密钥、所述第一终端设备的第二设备标识、所述第一随机数以及所述第二随机数，计算第一身份特征值；所述第一终端设备通过近场通信向所述第三终端设备发送所述第一身份特征值、所述第一终端设备的第二设备标识、公钥属性凭据的第二版本号以及所述第二随机数；所述第一终端设备接收所述第三终端设备返回的第二身份特征值；其中，所述第二身份特征值由所述第三终端设备在计算出第二共享密钥时，基于所述第二共享密钥、所述第二设备标识、所述第一随机数以及所述第二随机数计算得到，所述第二共享密钥基于所述第三终端设备的私钥以及所述第一终端设备的公钥计算得到；所述第一终端设备在确认所述第一身份特征值与所述第二身份特征值相同时，判定所述第三终端设备身份合法。

[0021] 结合第一方面的第六种可能的实现方式，在第一方面的第七种可能的实现方式中，所述第一终端设备基于所述第一设备标识以及所述第一版本号，获取所述第三终端设备的第一公钥，包括：所述第一终端设备从身份数据库中查找与所述第一设备标识匹配的设备标识；当查找到所述匹配的设备标识，且所述第一版本号小于或等于预存的公钥属性凭据的第二版本号时，从所述身份数据库中获取所述第三终端设备的公钥；当未查找到所述匹配的设备标识，且所述第一版本号大于预存的公钥属性凭据的第二版本号，向所述第三终端设备请求获取所述第一公钥。

[0022] 本方案中，通过比较公钥属性凭据的第一版本号以及第二版本号，来确认第三终端设备是否被撤销可信资格，或者确认第三终端设备是否为新加入的可信设备，这样对于离线设备也有一定的安全性，不必随时保持在线确认每个设备的公钥的有效性。其中，当所述第一版本号大于所述第二版本号时，判定第三终端设备为新加入的可信设备；当所述第一版本号小于所述第二版本号，且在本地数据库中未查找到与第一设备标识匹配的设备标识时，判定第三终端设备已被撤销可信资格。

[0023] 结合第一方面的第七种可能的实现方式，在第一方面的第八种可能的实现方式中，所述第一终端设备从身份数据库中查找与所述第一设备标识匹配的设备标识之后，还包括：当未查找到所述匹配的设备标识，且所述第一版本号小于预存的公钥属性凭据的第二版本号时，判定所述第三终端设备身份不合法。

[0024] 结合第一方面以及第一方面的任一种实现方式，在第一方面的第九种可能的实现方式中，所述第一终端设备在确认所述第三终端设备身份合法时，通过短距离无线通信技术将通信链路信息发送至所述第三终端设备，包括：所述第一终端设备在确认所述第三终端设备身份合法时，生成会话密钥，并通过短距离无线通信技术将所述会话密钥发送至所述第三终端设备；所述第一终端设备采用所述会话密钥对所述通信链路信息进行加密，并通过所述短距离无线通信技术将加密数据发送至所述第三终端设备。

[0025] 本方案中，通过会话密钥对通信链路信息进行加密，能够提高待分享数据在传输

过程中的安全性,即使其他不可信设备接收到加密后的通信链路信息,也无法直接获取到通信链路信息,进而避免其他不可信设备通过通信链路信息连接第二终端设备,进一步保护第二终端设备内的数据安全。

[0026] 第二方面,本申请实施例提供了一种信息共享装置,包括:身份验证单元,用于第一终端设备与第二终端设备建立通信连接后,并且在靠近第三终端设备时,通过近场通信NFC对所述第三终端设备进行身份验证;信息共享单元,用于在确认所述第三终端设备身份合法时,通过短距离无线通信技术将通信链路信息发送至所述第三终端设备,以触发所述第三终端设备在检测到所述第二终端设备时,使用所述通信链路信息与第二终端设备建立通信连接。

[0027] 可选地,短距离无线通信技术可以为NFC、蓝牙通信或无线保真(Wireless-Fidelity,WIFI)。

[0028] 上述方案,在第一终端设备与第二终端设备建立通信连接之后,将第一终端设备靠近第三终端设备时,即可方便快捷地使第一终端设备与第三终端设备建立通信连接,进而共享通信链路信息,以使得第三终端设备在检测到第二终端设备时,使用该通信链路信息与第二终端设备建立通信连接。既不需要其他设备参与数据交互,也不需要用户操控第三终端设备即可让第三终端设备与第二终端设备建立通信连接,可简化第三终端设备与第二终端设备建立通信连接的操作步骤,进而提高建立至少三个终端设备之间的通信连接的效率。

[0029] 结合第二方面,在第二方面的第一种可能的实现方式中,所述第三终端设备的蜂窝移动网络和无线局域网均处于关闭状态,所述短距离无线通信技术为NFC或蓝牙通信。

[0030] 本方案,由于第一终端设备与第三终端设备可以通过NFC或蓝牙通信共享信息,即使第三终端设备无法通过蜂窝移动网络或无线局域网接入互联网,第一终端设备也可与第三终端设备共享信息,使用场景不受互联网的限制,应用更广泛。

[0031] 结合第二方面,在第二方面的第二种可能的实现方式中,所述第二终端设备为预先与所述第一终端设备完成配对的终端设备,所述通信链路信息包括蓝牙配对信息,第三终端设备在接收到蓝牙配对信息后,并且检测到第二终端设备时,使用接收到的蓝牙配对信息与第二终端设备进行配对。

[0032] 结合第二方面,在第二方面或第二方面的第二种实现方式,在第二方面的第三种可能的实现方式中,所述信息共享单元发送的所述通信链路信息包括无线网的接入信息和/或NFC门禁识别信息。

[0033] 其中,无线网的接入信息用于连接路由器、接入点或个人热点。接入信息可以是SSID和接入密码。此时,第三终端可以在进入任一SSID对应的无线网的信号覆盖范围时,通过无线网的接入信息,接入第一终端设备当前接入的无线网或曾接入过的无线网。

[0034] NFC门禁识别信息用于标识授权信息,例如NFC门禁授权信息,此时第三终端设备可作为NFC门禁卡与第三终端设备进行通信,从而实现开门等功能。

[0035] 结合第二方面,在第二方面的第四种可能的实现方式中,所述身份验证单元包括:发送单元,用于所述第一终端设备与第二终端设备建立通信连接后,并且靠近第三终端设备时,通过NFC向所述第三终端设备发送身份认证通知消息;接收单元,用于获取所述第三终端设备在接收到所述身份认证通知消息时通过NFC返回的第一身份信息;验证单元,用于

基于所述第一身份信息以及预存的第二身份信息，对所述第三终端设备进行身份验证。

[0036] 结合第二方面的第四种可能的实现方式，在第二方面的第五种可能的实现方式中，所述第一身份信息包括所述第三终端设备的第一设备标识以及第一公钥；所述验证单元具体用于：基于所述第一设备标识从身份数据库中获取所述第三终端设备对应的预存的公钥，并基于所述第一公钥和所述预存的公钥对所述第三终端设备进行身份验证；其中，当所述第一公钥和所述预存的公钥相同时，判定所述第三终端设备身份合法。

[0037] 结合第二方面的第四种可能的实现方式，在第二方面的第六种可能的实现方式中，所述第一身份信息包括所述第三终端设备的第一设备标识、公钥属性凭据的第一版本号以及由所述第三终端设备生成的第一随机数；所述验证单元包括：公钥获取单元，用于基于所述第一设备标识以及所述第一版本号，获取所述第三终端设备的第一公钥；随机数生成单元，用于基于自身的私钥和所述第一公钥计算第一共享密钥，并生成第二随机数；计算单元，用于基于所述第一共享密钥、所述第一终端设备的第二设备标识、所述第一随机数以及所述第二随机数，计算第一身份特征值；所述发送单元还用于所述第一终端设备通过近场通信向所述第三终端设备发送所述第一身份特征值、所述第一终端设备的第二设备标识、公钥属性凭据的第二版本号以及所述第二随机数；所述接收单元还用于：接收所述第三终端设备返回的第二身份特征值；其中，所述第二身份特征值由所述第三终端设备在计算出第二共享密钥时，基于所述第二共享密钥、所述第二设备标识、所述第一随机数以及所述第二随机数计算得到，所述第二共享密钥基于所述第三终端设备的私钥以及所述第一终端设备的公钥计算得到；比较单元，用于在确认所述第一身份特征值与所述第二身份特征值相同时，判定所述第三终端设备身份合法。

[0038] 结合第二方面的第六种可能的实现方式，在第二方面的第七种可能的实现方式中，所述公钥获取单元具体用于：从身份数据库中查找与所述第一设备标识匹配的设备标识；当查找到所述匹配的设备标识，且所述第一版本号小于或等于预存的公钥属性凭据的第二版本号时，从所述身份数据库中获取所述第三终端设备的公钥；当未查找到所述匹配的设备标识，且所述第一版本号大于预存的公钥属性凭据的第二版本号，向所述第三终端设备请求获取所述第一公钥。

[0039] 本方案中，通过比较公钥属性凭据的第一版本号以及第二版本号，来确认第三终端设备是否被撤销可信资格，或者确认第三终端设备是否为新加入的可信设备，这样对于离线设备也有一定的安全性，不必随时保持在线确认每个设备的公钥的有效性。其中，当所述第一版本号大于所述第二版本号时，判定第三终端设备为新加入的可信设备；当所述第一版本号小于所述第二版本号，且在本地数据库中未查找到与第一设备标识匹配的设备标识时，判定第三终端设备已被撤销可信资格。

[0040] 结合第二方面的第七种可能的实现方式，在第二方面的第八种可能的实现方式中，所述公钥获取单元还用于：当未查找到所述匹配的设备标识，且所述第一版本号小于预存的公钥属性凭据的第二版本号时，判定所述第三终端设备身份不合法。

[0041] 结合第二方面以及第二方面的任一种实现方式，在第二方面的第九种可能的实现方式中，所述信息共享单元具体用于：在确认所述第三终端设备身份合法时，生成会话密钥，并通过短距离无线通信技术将所述会话密钥发送至所述第三终端设备；采用所述会话密钥对所述通信链路信息进行加密，并通过所述短距离无线通信技术将加密数据发送至所

述第三终端设备。

[0042] 本方案中，通过会话密钥对通信链路信息进行加密，能够提高待分享数据在传输过程中的安全性，即使其他不可信设备接收到加密后的通信链路信息，也无法直接获取到通信链路信息，进而避免其他不可信设备通过通信链路信息连接第二终端设备，进一步保护第二终端设备内的数据安全。

[0043] 第三方面，本申请实施例提供了一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现上述第一方面的任一种可能的实现方式的信息共享方法。

[0044] 第四方面，本申请实施例提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述第一方面的任一种可能的实现方式的信息共享方法。

[0045] 第五方面，本申请实施例提供了一种计算机程序产品，当计算机程序产品在终端设备上运行时，使得终端设备执行上述第一方面中任一种可能的实现方式的信息共享方法。

[0046] 本申请实施例与现有技术相比存在的有益效果是：

[0047] 在第一终端设备与第二终端设备建立通信连接之后，将第一终端设备靠近第三终端设备时，即可方便快捷地使第一终端设备与第三终端设备建立通信连接，进而共享通信链路信息，以使得第三终端设备在检测到第二终端设备时，使用该通信链路信息与第二终端设备建立通信连接。既不需要其他设备参与数据交互，也不需要用户操控第三终端设备，即可让第三终端设备与第二终端设备建立通信连接，可简化第三终端设备与第二终端设备建立通信连接的操作步骤，进而提高建立至少三个终端设备之间的通信连接的效率。

[0048] 由于第一终端设备与第三终端设备可以通过NFC或蓝牙通信共享信息，即使第三终端设备无法通过蜂窝移动网络或无线局域网接入互联网，第一终端设备也可与第三终端设备共享信息，使用场景不受互联网的限制，应用更广泛。

附图说明

[0049] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0050] 图1是本申请一实施例提供的信息共享方法的系统示意图；

[0051] 图2是本申请一实施例提供的信息共享方法的应用场景示意图；

[0052] 图3是本申请实施例提供的一种蓝牙配对界面的示意图；

[0053] 图4是本申请另一实施例提供的信息共享方法的应用场景示意图；

[0054] 图5是本申请一实施例提供的信息共享方法所适用于的手机的硬件结构示意图；

[0055] 图6是本申请一实施例提供的信息共享方法的示意性流程图；

[0056] 图7是本申请一实施例提供的信息共享方法中S101的细化流程图；

[0057] 图8是本申请实施例提供的一种信任环的注册方法的场景示意图；

[0058] 图9是本申请实施例提供的一种身份验证方法的交互图；

[0059] 图10是本申请一实施例提供的信息共享方法中S102的细化流程图；

[0060] 图11是本申请实施例提供的信息共享装置的结构示意图；

[0061] 图12是本申请一实施例提供的身份验证单元的结构示意图；

[0062] 图13是本申请另一实施例提供的身份验证单元的结构示意图；

[0063] 图14是本申请实施例提供的终端设备的结构示意图。

具体实施方式

[0064] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0065] 请参阅图1，图1是本申请一实施例提供的信息共享方法的系统示意图。在图1所示的系统示意图中，该系统中包括终端设备A、终端设备B以及终端设备C，终端设备A已与终端设备B建立通信连接。在本实施例中，终端设备A对应于权利要求中的第一终端设备，终端设备B对应于权利要求中的第二终端设备，终端设备C对应于权利要求中的第三终端设备。

[0066] 终端设备A以及终端设备C是属于同一用户账号下的可信设备，用户账号用于标识用户账号的拥有者的身份信息，用户账号可以是预先注册的华为账号。可信设备是指该用户账号的拥有者信任的用户设备，可信设备之间具有信息分享权限。终端设备A以及终端设备C预先已通过登录该用户账号，同步所有可信设备的身份信息。即，终端设备A以及终端设备C内预先存储有所有可信设备的身份信息。终端设备A以及终端设备C包括但不限于手机、笔记本电脑、平板电脑、可穿戴设备。终端设备B包括但不限于蓝牙耳机、路由器、接入点、个人热点设备、手机、门禁终端。

[0067] 当终端设备A靠近终端设备C时，终端设备A通过近场通信(Near Field Connection，NFC)对终端设备C进行身份验证，在确认终端设备C身份合法时，终端设备A与终端设备C可以通过NFC快捷地建立通信连接，之后，终端设备A与终端设备C可以通过短距离无线通信技术共享用于连接终端设备B的通信链路信息。短距离无线通信技术可以是NFC通信，也可以是蓝牙通信，还可以是无线保真(Wireless-Fidelity，WIFI)。通信链路信息可以是蓝牙配对信息，也可以是NFC标签，还可以是用于接入无线局域网的接入信息，接入信息可以是服务集标识(Service Set Identifier，SSID)和接入密码。例如，路由器的接入信息或接入密码。

[0068] NFC门禁识别信息用于标识授权信息，例如NFC门禁授权信息，此时终端设备C可作为NFC门禁卡与终端设备B进行通信，从而实现开门等功能，此时终端设备B为门禁终端。

