(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 113840266 A
(43)申请公布日 2021.12.24

(21)申请号 202010588451.7

(22)申请日 2020.06.24

(71)申请人 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 陈健

(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 孙静 臧建明

(51)Int.Cl.
H04W 4/80(2018.01)
H04W 12/06(2021.01)
H04W 76/14(2018.01)
H04W 76/40(2018.01)

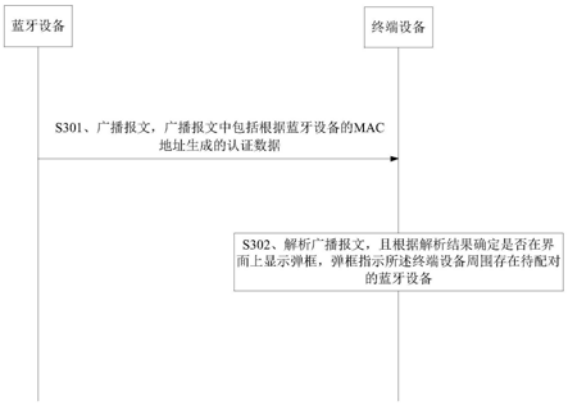
权利要求书2页 说明书21页 附图10页

(54)发明名称

蓝牙配对方法、装置、系统、电子设备和存储介质

(57)摘要

本申请实施例提供了一种蓝牙配对方法、装置、系统、电子设备和存储介质，该方法包括：终端设备接收来自蓝牙设备的广播报文，广播报文中包括认证数据，认证数据是蓝牙设备根据报文参数生成的，报文参数包括蓝牙设备的媒体访问控制MAC地址；终端设备采用预设的算法，解析广播报文；若终端设备解析广播报文得到蓝牙设备的MAC地址，则在终端设备的界面上显示弹框。本申请实施例中广播报文中不直接包含蓝牙设备的MAC地址，而包含有根据蓝牙设备的MAC地址获取的数据，鉴于广播报文中不直接包含蓝牙设备的MAC地址，使得蓝牙设备的MAC地址不能被轻易地获取、模仿，提高了配对安全性。



CN 113840266 A

1.一种蓝牙配对方法,其特征在于,包括:

终端设备接收来自蓝牙设备的广播报文,所述广播报文中包括认证数据,所述认证数据是所述蓝牙设备根据报文参数生成的,所述报文参数包括所述蓝牙设备的媒体访问控制MAC地址;

所述终端设备采用预设的算法,解析所述广播报文;

若所述终端设备解析所述广播报文得到所述蓝牙设备的MAC地址,则在所述终端设备的界面上显示弹框。

2.根据权利要求1所述的方法,其特征在于,所述认证数据是所述蓝牙设备采用加密算法对所述报文参数加密生成的,所述预设的算法为所述加密算法,所述终端设备解析所述广播报文得到所述蓝牙设备的MAC地址,包括:

所述终端设备解密所述认证数据,得到所述蓝牙设备的MAC地址。

3.根据权利要求2所述的方法,其特征在于,所述报文参数还包括所述蓝牙设备中存储的预共享的信息,所述终端设备解析所述广播报文得到所述蓝牙设备的MAC地址,包括:

所述终端设备解密所述认证数据,若所述认证数据中的预共享的信息与所述终端设备中存储的预共享的信息相同,则将解密得到的所述认证数据中的MAC地址作为所述蓝牙设备的MAC地址。

4.根据权利要求1所述的方法,其特征在于,所述认证数据是所述蓝牙设备采用单向散列算法对所述报文参数计算得到的,所述预设的算法为所述单向散列算法,所述终端设备采用预设的算法,解析所述广播报文,包括:

所述终端设备扫描周围存在的至少一个蓝牙设备,得到所述至少一个蓝牙设备的MAC地址;

所述终端设备采用所述单向散列算法,根据所述周围存在的每个蓝牙设备的MAC地址,得到至少一个新的认证数据;

相应的,所述终端设备解析所述广播报文得到所述蓝牙设备的MAC地址,包括:

将新的认证数据与所述认证数据相同的周围存在的蓝牙设备的MAC地址,作为所述蓝牙设备的MAC地址。

5.根据权利要求4所述的方法,其特征在于,所述报文参数还包括所述蓝牙设备中存储的预共享的信息,所述得到新的认证数据,包括:

所述终端设备采用所述单向散列算法,根据所述周围存在的每个蓝牙设备的MAC地址和所述终端设备中存储的预共享的信息,得到所述至少一个新的认证数据。

6.根据权利要求1-5中任一项所述的方法,其特征在于,所述广播报文中还包括随机广播地址;所述报文参数中还包括:所述随机广播地址和/或预留信息。

7.根据权利要求1-6中任一项所述的方法,其特征在于,所述弹框指示所述终端设备周围存在待配对的所述蓝牙设备,所述方法还包括:

接收用户对所述弹框的操作指令,所述操作指令指示与所述蓝牙设备配对连接。

8.根据权利要求1-7中任一项所述的方法,其特征在于,所述方法还包括:

在所述终端设备和所述蓝牙设备配对连接后,接收用户对所述终端设备的界面上显示的生成新的预共享的信息的控件的第一选择指令;

根据所述第一选择指令,生成新的预共享的信息。

9.根据权利要求8所述的方法,其特征在于,所述方法还包括:

存储所述蓝牙设备的MAC地址和所述新的预共享的信息的对应关系。

10.根据权利要求8或9所述的方法,其特征在于,所述方法还包括:

接收所述用户对所述终端设备的界面上显示的同步控件的第二选择指令;

根据所述第二选择指令,存储所述终端设备上登录的用户账号下的对应关系,所述用户账号下的对应关系为:登录过所述用户账号的终端设备中存储的蓝牙设备的MAC地址和新的预共享的信息的对应关系。

11.根据权利要求9或10所述的方法,其特征在于,所述报文参数还包括所述蓝牙设备中存储的预共享的信息,所述终端设备解析所述广播报文得到所述蓝牙设备的MAC地址,包括:

所述终端设备解密所述认证数据,若所述认证数据中的预共享的信息与所述终端设备中存储的预共享的信息相同,且所述述认证数据中的MAC地址为所述终端设备中存储的对应关系中的MAC地址,则将解密得到的所述认证数据中的MAC地址作为所述蓝牙设备的MAC地址。

12.一种蓝牙配对装置,其特征在于,包括:

收发模块,用于接收来自蓝牙设备的广播报文,所述广播报文中包括认证数据,所述认证数据是所述蓝牙设备根据报文参数生成的,所述报文参数包括所述蓝牙设备的媒体访问控制MAC地址;

处理模块,用于采用预设的算法,解析所述广播报文;

显示模块,用于若解析所述广播报文得到所述蓝牙设备的MAC地址,则在界面上显示弹框。

13.一种电子设备,其特征在于,包括:存储器、处理器和收发器;

所述处理器与所述存储器耦合,读取并执行所述存储器中的指令,以实现权利要求1-11中任一项所述的方法步骤;

所述收发器与所述处理器耦合,由所述处理器控制所述收发器进行消息收发。

14.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质中存储有计算机程序或指令,当所述计算机程序或指令被运行时,实现如权利要求1-11中任一项所述的方法。

蓝牙配对方法、装置、系统、电子设备和存储介质

技术领域

[0001] 本申请实施例涉及通信技术，尤其涉及一种蓝牙配对方法、装置、系统、电子设备和存储介质。

背景技术

[0002] 蓝牙是一种支持设备之间短距离通信的无线电技术，广泛应用于通信领域。为了避免耳机与终端设备连接时因为连接线造成的不便，蓝牙耳机应运而生。蓝牙耳机与终端设备配对连接后，二者之间可以进行数据传输。

[0003] 现有技术中，蓝牙耳机可以通过公用的信道发送广播报文，该广播报文中包括蓝牙耳机的媒体访问控制(media access control，MAC)地址。处于蓝牙耳机预设距离范围内的终端设备可以通过蓝牙低功耗(bluetooth low energy，BLE)扫描接收到广播报文后，可以解析该广播报文得到蓝牙耳机的MAC地址，终端设备可以在界面上以弹框的形式提醒用户周围有待配对的蓝牙设备。用户可以操作弹框以触发终端设备根据该MAC地址与蓝牙耳机进行配对连接。

[0004] 该种方式中，鉴于蓝牙耳机的MAC地址在广播报文中发送，易被获取及仿冒，导致终端设备连接不可信的蓝牙耳机，以及造成设备唯一标识符泄露(unique identifier，UID)，可能存在安全及隐私问题。

发明内容

[0005] 本申请技术方案提供一种蓝牙配对方法、装置、系统、电子设备和存储介质，能够提高终端设备和蓝牙设备的配对安全性。

[0006] 第一方面，本申请技术方案提供一种蓝牙配对方法，该方法可以应用于终端设备，也可以应用于终端设备中的芯片。下面以应用于终端设备为例对该方法进行描述，该方法中，终端设备可以接收来自蓝牙设备的广播报文，终端设备可以采用预设的算法，解析所述广播报文。其中，若所述终端设备解析所述广播报文得到所述蓝牙设备的MAC地址，则可以在所述终端设备的界面上显示弹框。

[0007] 其中，所述弹框可以指示所述终端设备周围存在待配对的所述蓝牙设备。若用户对所述弹框进行操作，则相应的终端设备可以接收操作指令，进而与蓝牙设备进行配对连接。

[0008] 应注意的是，本申请技术方案中的广播报文中可以包括认证数据。其中，所述认证数据可以是所述蓝牙设备根据报文参数生成的。本申请技术方案中的所述报文参数包括所述蓝牙设备的媒体访问控制MAC地址。也就是说，本申请技术方案中蓝牙设备发送的广播报文中不携带蓝牙设备的MAC地址，而是根据蓝牙设备的MAC地址生成认证数据携带在广播报文中。鉴于广播报文中不直接包含蓝牙设备的MAC地址，而包含有根据蓝牙设备的MAC地址获取的数据，使得蓝牙设备的MAC地址不能被轻易地获取、模仿，提高了配对安全性。

[0009] 本申请技术方案中可以采用加密算法，或者单向散列算法，根据蓝牙设备的MAC地

址,生成认证数据,终端设备也需要采用对应的加密算法,或者单向散列算法解析认证数据,以的带蓝牙设备的MAC地址。

[0010] 在一种实现方式中,所述认证数据是所述蓝牙设备采用加密算法对所述报文参数加密生成的,所述预设的算法为所述加密算法。终端设备可以采用加密算法解密所述认证数据,得到所述蓝牙设备的MAC地址。

[0011] 在一种实现方式中,所述认证数据是所述蓝牙设备采用单向散列算法对所述报文参数计算得到的,所述预设的算法为所述单向散列算法。由于单向散列算法为不可逆的算法,终端设备可以采用如下的方式解析认证数据:所述终端设备可以扫描周围存在的至少一个蓝牙设备,进而获取所述至少一个蓝牙设备的MAC地址。终端设备根据采用所述单向散列算法,且根据所述周围存在的每个蓝牙设备的MAC地址,得到每个蓝牙设备对应的新的认证数据。蓝牙设备可以将该新的认证数据和广播报文中的认证数据进行比较,并将新的认证数据与所述认证数据相同的周围存在的蓝牙设备的MAC地址,作为所述蓝牙设备的MAC地址。

[0012] 应理解,本申请技术方案中的单向散列算法可以包括但不限于为消息认证码(message authentication code,MAC)算法、基于口令的密钥派生算法-2(password-based key derivation function 2,PBKDF2)、哈希Hash算法等,哈希算法中可以采用SHA或MD5等算法。

[0013] 在一种实现方式中,终端设备的周围可能存在多个蓝牙设备,终端设备若一一根据每个蓝牙设备的MAC地址,采用单向散列算法计算得到新的认证数据,计算量较大。为了减少终端设备的计算量,本申请技术方案的所述广播报文中还包括:所述蓝牙设备的处理后的MAC地址。终端设备可以在扫描获取周围存在的蓝牙设备的MAC地址后,根据蓝牙设备的处理后的MAC地址,在扫描获取周围存在的蓝牙设备的MAC地址中获取待选择蓝牙设备的MAC地址,并根据该待选择蓝牙设备的MAC地址,采用单向散列算法计算得到新的认证数据。其中,该待选择蓝牙设备的MAC地址为可能是待配对的蓝牙设备。

[0014] 其中,在一种可能的实现方式中,所述处理后的MAC地址为截断处理后的MAC地址。终端设备可以在所述终端设备周围存在的蓝牙设备的MAC地址中,将包含有所述截断处理后的MAC地址的MAC地址作为上述待选择蓝牙设备的MAC地址。进而终端设备采用待选择蓝牙设备的MAC地址,并根据该待选择蓝牙设备的MAC地址,采用单向散列算法计算得到新的认证数据,并不是对终端设备周围存在的所有的蓝牙设备的MAC地址采用单向散列算法计算,能够减少终端设备的计算量。

[0015] 在上述技术方案的基础上,为了进一步提高配对的安全性,本申请技术方案中的报文参数中还可以包括预共享的信息。其中,预共享的信息为待配对的蓝牙设备和终端设备知道的信息。其他不能配对的蓝牙设备或终端设备中的预共享的信息可以不同。

[0016] 在报文参数中包含有预共享的信息时,在上述第一种方式中,终端设备可以解密所述认证数据,若所述认证数据中的预共享的信息与所述终端设备中存储的预共享的信息相同,则将解密得到的所述认证数据中的MAC地址作为所述蓝牙设备的MAC地址。

[0017] 在一种实现方式中,终端设备可以采用所述单向散列算法,根据所述周围存在的每个蓝牙设备的MAC地址和所述终端设备中存储的预共享的信息,得到所述至少一个新的认证数据,且将新的认证数据与所述认证数据相同的周围存在的蓝牙设备的MAC地址,作为

所述蓝牙设备的MAC地址。或者，本申请技术方案中可以根据所述待选择蓝牙设备的MAC地址和所述终端设备中存储的预共享的信息，得到所述至少一个新的认证数据，进而将新的认证数据与所述认证数据相同的周围存在的蓝牙设备的MAC地址，作为所述蓝牙设备的MAC地址。

[0018] 在该种场景下，至于终端设备采用哪种算法解析广播报文，终端设备可以采用预设的算法解析广播报文。或者，广播报文中可以携带算法的标识，终端设备根据该算法的标识，采用对应的算法解析广播报文。

