(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 104219058 A
(43)申请公布日 2014.12.17

(21)申请号 201410509606.8

(22)申请日 2014.09.28

(71)申请人 小米科技有限责任公司
地址 100085 北京市海淀区清河中街68号华润五彩城购物中心二期13层

(72)发明人 黄柏林 丁亮 尹家进

(74)专利代理机构 北京尚伦律师事务所 11477
代理人 代治国

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

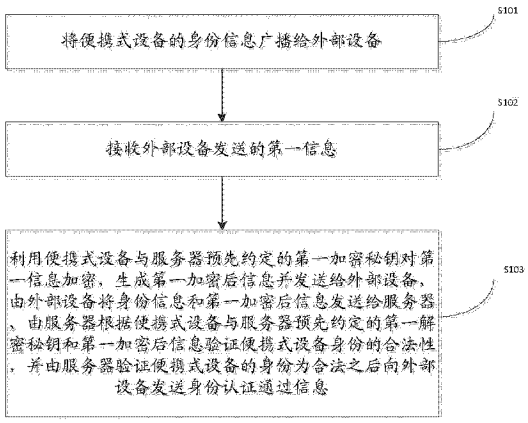
权利要求书5页 说明书17页 附图11页

(54)发明名称

身份认证、身份授权方法及装置

(57)摘要

本公开是关于身份认证、身份授权方法及装置，用以安全、便捷的完成身份认证、身份授权过程。身份认证的方法包括：将所述便携式设备的身份信息广播给外部设备；接收所述外部设备发送的第一信息；利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密，生成第一加密后信息并发送给所述外部设备，由所述外部设备将所述便携式设备的身份信息和第一加密后信息发送给所述服务器，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性，并由所述服务器验证所述便携式设备的身份为合法之后向所述外部设备发送身份认证通过信息。



CN 104219058 A

1. 一种身份认证方法，用于便携式设备，其特征在于，包括：

将所述便携式设备的身份信息广播给外部设备；

接收所述外部设备发送的第一信息；

利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密，生成第一加密后信息并发送给所述外部设备，由所述外部设备将所述便携式设备的身份信息和第一加密后信息发送给所述服务器，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性，并由所述服务器验证所述便携式设备的身份为合法之后向所述外部设备发送身份认证通过信息。

2. 根据权利要求 1 所述的方法，其特征在于，

所述第一信息为所述外部设备生成的随机码。

3. 根据权利要求 1 所述的方法，其特征在于，所述将所述便携式设备的身份信息广播给外部设备之后，所述方法还包括：

接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

检测所述外部设备是否为预先与所述便携式设备绑定的设备；

当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

4. 一种身份认证方法，用于外部设备，其特征在于，包括：

接收便携式设备的身份信息；

向所述便携式设备发送第一信息；

接收所述便携式设备发送的第一加密后信息，所述第一加密后信息由所述便携式设备利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密后生成；

向所述服务器发送所述便携式设备的身份信息和所述第一加密后信息，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性；

接收所述服务器验证所述便携式设备的身份为合法之后返回的身份认证通过信息。

5. 根据权利要求 4 所述的方法，其特征在于，包括：

所述第一信息为所述外部设备生成的随机码。

6. 根据权利要求 4 所述的方法，其特征在于，所述接收便携式设备的身份信息之后，所述方法还包括：

向服务器发送授权请求和所述便携式设备的身份信息；

接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

将所述第二加密信息发送给所述便携式设备；

接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

7. 一种身份授权方法，用于便携式设备，其特征在于，包括：

将所述便携式设备的身份信息广播给外部设备；

接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

检测所述外部设备是否为预先与所述便携式设备绑定的设备；

当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

8. 一种身份授权方法，用于外部设备，其特征在于，包括：

接收便携式设备的身份信息；

向服务器发送授权请求和所述便携式设备的身份信息；

接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

将所述第二加密信息发送给所述便携式设备；

接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

9. 一种身份认证装置，用于便携式设备，其特征在于，包括：

广播模块，用于将所述便携式设备的身份信息广播给外部设备；

第一接收模块，用于接收所述外部设备发送的第一信息；

加密模块，用于利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密，生成第一加密后信息并发送给所述外部设备，由所述外部设备将所述便携式设备的身份信息和第一加密后信息发送给所述服务器，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性，并由所述服务器验证所述便携式设备的身份为合法之后向所述外部设备发送身份认证通过信息。