[0069] 本申请方案，在终端设备A与终端设备B建立通信连接之后，将终端设备B靠近终端设备C，即可方便快捷地使终端设备B与终端设备C建立通信连接，不需要用户操控终端设备C，可简化终端设备C与终端设备A建立通信连接的操作步骤，进而提高建立至少三个终端设备之间的通信连接的效率。

[0070] 并且，由于终端设备B与终端设备C可以通过NFC共享信息，即使终端设备C无法通过蜂窝移动网络或无线局域网接入互联网，终端设备B也可与终端设备C共享信息，使用场景不受互联网的限制，应用更广泛。

[0071] 为了便于理解，下面结合具体的应用场景进行说明。

[0072] 请一并参阅图2以及图3，图2是本申请一实施例提供的信息共享方法的应用场景示意图，图3是本申请实施例提供的一种蓝牙配对界面的示意图。如图2所示，在用户想要将手机、笔记本电脑、智能手表中的至少两个同时与同一个蓝牙耳机配对的应用场景下，用户操控手机100打开如图3所示的蓝牙配对界面，触发手机100搜索附近的可用设备，在搜索到可用设备时，在交互界面中显示可用设备的ID(例如，蓝牙耳机ID、笔记本电脑ID、智能手表ID)，用户点击蓝牙耳机ID触发手机100与蓝牙耳机200进行配对。如果需要密码才能完成配对时，手机100的显示界面还会弹出提示用户输入密码的对话框，用户在该对话框中输入相应的密码并确认连接后，手机100即可与蓝牙耳机200完成配对。

[0073] 在手机100与蓝牙耳机200完成配对后，如果用户将手机100靠近笔记本电脑300或智能手表400，手机100可以基于NFC对笔记本电脑300或智能手表400进行身份校验，在确认笔记本电脑300或智能手表400身份合法时，与笔记本电脑300或智能手表400建立通信连接，之后，手机100可以与笔记本电脑300或智能手表400通过短距离无线通信技术共享用于与蓝牙耳机200进行配对的蓝牙配对信息，以使得笔记本电脑300或智能手表400在接收到该蓝牙配对信息时，保存该蓝牙配对信息，之后，在检测到蓝牙耳机200时，使用该蓝牙配对信息与蓝牙耳机200进行配对。短距离无线通信技术可以是NFC通信，也可以是蓝牙通信，还可以是WIFI。

[0074] 手机100与笔记本电脑300或智能手表400共享蓝牙配对信息后，在笔记本电脑300或智能手表400与蓝牙耳机200建立通信连接的过程中，用户不需要在智能手表的交互界面查找、选择蓝牙耳机的ID，也不需要输入蓝牙耳机的配对密钥就可以实现智能手表与蓝牙耳机的配对并建立通信连接，全程不需要用户参与，简化了智能手表与蓝牙耳机进行配对的操作步骤，进而提高建立手机、智能手表、笔记本电脑与蓝牙耳机之间的通信连接的效率。并且，由于手机100与笔记本电脑300或智能手表400可以通过NFC或蓝牙共享信息，因此，即使笔记本电脑、智能手表以及手机在未接入互联网的情况下，手机也能在离线状态下向处于离线状态的智能手表或笔记本电脑发送蓝牙配对信息。

[0075] 在另一应用场景中，终端设备之间可以共享用于接入无线局域网的通信链路信息。请一并参阅图4，图4是本申请另一实施例提供的信息共享方法的应用场景示意图。

[0076] 例如，用户携带手机100和手机600去朋友家，手机100和手机600均未连接过朋友家的无线路由器500，当用户在手机100的设置界面查找到无线路由器500的SSID时，点击该SSID，在弹出的密码输入界面输入无线路由器500的接入密码后点击确认“加入”，手机100成功接入该路由器。或者手机100在上次拜访时已连接过朋友家的无线路由器，在用户到朋友家时，手机100自动连接朋友家的无线路由器500。

[0077] 由于手机600未曾连接朋友家的无线路由器500，手机100在接入朋友家的无线路由器500时，用户可以将手机100靠近手机600，此时，手机100通过近程通信技术对手机600进行身份验证，手机100在验证手机600身份合法时，手机100与手机600建立通信连接。手机100与手机600可以通过短距离无线通信技术共享WIFI接入信息，以使手机600在接收到WIFI接入信息之后，并且检测到无线路由器500时，基于接收到的WIFI接入信息接入朋友家的无线路由器500。共享的WIFI接入信息可以是用于接入无线路由器500(或个人热点、无线接入点)的接入信息，还可以是手机100接入过的无线局域网的接入信息。

[0078] 再例如，用户上次带手机100去朋友家，手机100成功连接了朋友家的无线路由器500，然后回到自己家后，手机100和手机600交换了通信链路信息，手机600内保存了用于接入无线路由器500的WIFI接入信息。然后，用户只带手机600再去朋友家时，手机600在检测到无线路由器500时，也可以通过预先保存的WIFI接入信息连上无线路由器500。手机100接入无线路由器500后，在手机600与无线路由器500建立通信连接的过程中，用户不需要在手机600的交互界面查找、无线路由器500的SSID，也不需要输入无线路由器500的接入密码，手机600就可以连接无线路由器500，全程不需要用户参与，简化了手机600连接无线路由器500的操作步骤，进而提高手机600与无线路由器500之间的通信连接的效率。并且，由于手机100与手机600可以通过NFC或蓝牙共享信息即使手机600在未接入互联网的情况下，手机100也能向手机600发送无线路由器500的接入信息。

[0079] 可以理解的是，本申请中所使用的术语只是为了描述特定实施例的目的，而并非旨在作为对本申请的限制。如在本申请的说明书和所附权利要求书中所使用的那样，单数表达形式“一个”、“一种”、“所述”、“上述”、“该”和“这一”旨在也包括例如“一个或多个”这种表达形式，除非其上下文中明确地有相反指示。还应当理解，在本申请实施例中，“一个或多个”是指一个、两个或两个以上；“和/或”，描述关联对象的关联关系，表示可以存在三种关系；例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B的情况，其中A、B可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。

[0080] 本申请实施例提供的信息共享方法可以应用于手机、平板电脑、可穿戴设备、车载设备、增强现实(Augmented Reality，AR)/虚拟现实(Virtual Reality，VR)设备、笔记本电脑、上网本、个人数字助理(Personal Digital Assistant，PDA)等支持近程无线通信的终端设备上，本申请实施例对终端设备的具体类型不作任何限制。与终端设备通信配对或连接的终端设备可以是蓝牙耳机、无线接入点或个人热点等。

[0081] 当终端设备为可穿戴设备时，该可穿戴设备还可以是应用穿戴式技术对日常穿戴进行智能化设计、开发出可以穿戴的设备的总称，如眼镜、手套、手表、服饰及鞋等。可穿戴设备即直接穿在身上，或是整合到用户的衣服或配件的一种便携式设备。可穿戴设备不仅仅是一种硬件设备，更是通过软件支持以及数据交互、云端交互来实现强大的功能。广义穿戴式智能设备包括功能全、尺寸大、可不依赖手机实现完整或者部分的功能，如智能手表或智能眼镜等，以及只专注于某一类应用功能，需要和其它设备如手机配合使用，如各类进行体征监测的智能手环、智能首饰等。

[0082] 以所述终端设备为手机为例。图5示出的是与本申请实施例提供的手机的部分结构的框图。参考图5，手机5包括：射频(Radio Frequency，RF)电路510、存储器520、输入单元530、显示单元540、传感器550、音频电路560、WIFI模块570、处理器580、以及电源590等部件。本领域技术人员可以理解，图5中示出的手机结构并不构成对手机的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0083] 下面结合图5对手机5的各个构成部件进行具体的介绍：

[0084] RF电路510可用于收发信息或通话过程中，信号的接收和发送，特别地，将基站的下行信息接收后，给处理器580处理；另外，将设计上行的数据发送给基站。通常，RF电路包括但不限于天线、至少一个放大器、收发信机、耦合器、低噪声放大器(Low Noise Amplifier，LNA)、双工器等。此外，RF电路510还可以通过无线通信与网络和其他设备通信。

上述无线通信可以使用任一通信标准或协议，包括但不限于全球移动通讯系统(Global System of Mobile communication,GSM)、通用分组无线服务(General Packet Radio Service,GPRS)、码分多址(Code Division Multiple Access,CDMA)、宽带码分多址(Wideband Code Division Multiple Access,WCDMA)、长期演进(Long Term Evolution,LTE))、电子邮件、短消息服务(Short Messaging Service,SMS)等。

[0085] 存储器520可用于存储信息共享软件程序以及模块，处理器180通过运行存储在存储器520的信息共享软件程序以及模块，从而执行手机的各种功能应用以及数据处理。例如，处理器180内存储的信息共享软件程序可用于对如图1中的终端设备C进行身份验证。存储器520可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能、NFC通信功能、蓝牙通信功能等)等；存储数据区可存储根据手机的使用所创建的数据(比如音频数据、电话本、待共享的通信链路信息、无线网的接入信息、NFC门禁识别信息等)等。此外，存储器520可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

[0086] 输入单元530可用于接收输入的数字或字符信息，以及产生与手机5的用户设置以及功能控制有关的键信号输入。具体地，输入单元530可包括触控面板531以及其他输入设备532。触控面板531，也称为触摸屏，可收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触控面板531上或在触控面板531附近的操作)，并根据预先设定的程式驱动相应的连接装置。可选的，触控面板531可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换成触点坐标，再送给处理器580，并能接收处理器580发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触控面板531。除了触控面板531，输入单元530还可以包括其他输入设备532。具体地，其他输入设备532可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0087] 显示单元540可用于显示由用户输入的信息或提供给用户的信息以及手机的各种菜单。显示单元540可包括显示面板541，可选的，可以采用液晶显示器(Liquid Crystal Display,LCD)、有机发光二极管(Organic Light-Emitting Diode,OLED)等形式来配置显示面板541。进一步的，触控面板531可覆盖显示面板541，当触控面板531检测到在其上或附近的触摸操作后，传送给处理器580以确定触摸事件的类型，随后处理器580根据触摸事件的类型在显示面板541上提供相应的视觉输出。虽然在图5中，触控面板531与显示面板541是作为两个独立的部件来实现手机的输入和输入功能，但是在某些实施例中，可以将触控面板531与显示面板541集成而实现手机的输入和输出功能。

[0088] 手机5还可包括至少一种传感器550，比如光传感器、运动传感器以及其他传感器。具体地，光传感器可包括环境光传感器及接近传感器，其中，环境光传感器可根据环境光线的明暗来调节显示面板541的亮度，接近传感器可在手机移动到耳边时，关闭显示面板541和/或背光。作为运动传感器的一种，加速计传感器可检测各个方向上(一般为三轴)加速度的大小，静止时可检测出重力的大小及方向，可用于识别手机姿态的应用(比如横竖屏切换、相关游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等；至于手机还可

配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。

[0089] 音频电路560、扬声器561，传声器562可提供用户与手机之间的音频接口。音频电路160可将接收到的音频数据转换后的电信号，传输到扬声器561，由扬声器161转换为声音信号输出；另一方面，传声器562将收集的声音信号转换为电信号，由音频电路560接收后转换为音频数据，再将音频数据输出处理器580处理后，经RF电路510以发送给比如另一手机，或者将音频数据输出至存储器520以便进一步处理。

[0090] WIFI属于短距离无线传输技术，手机通过WIFI模块570可以帮助用户收发电子邮件、浏览网页和访问流式媒体等，它为用户提供了无线的宽带互联网访问。虽然图5示出了WIFI模块570，但是可以理解的是，其并不属于手机5的必须构成，完全可以根据需要在不改变发明的本质的范围内而省略。

[0091] 处理器580是手机的控制中心，利用各种接口和线路连接整个手机的各个部分，通过运行或执行存储在存储器520内的软件程序和/或模块，以及调用存储在存储器520内的数据，执行手机的各种功能和处理数据，从而对手机进行整体监控。可选的，处理器580可包括一个或多个处理单元；优选的，处理器580可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器580中。

[0092] 手机5还包括给各个部件供电的电源590(比如电池)，优选的，电源可以通过电源管理系统与处理器580逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。

[0093] 尽管未示出，手机5还可以包括摄像头。可选地，摄像头在手机500的上的位置可以为前置的，也可以为后置的，本申请实施例对此不作限定。

[0094] 可选地，手机5可以包括单摄像头、双摄像头或三摄像头等，本申请实施例对此不作限定。

[0095] 例如，手机5可以包括三摄像头，其中，一个为主摄像头、一个为广角摄像头、一个为长焦摄像头。

[0096] 可选地，当手机5包括多个摄像头时，这多个摄像头可以全部前置，或者全部后置，或者一部分前置、另一部分后置，本申请实施例对此不作限定。

[0097] 另外，尽管未示出，手机5还可以包括蓝牙模块等，蓝牙模块用于在如图2中的手机100与蓝牙耳机200完成配对时，将用于连接蓝牙耳机200的蓝牙配对信息按预设的存储路径存储到存储器580中，还用于在手机100与笔记本电路300或智能手表400建立通信连接时，基于预设的存储路径从存储器580中获取用于连接蓝牙耳机200的蓝牙配对信息，并采用蓝牙通信技术将获取到的蓝牙配对信息发送给笔记本电路300或智能手表400等，在此不再赘述。

[0098] 为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述。以下实施例可以在具有上述硬件结构的手机5上实现。以下实施例将以手机5为例，对本申请实施例提供的信息共享方法进行说明。

[0099] 请参阅图6，图6是本申请一实施例提供的信息共享方法的示意性流程图，作为示例而非限定，该方法可以应用于上述手机5中。本实例中的信息共享方法包括以下步骤：

[0100] S101：第一终端设备在与第二终端设备建立通信连接后，并且靠近第三终端设备

时，基于近场通信技术对所述第三终端设备进行身份验证。

[0101] 其中，第一终端设备可以存储有第三终端设备的身份信息。可以理解的是，第一终端设备除了可以是手机之外，也可以是笔记本电脑、平板电脑、可穿戴设备等终端；第二终端设备包括但不限于蓝牙耳机、路由器、接入点、个人热点设备、手机、门禁终端。第三终端设备可以是手机，也可以是笔记本电脑、平板电脑、可穿戴设备等终端。

[0102] 进一步地，第三终端设备可以处于离线状态，即，第三终端设备未启用蜂窝移动网络和无线局域网，或者当前无法通过蜂窝移动网络或无线局域网接入互联网。

[0103] 在第一终端设备与第二终端设备建立通信连接之后，用户需要将第一终端设备内的信息共享到第三终端设备时，可以将第一终端设备向第三终端设备所在的位置移动，以使第一终端设备靠近第三终端设备。第一终端设备可以检测第三终端设备发射的探测信号，并获取接收到的第三终端设备发射的探测信号的信号强度指示(Received Signal Strength Indication，RSSI)值。由于RSSI值的大小与接收端和发射端之间的距离有关，在一定程度上距离越近，RSSI值越大，因此，第一终端设备可以比较相邻两个时刻获取到的RSSI值，当相邻两个时刻获取到的RSSI值逐渐变大，判定第一终端设备向第三终端设备所在的位置靠近。此时，第一终端设备可以基于近场通信技术对所述第三终端设备进行身份验证。