[0019] 在上述技术方案的基础上，为了进一步提高配对的安全性，本申请技术方案中的广播报文中可以包括随机广播地址，且在所述报文参数中还包括：随机广播地址和/或预留信息。与现有技术中不同的是，现有技术中可以在广播报文中携带真实的广播地址，该真实的广播地址可能会泄露蓝牙设备的MAC地址，而本申请技术方案中在广播报文中携带随机生成的随机广播地址，避免了因为广播地址泄露蓝牙设备的MAC地址的可能性。

[0020] 相对应的，在报文参数中包含有随机广播地址时，在一种实现方式中，终端设备可以解密所述认证数据，若所述认证数据中的预共享的信息与所述终端设备中存储的预共享的信息相同，且解密得到的随机广播地址与广播报文中的随机广播地址相同，则将解密得到的所述认证数据中的MAC地址作为所述蓝牙设备的MAC地址。

[0021] 在一种实现方式中，终端设备可以采用所述单向散列算法，根据所述待选择蓝牙设备的MAC地址、所述终端设备中存储的预共享的信息，以及广播报文中的随机广播地址，得到所述至少一个新的认证数据，进而将新的认证数据与所述认证数据相同的周围存在的蓝牙设备的MAC地址，作为所述蓝牙设备的MAC地址。

[0022] 应理解，当报文参数中还包括预留信息时，在一种实现方式中，终端设备可以解密所述认证数据，若所述认证数据中的预共享的信息与所述终端设备中存储的预共享的信息相同，且解密得到的随机广播地址与广播报文中的随机广播地址相同，以及解密得到的预留信息与终端设备中的存储的预留信息相同，则将解密得到的所述认证数据中的MAC地址作为所述蓝牙设备的MAC地址。

[0023] 在一种实现方式中，终端设备可以采用所述单向散列算法，根据所述待选择蓝牙设备的MAC地址、所述终端设备中存储的预共享的信息、广播报文中的随机广播地址，以及终端设备中存储的预留信息，得到所述至少一个新的认证数据，进而将新的认证数据与所述认证数据相同的周围存在的蓝牙设备的MAC地址，作为所述蓝牙设备的MAC地址。

[0024] 因为相同型号或者相同品牌的蓝牙设备和终端设备中的预共享的信息可能相同，因此用户的终端设备的界面上可能会弹框显示其他用户的相同型号或者相同品牌的蓝牙设备。为了保证终端设备和蓝牙设备的配对私有化，本申请技术方案中在终端设备和蓝牙设备配对连接后，可以更新预共享的信息，使得该新的预共享的信息为终端设备和蓝牙设备私有的。

[0025] 其中，预共享的信息可以为终端设备与蓝牙设备配对连接后自动生成的，终端设备可以将该新的预共享的信息发送给蓝牙设备，终端设备和蓝牙设备均存储该新的预共享的信息，以使得终端设备和蓝牙设备中的预共享的信息同步。或者，在终端设备与蓝牙设备配对连接后，终端设备的蓝牙设置界面中会显示生成新的预共享的信息的控件，用户选择该控件，可以触发终端设备生成新的预共享的信息。相对应的，在所述终端设备和所述蓝牙

设备配对连接后，若终端设备接收用户对所述终端设备的界面上显示的生成新的预共享的信息的控件的第一选择指令，则根据所述第一选择指令，生成新的预共享的信息。

[0026] 应理解，终端设备可能与多个蓝牙设备进行配对连接，终端设备可以存储所述蓝牙设备的MAC地址和所述新的预共享的信息的对应关系，该对应关系可以称为信任设备列表，且该信任设备列表可以同步存储在登录该终端设备的用户账号下，存储在云端。也就是说，每个终端设备中可以存储有信任设备列表。

[0027] 在该种场景下，在一种实现方式中，终端设备可以解密所述认证数据，若所述认证数据中的预共享的信息与所述终端设备中存储的预共享的信息相同，且解密得到的随机广播地址与广播报文中的随机广播地址相同，以及解密得到的预留信息与终端设备中的存储的预留信息相同，并且解密得到的所述认证数据中的MAC地址为信任设备列表中存储的MAC地址，则可以将认证数据中的MAC地址作为所述蓝牙设备的MAC地址。

[0028] 在一种实现方式中，在所述终端设备周围存在的蓝牙设备的MAC地址中，若包含有所述截断处理后的MAC地址的MAC地址为所述终端设备中存储的对应关系中的MAC地址，则将该包含有所述截断处理后的MAC地址的MAC地址作为所述待选择蓝牙设备的MAC地址，且执行上述的方式，得到新的认证数据。若在所述终端设备周围存在的蓝牙设备的MAC地址中，包含有所述截断处理后的MAC地址的MAC地址不为所述终端设备中存储的对应关系中的MAC地址，则所述终端设备采用单向散列算法，计算所述包含有所述截断处理后的MAC地址的MAC地址和所述终端设备中存储的预共享的信息，得到所述新的认证数据。

[0029] 也就是说，当周围存在的蓝牙设备为已经配对连接过的蓝牙设备时，可以直接根据新的预共享的信息计算得到新的认证数据，当周围存在的蓝牙设备为未配对连接过的蓝牙设备时，可以直接根据终端设备中存储的未更新前的预共享的信息计算得到新的认证数据。

[0030] 在一种可能的实现方式中，当周围存在的蓝牙设备为未配对连接过的蓝牙设备时，终端设备的界面上可以弹窗显示“尝试用未更新的预共享的信息配对”，相应的，终端设备的蓝牙设置界面上可以显示有与新的蓝牙设备配对的控件，用户选择该控件后，可以触发终端设备直接根据终端设备中存储的未更新前的预共享的信息计算得到新的认证数据。也就是说，终端设备接收所述用户对所述终端设备的界面上显示的与新的蓝牙设备配对的控件的第三选择指令，可以根据该第三选择指令，根据终端设备中存储的未更新前的预共享的信息计算得到新的认证数据。

[0031] 第二方面，本申请技术方案提供一种蓝牙配对方法，该方法可以应用于蓝牙设备，也可以应用于蓝牙设备中的芯片。下面以应用于蓝牙设备为例对该方法进行描述，该方法中，蓝牙设备可以根据报文参数生成认证数据。其中，所述报文参数中包括所述蓝牙设备的媒体访问控制MAC地址。蓝牙设备在生成认证数据后，可以在广播报文中携带该认证数据，进而在配对时，向终端设备发送广播报文。

[0032] 在一种可能的实现方式中，所述蓝牙设备可以采用预设的算法，根据所述报文参数生成所述认证数据。其中，该预设的算法为加密算法或单向散列算法，所述报文参数中还可以包括：所述蓝牙设备中存储的预共享的信息。

[0033] 其中，若所述预设的算法为单向散列算法，则所述广播报文中还包括所述蓝牙设备的处理后的MAC地址。可选的，该处理后的MAC地址可以为截断处理后的MAC地址。

[0034] 在一种可能的实现方式中，所述报文参数中还包括：所述蓝牙设备中存储的预共享的信息，以及随机广播地址和/或预留信息生成所述认证数据；当所述报文参数中包括所述随机广播地址时，所述广播报文中包括所述随机广播地址。

[0035] 在一种可能的实现方式中，蓝牙设备可以接收来自所述终端设备的新的预共享的信息，且存储所述新的预共享的信息，以与终端设备中存储的新的预共享的信息保持同步。

[0036] 上述第二方面所提供的方法，其有益效果可以参见上述第一方面所带来的有益效果，在此不加赘述。

[0037] 第三方面，本申请技术方案提供一种蓝牙配对装置，包括：收发模块，用于接收来自蓝牙设备的广播报文，所述广播报文中包括认证数据，所述认证数据是所述蓝牙设备根据报文参数生成的，所述报文参数包括所述蓝牙设备的媒体访问控制MAC地址。处理模块，用于采用预设的算法，解析所述广播报文。显示模块，用于若解析所述广播报文得到所述蓝牙设备的MAC地址，则在界面上显示弹框。

[0038] 其中，所述弹框可以指示周围存在待配对的所述蓝牙设备。

[0039] 在一种可能的实现方式中，所述认证数据是所述蓝牙设备采用加密算法对所述报文参数加密生成的。所述处理模块，具体用于解密所述认证数据，得到所述蓝牙设备的MAC地址。

[0040] 在一种可能的实现方式中，所述报文参数还包括所述蓝牙设备中存储的预共享的信息。所述处理模块，具体用于解密所述认证数据，若所述认证数据中的预共享的信息与所述终端设备中存储的预共享的信息相同，则将解密得到的所述认证数据中的MAC地址作为所述蓝牙设备的MAC地址。

[0041] 在一种可能的实现方式中，所述认证数据是所述蓝牙设备采用单向散列算法对所述报文参数计算得到的。所述处理模块，具体用于扫描周围存在的至少一个蓝牙设备，获取所述至少一个蓝牙设备的MAC地址，采用所述单向散列算法，根据所述周围存在的每个蓝牙设备的MAC地址，得到至少一个新的认证数据，且将新的认证数据与所述认证数据相同的周围存在的蓝牙设备的MAC地址，作为所述蓝牙设备的MAC地址。

[0042] 在一种可能的实现方式中，所述报文参数还包括所述蓝牙设备中存储的预共享的信息。所述处理模块，具体用于采用所述单向散列算法，根据所述周围存在的每个蓝牙设备的MAC地址和所述终端设备中存储的预共享的信息，得到所述至少一个新的认证数据。

[0043] 在一种可能的实现方式中，所述广播报文中还包括随机广播地址；所述报文参数中还包括：随机广播地址和/或预留信息。

[0044] 在一种可能的实现方式中，所述收发模块，还用于接收用户对所述弹框的操作指令，所述操作指令指示与所述蓝牙设备配对连接。

[0045] 在一种可能的实现方式中，所述收发模块，还用于在终端设备和所述蓝牙设备配对连接后，接收用户对所述终端设备的界面上显示的生成新的预共享的信息的控件的第一选择指令。

[0046] 所述处理模块，还用于根据所述第一选择指令，生成新的预共享的信息。

[0047] 在一种可能的实现方式中，存储模块，用于存储所述蓝牙设备的MAC地址和所述新的预共享的信息的对应关系。

[0048] 在一种可能的实现方式中，所述收发模块，还用于接收所述用户对所述终端设备

的界面上显示的同步控件的第二选择指令。

[0049] 所述处理模块，还用于根据所述第二选择指令，存储所述终端设备上登录的用户账号下的对应关系，所述用户账号下的对应关系为：登录过所述用户账号的终端设备中存储的蓝牙设备的MAC地址和新的预共享的信息的对应关系。

[0050] 在一种可能的实现方式中，所述报文参数还包括所述蓝牙设备中存储的预共享的信息。所述处理模块，还用于解密所述认证数据，若所述认证数据中的预共享的信息与所述终端设备中存储的预共享的信息相同，且所述述认证数据中的MAC地址为所述终端设备中存储的对应关系中的MAC地址，则将解密得到的所述认证数据中的MAC地址作为所述蓝牙设备的MAC地址。

[0051] 上述第三方面所提供的装置，其有益效果可以参见上述第一方面所带来的有益效果，在此不加赘述。

[0052] 第四方面，本申请技术方案提供一种蓝牙配对装置，包括：处理模块，用于根据报文参数生成认证数据，其中，所述报文参数中包括所述蓝牙设备的媒体访问控制MAC地址。收发模块，用于向终端设备发送广播报文，所述广播报文中包括所述认证数据。

[0053] 在一种可能的实现方式中，处理模块，具体用于可以采用预设的算法，根据所述报文参数生成所述认证数据。其中，该预设的算法为加密算法或单向散列算法，所述报文参数中还可以包括：所述蓝牙设备中存储的预共享的信息。

[0054] 其中，若所述预设的算法为单向散列算法，则所述广播报文中还包括所述蓝牙设备的处理后的MAC地址。可选的，该处理后的MAC地址可以为截断处理后的MAC地址。

[0055] 在一种可能的实现方式中，所述报文参数中还包括：所述蓝牙设备中存储的预共享的信息，以及随机广播地址和/或预留信息生成所述认证数据；当所述报文参数中包括所述随机广播地址时，所述广播报文中包括所述随机广播地址。

[0056] 在一种可能的实现方式中，收发模块，还用于接收来自所述终端设备的新的预共享的信息。存储模块，用于存储所述新的预共享的信息，以与终端设备中存储的新的预共享的信息保持同步。

[0057] 第五方面，本申请技术方案提供一种蓝牙配对系统，包括第三方面所述的蓝牙配对装置，以及上述第四方面所述的蓝牙配对装置。也就是说，该蓝牙配对系统中包括上述的终端设备和蓝牙设备。

[0058] 第六方面，本申请技术方案提供一种电子设备，该电子设备可以为上述技术方案中的终端设备和蓝牙设备。所述种电子设备包括：处理器、存储器、收发器；所述收发器耦合至所述处理器，所述处理器控制所述收发器的收发动作；其中，存储器用于存储计算机可执行程序代码，程序代码包括指令；当处理器执行指令时，指令使所述电子设备执行如第一方面和第二方面所提供的方法。

[0059] 第七方面，本申请技术方案提供一种芯片，所述芯片上存储有计算机程序，在所述计算机程序被所述芯片执行时，实现如第一方面和第二方面所提供的方法。

[0060] 第八方面，本申请技术方案提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述第一方面和第二方面所提供的方法。

[0061] 第九方面，本申请技术方案提供一种计算机可读存储介质，所述计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机执行上述第一方面和第二方面所

提供的方法。

[0062] 本申请技术方案提供一种蓝牙配对方法、装置、系统、电子设备和存储介质，蓝牙设备在向终端设备发送的广播报文中可以不直接包含蓝牙设备的MAC地址，而包含有采用约定的算法根据蓝牙设备的MAC地址获取的数据，鉴于广播报文中不直接包含蓝牙设备的MAC地址，使得蓝牙设备的MAC地址不能被轻易地获取、模仿。另外，与该蓝牙设备进行配对的终端设备可以采用约定的算法解析得到蓝牙设备的MAC地址，进而在界面上实现弹框以配对。而不能解析得到蓝牙设备的MAC地址的终端设备不能弹框，其他不能解析成功的终端设备不能与蓝牙设备连接，提高了配对安全性。