10. 根据权利要求 9 所述的装置，其特征在于，所述装置还包括：

第二接收模块，用于在所述广播模块将所述便携式设备的身份信息广播给外部设备之后，接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

检测模块，用于检测所述外部设备是否为预先与所述便携式设备绑定的设备；

解密模块，用于当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

11. 一种身份认证装置，用于外部设备，其特征在于，包括：

第一接收模块，用于接收便携式设备的身份信息；

第一发送模块，用于向所述便携式设备发送第一信息；

第二接收模块，用于接收所述便携式设备发送的第一加密后信息，所述第一加密后信息由所述便携式设备利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密后生成；

第二发送模块，用于向所述服务器发送所述便携式设备的身份信息和所述第一加密后信息，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性；

第三接收模块，用于接收所述服务器验证所述便携式设备的身份为合法之后返回的身份认证通过信息。

12. 根据权利要求 11 所述的装置，其特征在于，所述装置还包括：

第三发送模块，用于在所述第一接收模块接收便携式设备的身份信息之后，向服务器发送授权请求和所述便携式设备的身份信息；

第四接收模块，用于接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

第四发送模块，用于将所述第二加密信息发送给所述便携式设备；

第五接收模块，用于接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

13. 一种身份授权装置，用于便携式设备，其特征在于，包括：

广播模块，用于将所述便携式设备的身份信息广播给外部设备；

接收模块，用于接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

检测模块，用于检测所述外部设备是否为预先与所述便携式设备绑定的设备；

解密模块，用于当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

14. 一种身份授权装置，用于外部设备，其特征在于，包括：

第一接收模块，用于接收便携式设备的身份信息；

第一发送模块，用于向服务器发送授权请求和所述身份信息；

第二接收模块，用于接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

第二发送模块，用于将所述第二加密信息发送给所述便携式设备；

第三接收模块，用于接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

15. 一种身份认证装置，用于便携式设备，其特征在于，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

将所述便携式设备的身份信息广播给外部设备；

接收所述外部设备发送的第一信息；

利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密，生成第一加密后信息并发送给所述外部设备，由所述外部设备将所述便携式设备的身份信息和第一加密后信息发送给所述服务器，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性，并由所述服务器验证所述便携式设备的身份为合法之后向所述外部设备发送身份认证通过信息。

16. 一种身份认证装置，用于外部设备，其特征在于，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

接收便携式设备的身份信息；

向所述便携式设备发送第一信息；

接收所述便携式设备发送的第一加密后信息，所述第一加密后信息由所述便携式设备利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密后生成；

向所述服务器发送所述便携式设备的身份信息和所述第一加密后信息，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性；

接收所述服务器验证所述便携式设备的身份为合法之后返回的身份认证通过信息。

17. 一种身份授权装置，用于便携式设备，其特征在于，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

将所述便携式设备的身份信息广播给外部设备；

接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

检测所述外部设备是否为预先与所述便携式设备绑定的设备；

当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

18. 一种身份授权装置，用于外部设备，其特征在于，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

接收便携式设备的身份信息；

向服务器发送授权请求和所述便携式设备的身份信息；

接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

将所述第二加密信息发送给所述便携式设备；

接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

身份认证、身份授权方法及装置

技术领域

[0001] 本公开涉及通讯技术领域，尤其涉及身份认证、身份授权方法及装置。

背景技术

[0002] 身份认证是确认操作者身份的过程，是保证系统安全的重要措施之一。当服务器提供服务时，需要确认来访者的身份，访问者有时也需要确认服务提供者的身份。密码技术在身份认证中起重要作用，相关技术中，主要通过用户输入密码或通过人脸识别、指纹识别等识别技术来验证用户身份。但用户输入密码比较麻烦，而且存在安全隐患；人脸识别、指纹识别技术同样需要用户进行操作，也比较麻烦。