[0104] 或者，第一终端设备可以采用近程无线通信技术探测在第一终端设备周围是否存在第三终端设备，并在检测到第三终端设备时，基于NFC对第三终端设备进行身份验证。

[0105] 例如，用户可以通过设置界面开启蓝牙功能，并将第一终端设备靠近第三终端设备。第一终端设备在开启蓝牙通信功能时，检测当前是否接收到蓝牙探测信号，当检测到其他设备发射的蓝牙探测信号时，判定在第一终端设备周围存在第三终端设备。或者，第一终端设备在开启NFC功能时，检测当前是否接收到NFC探测信号，当检测到其他设备发射的NFC探测信号时，判定在第一终端设备周围存在第三终端设备。可以理解的是，第一终端设备在检测到第三终端设备时，可以在显示界面中显示提示信息或提示图标，或者通过语音提示信息提醒用户当前检测到第三终端设备。该提示信息或提示图标用于提醒用户当前检测到第三终端设备。例如，第一终端设备当检测到支持蓝牙通信的第三终端设备时，在显示界面中显示第三终端设备的设备ID(例如，如图3所示的显示界面中的可用设备的ID)或者显示用于表示“当前检测到可连接的蓝牙设备”的提示信息。第一终端设备当检测到支持NFC通信的第三终端设备时，可以在显示界面显示第三终端设备的示意图像，或显示用于表示“当前检测到可连接的NFC设备”的提示信息。第三终端设备的示意图像可以类似于图1所示的手表、手机、平板电脑或笔记本电脑的示意图。

[0106] 进一步地，为了更准确地确定需要共享信息的终端设备，第一终端设备在检测到第三终端设备时，可以在确认任意时刻获得的RSSI值大于或等于预设阈值时，判定第一终端设备与第三终端设备之间的距离属于预设距离范围，用户此时需要使第一终端设备与第三终端设备实现信息共享。第一终端设备基于近场通信技术对第三终端设备进行身份验证。预设阈值基于预设距离范围内的RSSI设置，具体可根据实际情况进行设置，此处不做限制。

[0107] 第一终端设备对第三终端设备进行身份验证的方式可以为：第一终端设备通过NFC与第三终端设备进行通信，请求第三终端设备返回第三终端设备的身份信息。第一终端

设备在获取到第三终端设备的身份信息时，从身份数据库中查找与该身份信息匹配的身份信息，在查找到匹配的身份信息时，判定第三终端设备身份合法，在未查找到匹配的身份信息时，判定第三终端设备不合法。

[0108] 其中，该身份信息可以是第三终端设备的唯一身份识别信息，例如，介质访问控制(MediaAccess Control，MAC)地址，唯一识别码或唯一序列号。当第三终端设备为手机时，该唯一识别码为国际移动设备识别码(International Mobile Equipment Identity，IMEI)。

[0109] 该身份信息也可以是第三终端设备的密钥对中的公钥。密钥对包括公钥和私钥，密钥对可以是第三终端设备采用非对称加密算法生成。采用非对称加密算法生成密钥对的方法为现有技术，具体请参阅现有技术中的相关描述，此处不赘述。

[0110] 身份信息数据库中预先存储有第一终端设备允许共享信息的终端设备的身份信息。身份信息数据库中预先存储的终端设备的身份信息可以由用户预先输入，也可以由其他设备发送，此处不做限制。

[0111] S102：所述第一终端设备在确认所述第三终端设备身份合法时，通过短距离无线通信技术将通信链路信息发送至所述第三终端设备，以触发所述第三终端设备在检测到所述第二终端设备时，使用所述通信链路信息与第二终端设备建立通信连接。

[0112] 第一终端设备在确认第三终端设备的身份合法时，判定第三终端设备为可信设备，第一终端设备与第三终端设备协商通信端口，并基于协商好的通信端口建立安全传输通道。第一终端设备与第三终端设备协商在安全传输通道中需要使用的安全参数。其中，安全参数包括通信协议版本以及加密算法。

[0113] 第一终端设备可以从用于存储通信链路信息的存储区域获取通信链路信息，也可以弹出对话框提示用户选择通信链路信息，用户可以通过交互界面查找或选择通信链路信息。在获取到通信链路信息之后，采用协商好的通信协议，通过短距离无线通信技术将通信链路信息通过安全传输通道发送给第三终端设备，以使得第三终端设备在接收到通信链路信息之后，并且检测到第二终端设备时，使用通信链路信息与第二终端设备建立通信连接。

[0114] 可以理解的是，当第三终端设备可连接无线局域网时，短距离无线通信技术可以是NFC通信，也可以是蓝牙通信，还可以是WIFI。

[0115] 进一步地，当第三终端设备处于离线状态时，短距离无线通信技术为NFC或蓝牙通信。此时，第一终端设备和第三终端设备可以在离线状态共享文件，以使用户在没有网络的情况下，实现终端之间的数据共享。

[0116] 进一步地，当第二终端设备为预先与第一终端设备完成配对的终端设备时，通信链路信息包括用于与第二终端设备进行配对的蓝牙配对信息，以使得第三终端设备能够在接收到蓝牙配对信息后，并且检测到第二终端设备时，使用该蓝牙配对信息与第二终端设备进行蓝牙配对。

[0117] 进一步地，通信链路信息还可以包括无线网的接入信息和/或NFC门禁识别信息。

[0118] 可以理解的是，第一终端设备在当前已与第三终端设备建立通信连接时，默认通信链路信息为用于与第三终端设备建立通信连接的通信链路信息。

[0119] 通信链路信息可以包括第一终端设备当前连接或曾连接的所有第三终端设备对应的通信链路信息。例如，第一终端设备已连接过的所有无线接入点、个人热点或路由器各

自对应的通信链路信息。

[0120] 通信链路信息可以存储于第一终端设备内的无线网卡管理程序的配置文件中。例如,通信链路信息的存储路径可以为/data/misc/wifi/wpa_supplicant.conf。

[0121] 例如,如图2所示的应用场景中,手机100采用协商好的通信协议,将与蓝牙耳机200进行配对的蓝牙配对信息通过建立的安全传输通道发送给智能手表400,以使智能手表400在接收到蓝牙配对信息时,基于蓝牙配对信息中包含的蓝牙耳机的ID,查找蓝牙耳机200,在查找到蓝牙耳机200时,基于蓝牙耳机与手机的配对链路以及蓝牙配对时使用的配对密钥,与蓝牙耳机200建立通信连接。

[0122] 手机100在建立与笔记本电脑300之间的安全传输通道时,也可以从本地数据库中获取用于与蓝牙耳机200进行配对的蓝牙配对信息;并采用协商好的通信协议,将蓝牙配对信息通过与笔记本电脑300的安全传输通道发送给笔记本电脑300,以使笔记本电脑300在接收到蓝牙配对信息时,基于蓝牙配对信息中包含的蓝牙耳机的ID,查找蓝牙耳机200,在查找到蓝牙耳机200时,基于蓝牙耳机与手机的配对链路以及蓝牙配对时使用的配对密钥,与蓝牙耳机200建立通信连接。

[0123] 此时,用户不需要在智能手表400和笔记本电脑300中查找蓝牙耳机的ID以及输入配对密码,智能手表400和笔记本电脑300就可以自动连接蓝牙耳机200。

[0124] 再例如,在如图4所示的应用场景中,手机100建立用于与手机600进行数据交互的安全传输通道时,采用协商好的通信协议,将WIFI接入信息通过与手机600的安全传输通道发送给手机600,以使手机600在接收到WIFI接入信息后,并且检测到无线路由器500时,基于获取到的SSID以及接入密码,接入无线路由器500。

[0125] 此时,手机500在用户没有输入WIFI接入密码时,也可以自动连接手机100之前已连接过的无线路由器、无线接入点或个人热点。

[0126] 可以理解的是,第一终端设备与第三终端设备建立通信连接后,第三终端设备也可以向第一终端设备发送需要共享的信息。

[0127] 上述方案,在第一终端设备与第二终端设备建立通信连接之后,将第一终端设备靠近第三终端设备时,即可方便快捷地使第一终端设备与第三终端设备建立通信连接,进而共享通信链路信息,以使得第三终端设备在检测到第二终端设备时,使用该通信链路信息与第二终端设备建立通信连接。既不需要其他设备参与数据交互,也不需要用户操控第三终端设备即可让第三终端设备与第二终端设备建立通信连接,可简化第三终端设备与第二终端设备建立通信连接的操作步骤,进而提高建立至少三个终端设备之间的通信连接的效率。第一终端设备和第三终端设备可以在离线状态共享文件,以使用户在没有网络的情况下,实现终端之间的数据共享。

[0128] 进一步地,在另一实施例中,对图1中的S101进行了细化,请阅图7,图7是本申请一实施例提供的信息共享方法中S101的细化流程图。S101可以具体包括S1031～S1033,具体如下:

[0129] S1031:所述第一终端设备在与所述第二终端设备建立通信连接后,并且靠近第三终端设备时,通过NFC向所述第三终端设备发送身份认证通知消息;

[0130] S1032:所述第一终端设备获取所述第三终端设备在接收到所述身份认证通知消息时通过NFC返回的第一身份信息;

[0131] S1033:所述第一终端设备基于所述第一身份信息以及预存的第二身份信息,对所述第三终端设备进行身份验证。

[0132] 例如,第一终端设备与第二终端设备建立通信连接后,并且靠近第三终端设备时,可以采用NFC技术向第三终端设备发送身份认证通知消息,以指示第三终端设备在接收到身份认证通知消息时,基于身份认证通知消息包含或携带的第一终端设备的设备标识,将自身的第一身份信息返回给第一终端设备。第一终端设备在获取到第三终端设备发送的第一身份信息时,从身份信息数据库中预存的第二身份信息中查找与第三终端设备发送的身份信息相匹配的身份信息,当查找到匹配的身份信息时,判定第三终端设备的身份验证结果为验证通过;当未查找到匹配的身份信息时,判定第三终端设备的身份验证结果为验证失败。

[0133] 进一步地,第一身份信息可以包括第三终端设备的第一设备标识以及第一公钥。

[0134] 进一步地,第一身份信息可以包括第三终端设备的第一设备标识、公钥属性凭据的第一版本号以及由第三终端设备生成的第一随机数。第一随机数可以是第三终端设备在接收到第一终端设备发送的身份认证通知消息时生成,也可以预先生成,此处不做限制。

[0135] 进一步地,在一实施方式中,当第一身份信息包括第三终端设备的第一设备标识以及第一公钥时,S1033具体为:所述第一终端设备基于所述第一设备标识从身份数据库中获取所述第三终端设备对应的预存的公钥,并基于所述第一公钥和所述预存的公钥对所述第三终端设备进行身份验证;其中,当所述第一公钥和所述预存的公钥相同时,判定所述第三终端设备身份合法。

[0136] 具体地,第一终端设备在查找到第三终端设备对应的预存的公钥时,将第一身份信息中的第一公钥与获取到的预存的公钥进行比较,以对第三终端设备进行身份验证。当比较结果为第一公钥和所述预存的公钥相同时,第一终端设备判定第三终端设备身份合法;当比较结果为第一公钥和所述预存的公钥不相同时,第一终端设备判定第三终端设备身份不合法。

[0137] 进一步地,在另一实施方式中,当第一身份信息包括第三终端设备的第一设备标识、公钥属性凭据的第一版本号以及由第三终端设备生成的第一随机数时,公钥属性凭据的版本号主要是为了确认对方是否已被撤销(从信任环中移除),或是新加入信任环的设备,这样对于离线设备也可以有一定的安全性,不需要随时保持在线确认每个设备证书的有效性。S1033包括以下步骤:

[0138] S1:所述第一终端设备基于所述第一设备标识以及所述第一版本号,获取所述第三终端设备的第一公钥。

[0139] 第一终端设备可以从本地数据库中查找与第一设备标识匹配的设备标识,并在查找到匹配的设备标识时,基于第一设备标识从本地数据库中获取第三终端设备的公钥属性的第二版本号,基于比较结果确定当前是从本地获取第三终端设备的第一公钥,还是向第三终端设备请求返回第一公钥。当第一版本号小于或等于第一版本号时,从本地获取第三终端设备的第一公钥;当第一版本号大于第一版本号时,向第三终端设备请求返回第一公钥。

[0140] 本实施例方式中,通过查找与第一设备标识匹配的设备标识来确认第三终端设备是否为新加入的可信设备,通过比较公钥属性凭据的第一版本号以及第二版本号,来确认

第三终端设备是否被撤销可信资格，这样对于离线设备也有一定的安全性，不必随时保持在线确认每个设备的公钥的有效性。

[0141] 其中，当未查找到匹配的设备标识时，第三终端设备为新加入的可信设备；当第一版本号小于第二版本号，且未查找到匹配的设备标识时，第三终端设备被撤销可信资格。

[0142] 进一步地，S1具体包括：所述第一终端设备从身份数据库中查找与所述第一设备标识匹配的设备标识；

[0143] 当查找到所述匹配的设备标识，且所述第一版本号小于或等于预存的公钥属性凭据的第二版本号时，从所述身份数据库中获取所述第三终端设备的公钥；

[0144] 当未查找到所述匹配的设备标识，且所述第一版本号大于预存的公钥属性凭据的第二版本号，向所述第三终端设备请求获取所述第一公钥。

[0145] 可以理解的是，当未查找到所述匹配的设备标识，且所述第一版本号小于预存的公钥属性凭据的第二版本号时，判定所述第三终端设备身份不合法。

[0146] S2：所述第一终端设备基于自身的私钥和所述第一公钥计算第一共享密钥，并生成第二随机数。

[0147] 第一终端设备可以基于第一终端设备的私钥以及第三终端设备的第一公钥，采用消息摘要算法计算得到共享密钥；也可以采用哈希算法计算第一终端设备的私钥以及第三终端设备的第一公钥的哈希值，得到共享密钥；还可以通过其他算法计算共享密钥，在此不对计算共享密钥的方式做限定。

[0148] S3：所述第一终端设备基于所述第一共享密钥、所述第一终端设备的第二设备标识、所述第一随机数以及所述第二随机数，计算第一身份特征值。

[0149] 第一终端设备可以将第一共享密钥、第一终端设备的第二设备标识、第一随机数以及第二随机数拼接成一条消息，并采用消息摘要算法计算该消息的摘要值，得到第一身份特征值。