附图说明

[0063] 图1为终端设备的界面示意图；

[0064] 图2为本申请实施例提供的蓝牙配对方法的场景示意图；

[0065] 图3为本申请实施例提供的蓝牙配对方法的一实施例的流程示意图；

[0066] 图4为本申请实施例提供的蓝牙配对方法的另一实施例的流程示意图；

[0067] 图5为本申请实施例提供的蓝牙配对方法的另一实施例的流程示意图；

[0068] 图6为本申请实施例中提供的广播报文的结构示意图；

[0069] 图7为本申请实施例提供的蓝牙配对方法的另一实施例的流程示意图；

[0070] 图8为本申请实施例提供的蓝牙配对方法的另一实施例的流程示意图；

[0071] 图9为本申请实施例提供的终端设备的界面变化示意图一；

[0072] 图10为本申请实施例提供的终端设备的界面变化示意图二；

[0073] 图11为本申请实施例提供的蓝牙配对方法的另一实施例的流程示意图；

[0074] 图12为本申请实施例提供的终端设备的界面示意图；

[0075] 图13为本申请实施例提供的蓝牙配对装置的结构示意图；

[0076] 图14为本申请实施例提供的电子设备的结构示意图。

具体实施方式

[0077] 蓝牙设备多种多样，如蓝牙耳机、蓝牙手表、蓝牙手环等。终端设备与蓝牙设备进行配对时，用户可以在终端设备上操作，打开终端设备的蓝牙功能，以实现终端设备对周围的蓝牙设备的扫描。终端设备可以将扫描发现的蓝牙设备显示在界面上，用户在界面上点击需求连接的蓝牙设备的标识，进而实现终端设备与蓝牙设备的配对。在终端设备与蓝牙设备的配对完成后，二者可以建立蓝牙连接。

[0078] 终端设备与蓝牙设备的配对过程，可以为两个设备之间相互认证的过程。终端设备与蓝牙设备配对后，终端设备与蓝牙设备之后的连接可以不必每次都要进行配对。其中，终端设备与蓝牙设备的配对可以采用个人识别密码(personal identification number，PIN)认证的方式进行相互认证。在终端设备与蓝牙设备的配对后，终端设备可以根据蓝牙设备的媒体访问控制(media access control，MAC)地址建立连接。应理解，此处对终端设备与蓝牙设备之间进行配对和连接的过程为简述，具体可以参考蓝牙配对和连接的标准协议中的相关说明。

[0079] 上述由用户在终端设备上操作完成的蓝牙配对方式较为复杂，为了解决该问题，

还提供了一种蓝牙设备发送广播报文，终端设备在发现蓝牙设备时进行配对连接。其中，蓝牙设备可以通过公用的信道发送广播报文，广播报文中可以包括广播地址、蓝牙设备的型号、MAC地址等信息，或者将蓝牙设备的MAC地址作为广播地址进行广播。

[0080] 处于蓝牙设备预设距离范围内的终端设备可以通过蓝牙低功耗(bluetooth low energy，BLE)扫描接收到广播报文后，可以解析广播报文得到蓝牙耳机的MAC地址。终端设备可以在界面上以弹框的形式提醒用户周围有待配对的蓝牙设备，用户在界面上操作弹框，能够触发终端设备根据该MAC地址与蓝牙耳机进行配对。应理解，终端设备上的蓝牙功能处于开启状态。

[0081] 示例性的，图1为终端设备的界面示意图。如图1所示，终端设备在解析广播报文得到蓝牙耳机的MAC地址后，可以在界面上显示弹框，如该弹框中显示有蓝牙设备的型号，以及“配对”控件和“取消”控件。用户点击“配对”控件可以触发终端设备和蓝牙设备进行配对连接。

[0082] 然而，蓝牙设备发送广播报文的信道为公开的数据传输信道，除了蓝牙设备需求连接的终端设备外，其他处于蓝牙设备预设距离范围内、具有BLE扫描功能的设备，都可以扫描并接收到该广播报文，因此蓝牙设备的广播报文易泄露。蓝牙设备的MAC地址是蓝牙设备的硬件地址，例如设备标识符，可以唯一标识蓝牙设备。同样，设备标识符也可用于标识用户身份。上述的广播报文可能会导致蓝牙设备的MAC地址可以轻易地被外界获取，安全性低。

[0083] 另，由于蓝牙设备的MAC地址等设备信息在广播报文中明文发送，易被获取的同时，也易被分析，进而模仿数据格式，伪造广播报文，也可以达到使得终端设备扫描并弹框的目的。因此，终端设备容易连接至非可信的蓝牙设备甚至恶意蓝牙设备，安全性低。示例性的，如图1中所示的弹框中显示的蓝牙设备，可能为恶意模仿数据格式的蓝牙设备。

[0084] 为了解决上述问题，本申请实施例提供了一种蓝牙配对方法，在蓝牙设备发送的广播报文中可以不直接包含蓝牙设备的MAC地址，而包含有采用约定的算法根据蓝牙设备的MAC地址获取的数据，与该蓝牙设备进行配对的终端设备可以采用约定的算法解析得到蓝牙设备的MAC地址，进而在界面上实现弹框以配对，而对于不能解析得到蓝牙设备的MAC地址的终端设备不能弹框。鉴于广播报文中可以不直接包含蓝牙设备的MAC地址，使得蓝牙设备的MAC地址不能被轻易地获取、模仿。其他不能解析成功的终端设备也不能与蓝牙设备连接，提高了配对安全性。

[0085] 图2为本申请实施例提供的蓝牙配对方法的场景示意图。如图2所示，本申请实施例提供的蓝牙配对方法，可以应用在蓝牙设备和终端设备之间。蓝牙设备如可以为蓝牙耳机、蓝牙手环、蓝牙手表、蓝牙音箱、智慧家庭(smart home)中的蓝牙终端等。上述的终端设备可以为终端Terminal、用户设备(user equipment，UE)、移动台(mobile station，MS)、移动终端(mobile terminal，MT)等。终端设备可以是手机(mobile phone)、平板电脑(pad)、带蓝牙功能的电脑、虚拟现实(virtual reality，VR)终端设备、增强现实(augmented reality，AR)终端设备、工业控制(industrial control)中的无线终端、无人驾驶(self driving)中的无线终端、远程手术(remote medical surgery)中的无线终端、智能电网(smart grid)中的无线终端、运输安全(transportation safety)中的无线终端、智慧城市(smart city)中的无线终端、智慧家庭(smart home)中的无线终端等。应理解，图2中以蓝

牙设备为蓝牙耳机,终端设备为智能手机为例进行示例。

[0086] 下面结合具体的实施例对本申请实施例提供的蓝牙配对方法进行说明。下面这几个实施例可以相互结合,对于相同或相似的概念或过程可能在某些实施例不再赘述。

[0087] 图3为本申请实施例提供的蓝牙配对方法的一实施例的流程示意图。如图3所示,本申请实施例提供的蓝牙配对方法可以包括:

[0088] S301,蓝牙设备发送广播报文,广播报文中包括根据蓝牙设备的MAC地址生成的认证数据。

[0089] S302,终端设备解析广播报文,根据解析结果确定是否在界面上显示弹框,弹框可以指示终端设备周围存在待配对的蓝牙设备。

[0090] 上述S301中,本申请实施例中,广播报文中并未包括蓝牙设备的MAC地址,而是包括了根据蓝牙设备的MAC地址生成的认证数据。应理解,本申请实施例中的认证数据可以为蓝牙设备根据报文参数生成的,而在本申请实施例中,报文参数中包括蓝牙设备的MAC地址。

[0091] 其中,用户可以触发蓝牙设备发送广播报文。示例性的,若蓝牙设备为与终端设备未配对过的设备,则用户可以通过按压蓝牙设备上的控件(例如蓝牙设备上的按键),或者用户滑动、点击蓝牙设备界面上的控件等方式触发蓝牙设备发送广播报文。或者,蓝牙设备在与终端设备之间的连接断开之后,在下次连接需要配对时(如长时间未进行连接需要配对验证),蓝牙设备发送广播报文。本申请实施例中并不对触发蓝牙设备发送广播报文的场景以及条件进行限制,上述两种场景仅为示例。

[0092] 本申请实施例中蓝牙设备在发送广播报文时,可以根据蓝牙设备的MAC地址生成认证数据。其中,本申请实施例中生成认证数据的一种可能的实现方式为:蓝牙设备按照预设的算法对蓝牙设备的MAC地址进行计算,得到认证数据。该预设的算法可以为单向散列算法,无法通过逆向破解的算法,如消息认证码(message authentication code,MAC)算法、基于口令的密钥派生算法-2(password-based key derivation function 2,PBKDF2)、哈希Hash算法等,哈希算法中可以采用SHA或MD5等算法。

[0093] 示例性的,若采用PBKDF2算法对蓝牙设备的MAC地址进行计算时,具体可见下式:

[0094] AuthData＝PBKDF2(BTAddrData)

[0095] 其中,AuthData为认证数据,BTAddrData为蓝牙设备的MAC地址。

[0096] 本申请实施例中生成认证数据的另一种可能的实现方式为:预设的算法为加密算法,蓝牙设备采用加密算法对蓝牙设备的MAC地址进行加密,生成认证数据。加密算法可以为对称加密算法或非对称加密算法等。

[0097] 上述S302中,终端设备在接收到来自蓝牙设备的广播报文后,可以解析广播报文。其中,为了保证认证数据的安全性,广播报文不为其他终端设备所解析,在出厂前蓝牙设备和终端设备中可以预先约定算法。终端设备可以采用预设的算法解析广播报文,根据解析结果确定是否在界面上显示弹框。应理解,本申请实施例中的弹框可以与上述图1相同,例如可以显示蓝牙设备的信息,以及“配对”控件和“取消”控件,蓝牙设备的信息如蓝牙设备的型号、厂商标志logo等。

[0098] 其中,若预设的算法为上述的单向散列算法,则终端设备在接收到广播报文后,可以扫描周围的蓝牙设备,以获取周围存在的蓝牙设备的MAC地址,进而根据周围存在的蓝牙

设备的MAC地址，采用预设的单向散列算法，计算得到新的认证数据。终端设备通过对比新的认证数据和广播报文中的认证数据是否一致，进而确定是否在界面上显示弹框。

[0099] 若终端设备的周围存在一个蓝牙设备时，采用该蓝牙设备MAC地址计算得到新的认证数据，若该新的认证数据与广播报文中的认证数据一致，则确定该蓝牙设备即为待配对的蓝牙设备，进而在界面上显示弹框，弹框中显示该蓝牙设备的信息。反之，终端设备在界面上不显示弹框。

[0100] 若终端设备的周围存在多个蓝牙设备时，终端设备采用预设的单向散列算法依次对每个蓝牙设备的MAC地址计算，以得到多个新的认证数据。若该多个新的认证数据中存在与广播报文中的认证数据一致的数据时，将一致的新的认证数据对应的蓝牙设备确定为待配对的蓝牙设备，并在界面上显示弹框，该弹框中可以显示该蓝牙设备的信息。

[0101] 其中，若预设的算法为上述的加密算法，因为加密算法为可逆向解密的，因此本申请实施例中终端设备可以采用与该预设的加密算法对应的解密算法，对该认证数据进行解密。若终端设备采用预设的解密算法能够解析认证数据，得到蓝牙设备的MAC地址，则确定该蓝牙设备为待配对的蓝牙设备，可以在界面上显示弹框，该弹框中可以显示该蓝牙设备的信息。反之，若终端设备采用预设的解密算法不能够解析认证数据，则不显示弹框。

[0102] 应理解，终端设备在界面上显示弹框后，用户可以点击“配对”或“连接”，以触发终端设备和蓝牙设备的配对连接流程，该配对连接流程具体可以参照上述的相关描述。

[0103] 本申请实施例中提供的蓝牙配对方法包括：蓝牙设备发送广播报文，广播报文中包括根据蓝牙设备的MAC地址生成的认证数据，终端设备解析广播报文，根据解析结果确定是否在界面上显示弹框。弹框可以指示终端设备周围存在待配对的蓝牙设备。本申请实施例中广播报文中不直接包含蓝牙设备的MAC地址，而包含有采用约定的算法根据蓝牙设备的MAC地址获取的数据，鉴于广播报文中不直接包含蓝牙设备的MAC地址，使得蓝牙设备的MAC地址不能被轻易地获取、模仿。另外，与该蓝牙设备进行配对的终端设备可以采用约定的算法解析得到蓝牙设备的MAC地址，进而在界面上实现弹框以配对。而不能解析得到蓝牙设备的MAC地址的终端设备不能弹框，其他不能解析成功的终端设备不能与蓝牙设备连接，提高了配对安全性。

[0104] 上述实施例中，蓝牙设备可以采用预设的算法，根据MAC地址生成认证数据。若一恶意终端采用目前已有的单向散列算法依次计算新的认证数据，或者采用目前已有的解密算法解密认证数据，也能够得到蓝牙设备的MAC地址，进而进行恶意模仿。为了进一步提高配对安全性，本申请实施例中可以根据蓝牙设备和终端设备知道的其他数据(报文参数可以包括蓝牙设备和MAC地址和蓝牙设备和终端设备约定的其他数据)，计算获取认证数据，进而使得不知道该其他数据的终端设备，不能解析广播报文，这样可以提高蓝牙配对的安全性。下述结合图4对本申请实施例提供的蓝牙配对方法进行说明。图4为本申请实施例提供的蓝牙配对方法的另一实施例的流程示意图。如图4所示，该蓝牙配对方法可以包括：

[0105] S401，蓝牙设备根据预共享的信息和蓝牙设备的MAC地址，采用预设的算法，生成认证数据。

[0106] S402，蓝牙设备发送广播报文，广播报文中包括认证数据。

[0107] S403，终端设备解析广播报文，且根据解析结果确定是否在界面上显示弹框。

[0108] 上述S401中，与上述S301中生成认证数据的方式类似的，本申请实施例中可以采

用预设的算法获取认证数据，预设的算法如单向散列算法或加密算法。与上述S301不同的是，获取认证数据的报文参数不同。上述S301中获取认证数据的报文参数可以为蓝牙设备的MAC地址，而本申请实施例中获取认证数据的报文参数为预共享的信息和蓝牙设备的MAC地址。