发明内容

[0003] 为克服相关技术中存在的问题，本公开实施例提供身份认证、身份授权方法及装置，用以安全、便捷的完成身份认证、身份授权过程。

[0004] 根据本公开实施例的第一方面，提供一种身份认证方法，用于便携式设备，包括：

[0005] 将所述便携式设备的身份信息广播给外部设备；

[0006] 接收所述外部设备发送的第一信息；

[0007] 利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密，生成第一加密后信息并发送给所述外部设备，由所述外部设备将所述便携式设备的身份信息和第一加密后信息发送给所述服务器，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性，并由所述服务器验证所述便携式设备的身份为合法之后向所述外部设备发送身份认证通过信息。

[0008] 在一个实施例中，所述第一信息可以为所述外部设备生成的随机码。

[0009] 在一个实施例中，所述将所述便携式设备的身份信息广播给外部设备之后，所述方法还可包括：

[0010] 接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0011] 检测所述外部设备是否为预先与所述便携式设备绑定的设备；

[0012] 当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

[0013] 本公开的实施例提供的技术方案可以包括以下有益效果：

[0014] 本公开的技术方案利用便携式设备的便携性，通过便携式设备、外部设备、服务器之间一些验证信息的交互，来完成便携式设备的身份认证过程，从而验证便携式设备为合法设备，能够代表用户身份。此时，由于用户携带便携式设备，所以无需用户输入密码且无需用户进行操作便可安全、便捷的完成身份认证过程。

[0015] 根据本公开实施例的第二方面，提供一种身份认证方法，用于外部设备，包括：

[0016] 接收便携式设备的身份信息；

[0017] 向所述便携式设备发送第一信息；

[0018] 接收所述便携式设备发送的第一加密后信息，所述第一加密后信息由所述便携式设备利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密后生成；

[0019] 向所述服务器发送所述便携式设备的身份信息和所述第一加密后信息，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性；

[0020] 接收所述服务器验证所述便携式设备的身份为合法之后返回的身份认证通过信息。

[0021] 在一个实施例中，所述第一信息可以为所述外部设备生成的随机码。

[0022] 在一个实施例中，所述接收便携式设备的身份信息之后，所述方法还可包括：

[0023] 向服务器发送授权请求和所述便携式设备的身份信息；

[0024] 接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0025] 将所述第二加密信息发送给所述便携式设备；

[0026] 接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

[0027] 本公开的实施例提供的技术方案可以包括以下有益效果：

[0028] 本公开的技术方案利用便携式设备的便携性，通过便携式设备、外部设备、服务器之间一些验证信息的交互，来完成便携式设备的身份认证过程，从而验证便携式设备为合法设备，能够代表用户身份。此时，由于用户携带便携式设备，所以无需用户输入密码且无需用户进行操作便可安全、便捷的完成身份认证过程。

[0029] 根据本公开实施例的第三方面，提供一种身份授权方法，用于便携式设备，包括：

[0030] 将所述便携式设备的身份信息广播给外部设备；

[0031] 接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0032] 检测所述外部设备是否为预先与所述便携式设备绑定的设备；

[0033] 当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

[0034] 本公开的实施例提供的技术方案可以包括以下有益效果：

[0035] 本公开的技术方案通过服务器对外部设备发送的信息进行加密，便携式设备检验外部设备是否与其绑定，并对该信息进行解密来完成身份授权过程。该过程基于便携式设备的解密功能对外部设备完成身份授权，无需任何设备广播自身密钥，避免了因广播密钥导致的安全问题，提高了安全性。

[0036] 根据本公开实施例的第四方面，提供一种身份授权方法，用于外部设备，包括：

[0037] 接收便携式设备的身份信息；

[0038] 向服务器发送授权请求和所述便携式设备的身份信息；

[0039] 接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0040] 将所述第二加密信息发送给所述便携式设备；

[0041] 接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

[0042] 本公开的实施例提供的技术方案可以包括以下有益效果：

[0043] 本公开的技术方案通过服务器对外部设备发送的信息进行加密，便携式设备检验外部设备是否与其绑定，并对该信息进行解密来完成身份授权过程。该过程基于便携式设备的解密功能对外部设备完成身份授权，无需任何设备广播自身密钥，避免了因广播密钥导致的安全问题，提高了安全性。