[0150] 第一终端设备也可以以共享密钥计算该消息的消息认证码(Message Authentication Code，MAC)值，得到第一身份特征值。

[0151] 具体地，第一终端设备可以将第一终端设备的设备ID、第一随机数以及第二随机数作为一条消息M，采用消息摘要算法计算出该消息M的摘要值，并在共享密钥的作用下由该摘要值计算出MAC值。或者，第一终端设备在共享密钥的参与下采用消息认证算法计算消息M的MAC值。例如，采用共享密钥对消息M的摘要值进行加密得到MAC值，或者采用共享密钥对消息M加密得到MAC值。

[0152] S4：所述第一终端设备通过近场通信向所述第三终端设备发送所述第一身份特征值、所述第一终端设备的第二设备标识、公钥属性凭据的第二版本号以及所述第二随机数。

[0153] S5：所述第一终端设备接收所述第三终端设备返回的第二身份特征值；其中，所述第二身份特征值由所述第三终端设备在计算出第二共享密钥时，基于所述第二共享密钥、所述第二设备标识、所述第一随机数以及所述第二随机数计算得到，所述第二共享密钥基于所述第三终端设备的私钥以及所述第一终端设备的公钥计算得到。

[0154] 第三终端设备计算共享密钥的方法与第一终端设备计算共享密钥的方法相同，第三终端设备计算第二身份特征值的方法与第一终端设备计算第一身份特征值的方法相同，此处不赘述。

[0155] S6:所述第一终端设备在确认所述第一身份特征值与所述第二身份特征值相同时,判定所述第三终端设备身份合法。

[0156] 下面结合身份验证方法的交互图详细阐述身份验证过程,具体如下:

[0157] 在S1之前,第一终端设备以及第三终端设备预先通过登录同一用户账号向服务器发送自己的公钥进行注册,当第三终端设备处于断网状态,且第一终端设备通过NFC检测到第三终端设备时,基于第三终端设备的公钥对第三终端设备进行身份认证。

[0158] 具体地,请一并参阅图8,图8是本申请实施例提供的一种信任环的注册方法的场景示意图。图8中,笔记本电脑、平板电脑以及手机是已经登录同一用户账号,且向服务器发送自身的公钥注册成功的设备,即已加入信任环。智能手表是还未加入信任环的设备。

[0159] 由于每个终端设备都可以拥有一个公私钥对,当用户购买了新的终端设备(例如,智能手表)时,可以触发智能手表采用非对称加密算法生成公私钥对。用户操控新的智能手表进入账号登录界面,并在账号登录界面中输入用户账号以及登录密码向服务器发送登录请求,服务器在接收到登录请求时,基于数据库中存储的注册账号及注册密码,校验登录请求中的用户账号以及登录密码是否正确,并在确认登录请求中的用户账号以及登录密码正确时,允许智能手表登录并与其建立通信连接。此时,智能手表可以显示登录成功的交互界面,用户可以操控智能手表进入用于注册信任环的交互界面,用户可以通过该交互界面输入或选择智能手表的公钥,并点击“注册”选项,触发智能手表向服务器发送注册请求。注册请求包括智能手表的设备标识及其公钥。

[0160] 服务器在接收到注册请求时,解析出注册请求中包含的设备标识以及公钥,并建立该设备标识及公钥之间的关联关系,将智能手表添加至信任环,向智能手表返回信任环中的现有设备的设备标识及各自的公钥,之后,向信任环中的现有设备广播智能手表的设备标识以及公钥,以通知信任环中的现有设备当前有新设备加入信任环,以指示信任环中的现有设备存储智能手表的设备标识以及公钥。这样一来,加入信任环的每个设备内存有已加入信任环的所有设备的设备标识及其公钥。

[0161] 请一并参阅图9,图9是本申请实施例提供的一种身份验证方法的交互图。第一终端设备采用以下方式对第三终端设备进行身份验证:

[0162] 1、第一终端设备在检测到第三终端设备时,可以采用NFC技术向第三终端设备发送身份认证通知消息。

[0163] 2、第三终端设备在接收到身份认证通知消息时,向第一终端设备发送认证请求信息,认证请求信息中包括第三终端设备的设备ID、第三终端设备的公钥属性凭据的版本号以及由第三终端设备生成的第一随机数。

[0164] 3、第一终端设备在接收到第三终端设备发送的认证请求信息时,对认证请求信息进行解析,得到第三终端设备的设备ID、第三终端设备的公钥属性凭据的版本号以及由第三终端设备生成的第一随机数;在本地公钥目录执行以下步骤:

[0165] a)查找第三终端设备的设备ID,并比较本地公钥目录存储的版本号与对方发来的版本号,也即,比较接收到的公钥属性凭据的版本号(第三终端设备发送的公钥属性凭据的第一版本号)与本地存储的版本号(本地存储的第三终端设备对应的公钥属性凭据的第二版本号),判断接收到的公钥属性凭据的版本号是否为最新的版本号。版本号主要是为了确认对方是否已被撤销(从信任环中移除),或是新加入信任环的设备。如此对于离线设备也

可以有一定的安全性，不需要随时保持在线确认每个设备证书的有效性。

[0166] b)基于查找结果以及比较结果，按下表中的处理策略进行处理，从而获取第三终端设备的公钥。

[0167] 其中，当未查找到第三终端设备的设备ID，且本地存储的版本号小于对方发来的版本号时，判定第三终端设备是新加入信任环的设备，本地公钥目录存储的第三终端设备的公钥以及公钥属性凭据为旧版本，向第三终端设备发送公钥获取请求信息，以请求获取第三终端设备的公钥以及公钥属性凭据；

[0168] 当未查找到第三终端设备的设备ID，且本地存储的版本号大于对方发来的版本号时，判定本地存储的数据为最新版本，本地公钥目录最后更新后，第三终端设备的数据已不在本地公钥目录中，第三终端设备已被撤销信任资格；此时第一终端设备判定第三终端设备不可信，拒绝连接第三终端设备；

[0169] 当查找到第三终端设备的设备ID，且本地存储的版本号大于对方发来的版本号时，判定本地公钥目录存储的数据为最新版本，使用本地公钥目录中存储的第三终端设备的公钥对第三终端设备进行身份验证，从本地公钥目录获取第三终端设备的公钥，不再需要第三终端设备发送公钥及公钥属性凭据。

[0170]

比较接收到的版本号与本地存储的版本号	查找是否存在接收到的设备ID	处理方法
接收到的版本号大于本地存储的版本号	不存在	要求对方发送公钥以及公钥属性凭据
接收到的版本号小于本地存储的版本号	不存在	拒绝连接，认证结果为不可信
接收到的版本号小于本地存储的版本号	存在	使用本地目录中的公钥，不需要对方发送公钥以及公钥属性凭据

[0171] 4、第一终端设备在获取到第三终端设备的公钥时，第一终端设备以自己的私钥与第三终端设备的公钥计算共享密钥。可以理解的是，第一终端设备可以基于第一终端设备的私钥以及第三终端设备的公钥，采用消息摘要算法计算得到共享密钥；也可以采用哈希算法计算第一终端设备的私钥以及第三终端设备的公钥的哈希值，得到共享密钥；还可以通过其他算法计算共享密钥，在此不对计算共享密钥的方式做限定。

[0172] 5、第一终端设备生成第二随机数，以共享密钥计算第一终端设备的设备ID、由第三终端设备生成的第一随机数以及由第一终端设备生成的第二随机数所对应的消息认证码MAC值。

[0173] 具体地，第一终端设备可以将第一终端设备的设备ID、第一随机数以及第二随机数作为一条消息M，采用消息摘要算法计算出该消息M的摘要值，并在共享密钥的作用下由该摘要值计算出MAC值。或者，第一终端设备在共享密钥的参与下采用消息认证算法计算消息M的MAC值。例如，采用共享密钥对消息M的摘要值进行加密得到MAC值，或者采用共享密钥对消息M加密得到MAC值。

[0174] 6、第一终端设备采用NFC技术将自己的设备ID、自己的公钥属性凭据的版本号、第二随机数发送给第三终端设备;可以理解的是,当第三终端设备需要对第一终端设备进行身份验证时,第一终端设备还可以将计算得到的MAC值发送给第三终端设备,以使第三终端设备在计算出共享密钥时,采用共享密钥验证该MAC值,从而对第一终端设备进行身份验证。

[0175] 7、第三终端设备在获取到第一终端设备的设备ID以及公钥属性凭据的版本号时,进行以下处理:

[0176] 查找第一终端设备的设备ID,并比较本地存储的版本号与对方发来的版本号;基于查找结果以及比较结果,按上表中的处理策略进行处理;

[0177] 其中,当未查找到第一终端设备的设备ID,且本地存储的版本号小于对方发来的版本号时,判定第一终端设备是新加入信任环的设备,本地公钥目录存储的第一终端设备的公钥以及公钥属性凭据为旧版本,向第一终端设备发送公钥获取请求信息,以请求获取第一终端设备的公钥以及公钥属性凭据;

[0178] 当未查找到第一终端设备的设备ID,且本地存储的版本号大于对方发来的版本号时,判定本地公钥目录存储的数据为最新版本,本地公钥目录最后更新后,第一终端设备的数据已不在本地公钥目录中,第一终端设备已被撤销信任资格;此时第三终端设备判定第一终端设备不可信,拒绝连接第一终端设备;

[0179] 当查找到第一终端设备的设备ID,且本地存储的版本号大于对方发来的版本号时,判定本地公钥目录存储的数据为最新版本,使用本地公钥目录中存储的第一终端设备的公钥对第一终端设备进行身份验证,从本地公钥目录获取第一终端设备的公钥,不再需要第一终端设备发送公钥及公钥属性凭据。

[0180] 8、第三终端设备在获取到第一终端设备的公钥时,第三终端设备以自己的私钥与第一终端设备的公钥计算共享密钥。可以理解的是,第三终端设备可以基于第三终端设备的私钥以及第一终端设备的公钥,采用消息摘要算法计算得到共享密钥;也可以采用哈希算法计算第三终端设备的私钥以及第一终端设备的公钥的哈希值,得到共享密钥;还可以通过其他算法计算共享密钥,在此不对计算共享密钥的方式做限定。由于密钥协商算法(Elliptic CurvesDiffie-Hellman,ECDH)具有交换性,因此,第一终端设备以及第三终端设备计算得到的共享密钥相同。

[0181] 9、第三终端设备以共享密钥计算第一终端设备的设备ID、由第三终端设备生成的第一随机数以及由第一终端设备生成的第二随机数所对应的MAC值。

[0182] 10、采用NFC技术将计算得到的MAC值发送给第一终端设备。

[0183] 其中,第三终端设备计算消息认证码MAC值的方法与第一终端设备计算消息认证码MAC值的方法相同,具体请参阅上述第一终端设备计算消息认证码MAC值的描述,此处不赘述。

[0184] 可选地,当第三终端设备接收到第一终端设备发送的MAC值时,可以采用共享密钥验证第一终端设备发送的MAC值,从而对第一终端设备进行身份验证。

[0185] 例如,当第一终端设备发送的MAC值由共享密钥对第一终端设备的设备ID、第一随机数以及第二随机数进行加密得到时,第三终端设备可以采用计算得到的共享密钥对第一终端设备发送的MAC值进行解密,如果解密得到第一终端设备的设备ID、第一随机数以及第

二随机数时，判定第一终端设备身份合法，身份验证通过；如果解密后得到的数据与第一终端设备的设备ID、第一随机数以及第二随机数中的任一个不相同时，判定第一终端设备身份不合法，身份验证失败。

[0186] 再例如，当第一终端设备发送的MAC值由共享密钥对摘要值(该摘要值由第一终端设备的设备ID、第一随机数以及第二随机数计算得到)进行加密得到时，第三终端设备可以采用计算得到的共享密钥对第一终端设备发送的MAC值进行解密，如果解密得到的摘要值，并采用消息摘要算法计算第一终端设备的设备ID、第一随机数以及第二随机数所对应的摘要值；如果解密得到的摘要值与计算得到的摘要值相同，判定第一终端设备身份合法，身份验证通过；如果解密得到的摘要值与计算得到的摘要值不同时，判定第一终端设备身份不合法，身份验证失败。

[0187] 11、第一终端设备在接收到第三终端设备发送的MAC值时，将接收到的MAC值与发送给第三终端设备的MAC值进行比较，当两者相同时，判定第三终端设备的身份合法，身份验证通过；当两者不同时，判定第三终端设备身份不合法，身份验证失败。

[0188] 为了便于理解，下面结合具体的应用场景对上述过程描述，具体如下：

[0189] 请继续参阅图2，在图2中，手机100为第一终端设备，蓝牙耳机200为附件设备，笔记本电脑300以及智能手表400为第三终端设备。

[0190] 在一应用场景中，假设，用户早上去上班时，携带了手机100、蓝牙耳机200以及智能手表400去上班，用户的笔记本电脑300放在家中。智能手表400以及笔记本电脑300均未接入互联网，即处于断网状态。手机100、智能手表400以及笔记本电脑300预先均通过登录同一个用户账号向服务器完成注册(注册过程具体请参阅图8及图8注册过程的相关描述)，即，手机100、智能手表400以及笔记本电脑300均已加入信任环中。手机100中预先存储了智能手表400以及笔记本电脑300的身份信息，智能手表400中预先存储了手机100以及笔记本电脑300的身份信息，笔记本电脑300中预先存储了手机100以及智能手表400的身份信息。身份信息以公钥为例进行说明。

[0191] 在下班回家途中，用户想要通过蓝牙耳机听音乐时，通过手机100的交互界面开启手机100的蓝牙功能并搜索蓝牙设备；当手机100的交互界面显示查找到的蓝牙耳机200的ID时，点击该ID以触发手机100连接该蓝牙耳机200；之后，在手机100弹出的配对界面中输入配对密钥，点击确认配对连接，以使手机100与蓝牙耳机200完成配对，建立通信连接。

[0192] 在手机100与蓝牙耳机200建立通信连接后，用户可以将手机100靠近智能手表400。此时，手机100可以采用蓝牙通信技术检测在手机100的通信范围内是否存在可连接的蓝牙设备，以检测用户随身携带的其他可连接的蓝牙设备。手机100在检测到用户随身携带有已开启蓝牙功能的智能手表400时，采用NFC技术与智能手表400进行通信，对智能手表400进行身份验证。可以理解的是，在其他实施例中，手机100可以采用NFC技术检测在手机100的通信范围内是否存在可连接的支持NFC通信的设备。

[0193] 当手机100检测到用户当前随身携带的可连接的智能手表400时，可以通过文字或语音消息提醒用户当前检测到可连接的智能手表，手机100可以采用NFC技术向智能手表400发送身份认证通知消息，以指示智能手表400在接收到身份认证通知消息时，向手机100发送认证请求信息，认证请求信息中包括智能手表400的设备ID、智能手表400的公钥属性凭据的版本号以及由智能手表400生成的第一随机数。

[0194] 手机100在接收到智能手表400发送的认证请求信息时，解析出该认证请求信息中的智能手表400的设备ID、智能手表400的公钥属性凭据的版本号以及第一随机数。