[0109] 应理解，预共享的信息可以为蓝牙设备和终端设备在设备生产阶段预先写入的，适配的蓝牙设备和终端设备的预共享的信息相同。其中，适配的蓝牙设备和终端设备指的是可以配对的蓝牙设备和终端设备，如相同品牌的蓝牙耳机和终端设备。示例性的，如一品牌的A型号的蓝牙耳机、B型号的蓝牙耳机均可以与C型号的终端设备进行蓝牙配对，则A型号的蓝牙耳机、B型号的蓝牙耳机和C型号的终端设备中的预共享的信息可以相同。

[0110] 本申请实施例中，针对不同的单向散列算法，蓝牙设备采用的预共享的信息不同。如，当单向散列算法为MAC算法或PBKDF2算法时，预共享的信息可以为：预共享的口令(PreSharePwd)。当单向散列算法为Hash算法时，预共享的信息可以为预共享的盐值(PreShareSalt)。应理解，当预设的算法为加密算法时，预共享的信息可以为预共享的密钥(PreShareKey)。

[0111] 示例性的，若蓝牙设备采用MAC算法对预共享的信息和蓝牙设备的MAC地址生成认证数据时，具体可见下式：

[0112] AuthData＝MAC(BTAddrData,PreSharePwd)

[0113] 其中，PreSharePwd为预共享的口令。蓝牙设备的MAC地址和预共享的信息分别为生成认证数据的报文参数。应理解，在采用不同的算法获取认证数据时，上述的PreShareInfo可以替换为PreSharePwd、PreShareSalt或PreShareKey。

[0114] 上述S402中的实施方式可以参照上述实施例中S301中的相关描述，在此不做赘述。

[0115] 上述S403中，终端设备在接收到广播报文后，可以解析广播报文。本申请实施例中蓝牙设备和终端设备中可以预设算法，具体可以参照上述S302的相关描述。

[0116] 应注意，当预设的算法为加密算法时，终端设备可以采用预设的解密算法解析认证数据，以得到蓝牙设备的MAC地址和广播报文中的预共享的信息。其中，若广播报文中的预共享的信息和终端设备中存储的预共享的信息相同时，终端设备确定该蓝牙设备为待配对的蓝牙设备，进而可以在界面上显示弹框。若终端设备采用预设的解密算法解析得到的广播报文中的预共享的信息和终端设备中存储的预共享的信息不同，则终端设备在界面上不显示弹框。

[0117] 应理解，本申请实施例中采用预共享的信息进行加密算法处理的方式，避免了恶意的蓝牙设备模仿蓝牙设备的MAC地址，使得终端设备弹框的问题。其中，恶意的蓝牙设备并不知道蓝牙设备和终端设备的预共享的信息，进而终端设备在接收到恶意的蓝牙设备的广播报文后，解密该广播报文得到的预共享的信息与终端设备中存储的预共享的信息不同，因此不会显示弹框，提高了配对安全性。

[0118] 当预设的算法为单向散列算法时，终端设备可以扫描获取周围存在的蓝牙设备的MAC地址，具体见上述S302中的相关描述。终端设备可以根据蓝牙设备的MAC地址和终端设备中存储的预共享的信息，采用预设的单向散列算法计算新的认证数据。当新的认证数据与广播报文中的任何认证数据一致时，终端设备确定发送该广播报文的蓝牙设备为待配对

的蓝牙设备，进而在界面上可以显示弹框。应理解，当终端设备周围存在一个或多个蓝牙设备时，终端设备确定是否弹框的方式可以参照上述S302中的相关描述。

[0119] 其中，蓝牙设备采用单向散列算法获取认证数据，终端设备周围存在多个蓝牙设备时，为了减少终端设备在获取新的认证数据时，需要根据周围的每个蓝牙设备的MAC地址和终端设备中存储的预共享的信息计算得到新的认证数据的问题。本申请实施例中的广播报文中还可以包括蓝牙设备的处理后的MAC地址，即并非直接包括蓝牙设备的MAC地址。其中，对蓝牙设备的MAC地址的处理方式可以为截断处理、位移处理或置换处理等。

[0120] 应理解，对蓝牙设备的MAC地址的处理方式为蓝牙设备和终端设备预先约定的。下面针对广播报文中还可以包括蓝牙设备的处理后的MAC地址，以及在上述可能的三种处理方式下终端设备解析广播报文的方式进行说明：

[0121] 第一种方式：广播报文中包括截断处理后的蓝牙设备的MAC地址。

[0122] 截断处理指的是将蓝牙设备的MAC地址截掉一部分，保留剩余部分的MAC地址。示例性的，蓝牙设备的MAC地址为11:22:33:44:55:66，截断处理后的MAC地址可以为保留后2个字节，如55:66，或者截断处理后的MAC地址可以为保留后1个字节66等。

[0123] 相应的，终端设备在接收到广播报文后，可以在广播报文中获取截断后的蓝牙设备的MAC地址。终端设备在扫描获取周围存在的蓝牙设备的MAC地址，可以与广播报文中截断后的蓝牙设备的MAC地址相比较，将周围存在的蓝牙设备的MAC地址中包含有截断后的蓝牙设备的MAC地址的蓝牙设备作为待选择蓝牙设备。终端设备根据待选择蓝牙设备的MAC地址和终端设备中存储的预共享的信息，采用预设的算法获取新的认证数据。

[0124] 鉴于广播报文中包括截断处理后的蓝牙设备的MAC地址，本申请实施例中终端设备不需要根据周围存在的每个蓝牙设备的MAC地址，计算以获取新的认证数据，而是根据周围包含有截断处理后的MAC地址的蓝牙设备的MAC地址获取新的认证数据，能够减少终端设备的计算量，进而提高配对效率。

[0125] 第二种方式：广播报文中包括位移处理后的蓝牙设备的MAC地址。

[0126] 位移处理指的是将蓝牙设备的MAC地址中的每个字节按照预设位移方式进行移动。示例性的，蓝牙设备的MAC地址为11:22:33:44:55:66，位移处理为将每个字节向后移动两位，进而得到位移处理后的蓝牙设备的MAC地址为55:66:11:22:33:44。或者位移处理为将每个字节向后移动四位，或者位移处理为将每个字节向前移动一位等。

[0127] 相应的，终端设备在接收到广播报文后，可以获取位移处理后的蓝牙设备的MAC地址，进而还原得到蓝牙设备的MAC地址。终端设备在获取新的认证数据时，可以根据得到的蓝牙设备的MAC地址和终端设备中存储的预共享的信息，采用预设的算法获取新的认证数据。

[0128] 应理解，鉴于广播报文中包括位移处理后的蓝牙设备的MAC地址，本申请实施例中终端设备不需要扫描获取周围的存在的每个蓝牙设备的MAC地址，而是根据还原处理得到的蓝牙设备的MAC地址计算新的认证数据，能够减少终端设备的计算量，进而提高配对效率。

[0129] 第三种方式：广播报文中包括置换处理后的蓝牙设备的MAC地址。

[0130] 置换处理指的是将蓝牙设备的MAC地址中的每个字节按照预设置换方式置换。示例性的，蓝牙设备的MAC地址为11:22:33:44:55:66，置换处理为将数字置换为字母，或者存

在字母时将字母置换为数字。如1置换后的数字为A,2置换后的数字为B,3置换后的数字为C,4置换后的字母为D,5置换后的字母为E,6置换后的字母为F,即置换处理后的蓝牙设备的MAC地址为AA:BB:CC:DD:EE:FF。

[0131] 相应的,终端设备在接收到广播报文后,可以获取置换处理后的蓝牙设备的MAC地址,进而得到蓝牙设备的MAC地址。终端设备在获取新的认证数据时,可以根据得到的蓝牙设备的MAC地址和终端设备中存储的预共享的信息,采用预设的算法获取新的认证数据。应理解,广播的蓝牙设备和终端设备中存储相同的置换表,终端设备可以根据存储的置换表,还原得到蓝牙设备的MAC地址。

[0132] 其中,第三种方式的技术效果具体可以参照上述第二种方式中的技术效果。

[0133] 在一种实现方式中,本申请实施例中适配的蓝牙设备和终端设备获取认证数据的方式采用的算法可以为非预先设置的,相应的,广播报文中还可以包括算法标识,算法标识表征蓝牙设备获取认证数据采用的算法。同理的,终端设备在接收到广播报文后,可以根据算法标识确定蓝牙设备获取认证数据采用的算法,进而采用对应的算法解析广播报文。

[0134] 鉴于本申请实施例中蓝牙设备获取认证数据时采用了预共享的信息,因此即使其他终端设备接收到了蓝牙设备的广播报文,能够确定蓝牙设备采用的算法,但该其他终端设备采用对应的算法也不能得到一致的认证数据,进而不在界面上弹框,保证了配对的安全性。

[0135] 图5为本申请实施例提供的蓝牙配对方法的另一实施例的流程示意图。因为广播报文中包括广播地址,广播地址能够表征广播报文的来源。本实施例中为了进一步不泄露蓝牙设备的MAC地址,如图5所示,本申请实施例中可以在上述S401之前还包括:

[0136] S404,蓝牙设备生成随机广播地址。

[0137] 应理解,本申请实施例中随机广播地址与真实广播地址可以关联或无关。也就是说,蓝牙设备可以按照预设规则,根据真实广播地址生成随机广播地址,或者蓝牙设备随机生成随机广播地址。其中,广播报文中包括该随机广播地址。

[0138] 可选的,上述实施例中的S401可以替换为S401':蓝牙设备根据随机广播地址、预共享的信息和蓝牙设备的MAC地址,采用预设的算法,生成认证数据。

[0139] 示例性的,若蓝牙设备采用MAC算法对预共享的信息和蓝牙设备的MAC地址生成认证数据时,具体可见下式:

[0140] AuthData=MAC(AdvAddr||BTAddrData,PreSharePwd)

[0141] 其中,AdvAddr为随机广播地址,||表示对随机广播地址和蓝牙设备的MAC地址进行拼接,拼接后的随机广播地址和蓝牙设备的MAC地址作为生成认证数据的报文参数,预共享的信息作为生成认证数据的报文参数。示例性的,如蓝牙设备的MAC地址为11:22:33:44:55:66,随机广播地址为D2:34:E3:2B:87,则对随机广播地址和蓝牙设备的MAC地址进行拼接后,得到11:22:33:44:55:66:D2:34:E3:2B:87。

[0142] 若蓝牙设备采用Hash算法对随机广播地址、预共享的信息和蓝牙设备的MAC地址进行计算时,具体可见下式:

[0143] AuthData=Hash(AdvAddr||BTAddrData,PreShareSalt)

[0144] 其中,PreShareSalt为预共享的盐值。

[0145] 示例性的,若蓝牙设备采用加密算法对预共享的信息和蓝牙设备的MAC地址进行

加密计算,具体可见下式:

[0146] AuthData＝Encryp(AdvAddr||BTAddrData,PreShareKey)

[0147] 其中,PreShareKey为预共享的密钥。

[0148] 相对应的,上述S402可以替换为S402'。

[0149] S402',蓝牙设备发送广播报文,若预设的算法为单向散列算法,则广播报文中包括认证数据、处理后的MAC地址和随机广播地址,若预设的算法为加密算法,则广播报文中包括认证数据和随机广播地址。

[0150] 图6为本申请实施例中提供的广播报文的结构示意图。如图6所示,广播报文中包括随机广播地址D5:ED:ED:A4:BC:5F,截断处理后的MAC地址为55:66,认证数据为sh8h1hh9E7rHF93G。应理解,其中的随机广播地址、截断处理后的MAC地址以及认证数据仅为示例说明。

[0151] 在该种场景下,终端设备接收到广播报文后,可以根据处理后的MAC地址得到蓝牙设备的MAC地址,根据蓝牙设备的MAC地址、广播报文中的随机广播地址和终端设备中存储的预共享的信息,计算的得到新的认证数据。若新的认证数据和广播报文中的认证数据一致,则终端设备在界面上显示弹框。

[0152] 应注意,认证数据和新的认证数据采用的报文参数为预先约定的,如蓝牙设备生成认证数据的报文参数为蓝牙设备的MAC地址、随机广播地址和预共享的信息,则终端设备在获取新的认证数据时,采用的报文参数也为蓝牙设备的MAC地址、随机广播地址和预共享的信息。

[0153] 其中,若预设的算法为加密算法,在该种场景下,终端设备在接收到广播报文后,可以采用解密算法获取认证数据中的随机广播地址、预共享的信息和蓝牙设备的MAC地址,进而比对该认证数据中的随机广播地址是否与广播报文中的随机广播地址一致,且比较认证数据中的预共享的信息是否与终端设备中存储的预共享的信息一致,在随机广播地址和预共享的信息均一致的情况下,终端设备在界面上显示弹框。

[0154] 在上述实施例的基础上,图7为本申请实施例提供的蓝牙配对方法的另一实施例的流程示意图。为了进一步提高认证数据的安全性,在上述实施例的基础上,蓝牙设备可以在获取认证数据时,增加报文参数“预留信息”,例如上述S401可以替换为S401”:蓝牙设备根据随机广播地址、预共享的信息、蓝牙设备的MAC地址和预留信息,采用预设的算法,生成认证数据。其中,预留信息可以包括如下至少一项:芯片标识符、芯片的型号。应注意,适配的蓝牙设备或终端设备中存储有相同的预留信息。

[0155] 本申请实施例中,为了进一步提高配对安全性,本申请实施例中可以根据适配的蓝牙设备和终端设备知道的其他数据,如预共享的信息、预留信息等,计算获取认证数据,进而使得不知道该其他数据的终端设备,不能解析广播报文,可以提高蓝牙配对的安全性。本申请实施例中蓝牙设备还可以生成随机广播地址,避免了泄露了广播报文的来源以泄露蓝牙设备的MAC地址,进一步提高了蓝牙配对的安全性。另外,本申请实施例中的广播报文中还可以包括处理后的MAC地址,终端设备可以根据处理后的MAC地址获取蓝牙设备的完整的MAC地址,进而减少终端设备周围有多个蓝牙设备时均需要计算得到认证数据的计算量,提高蓝牙配对效率。

[0156] 本申请上述实施例可以实现相同型号、或者相同品牌的终端设备和蓝牙设备能够

的安全配对，但还会存在如下情况：对于相同型号、相同品牌适配的蓝牙设备和终端设备，终端设备能够接收到来自两个蓝牙设备的广播报文，终端设备在界面上可以两次弹框；或者，一个蓝牙设备发送的广播报文由两个终端设备接收，则该两个终端设备也可以均会弹框。

[0157] 示例性的，在公共场所，用户自己的A型号的蓝牙耳机发送广播报文后，除了自己的终端设备能够接收到该广播报文，在界面上弹框。处于该蓝牙耳机周围的其他与该A型号的蓝牙耳机的其他终端设备(非用户的终端设备)也能够弹框。或者，用户的终端设备能够接收到用户的蓝牙耳机的广播报文，也能够接收到适配的非用户的蓝牙耳机的广播报文，因此在终端设备上显示两次弹框，用户体验低。

[0158] 为了保证用户的蓝牙耳机和终端设备的私有化，例如，用户的终端设备上不弹框显示别的用户的蓝牙设备。图8为本申请实施例提供的蓝牙配对方法的另一实施例的流程示意图。如图8所示，本申请实施例中在上述S403之后，还可以包括：

[0159] S405，若终端设备在界面上显示弹框，接收到用户对弹框的操作，则与蓝牙设备配对连接。

[0160] 例如，弹框可以显示有“连接”。用户点击“连接”，终端设备与蓝牙设备配对连接。

[0161] S406，终端设备生成新的预共享的信息。

[0162] S407，终端设备更新预共享的信息。

[0163] S408，终端设备向蓝牙设备发送新的预共享的信息。

[0164] S409，蓝牙设备更新预共享的信息。

[0165] 应理解，本申请实施例中的S407和S408没有先后顺序的区分，二者可以同时执行。

[0166] 应理解，上述S405中终端设备在界面上显示弹框可如图1所示。本申请实施例中，用户点击了“配对”控件，例如“连接”按钮，该操作用于终端设备与蓝牙设备配对连接。相应的，终端设备接收用户对弹框的操作后，可以与蓝牙设备配对连接。

[0167] 上述S406中，终端设备可以生成新的预共享的信息。本申请实施例中，新的预共享的信息与预共享的信息可以关联或无关，也就是说，终端设备可以在原预共享的信息的基础上，采用预设规则生成新的预共享的信息，或者，终端设备可以随机生成新的预共享的信息。应理解，此处的预共享的信息为生产阶段设置的预共享的信息。

[0168] 上述S407中，本申请实施例中终端设备可以更新预共享的信息。如终端设备可以存储该新的预共享的信息，标记预共享的信息(即生产阶段设置的预共享的信息)为失效状态。其中失效状态可以指示该预共享的信息不可用，例如不能用于配对时验证认证数据。或者，本申请实施例中终端设备还可以删除预共享的信息，存储新的预共享的信息。其中，预共享的信息和新的预共享的信息可以均存储在终端设备的安全存储区域。

[0169] 上述S408中，终端设备生成新的预共享的信息，可以向蓝牙设备发送新的预共享的信息，以使与蓝牙设备之间同步该新的预共享的信息。其中，蓝牙设备下次发送广播报文时，可以根据该新的预共享的信息、蓝牙设备的MAC地址、随机生成的广播地址、预留信息(可选的)等，采用预设的算法，生成认证数据。

[0170] 同理的，蓝牙设备在接收到新的预共享的信息时，可以更新蓝牙设备中存储的预共享的信息。其中，蓝牙设备更新预共享的信息的方式可以参照终端设备更新预共享的信息的方式，见上述的相关描述。

[0171] 在一种可能的场景下，在终端设备和蓝牙设备配对连接后，终端设备可以在蓝牙设置界面上显示触发终端设备生成新的预共享的信息的控件，用户选择该控件，触发终端设备生成新的预共享的信息。

[0172] 图9为本申请实施例提供的终端设备的界面变化示意图一。如图9所示，终端设备的界面901上显示有终端设备的蓝牙名称Aaa、生成新的预共享的信息的控件91，以及已配对的蓝牙设备Aab。其中，该控件下方可以显示有该控件的功能介绍“打开该控件更新预共享的信息，让您的终端设备和蓝牙设备一一对应”。示例性的，用户终端设备打开该控件91，可触发终端设备生成新的预共享的信息，相应的，界面901跳转至界面902。其中，处于打开状态的控件可以为阴影填充所示，处于关闭状态的控件可以为白色填充所示。

[0173] 本申请实施例中用户的终端设备和蓝牙设备同步了新的预共享的信息，因此在下次用户的蓝牙设备发送广播报文后，相同类型或品牌的其他终端设备采用原先生产阶段设置的预共享的信息得到的新的认证数据与用户的蓝牙设备的广播报文中的认证数据不一致，或者该其他终端设备解密得到的预共享的信息与其他终端设备中存储的预共享的信息不一致，进而其他终端设备在接收到用户的蓝牙设备的广播报文后，在界面上不显示弹框，保证了用户的蓝牙设备和终端设备的私有化，保证了设备的隐私安全。

[0174] 另外，在上述实施例的基础上，本申请实施例中提供的蓝牙配对方法还能够将终端设备的新的预共享的信息同步至云端(如云服务器中)，云端可以将终端设备的标识和新的预共享的信息对应存储。终端设备的标识如可以为登录终端设备的用户账号。应理解，对于一个终端设备来说，终端设备与一个蓝牙设备配对连接后，生成一个新的预共享的信息，与另一个蓝牙设备配对连接后，还可以生成另一个新的预共享的信息。终端设备与不同的蓝牙设备配对连接后生成的新的预共享的信息不同。示例性的，智能手机与蓝牙耳机配对连接后，可以生成新的预共享的信息1，如Aaaaaa；智能手机与蓝牙手环配对连接后，可以生成新的预共享的信息2，如Bbbbbb。预共享的信息1与预共享的信息2不同。

[0175] 因此，一个终端设备可能与多个蓝牙设备均配对连接过，因此，云端中可以存储有终端设备的用户账号对应的多个新的预共享的信息和蓝牙设备的标识，如下表一的信任设备列表所示：

[0176] 表一

[0177]

用户账号	新的预共享的信息	蓝牙设备的标识
用户账号a	Aaaaaa	蓝牙设备1
	Bbbbbb	蓝牙设备2
	Cccccc	蓝牙设备3

[0178] 如上表一中，蓝牙设备的标识可以为蓝牙设备的型号、蓝牙设备的MAC地址，或者其他用于表示蓝牙设备的信息。

[0179] 在该种场景下，在用户更换终端设备后，用户可以在更换后的终端设备上登录该用户账号，可实现该终端设备与蓝牙设备的连接。示例性的，用户的蓝牙设备为蓝牙设备1，用户的终端设备为终端设备1’，登录终端设备1’的用户账号为用户账号a。蓝牙设备1和终端设备1’配对连接后，终端设备1’中存储有用户账号a和蓝牙设备1，以及新的预共享的信息Aaaaaa的对应关系。在用户将终端设备更换为终端设备2’，或者在终端设备2’上登录该用户账号a后，终端设备2’可以同步终端设备1’中的如上表一，终端设备2’可以存储上述信

任设备列表。

[0180] 在另一种实现方式中，在图9的基础上，终端设备的蓝牙的设置界面上还可以显示有同步控件92，用户在另一终端设备上登录用户账号后，可以选择该同步控件92，以触发该终端设备同步该用户账号下的信任设备列表。

[0181] 示例性的，图10为本申请实施例提供的终端设备的界面变化示意图二。如图10所示，界面1001中显示有同步控件，该同步控件92的下方还可以显示有该同步控件的功能介绍，如“同步您的账号下的蓝牙设备和新的预共享的信息”。示例性的，用户在选择该同步控件92后，界面1001跳转至界面1002，以触发终端设备存储该用户账号下对应的新的预共享的信息和蓝牙设备的标识。这样可以存储上述信任设备列表。也就是说，该终端设备中存储有该用户账号下对应的新的预共享的信息，以及生产阶段设置的预共享的信息。

[0182] 相应的，图11为本申请实施例提供的蓝牙配对方法的另一实施例的流程示意图。如图11所示，本申请实施例提供的蓝牙配对方法可以包括：

[0183] S1101，蓝牙设备生成随机广播地址。

[0184] S1102，蓝牙设备根据随机广播地址、预共享的信息和蓝牙设备的MAC地址，采用预设的算法，生成认证数据。

[0185] S1103，蓝牙设备发送广播报文，若预设的算法为单向散列算法，则广播报文中可以包括随机广播地址、处理后的MAC地址和认证数据，若预设的算法为加密算法，则广播报文中可以包括随机广播地址和认证数据。

[0186] S1104，若蓝牙设备是信任设备列表中的设备，则终端设备在界面上显示弹框。

[0187] 上述S1101-S1103中的实施方式可以参照上述实施例中S404、S401’-S403’中的相关描述。

[0188] 上述S1104中，此处对本申请实施例中可能实现的两种方式进行说明：

[0189] 第一种可能实现的方式：

[0190] 同一用户账号对应的终端设备生成的新的预共享的信息可以相同，也就是说，若终端设备上登录一用户账号，则与该终端设备配对过的蓝牙设备中存储的新的预共享的信息相同，例如该用户账号下的信任设备列表中的新的预共享的信息相同。若更换终端设备，登录与之前终端设备相同的用户账号，则与更换终端设备配对过的蓝牙设备中存储的新的预共享的信息相同。示例性的，该用户账号下的信任设备列表可以如下表二所示：

[0191] 表二

[0192]

用户账号	新的预共享的信息	蓝牙设备的标识
用户账号a	Aaaaaa	蓝牙设备1的MAC地址
		蓝牙设备2的MAC地址
		蓝牙设备3的MAC地址

[0193] 在该种方式中，若预设的算法为单向散列算法，表二中的蓝牙设备的标识为蓝牙设备的MAC地址，终端设备接收到广播报文后，可以根据广播报文中处理后的蓝牙MAC地址和信任设备列表中多个蓝牙设备的MAC地址，确定周围存在的蓝牙设备是否为信任设备列表中的蓝牙设备。其中，在确定广播报文中的蓝牙MAC地址和信任设备列表中的MAC地址相同时，可以确定该蓝牙设备即为信任设备列表中的蓝牙设备。

[0194] 在该种场景下，若处理后的MAC地址是采用截断处理获取的，则可能根据处理后的

蓝牙MAC地址和信任设备列表中的蓝牙设备的MAC地址，可以确定周围存在信任设备列表中的多个蓝牙设备。其中，终端设备可以依次生成该多个蓝牙设备对应的新的认证数据，在新的认证数据中有与广播报文中的认证数据一致的数据时，可以确定该蓝牙设备为信任设备列表中的蓝牙设备。

[0195] 在该种方式中，若预设的算法为加密算法，广播报文中包括随机广播地址和认证数据，本实施例中终端设备可以采用新的预共享的信息(例如，新的预共享的密钥)解密认证数据，以得到认证数据中的蓝牙设备的MAC地址和预共享的信息，若认证数据中的蓝牙设备的MAC地址为信任设备列表中的MAC地址时，可以确定该蓝牙设备为信任设备列表中的蓝牙设备。

[0196] 第二种可能实现的方式：

[0197] 同一用户账号对应的终端设备在与不同的蓝牙设备配对连接后，生成的新的预共享的信息不同，例如上述表一所示。该种场景下，若预设的算法为加密算法，终端设备采用与加密算法对应的解密算法解密时，可以依次采用信任设备列表中的预共享的信息(例如新的预共享的密钥)解密认证数据，计算量较大。

[0198] 为了减少终端设备解密时采用不同的新的预共享的信息解密认证数据，以减少终端设备的计算量，本实施例中可以在该种场景下采用单向散列算法获取认证数据生成广播报文。在该种场景下，可以采用与上述第一种可能实现的方式中相同的方式，确定发送广播报文的蓝牙设备是否为信任设备列表中的蓝牙设备。与上述第一种可能实现的方式不同的是，该种方式中每个不同的蓝牙设备对应的新的预共享的信息不同。

[0199] 示例性的，如用户在智能手机1’上登录用户账号a，用户新买了一个智能手机2’，在该智能手机2’上登录用户账号a，或者用户在平板电脑上登录用户账号a，则该智能手机2’和平板电脑均能够同步上述信任设备列表。在智能手机2’或平板电脑与蓝牙设备配对时，可以根据信任设备列表与蓝牙设备进行配对。在智能手机2’或平板电脑接收到广播报文后，若确定发送广播报文的蓝牙设备为信任设备列表中的蓝牙设备，则在界面上显示弹框。

[0200] 应注意，若终端设备接收到广播报文后，终端设备确定发送广播报文的蓝牙设备不是信任设备列表中的蓝牙设备，终端设备在界面上不显示弹框。但实际应用过程中，还存在这种场景：若终端设备同步用户账号下的信任设备列表后，用户购入新的蓝牙设备，即该新的蓝牙设备不是信任设备列表中的蓝牙设备，此时终端设备采用新的预共享的信息无法在界面上显示弹框，进而无法与该新的蓝牙设备连接。

[0201] 为了解决该问题，本实施例中可以在终端设备的蓝牙的设置界面上还可以显示有“与新的蓝牙设备配对”的控件，用户选择该“与新的蓝牙设备配对”的控件，可以触发终端设备激活预先设置的预共享的信息，进而采用该预共享的信息实现与蓝牙设备的配对。其中，采用预共享的信息与蓝牙设备配对的步骤可以参照上述实施例图3、图4和图5中的相关描述。

[0202] 应注意，终端设备的蓝牙的设置界面上还可以显示的“与新的蓝牙设备配对”的控件93可以如图12所示，图12为本申请实施例提供的终端设备的界面示意图。

[0203] 本申请实施例中，终端设备可以将配对的蓝牙设备的信息同步至云端的用户账号下，进而在其他终端设备上登录该用户账号时，可以与该用户账号下的蓝牙设备进行配对，

本申请实施例能够实现登录相同用户账号的其他终端设备与蓝牙设备的配对，进而使得用户的多个终端设备均可以和蓝牙设备进行配对。

[0204] 图13为本申请实施例提供的蓝牙配对装置的结构示意图。本实施例所涉及的蓝牙配对装置可以为前述所说的终端设备，也可以为应用于终端设备的芯片。该蓝牙配对装置可以用于执行上述方法实施例中终端设备的动作。如图13所示，该蓝牙配对装置可以包括：收发模块1301、处理模块1302、显示模块1303和存储模块1304。其中，