[0195] 手机100在本地公钥数据库中查找智能手表400的设备ID，并比较本地存储的公钥属性凭据的版本号与智能手表400发送的公钥属性凭据的版本号。手机基于查找结果以及比较结果，按以下方式获取智能手表400的公钥。

[0196] 其中，手机100在未查找到智能手表400的设备ID，且本地存储的版本号小于智能手表400发来的版本号时，判定智能手表400是新加入信任环的设备，向智能手表400发送公钥获取请求信息，以请求获取智能手表400的公钥以及公钥属性凭据。

[0197] 手机100当查找到智能手表400的设备ID，且本地存储的版本号大于智能手表400发来的版本号时，判定本地目录存储的数据为最新版本，使用本地中存储的智能手表400的公钥对第三终端设备进行身份验证，从本地获取智智能手表400的公钥，不再需要智智能手表400发送公钥及公钥属性凭据。

[0198] 可以理解的是，手机100在未查找到智能手表400的设备ID，且本地存储的版本号大于智能手表400发来的版本号时，判定本地目录存储的数据为最新版本，本地目录最后更新后，智能手表400的数据已不在本地目录中，智能手表400已被撤销信任资格；此时手机100判定智能手表400不可信，智能手表400身份验证失败，手机100拒绝连接智能手表400。

[0199] 手机100在获取到智能手表400的公钥时，手机100以自己的私钥与智能手表400的公钥计算共享密钥。可以理解的是，手机100可以基于手机100的私钥以及智能手表400的公钥，采用消息摘要算法计算得到共享密钥；也可以采用哈希算法计算手机100的私钥以及智能手表400的公钥的哈希值，得到共享密钥；还可以通过其他算法计算共享密钥，在此不对计算共享密钥的方式做限定。

[0200] 手机100生成第二随机数，以共享密钥计算手机100的设备ID、由智能手表400生成的第一随机数以及由手机100生成的第二随机数所对应的MAC值。

[0201] 具体地，手机100可以将手机100的设备ID、第一随机数以及第二随机数作为一条消息M，采用消息摘要算法计算出该消息M的摘要值，并在共享密钥的作用下由该摘要值计算出MAC值。或者，手机100在共享密钥的参与下采用消息认证算法计算消息M的MAC值。例如，采用共享密钥对消息M的摘要值进行加密得到MAC值，或者采用共享密钥对消息M加密得到MAC值。

[0202] 手机100采用NFC技术将自己的设备ID、自己的公钥属性凭据的版本号、第二随机数发送给智能手表400；可以理解的是，当智能手表400需要对手机100进行身份验证时，手机100还可以将计算得到的MAC值发送给智能手表400，以使智能手表400在计算出共享密钥时，采用共享密钥验证手机100发送的MAC值，从而对手机100进行身份验证。

[0203] 智能手表400在获取到手机100的设备ID以及公钥属性凭据的版本号时，进行以下处理：

[0204] a)智能手表400查找手机100的设备ID，并比较本地存储的版本号与手机100发来的版本号；基于查找结果以及比较结果，按按以下方式获取手机100的公钥：

[0205] 其中，智能手表400在未查找到手机100的设备ID，且本地存储的版本号小于手机100发来的版本号时，判定手机100是新加入信任环的设备，本地目录存储的手机100的公钥以及公钥属性凭据为旧版本，向手机100发送公钥获取请求信息，以请求获取手机100的公

钥以及公钥属性凭据。

[0206] 智能手表400当查找到手机100的设备ID，且本地存储的版本号大于对方发来的版本号时，判定本地目录存储的数据为最新版本，使用本地目录中存储的手机100的公钥对手机100进行身份验证，从本地目录获取手机100的公钥，不再需要手机100发送公钥及公钥属性凭据。

[0207] 智能手表400当未查找到手机100的设备ID，且本地存储的版本号大于手机100发来的版本号时，判定本地目录存储的数据为最新版本，本地目录最后更新后，手机100的数据已不在本地目录中，手机100已被撤销信任资格；此时智能手表400判定手机100不可信，手机100身份验证失败，智能手表400拒绝连接手机100。

[0208] b)智能手表400在获取到手机100的公钥时，智能手表400以自己的私钥与手机100的公钥计算共享密钥。可以理解的是，智能手表400可以基于智能手表400的私钥以及手机100的公钥，采用消息摘要算法计算得到共享密钥；也可以采用哈希算法计算智能手表400的私钥以及手机100的公钥的哈希值，得到共享密钥；还可以通过其他算法计算共享密钥，在此不对计算共享密钥的方式做限定。由于密钥协商算法ECDH具有交换性，因此，手机100以及智能手表400计算得到的共享密钥相同。

[0209] c)智能手表400以共享密钥计算手机100的设备ID、由智能手表400生成的第一随机数以及由手机100生成的第二随机数所对应的消息认证码MAC值，并基于手机100的设备ID，采用NFC技术将计算得到的MAC值发送给手机100。

[0210] 其中，智能手表400计算消息认证码MAC值的方法与手机100计算消息认证码MAC值的方法相同，具体请参阅上述手机100计算消息认证码MAC值的描述，此处不赘述。

[0211] 可选地，当智能手表400接收到手机100发送的MAC值时，可以采用共享密钥验证手机100发送的MAC值，从而对手机100进行身份验证。

[0212] 例如，当手机100发送的MAC值由共享密钥对手机100的设备ID、第一随机数以及第二随机数进行加密得到时，智能手表400可以采用计算得到的共享密钥对手机100发送的MAC值进行解密，如果解密得到手机100的设备ID、第一随机数以及第二随机数时，判定手机100身份合法，身份验证通过；如果解密后得到的数据与手机100的设备ID、第一随机数以及第二随机数中的任一个不相同时，判定手机100身份不合法，身份验证失败。

[0213] 再例如，当手机100发送的MAC值由共享密钥对摘要值(该摘要值由手机100的设备ID、第一随机数以及第二随机数计算得到)进行加密得到时，智能手表400可以使用计算得到的共享密钥对手机100发送的MAC值进行解密，如果解密得到的摘要值，并采用消息摘要算法计算手机100的设备ID、第一随机数以及第二随机数所对应的摘要值；如果解密得到的摘要值与计算得到的摘要值相同，判定手机100身份合法，身份验证通过；如果解密得到的摘要值与计算得到的摘要值不同时，判定手机100身份不合法，身份验证失败。

[0214] 手机100在接收到智能手表400发送的MAC值时，将接收到的MAC值与发送给智能手表400的MAC值进行比较，当两者相同时，判定智能手表400的身份合法，身份验证通过，执行S102；当两者不同时，判定智能手表400身份不合法，身份验证失败。

[0215] 可以理解的是，手机100在对智能手表400完成身份验证时，可以在显示界面显示身份验证结果，或语音播报身份验证结果。

[0216] 在另一应用场景中，当用户回到家时，用户靠近放置笔记本电脑300的位置时，手

机100采用蓝牙通信技术检测在家中是否存在可连接的蓝牙设备，或者，手机100采用NFC技术检测手机100附近是否存在可连接的NFC设备。手机100在检测到家中放置的已开启蓝牙功能的笔记本电脑300时，采用NFC技术与笔记本电脑进行通信，按照上述方法对笔记本电脑300进行身份验证。

[0217] 在另一应用场景中，在图4中，手机100为第一终端设备，无线路由器、无线接入点或个人热点500为第三终端设备，手机600为第三终端设备。

[0218] 由于手机600未曾连接朋友家的无线路由器500，手机100在接入朋友家的无线路由器500时，用户可以将手机100靠近手机600，此时，手机100通过蓝牙通信或NFC检测当前启用近程通信功能的手机300，并在检测到手机300时，采用NFC技术按照上述方法对手机600进行身份验证。

[0219] 第一终端设备在判定第三终端设备身份合法时，判定身份验证通过，执行上述S102；在判定第三终端设备身份不合法时，结束本次流程。

[0220] 进一步地，当第一终端设备生成了会话密钥时，S102具体为：将通信链路信息通过所述会话密钥进行加密，并通过所述安全传输通道将加密后的通信链路信息发送至所述第三终端设备。

[0221] 进一步地，在另一实施例中，对S102进行了细化，请参阅图10，图10是本申请一实施例提供的信息共享方法中S102的细化流程图。为了提高通过安全传输通道传输的数据的安全性，S102包括S1021～S1022，具体如下：

[0222] S1021：所述第一终端设备在确认所述第三终端设备身份合法时，生成会话密钥，并通过短距离无线通信技术将所述会话密钥发送至所述第三终端设备。

[0223] S1022：所述第一终端设备采用所述会话密钥对所述通信链路信息进行加密，并通过所述短距离无线通信技术将加密数据发送至所述第三终端设备。

[0224] 在S1021中，第一终端设备在确认第三终端设备的身份合法时，生成会话密钥，并与第三终端设备建立安全传输通道，通过安全传输通道将会话密钥发送给第三终端设备。会话密钥用于采用协商好的加密算法对通过安全传输通道传输的数据进行加密或解密。

[0225] 第一终端设备从用于存储通信链路信息的存储区域获取通信链路信息，并采用协商好的加密算法，用会话密钥对通信链路信息进行加密，将加密后的通信链路信息通过安全传输通道发送给第三终端设备。

[0226] 在一实施方式中，第一终端设备可以使用第三终端设备的公钥随机生成会话密钥。

[0227] 在另一实施方式中，第一终端设备可以基于S101中计算得到的共享密钥、固定派生因子、由第三终端设备生成的第一随机数以及由第一终端设备生成的第二随机数，生成会话密钥。固定派生因子为用于标识认证业务的固定随机数。该固定随机数的长度可以是8字节(Byte)，但并不限于此，可以根据实际需要设置为其他长度。认证业务包括但不限于文件快传、快速热点共享、共享通信链路、短信转发或通话中继。

[0228] 第一终端设备基于共享密钥、固定派生因子、第一随机数以及第二随机数，生成会话密钥的方法可以是：采用消息摘要算法计算由共享密钥、固定派生因子、第一随机数以及第二随机数构成的消息的摘要值，将该摘要值作为会话密钥；还可以是：在共享密钥的参与下，采用消息认证算法计算由共享密钥、固定派生因子、第一随机数以及第二随机数构成的

消息的MAC值，并将该MAC值作为会话密钥。可以理解的是，第一终端设备还可以采用其他算法生成会话密钥，此处不做限制。

[0229] 下面结合具体的应用场景描述信息共享过程：

[0230] 例如，在如图2所示的应用场景中，手机100在判定智能手表400可信时，生成会话密钥，建立用于与智能手表400进行数据交互的安全传输通道，并将会话密钥通过该安全传输通道发送给智能手表400。手机100从本地数据库中获取用于与蓝牙耳机200进行配对的蓝牙配对信息。蓝牙配对信息至少包括蓝牙耳机的ID、蓝牙耳机与手机的配对链路以及蓝牙配对时使用的配对密钥。之后，手机100基于协商好的加密算法，用会话密钥对待分享的蓝牙配对信息进行加密，并采用协商好的通信协议，将加密后的蓝牙配对信息通过建立的安全传输通道发送给智能手表400，以使智能手表400在接收到加密的蓝牙配对信息时，采用会话密钥对其进行解密，得到蓝牙配对信息；并基于蓝牙配对信息中包含的蓝牙耳机的ID，查找蓝牙耳机200，在查找到蓝牙耳机200时，基于蓝牙耳机与手机的配对链路以及蓝牙配对时使用的配对密钥，与蓝牙耳机200建立通信连接。

[0231] 手机100在判定笔记本电脑300可信时，建立用于与手机200进行数据交互的安全传输通道，并将会话密钥通过该安全传输通道发送给笔记本电脑300。安全传输通道用于手机100向笔记本电脑300发送加密后的蓝牙配对信息。手机100从本地数据库中获取用于与蓝牙耳机200进行配对的蓝牙配对信息；并基于协商好的加密算法，用会话密钥对待分享的蓝牙配对信息进行加密，并采用协商好的通信协议，将加密后的蓝牙配对信息通过与笔记本电脑300的安全传输通道发送给笔记本电脑300，以使笔记本电脑300在接收到加密的蓝牙配对信息时，采用会话密钥对其解密，得到蓝牙配对信息；并基于蓝牙配对信息中包含的蓝牙耳机的ID，查找蓝牙耳机200，在查找到蓝牙耳机200时，基于蓝牙耳机与手机的配对链路以及蓝牙配对时使用的配对密钥，与蓝牙耳机200建立通信连接。

[0232] 此时，用户不需要在智能手表400和笔记本电脑300查找蓝牙耳机的ID以及输入配对密码，智能手表400和笔记本电脑300就可以自动连接蓝牙耳机200。

[0233] 再例如，在如图4所示的应用场景中，手机100在判定手机600可信时，生成会话密钥，建立用于与手机600进行数据交互的安全传输通道，并将会话密钥通过该安全传输通道发送给手机600。手机100从本地数据库中获取WIFI接入信息，该WIFI接入信息用于接入路由器500(或个人热点、无线接入点)，WIFI接入信息至少包括SSID以及接入密码。手机100用会话密钥对待分享的WIFI接入信息进行加密，并采用协商好的通信协议，将加密后的WIFI接入信息通过与手机600的安全传输通道发送给手机600，以使手机600在接收到加密的WIFI接入信息时，采用会话密钥对其解密，得到WIFI接入信息，从而使得手机能够600在检测到无线路由器500时基于获取到的SSID以及接入密码，接入无线路由器500。

[0234] 可以理解的是，手机100还可以将其连接过的所有无线接入点、个人热点或路由器各自对应的SSID及接入密码发送给手机600。例如，当用户携带手机100去朋友家，在手机100的交互界面手动输入朋友家的无线路由器500的SSID和接入密码，触发手机100连接该无线接入点后，用户回家后，手机100与新手机600交换了通信链路信息，将用于接入无线路由器500的WIFI接入信息发送给了新手机600。当用户携带新手机600再次去朋友家时，由于手机600中已经同步了手机100中存储的已连接过的所有无线路由器的WIFI接入信息，新手机600在检测到朋友家的无线路由器500发出的无线信号时，基于该无线路由器500的SSID

及接入密码，与该无线路由器500建立通信连接，从而使得新手机600自动连接朋友家的无线路由器500。

[0235] 此时，手机600在用户没有输入WIFI接入密码时，也可以自动连接手机100之前已连接过的无线路由器、无线接入点或个人热点。

[0236] 在另一应用场景中，当手机100获取了NFC门禁识别信息，例如，手机100获取了门禁卡的NFC开门权限、NFC视频权限时，手机100建立用于与手机600进行数据交互的安全传输通道，用会话密钥对NFC开门权限信息或NFC视频权限信息进行加密，并采用协商好的通信协议，将加密后的NFC开门权限信息或NFC视频权限信息通过与手机600的安全传输通道发送给手机600，以使手机600在接收到加密的NFC开门权限信息或NFC视频权限信息时，采用会话密钥对其解密，得到NFC开门权限信息或NFC视频权限信息，从而使得手机600能够作为NFC门禁卡。用户在需要通过手机600开门时，可以将手机600靠近NFC门禁感应器，以使手机600基于获取到的NFC开门权限信息或NFC视频权限信息解除门禁。