[0205] 收发模块1301，用于接收来自蓝牙设备的广播报文，所述广播报文中包括认证数据，所述认证数据是所述蓝牙设备根据报文参数生成的，所述报文参数包括所述蓝牙设备的媒体访问控制MAC地址。

[0206] 处理模块1302，用于采用预设的算法，解析所述广播报文。

[0207] 显示模块1303，用于若解析所述广播报文得到所述蓝牙设备的MAC地址，则在界面上显示弹框，所述弹框可以指示周围存在待配对的所述蓝牙设备。

[0208] 在一种可能的实现方式中，所述认证数据是所述蓝牙设备采用加密算法对所述报文参数加密生成的。所述处理模块1302，具体用于解密所述认证数据，得到所述蓝牙设备的MAC地址。

[0209] 在一种可能的实现方式中，所述报文参数还包括所述蓝牙设备中存储的预共享的信息。所述处理模块1302，具体用于解密所述认证数据，若所述认证数据中的预共享的信息与所述终端设备中存储的预共享的信息相同，则将解密得到的所述认证数据中的MAC地址作为所述蓝牙设备的MAC地址。

[0210] 在一种可能的实现方式中，所述认证数据是所述蓝牙设备采用单向散列算法对所述报文参数计算得到的。所述处理模块1302，具体用于扫描周围存在的至少一个蓝牙设备，获取所述至少一个蓝牙设备的MAC地址，采用所述单向散列算法，根据所述周围存在的每个蓝牙设备的MAC地址，得到至少一个新的认证数据，且将新的认证数据与所述认证数据相同的周围存在的蓝牙设备的MAC地址，作为所述蓝牙设备的MAC地址。

[0211] 在一种可能的实现方式中，所述报文参数还包括所述蓝牙设备中存储的预共享的信息。所述处理模块1302，具体用于采用所述单向散列算法，根据所述周围存在的每个蓝牙设备的MAC地址和所述终端设备中存储的预共享的信息，得到所述至少一个新的认证数据。

[0212] 在一种可能的实现方式中，所述广播报文中还包括随机广播地址；所述报文参数中还包括：随机广播地址和/或预留信息。

[0213] 在一种可能的实现方式中，所述收发模块1301，还用于接收用户对所述弹框的操作指令，所述操作指令指示与所述蓝牙设备配对连接。

[0214] 在一种可能的实现方式中，所述收发模块1301，还用于在终端设备和所述蓝牙设备配对连接后，接收用户对所述终端设备的界面上显示的生成新的预共享的信息的控件的第一选择指令。

[0215] 所述处理模块1302，还用于根据所述第一选择指令，生成新的预共享的信息。

[0216] 在一种可能的实现方式中，存储模块1304，用于存储所述蓝牙设备的MAC地址和所述新的预共享的信息的对应关系。

[0217] 在一种可能的实现方式中，所述收发模块1301，还用于接收所述用户对所述终端设备的界面上显示的同步控件的第二选择指令。

[0218] 所述处理模块1302，还用于根据所述第二选择指令，存储所述终端设备上登录的用户账号下的对应关系，所述用户账号下的对应关系为：登录过所述用户账号的终端设备中存储的蓝牙设备的MAC地址和新的预共享的信息的对应关系。

[0219] 在一种可能的实现方式中，所述报文参数还包括所述蓝牙设备中存储的预共享的信息。所述处理模块1302，还用于解密所述认证数据，若所述认证数据中的预共享的信息与所述终端设备中存储的预共享的信息相同，且所述述认证数据中的MAC地址为所述终端设备中存储的对应关系中的MAC地址，则将解密得到的所述认证数据中的MAC地址作为所述蓝牙设备的MAC地址。

[0220] 本申请实施例提供的蓝牙配对装置，可以执行上述方法实施例中终端设备的动作，其实现原理和技术效果类似，在此不再赘述。

[0221] 需要说明的是，应理解以上收发模块实际实现时可以为收发器、或者包括发送器和接收器。而处理模块可以以软件通过处理元件调用的形式实现；也可以以硬件的形式实现。例如，处理模块可以为单独设立的处理元件，也可以集成在上述装置的某一个芯片中实现，此外，也可以以程序代码的形式存储于上述装置的存储器中，由上述装置的某一个处理元件调用并执行以上处理模块的功能。此外这些模块全部或部分可以集成在一起，也可以独立实现。这里所述的处理元件可以是一种集成电路，具有信号的处理能力。在实现过程中，上述方法的各步骤或以上各个模块可以通过处理器元件中的硬件的集成逻辑电路或者软件形式的指令完成。

[0222] 例如，以上这些模块可以是被配置成实施以上方法的一个或多个集成电路，例如：一个或多个专用集成电路(application specific integrated circuit,ASIC)，或，一个或多个微处理器(digital signal processor,DSP)，或，一个或者多个现场可编程门阵列(field programmable gate array,FPGA)等。再如，当以上某个模块通过处理元件调度程序代码的形式实现时，该处理元件可以是通用处理器，例如中央处理器(central processing unit,CPU)或其它可以调用程序代码的处理器。再如，这些模块可以集成在一起，以片上系统(system-on-a-chip,SOC)的形式实现。

[0223] 图14为本申请实施例提供的电子设备的结构示意图。如图14所示，该电子设备可以为上述的终端设备，该电子设备可以包括：处理器1401(例如CPU)、存储器1402、收发器1403；收发器1403耦合至处理器1401，处理器1401控制收发器1403的收发动作；存储器1402可能包含高速随机存取存储器(random-access memory,RAM)，也可能还包括非易失性存储器(non-volatile memory,NVM)，例如至少一个磁盘存储器，存储器1402中可以存储各种指令，以用于完成各种处理功能以及实现本申请的方法步骤。可选的，本申请涉及的电子设备还可以包括：电源1404、通信总线1405、通信端口1406和显示器1407。收发器1403可以集成在电子设备的收发信机中，也可以为电子设备上独立的收发天线。通信总线1405用于实现元件之间的通信连接。上述通信端口1406用于实现电子设备与其他外设之间进行连接通信。显示器用于显示终端设备的界面。

[0224] 在本申请实施例中，上述存储器1402用于存储计算机可执行程序代码，程序代码包括指令；当处理器1401执行指令时，指令使电子设备的处理器1401执行上述方法实施例中终端设备的处理动作，使收发器1403执行上述方法实施例中终端设备的收发动作，其实现原理和技术效果类似，在此不再赘述。

[0225] 在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行计算机程序指令时，全部或部分地产生按照本申请实施例的流程或功能。计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。可用介质可以是磁性介质，(例如，软盘、硬盘、磁带)、光介质(例如，DVD)、或者半导体介质(例如固态硬盘Solid State Disk(SSD))等。

[0226] 本文中的术语“多个”是指两个或两个以上。本文中术语“和/或”，仅仅是一种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这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系；在公式中，字符“/”，表示前后关联对象是一种“相除”的关系。

[0227] 可以理解的是，在本申请实施例的实施例中涉及的各种数字编号仅为描述方便进行的区分，并不用来限制本申请实施例的实施例的范围。

[0228] 可以理解的是，在本申请实施例的实施例中，上述各过程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例的实施过程构成任何限定。

图1

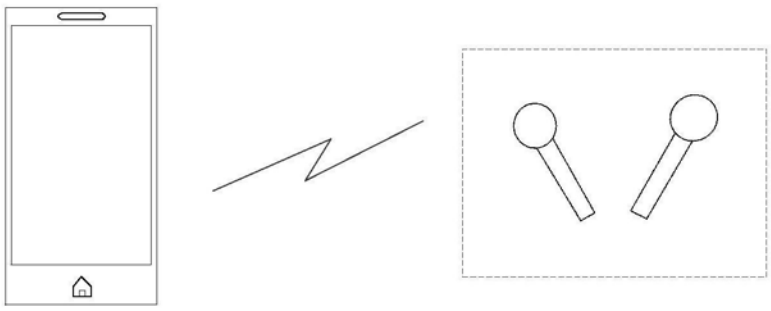


图2

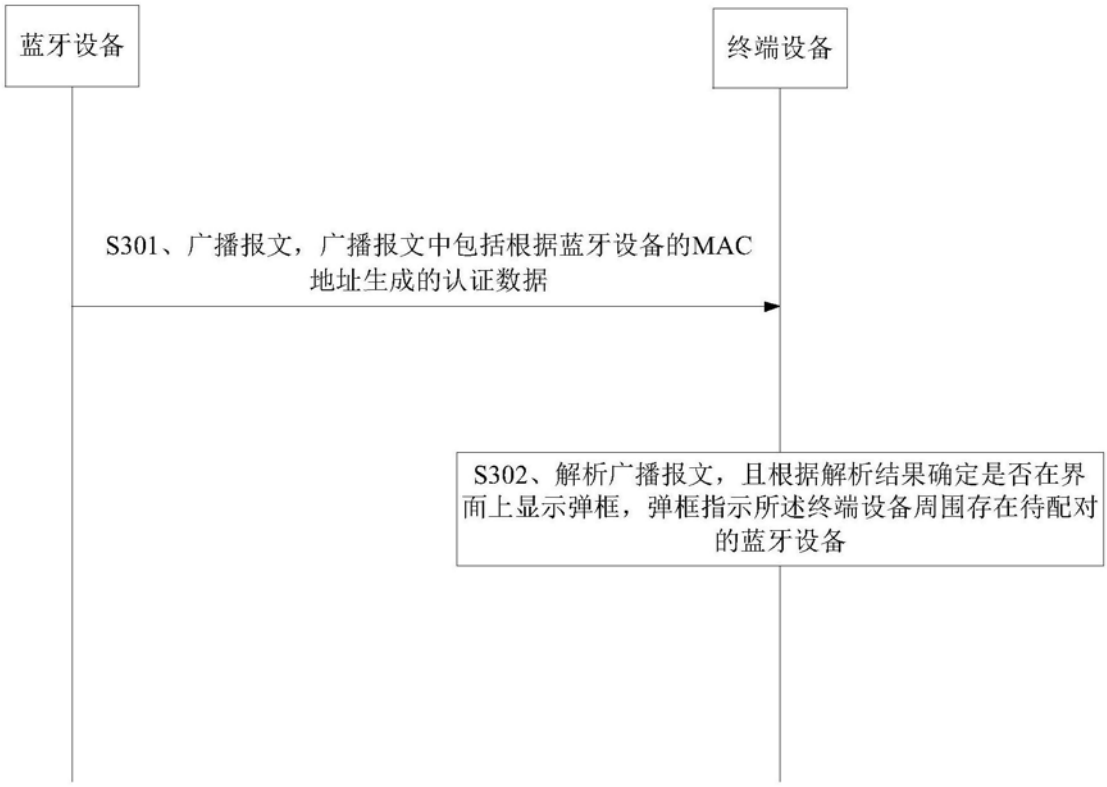

蓝牙设备
终端设备
S301、广播报文，广播报文中包括根据蓝牙设备的MAC地址生成的认证数据
S302、解析广播报文，且根据解析结果确定是否在界面上显示弹框，弹框指示所述终端设备周围存在待配对的蓝牙设备

图3

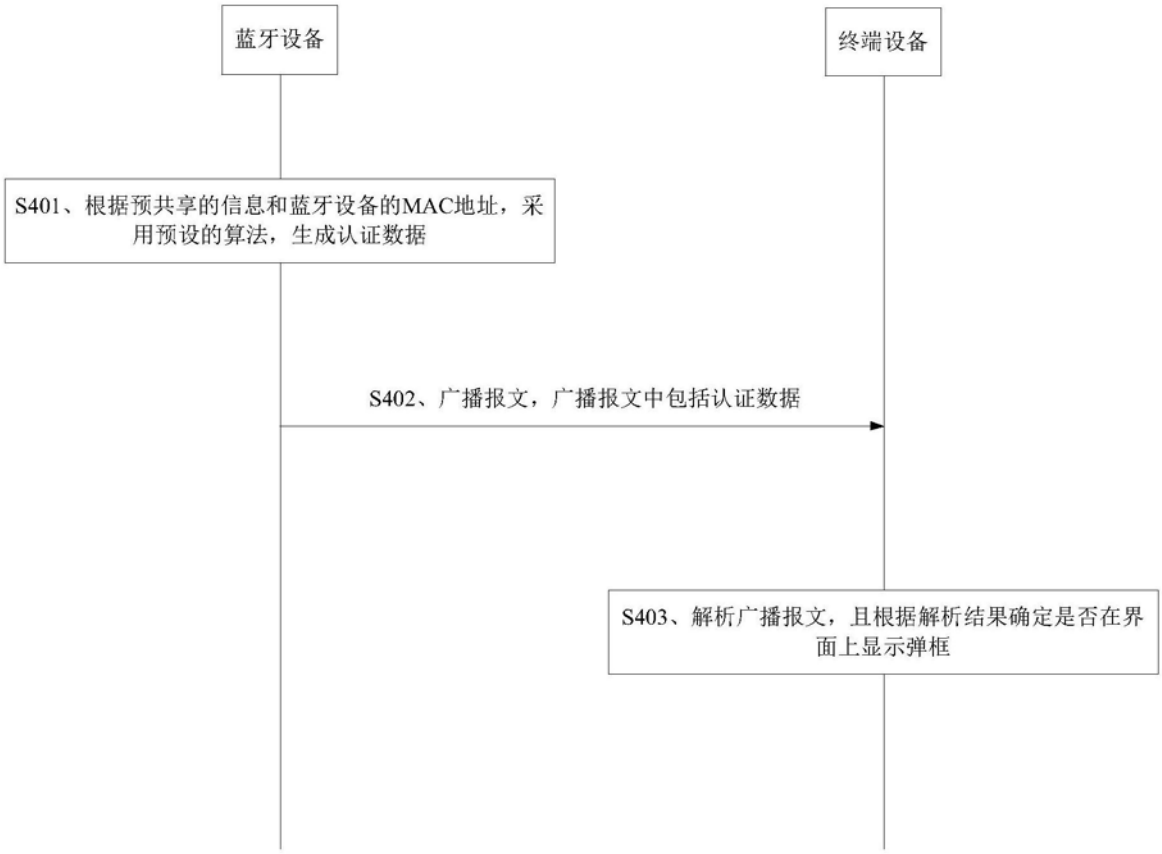

蓝牙设备
终端设备
S401、根据预共享的信息和蓝牙设备的MAC地址，采用预设的算法，生成认证数据
S402、广播报文，广播报文中包括认证数据
S403、解析广播报文，且根据解析结果确定是否在界面上显示弹框

图4

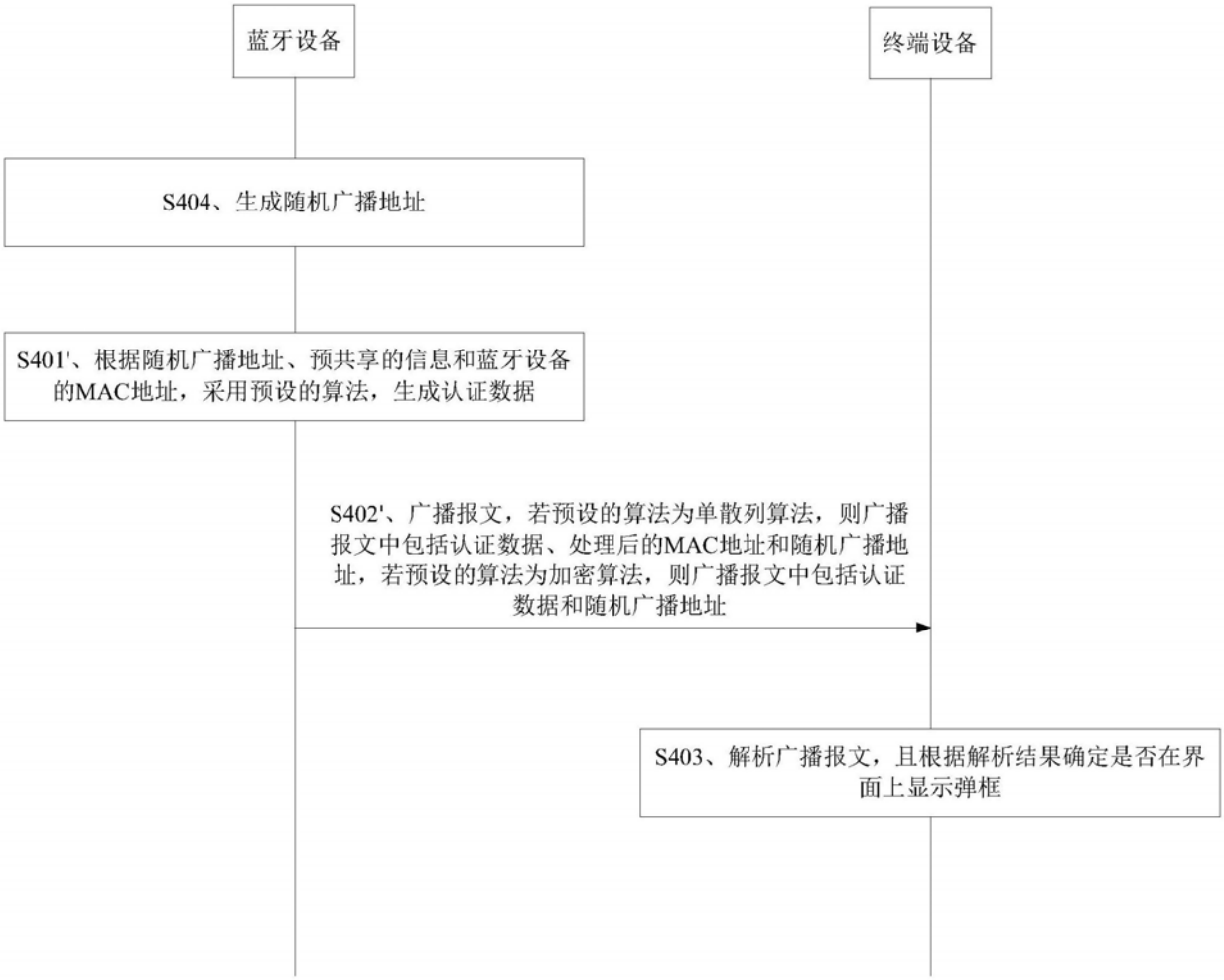


图5

D5:ED:ED:A4:BC:5F	随机广播地址	广播报文
sh8hlhh9E7rHF93G	认证数据	
55:66	截断处理后的MAC地址	

图6

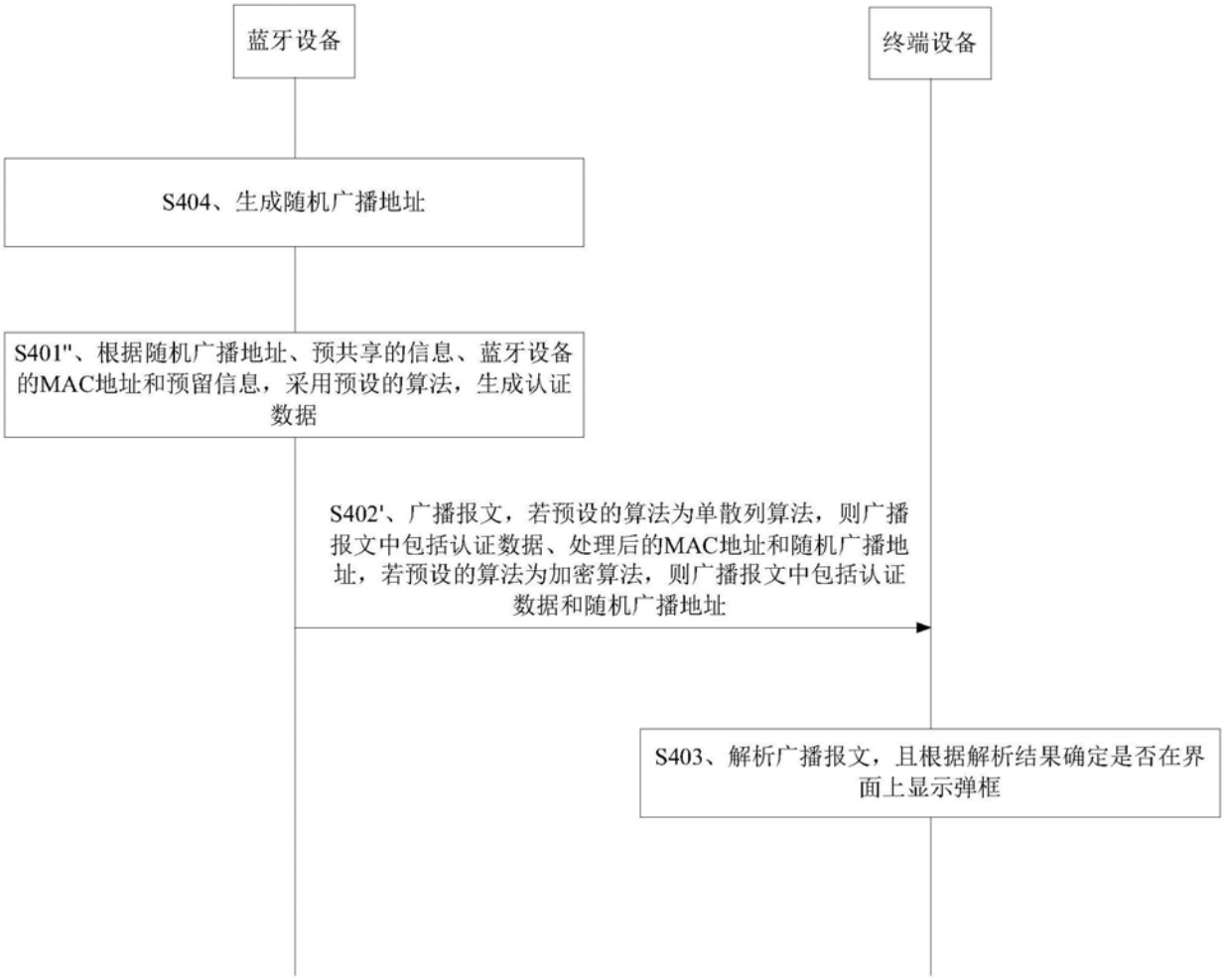

蓝牙设备
终端设备
S404、生成随机广播地址
S401"、根据随机广播地址、预共享的信息、蓝牙设备的MAC地址和预留信息，采用预设的算法，生成认证数据
S402'、广播报文，若预设的算法为单散列算法，则广播报文中包括认证数据、处理后的MAC地址和随机广播地址，若预设的算法为加密算法，则广播报文中包括认证数据和随机广播地址
S403、解析广播报文，且根据解析结果确定是否在界面上显示弹框

图7

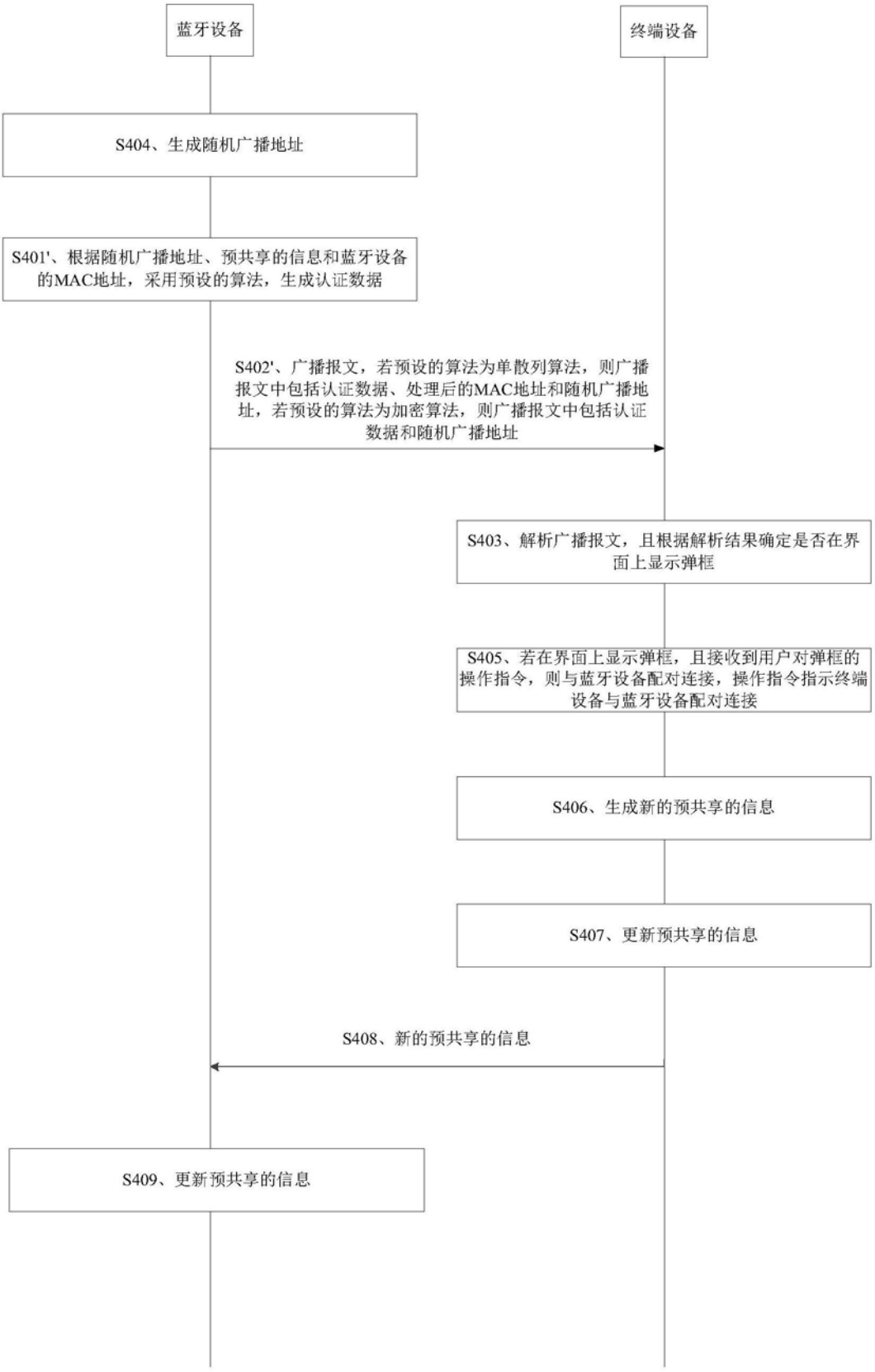

蓝牙设备
终端设备
S404、生成随机广播地址
S401'、根据随机广播地址、预共享的信息和蓝牙设备的MAC地址，采用预设的算法，生成认证数据
S402'、广播报文，若预设的算法为单散列算法，则广播报文中包括认证数据、处理后的MAC地址和随机广播地址，若预设的算法为加密算法，则广播报文中包括认证数据和随机广播地址
S403、解析广播报文，且根据解析结果确定是否在界面上显示弹框
S405、若在界面上显示弹框，且接收到用户对弹框的操作指令，则与蓝牙设备配对连接，操作指令指示终端设备与蓝牙设备配对连接
S406、生成新的预共享的信息
S407、更新预共享的信息
S408、新的预共享的信息
S409、更新预共享的信息