[0237] 此时，用户不需要手动对手机600进行NFC门禁授权，手机600也可作为门禁卡使用。

[0238] 上述方案，对于同一用户账号下的终端设备，第一终端设备在与第二终端设备建立通信连接之后，并且近距离发现第三终端设备时，即使第三终端设备处于断网状态，第一终端设备也可以通过近场通信技术与第三终端设备建立通信连接，从而将通信链路信息同步到第三终端设备。不需要用户参与，第三终端设备即可通过第一终端设备共享的通信链路信息与第二终端设备建立通信连接。通过这种方式，能够简化至少三个终端设备建立通信连接的操作步骤，从而减少用户操作，进而提高建立至少三个终端设备之间的通信连接的效率。

[0239] 由于第一终端设备和第三终端设备通过NFC交换信息，第一终端设备和第三终端设备可以在离线状态共享文件，以使用户在没有网络的情况下，实现终端之间的数据共享。

[0240] 通过会话密钥对通信链路信息进行加密，能够提高待分享数据在传输过程中的安全性，即使其他不可信设备接收到加密后的通信链路信息，也无法直接获取到通信链路信息，进而避免其他不可信设备通过通信链路信息连接第二终端设备，进一步保护第二终端设备内的数据安全。

[0241] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

[0242] 对应于上文实施例所述的信息共享方法，图11示出了本申请实施例提供的信息共享装置的结构示意框图，为了便于说明，仅示出了与本申请实施例相关的部分。信息共享装置9包括身份验证单元910以及信息共享单元920。其中，

[0243] 身份验证单元910，用于第一终端设备与第二终端设备建立通信连接后，并且靠近第三终端设备时，通过近场通信NFC对所述第三终端设备进行身份验证；身份验证单元910将身份验证结果发送给信息共享单元920。

[0244] 身份验证单元910用于执行图6对应的实施例中S101，具体实现过程请参阅S101的具体描述，此处不赘述。

[0245] 信息共享单元920，用于接收身份验证单元910发送的身份验证结果，在确认所述

第三终端设备身份合法时，通过短距离无线通信技术将通信链路信息发送至所述第三终端设备，以触发所述第三终端设备在检测到所述第二终端设备时，使用通信链路信息与所述第二终端设备建立通信连接。

[0246] 信息共享单元920用于执行图6对应的实施例中的S102，具体实现过程请参阅S102的具体描述，此处不赘述。

[0247] 可选地，短距离无线通信技术可以为NFC、蓝牙通信或无线保真(Wireless-Fidelity,WIFI)。

[0248] 进一步地，所述第三终端设备的蜂窝移动网络和无线局域网均处于关闭状态，所述短距离无线通信技术为NFC或蓝牙通信。

[0249] 其中，第三终端设备的蜂窝移动网络和无线局域网均处于关闭状态是指：第三终端设备未启用蜂窝移动网络和无线局域网，或者当前无法通过蜂窝移动网络或无线局域网接入互联网。进一步地，所述第二终端设备为预先与所述第一终端设备完成配对的终端设备，信息共享单元920发送的所述通信链路信息包括用于与第二终端设备进行配对的蓝牙配对信息，以使第三终端设备在接收到蓝牙配对信息后，并且检测到第二终端设备时，使用接收到的蓝牙配对信息与第二终端设备进行配对。

[0250] 进一步地，信息共享单元920发送的所述通信链路信息包括无线网的接入信息和/或NFC门禁识别信息。

[0251] 其中，无线网的接入信息用于连接路由器、接入点或个人热点。接入信息可以是SSID和接入密码。此时，第三终端可以在进入任一SSID对应的无线网的信号覆盖范围时，通过无线网的接入信息，接入第一终端设备当前接入的无线网或曾接入过的无线网。

[0252] NFC门禁识别信息用于标识授权信息，例如NFC门禁授权信息，此时第三终端设备可作为NFC门禁卡与第二终端设备进行通信，从而实现开门等功能。

[0253] 可选地，请一并参阅图12，图12是本申请一实施例提供的身份验证单元的结构示意图，身份验证单元910包括：

[0254] 发送单元911，用于所述第一终端设备在靠近第三终端设备时，通过NFC向所述第三终端设备发送身份认证通知消息；发送单元911向接收单元912发送通知消息，以通知接收单元912接收第三终端设备返回的第一身份信息。

[0255] 接收单元912，用于接收发送单元911发送的通知消息，获取所述第三终端设备在接收到所述身份认证通知消息时通过NFC返回的第一身份信息；接收单元912将所述第一身份信息发送给验证单元913。

[0256] 验证单元913，用于接收接收单元912发送的第一身份信息，基于所述第一身份信息以及预存的第二身份信息，对所述第三终端设备进行身份验证。

[0257] 进一步地，所述第一身份信息包括所述第三终端设备的第一设备标识以及第一公钥；

[0258] 验证单元913具体用于：基于所述第一设备标识从身份数据库中获取所述第三终端设备对应的预存的公钥，并基于所述第一公钥和所述预存的公钥对所述第三终端设备进行身份验证；其中，当所述第一公钥和所述预存的公钥相同时，判定所述第三终端设备身份合法。

[0259] 进一步地，所述第一身份信息包括所述第三终端设备的第一设备标识、公钥属性

凭据的第一版本号以及由所述第三终端设备生成的第一随机数；

[0260] 请一并参阅图13，图13是本申请另一实施例提供的身份验证单元的结构示意图，验证单元913具体可以包括：

[0261] 公钥获取单元9131，用于接收接收单元912发送的所述第一身份信息，基于所述第一身份信息中的所述第一设备标识以及所述第一版本号，获取所述第三终端设备的第一公钥；公钥获取单元9131将所述第一公钥发送给随机数生成单元9132；

[0262] 随机数生成单元9132，用于接收公钥获取单元9131发送的所述第一公钥，基于自身的私钥和所述第一公钥计算第一共享密钥，并生成第二随机数；随机数生成单元9132将所述第一共享密钥、所述第一终端设备的第二设备标识、所述第一随机数以及所述第二随机数发送给计算单元9133；

[0263] 计算单元9133，用于接收随机数生成单元9132发送的数据，基于所述第一共享密钥、所述第一终端设备的第二设备标识、所述第一随机数以及所述第二随机数，计算第一身份特征值；计算单元9133将所述第一身份特征值发送给比较单元9134，并通知发送单元911向所述第三终端设备发送所述第一身份特征值、所述第一终端设备的第二设备标识、公钥属性凭据的第二版本号以及所述第二随机数；

[0264] 发送单元911还用于接收发送单元911发送的通知消息，通过近场通信向所述第三终端设备发送所述第一身份特征值、所述第一终端设备的第二设备标识、公钥属性凭据的第二版本号以及所述第二随机数；发送单元911通知接收单元接收所述第三终端设备发送的第二身份特征值；

[0265] 接收单元912还用于：接收发送单元911发送的通知消息，接收所述第三终端设备返回的第二身份特征值；其中，所述第二身份特征值由所述第三终端设备在计算出第二共享密钥时，基于所述第二共享密钥、所述第二设备标识、所述第一随机数以及所述第二随机数计算得到，所述第二共享密钥基于所述第三终端设备的私钥以及所述第一终端设备的公钥计算得到；接收单元912将所述第二身份特征值发送给比较单元9134；

[0266] 比较单元9134，用于接收计算单元9133发送的所述第一身份特征值以及接收接收单元912发送的所述第二身份特征值，并比较所述第一身份特征值与所述第二身份特征值，在确认所述第一身份特征值与所述第二身份特征值相同时，判定所述第三终端设备身份合法。

[0267] 进一步地，公钥获取单元9131具体用于：

[0268] 从身份数据库中查找与所述第一设备标识匹配的设备标识；

[0269] 当查找到所述匹配的设备标识，且所述第一版本号小于或等于预存的公钥属性凭据的第二版本号时，从所述身份数据库中获取所述第三终端设备的公钥；

[0270] 当未查找到所述匹配的设备标识，且所述第一版本号大于预存的公钥属性凭据的第二版本号，向所述第三终端设备请求获取所述第一公钥。

[0271] 进一步地，公钥获取单元9131还用于：当未查找到所述匹配的设备标识，且所述第一版本号小于预存的公钥属性凭据的第二版本号时，判定所述第三终端设备身份不合法。

[0272] 进一步地，所述信息共享单元920具体用于：

[0273] 在确认所述第三终端设备身份合法时，生成会话密钥，并通过短距离无线通信技术将所述会话密钥发送至所述第三终端设备；

[0274] 采用所述会话密钥对所述通信链路信息进行加密，并通过所述短距离无线通信技术将加密数据发送至所述第三终端设备。

[0275] 本方案中，通过会话密钥对通信链路信息进行加密，能够提高待分享数据在传输过程中的安全性，即使其他不可信设备接收到加密后的通信链路信息，也无法直接获取到通信链路信息，进而避免其他不可信设备通过通信链路信息连接第二终端设备，进一步保护第二终端设备内的数据安全。

[0276] 至少两个终端设备可以在离线状态共享文件，以使用户在没有网络的情况下，实现终端之间的数据共享。

[0277] 请参阅图14，图14为本申请一实施例提供的终端设备的结构示意图。如图14所示，该终端设备1414包括：至少一个处理器1410(图14中仅示出一个)处理器、存储器1420以及存储在所述存储器1420中并可在所述至少一个处理器1410上运行的计算机程序1421，所述处理器1410执行所述计算机程序1421时实现上述任意各个信息共享方法实施例中的步骤。

[0278] 终端设备14可以是手机、笔记本电脑、智能手表等可穿戴设备。该终端设备可包括，但不仅限于，处理器1410、存储器1420。本领域技术人员可以理解，图14仅仅是终端设备14的举例，并不构成对终端设备14的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如还可以包括输入输出设备、网络接入设备等。

[0279] 所称处理器1410可以是中央处理单元(Central Processing Unit，CPU)，该处理器1410还可以是其他通用处理器、数字信号处理器(Digital Signal Processor，DSP)、专用集成电路(Application Specific Integrated Circuit，ASIC)、现成可编程门阵列(Field-Programmable GateArray，FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0280] 存储器1420在一些实施例中可以是终端设备14的内部存储单元，例如终端设备14的硬盘或内存。存储器1420在另一些实施例中也可以是终端设备14的外部存储设备，例如终端设备14上的智能存储卡(Smart Media Card，SMC)，安全数字(Secure Digital，SD)卡，闪存卡(Flash Card)等。进一步地，存储器1420还可以既包括终端设备14的内部存储单元也包括外部存储设备。存储器1420用于存储操作系统、应用程序、引导装载程序(BootLoader)、数据以及其他程序等，例如所述计算机程序的程序代码等。所述存储器1420还可以用于暂时地存储已经输出或者将要输出的数据。

[0281] 在本申请实施例中，处理器1410通过调用存储器存储的计算机程序1421，执行如下操作：

[0282] 处理器1410用于：第一终端设备与第二终端设备建立通信连接后，并且在靠近第三终端设备时，通过近场通信NFC对所述第三终端设备进行身份验证；

[0283] 以及用于在确认所述第三终端设备身份合法时，通过短距离无线通信技术将通信链路信息发送至所述第三终端设备，以触发所述第三终端设备在检测到所述第二终端设备时，使用所述通信链路信息与第二终端设备建立通信连接。

[0284] 可选地，所述第三终端设备的蜂窝移动网络和无线局域网均处于关闭状态，所述短距离无线通信技术为NFC或蓝牙通信。

[0285] 可选地，所述第二终端设备为预先与所述第一终端设备完成配对的终端设备，所

述通信链路信息包括用于与所述第二终端设备进行配对的蓝牙配对信息。

[0286] 可选地，所述通信链路信息包括无线网的接入信息和/或NFC门禁识别信息。

[0287] 可选地，处理器1410具体用于：

[0288] 在靠近第三终端设备时，通过NFC向所述第三终端设备发送身份认证通知消息；

[0289] 获取所述第三终端设备在接收到所述身份认证通知消息时通过NFC返回的第一身份信息；

[0290] 基于所述第一身份信息以及预存的第二身份信息，对所述第三终端设备进行身份验证。

[0291] 进一步地，所述第一身份信息包括所述第三终端设备的第一设备标识以及第一公钥；

[0292] 处理器1410具体用于：基于所述第一设备标识从身份数据库中获取所述第三终端设备对应的预存的公钥，并基于所述第一公钥和所述预存的公钥对所述第三终端设备进行身份验证；其中，当所述第一公钥和所述预存的公钥相同时，判定所述第三终端设备身份合法。

[0293] 进一步地，所述第一身份信息包括所述第三终端设备的第一设备标识、公钥属性凭据的第一版本号以及由所述第三终端设备生成的第一随机数；

[0294] 处理器1410具体用于：

[0295] 基于所述第一设备标识以及所述第一版本号，获取所述第三终端设备的第一公钥；

[0296] 基于自身的私钥和所述第一公钥计算第一共享密钥，并生成第二随机数；

[0297] 基于所述第一共享密钥、所述第一终端设备的第二设备标识、所述第一随机数以及所述第二随机数，计算第一身份特征值；

[0298] 控制天线通过近场通信向所述第三终端设备发送所述第一身份特征值、所述第一终端设备的第二设备标识、公钥属性凭据的第二版本号以及所述第二随机数；

[0299] 获取天线接收的所述第三终端设备返回的第二身份特征值；其中，所述第二身份特征值由所述第三终端设备在计算出第二共享密钥时，基于所述第二共享密钥、所述第二设备标识、所述第一随机数以及所述第二随机数计算得到，所述第二共享密钥基于所述第三终端设备的私钥以及所述第一终端设备的公钥计算得到；

[0300] 在确认所述第一身份特征值与所述第二身份特征值相同时，判定所述第三终端设备身份合法。

[0301] 进一步地，处理器1410具体用于包括：

[0302] 从身份数据库中查找与所述第一设备标识匹配的设备标识；

[0303] 当查找到所述匹配的设备标识，且所述第一版本号小于或等于预存的公钥属性凭据的第二版本号时，从所述身份数据库中获取所述第三终端设备的公钥；

[0304] 当未查找到所述匹配的设备标识，且所述第一版本号大于预存的公钥属性凭据的第二版本号，向所述第三终端设备请求获取所述第一公钥。

[0305] 进一步地，在从身份数据库中查找与所述第一设备标识匹配的设备标识之后，处理器1410具体用于：当未查找到所述匹配的设备标识，且所述第一版本号小于预存的公钥属性凭据的第二版本号时，判定所述第三终端设备身份不合法。

[0306] 进一步地，处理器1410具体用于包括：

[0307] 在确认所述第三终端设备身份合法时，生成会话密钥，并通过短距离无线通信技术将所述会话密钥发送至所述第三终端设备；

[0308] 采用所述会话密钥对所述通信链路信息进行加密，并控制天线通过所述短距离无线通信技术将加密数据发送至所述第三终端设备。

[0309] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中，上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。另外，各功能单元、模块的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0310] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述或记载的部分，可以参见其它实施例的相关描述。

[0311] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

[0312] 在本申请所提供的实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的系统实施例仅仅是示意性的，例如，所述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通讯连接可以是通过一些接口，装置或单元的间接耦合或通讯连接，可以是电性，机械或其它的形式。

[0313] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0314] 另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0315] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请实现上述实施例方法中的全部或部分流程，可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质至少可

以包括:能够将计算机程序代码携带到终端设备14的任何实体或装置、记录介质、计算机存储器、只读存储器(Read-Only Memory,ROM)、随机存取存储器(Random Access Memory,RAM)、电载波信号、电信信号以及软件分发介质。例如U盘、移动硬盘、磁碟或者光盘等。在某些司法管辖区,根据立法和专利实践,计算机可读介质不可以是电载波信号和电信信号。

[0316] 以上所述实施例仅用以说明本申请的技术方案,而非对其限制;尽管参照前述实施例对本申请进行了详细的说明,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申请各实施例技术方案的精神和范围,均应包含在本申请的保护范围之内。

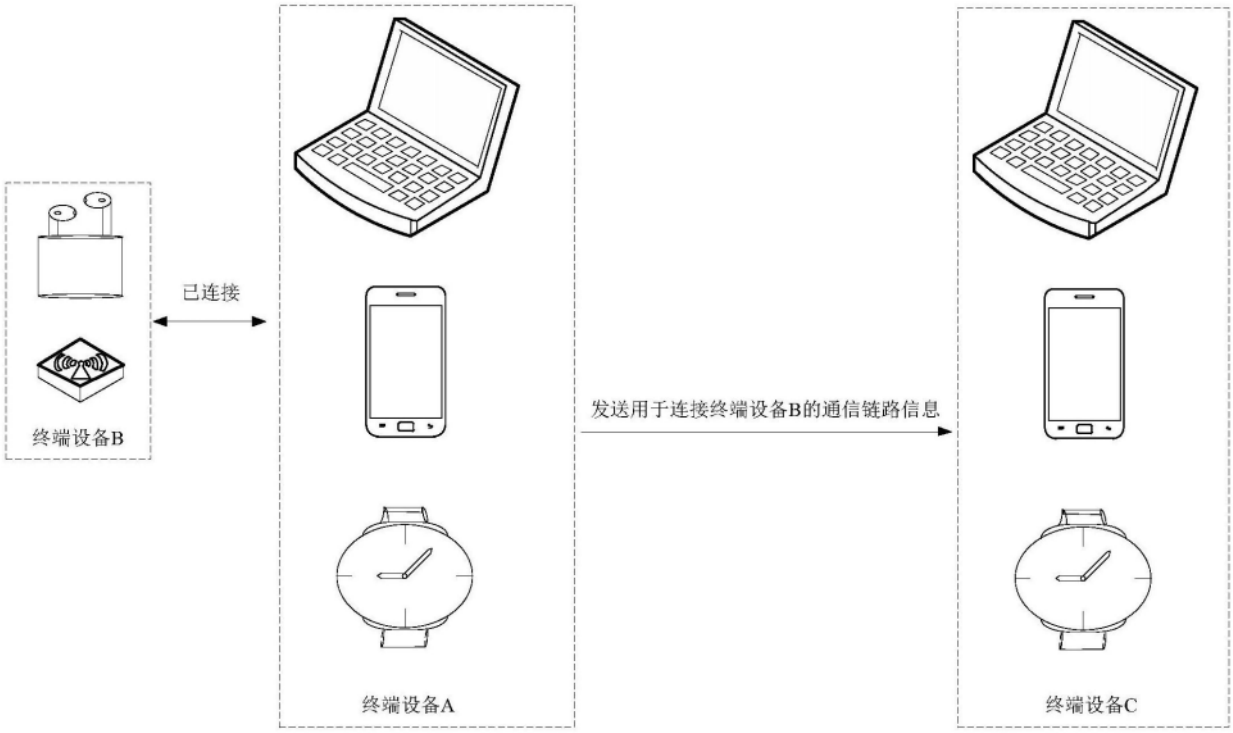

已连接
终端设备B
终端设备A
发送用于连接终端设备B的通信链路信息
终端设备C

图1

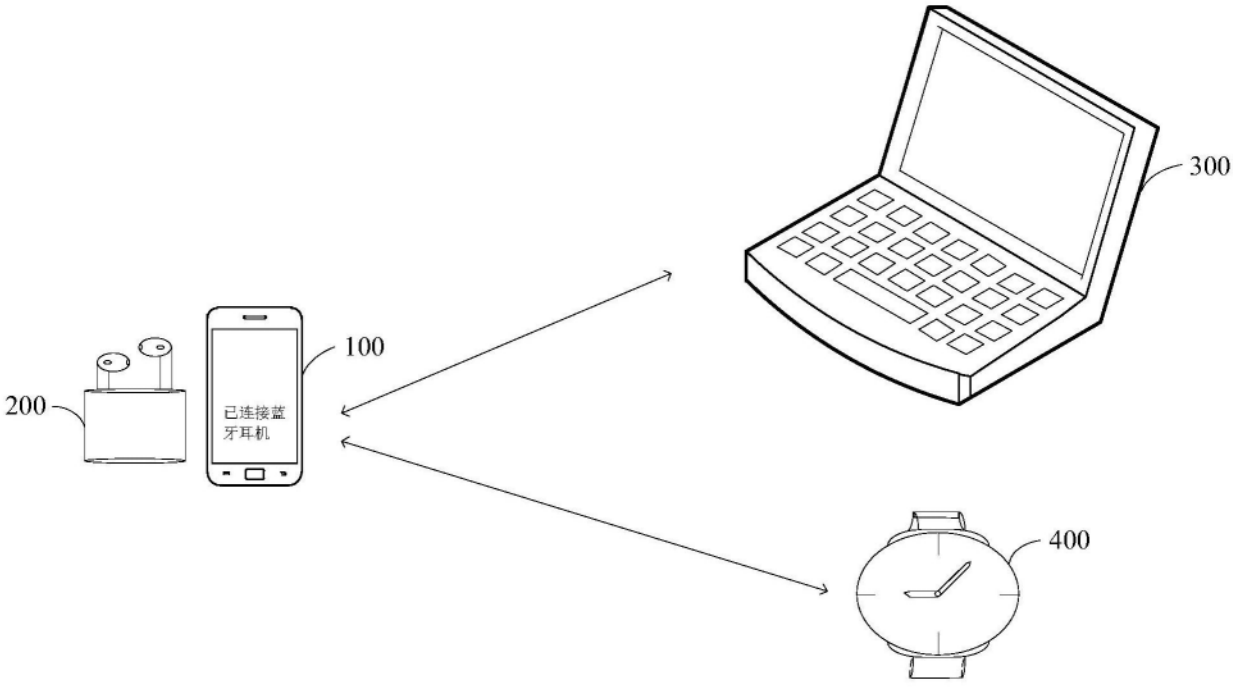

300
100
200
已连接蓝牙耳机
400

图2


蓝牙
蓝牙
开
可用设备
蓝牙耳机ID
笔记本电脑ID
智能手表ID
……

图3

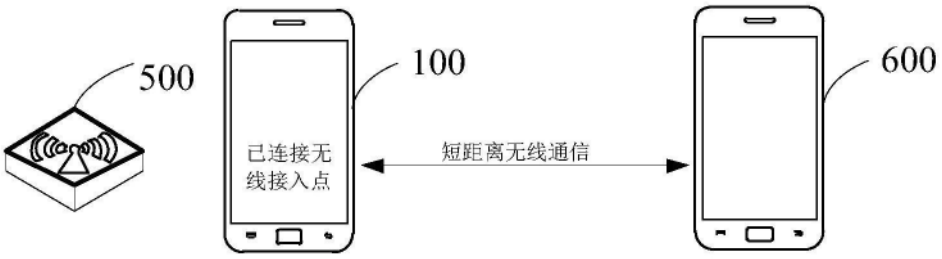

500
100
600
已连接无线接入点
短距离无线通信

图4

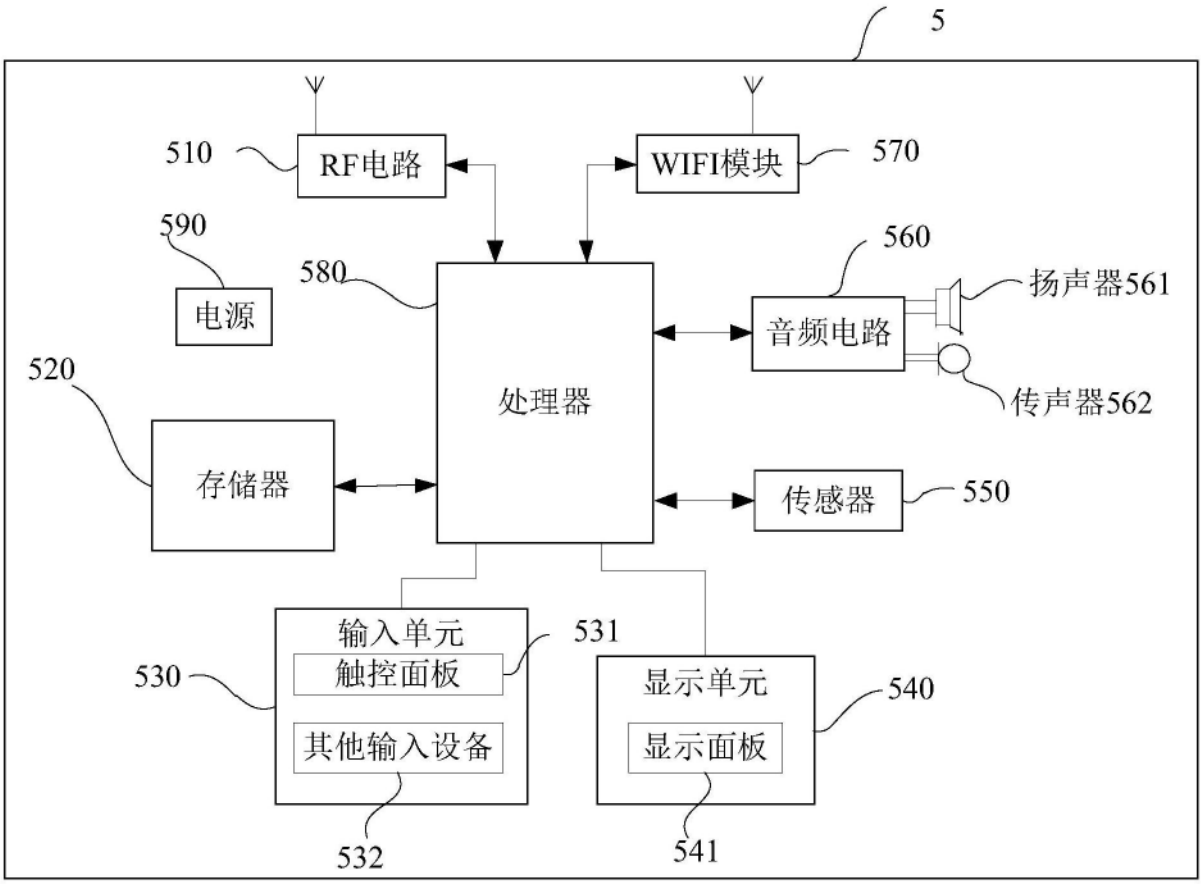

5
510
RF电路
WIFI模块
570
590
电源
580
560
扬声器561
音频电路
520
处理器
传声器562
存储器
传感器
550
输入单元
531
530
触控面板
显示单元
540
其他输入设备
显示面板
532
541

图5

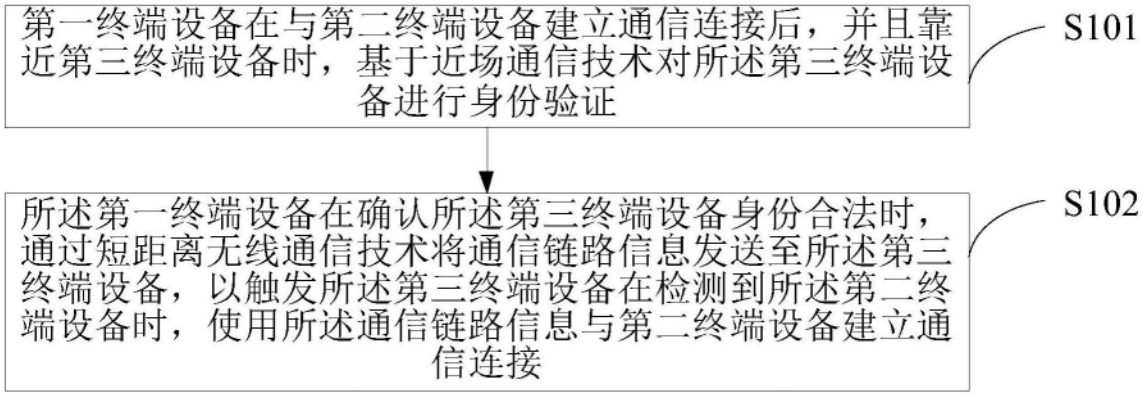

第一终端设备在与第二终端设备建立通信连接后，并且靠近第三终端设备时，基于近场通信技术对所述第三终端设备进行身份验证
S101
所述第一终端设备在确认所述第三终端设备身份合法时，通过短距离无线通信技术将通信链路信息发送至所述第三终端设备，以触发所述第三终端设备在检测到所述第二终端设备时，使用所述通信链路信息与第二终端设备建立通信连接
S102

图6

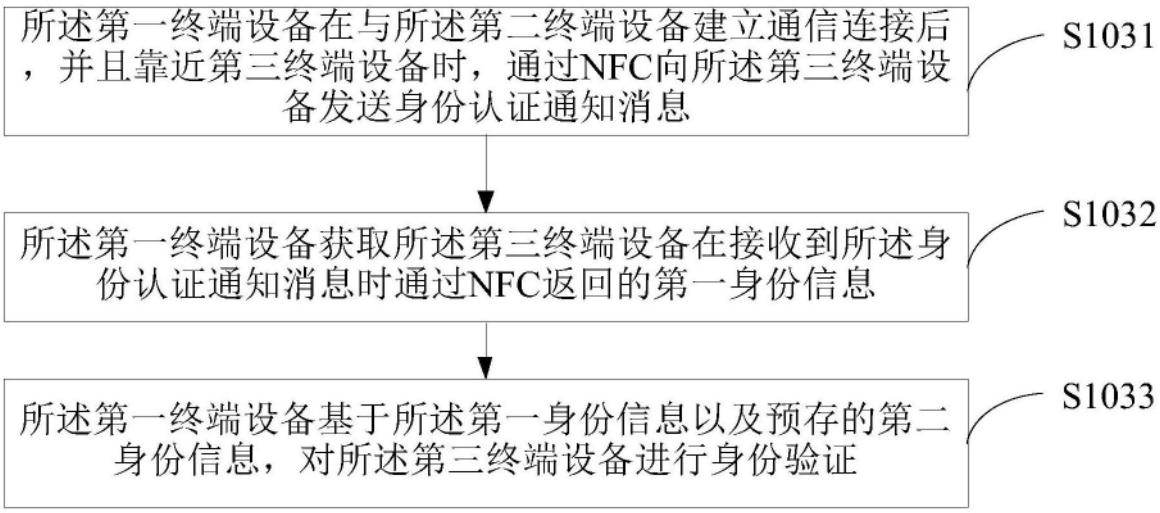

所述第一终端设备在与所述第二终端设备建立通信连接后，并且靠近第三终端设备时，通过NFC向所述第三终端设备发送身份认证通知消息
S1031
所述第一终端设备获取所述第三终端设备在接收到所述身份认证通知消息时通过NFC返回的第一身份信息
S1032
所述第一终端设备基于所述第一身份信息以及预存的第二身份信息，对所述第三终端设备进行身份验证
S1033