图8

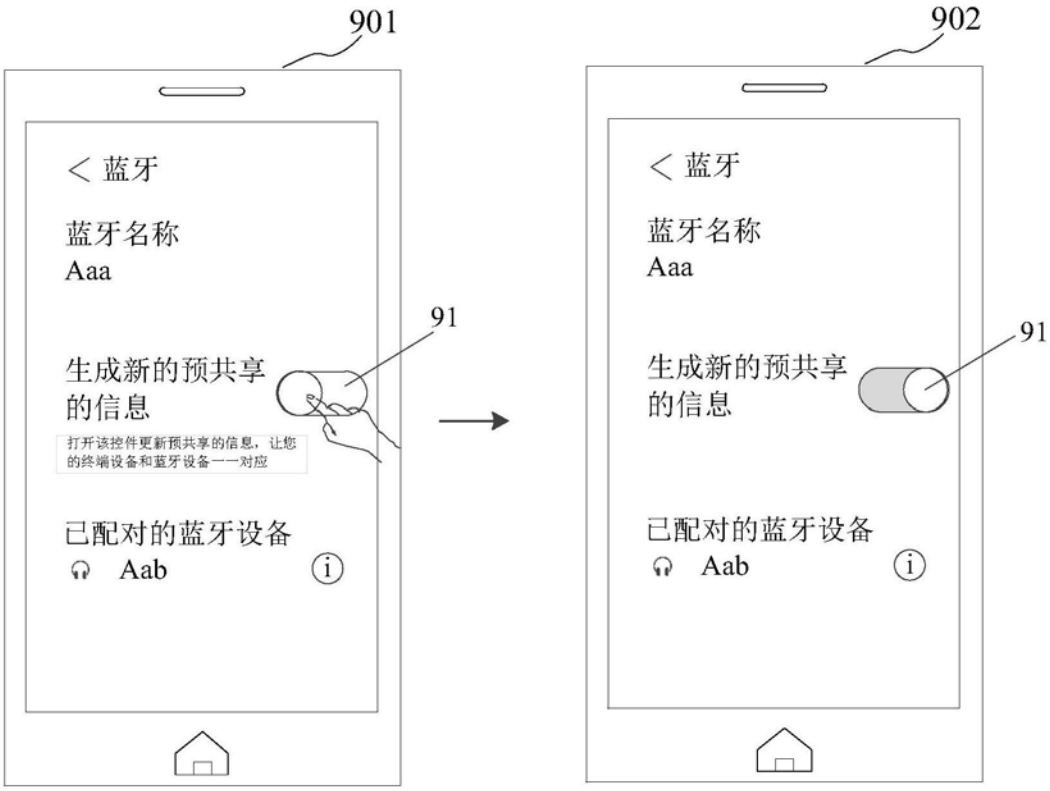

901
902
< 蓝牙
蓝牙名称
Aaa
生成新的预共享的信息
打开该控件更新预共享的信息，让您的终端设备和蓝牙设备一一对应
已配对的蓝牙设备
Aab
91

图9

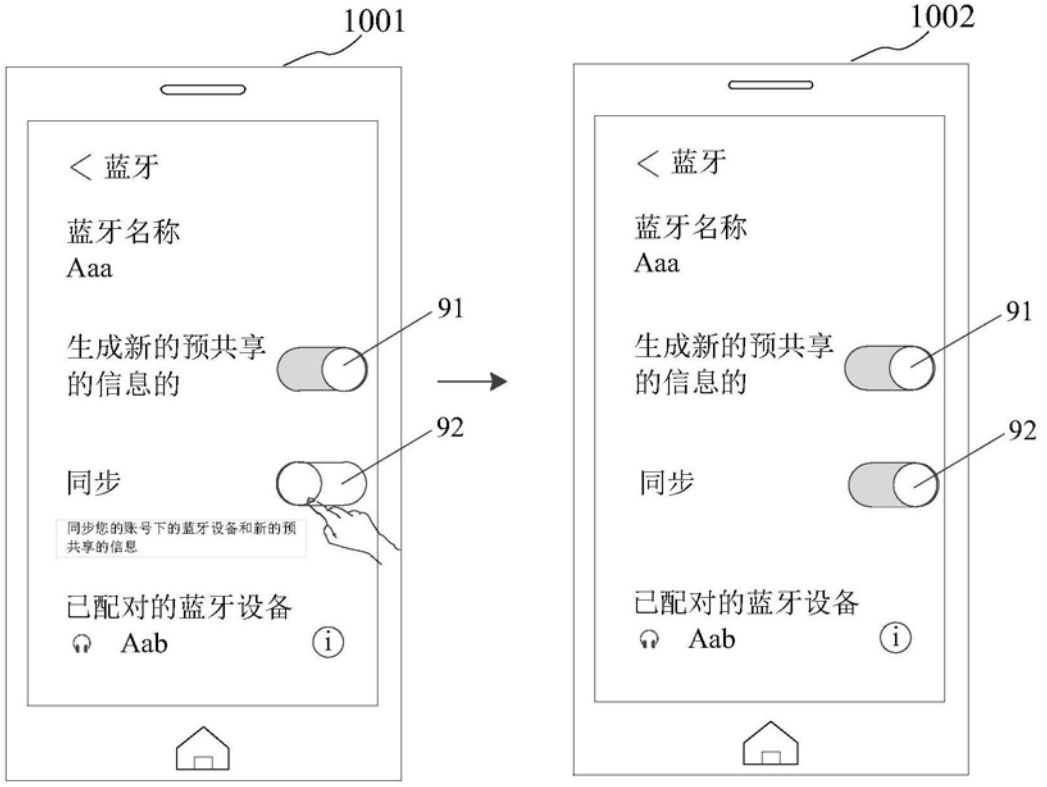

1001
1002
< 蓝牙
蓝牙名称
Aaa
生成新的预共享的信息的
同步
同步您的账号下的蓝牙设备和新的预共享的信息
已配对的蓝牙设备
Aab
91
92

图10

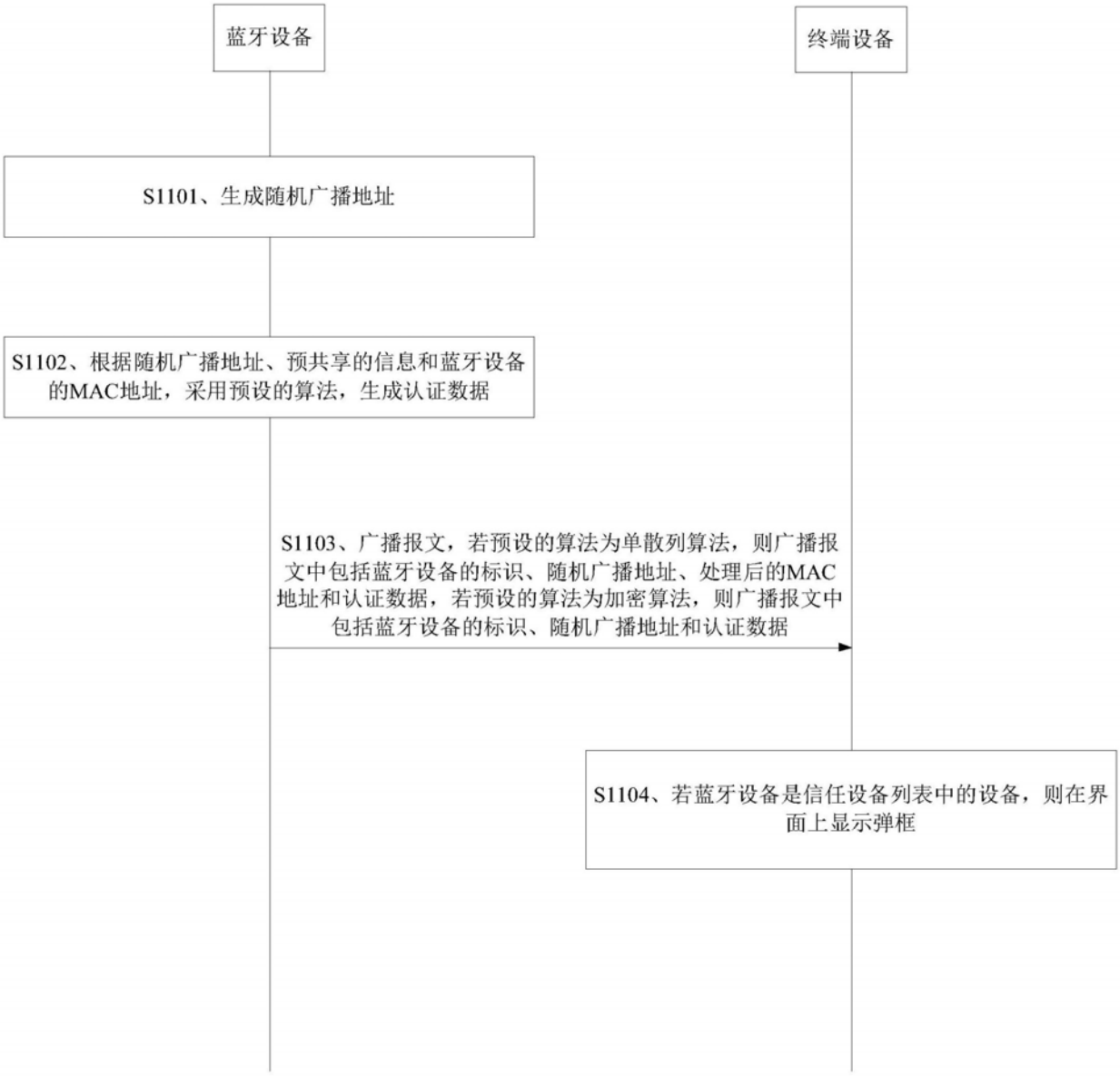

蓝牙设备
终端设备
S1101、生成随机广播地址
S1102、根据随机广播地址、预共享的信息和蓝牙设备的MAC地址，采用预设的算法，生成认证数据
S1103、广播报文，若预设的算法为单散列算法，则广播报文中包括蓝牙设备的标识、随机广播地址、处理后的MAC地址和认证数据，若预设的算法为加密算法，则广播报文中包括蓝牙设备的标识、随机广播地址和认证数据
S1104、若蓝牙设备是信任设备列表中的设备，则在界面上显示弹框

图11

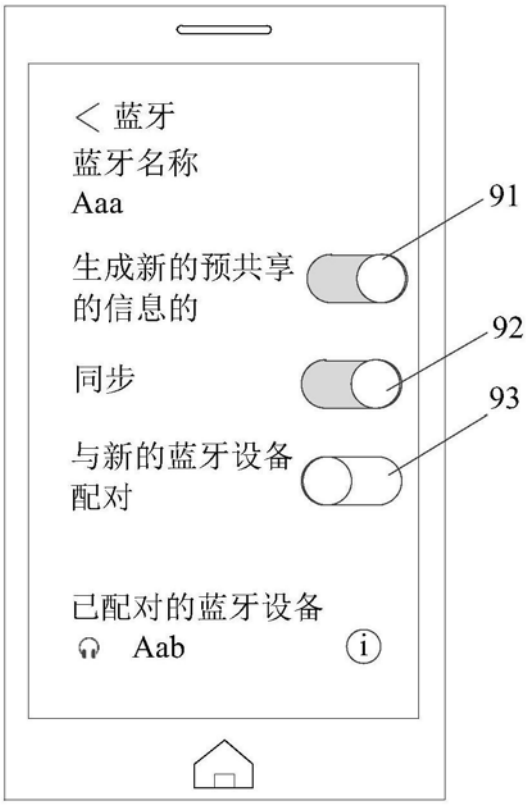

< 蓝牙
蓝牙名称
Aaa
生成新的预共享的信息的
同步
与新的蓝牙设备配对
已配对的蓝牙设备
Aab
91
92
93

图12

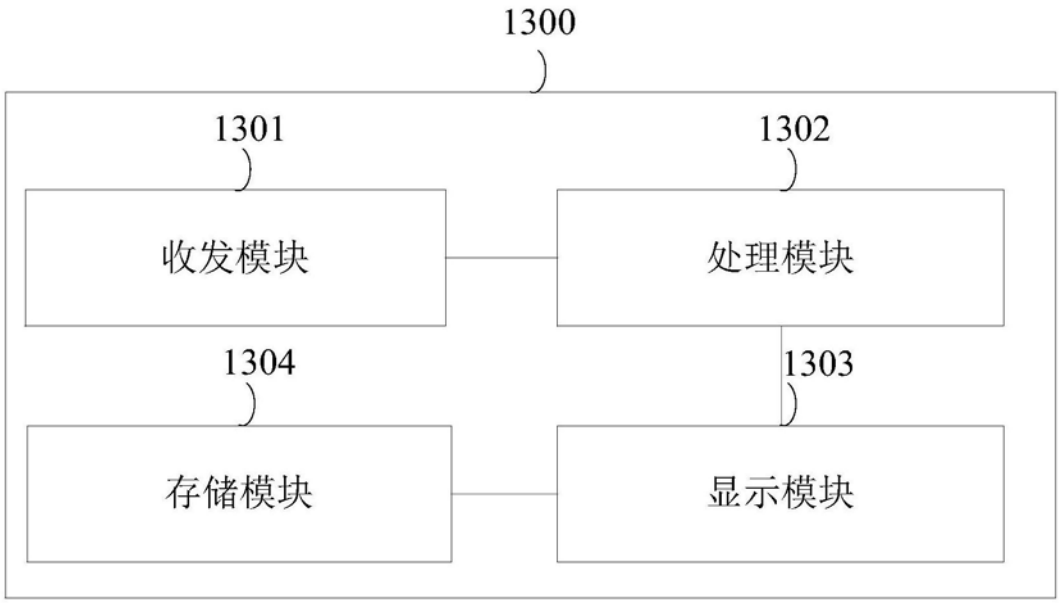

1300
1301
收发模块
1302
处理模块
1304
存储模块
1303
显示模块

图13

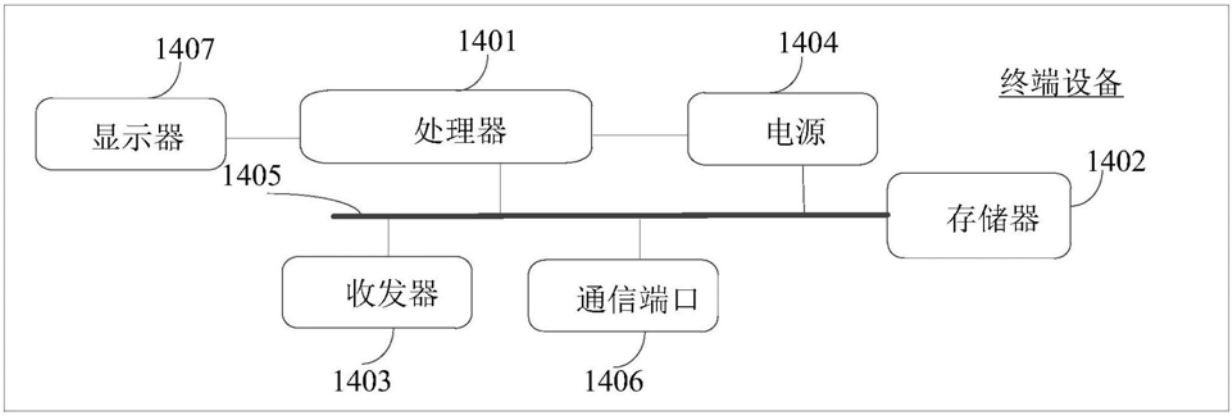

1407
1401
1404
终端设备
显示器
处理器
电源
1405
1402
存储器
收发器
通信端口
1403
1406

图14