图7

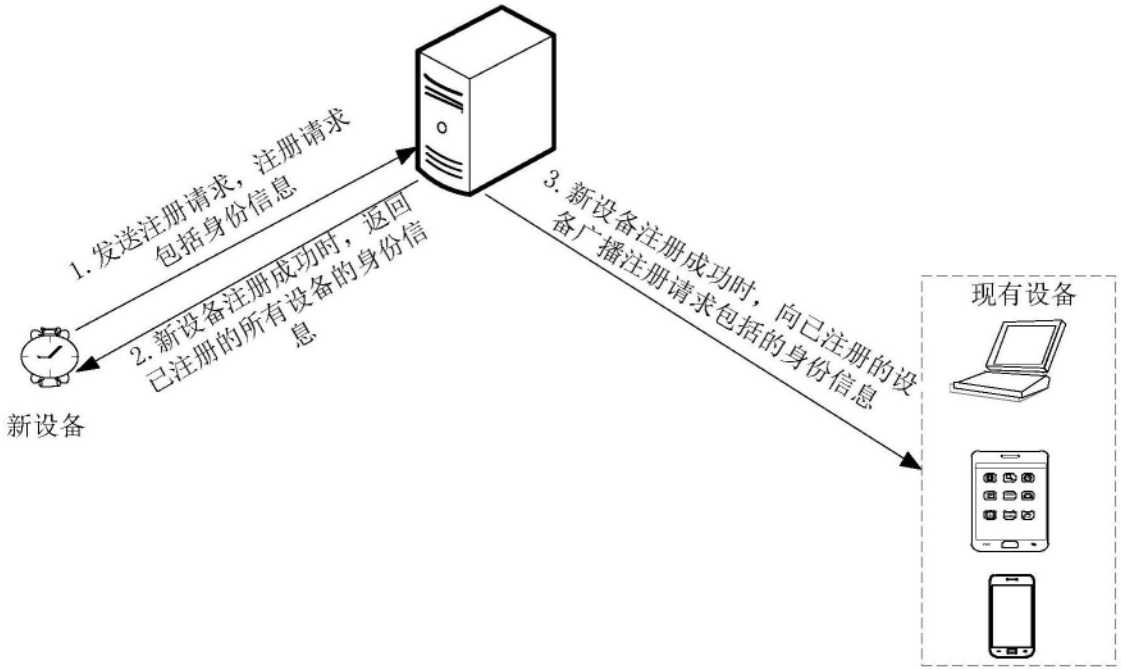

1.发送注册请求，注册请求包括身份信息
2.新设备注册成功时，返回已注册的所有设备的身份信息
3.新设备注册成功时，向已注册的设备广播注册请求包括的身份信息
新设备
现有设备

图8

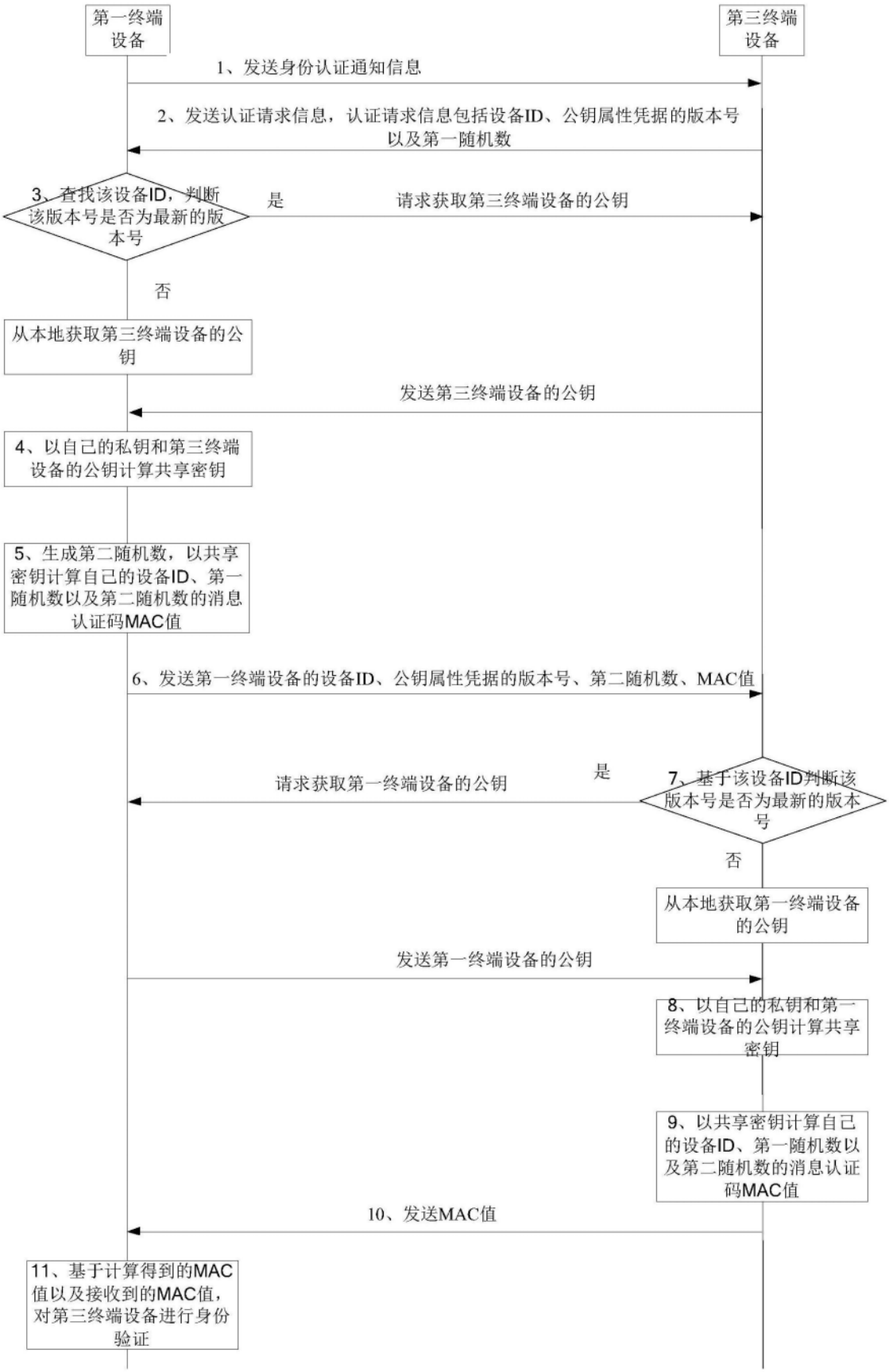

第一终端设备
第三终端设备
1、发送身份认证通知信息
2、发送认证请求信息，认证请求信息包括设备ID、公钥属性凭据的版本号以及第一随机数
3、查找该设备ID，判断该版本号是否为最新的版本号
是
请求获取第三终端设备的公钥
否
从本地获取第三终端设备的公钥
发送第三终端设备的公钥
4、以自己的私钥和第三终端设备的公钥计算共享密钥
5、生成第二随机数，以共享密钥计算自己的设备ID、第一随机数以及第二随机数的消息认证码MAC值
6、发送第一终端设备的设备ID、公钥属性凭据的版本号、第二随机数、MAC值
是
请求获取第一终端设备的公钥
7、基于该设备ID判断该版本号是否为最新的版本号
否
从本地获取第一终端设备的公钥
发送第一终端设备的公钥
8、以自己的私钥和第一终端设备的公钥计算共享密钥
9、以共享密钥计算自己的设备ID、第一随机数以及第二随机数的消息认证码MAC值
10、发送MAC值
11、基于计算得到的MAC值以及接收到的MAC值，对第三终端设备进行身份验证

图9

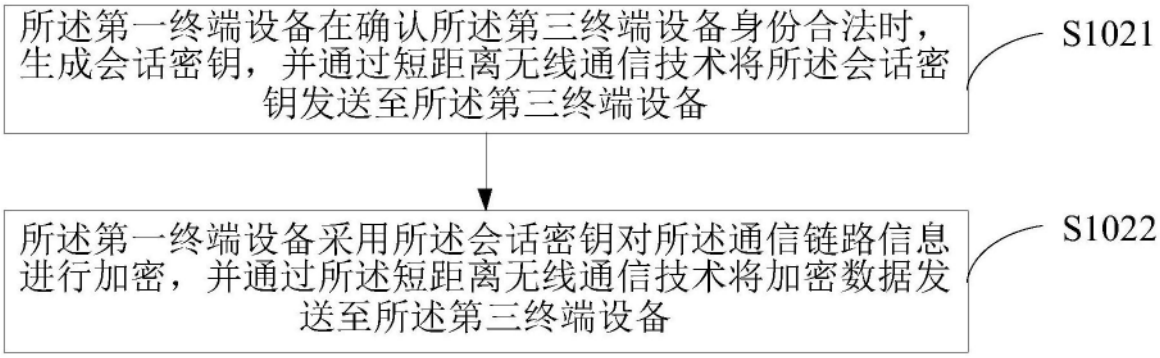

所述第一终端设备在确认所述第三终端设备身份合法时，生成会话密钥，并通过短距离无线通信技术将所述会话密钥发送至所述第三终端设备
S1021
所述第一终端设备采用所述会话密钥对所述通信链路信息进行加密，并通过所述短距离无线通信技术将加密数据发送至所述第三终端设备
S1022

图10

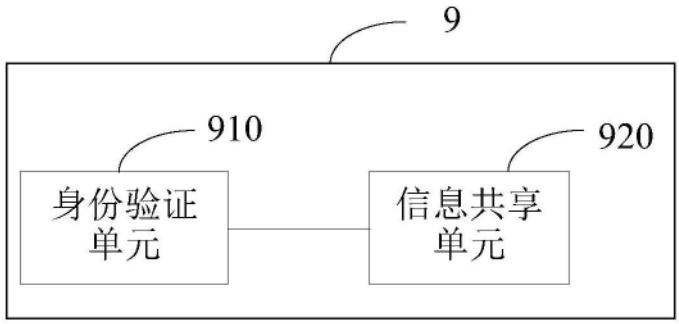

9
910
身份验证单元
920
信息共享单元

图11

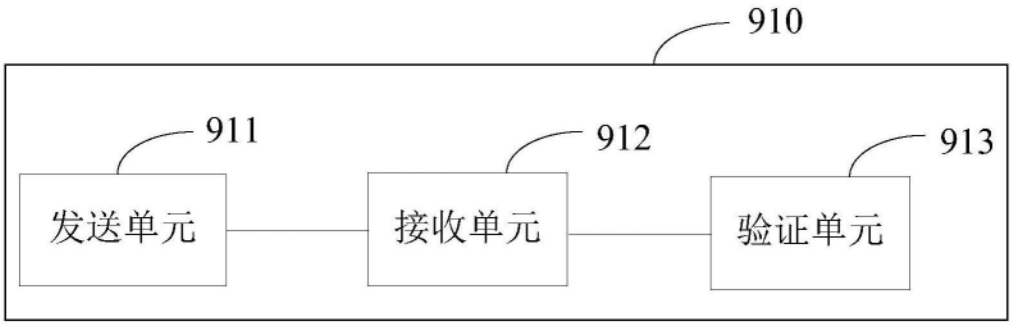

910
911
发送单元
912
接收单元
913
验证单元

图12

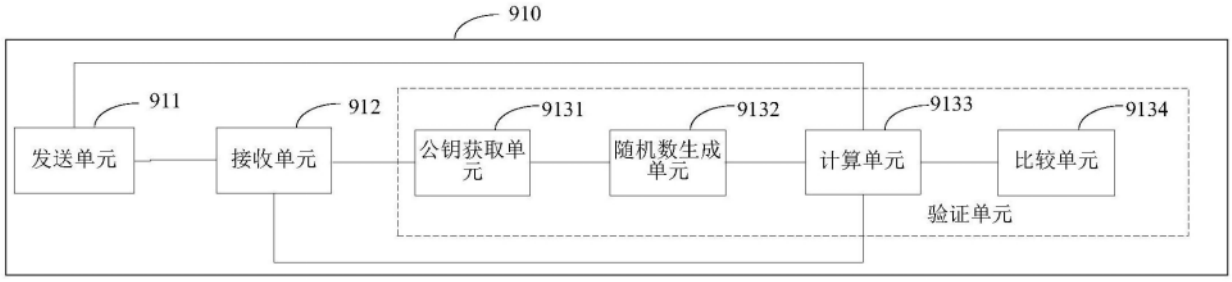

910
911
发送单元
912
接收单元
9131
公钥获取单元
9132
随机数生成单元
9133
计算单元
9134
比较单元
验证单元

图13

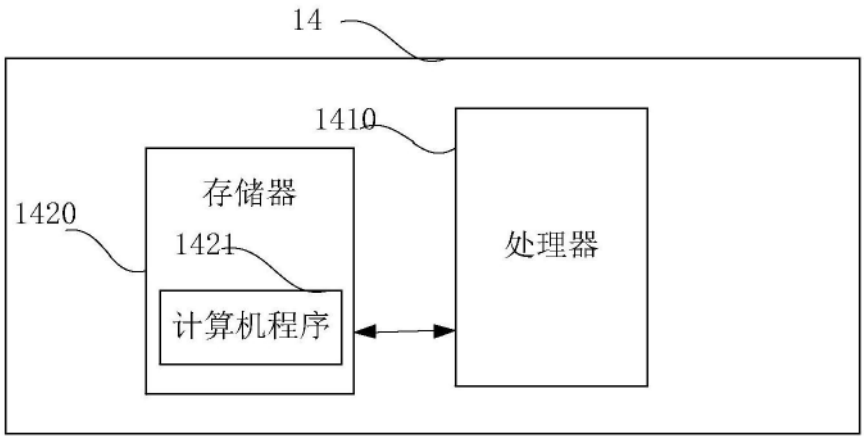

14
1410
处理器
存储器
1420
1421
计算机程序

图14