[0044] 根据本公开实施例的第五方面，提供一种身份认证装置，用于便携式设备，包括：

[0045] 广播模块，用于将所述便携式设备的身份信息广播给外部设备；

[0046] 第一接收模块，用于接收所述外部设备发送的第一信息；

[0047] 加密模块，用于利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密，生成第一加密后信息并发送给所述外部设备，由所述外部设备将所述便携式设备的身份信息和第一加密后信息发送给所述服务器，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性，并由所述服务器验证所述便携式设备的身份为合法之后向所述外部设备发送身份认证通过信息。

[0048] 在一个实施例中，所述装置还可包括：

[0049] 第二接收模块，用于在所述广播模块将所述便携式设备的身份信息广播给外部设备之后，接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0050] 检测模块，用于检测所述外部设备是否为预先与所述便携式设备绑定的设备；

[0051] 解密模块，用于当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

[0052] 根据本公开实施例的第六方面，提供一种身份认证装置，用于外部设备，包括：

[0053] 第一接收模块，用于接收便携式设备的身份信息；

[0054] 第一发送模块，用于向所述便携式设备发送第一信息；

[0055] 第二接收模块，用于接收所述便携式设备发送的第一加密后信息，所述第一加密后信息由所述便携式设备利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密后生成；

[0056] 第二发送模块，用于向所述服务器发送所述便携式设备的身份信息和所述第一加

密后信息，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性；

[0057] 第三接收模块，用于接收所述服务器验证所述便携式设备的身份为合法之后返回的身份认证通过信息。

[0058] 在一个实施例中，所述第一信息可以为所述外部设备生成的随机码。

[0059] 在一个实施例中，所述装置还可包括：

[0060] 第三发送模块，用于在所述第一接收模块接收便携式设备的身份信息之后，向服务器发送授权请求和所述便携式设备的身份信息；

[0061] 第四接收模块，用于接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0062] 第四发送模块，用于将所述第二加密信息发送给所述便携式设备；

[0063] 第五接收模块，用于接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

[0064] 根据本公开实施例的第七方面，提供一种身份授权装置，用于便携式设备，包括：

[0065] 广播模块，用于将所述便携式设备的身份信息广播给外部设备；

[0066] 接收模块，用于接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0067] 检测模块，用于检测所述外部设备是否为预先与所述便携式设备绑定的设备；

[0068] 解密模块，用于当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

[0069] 根据本公开实施例的第八方面，提供一种身份授权装置，用于外部设备，包括：

[0070] 第一接收模块，用于接收便携式设备的身份信息；

[0071] 第一发送模块，用于向服务器发送授权请求和所述便携式设备的身份信息；

[0072] 第二接收模块，用于接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0073] 第二发送模块，用于将所述第二加密信息发送给所述便携式设备；

[0074] 第三接收模块，用于接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

[0075] 根据本公开实施例的第九方面，提供一种身份认证装置，用于便携式设备，包括：

[0076] 处理器；

[0077] 用于存储处理器可执行指令的存储器；

[0078] 其中，所述处理器被配置为：

[0079] 将所述便携式设备的身份信息广播给外部设备；

[0080] 接收所述外部设备发送的第一信息；

[0081] 利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密，生成第一加密后信息并发送给所述外部设备，由所述外部设备将所述便携式设备的身份信息和第一加密后信息发送给所述服务器，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性，并由所述服务器验证所述便携式设备的身份为合法之后向所述外部设备发送身份认证通过信息。

[0082] 根据本公开实施例的第十方面，提供一种身份认证装置，用于外部设备，包括：

[0083] 处理器；

[0084] 用于存储处理器可执行指令的存储器；

[0085] 其中，所述处理器被配置为：

[0086] 接收便携式设备的身份信息；

[0087] 向所述便携式设备发送第一信息；

[0088] 接收所述便携式设备发送的第一加密后信息，所述第一加密后信息由所述便携式设备利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密后生成；

[0089] 向所述服务器发送所述便携式设备的身份信息和所述第一加密后信息，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性；

[0090] 接收所述服务器验证所述便携式设备的身份为合法之后返回的身份认证通过信息。

[0091] 根据本公开实施例的第十一方面，提供一种身份授权装置，用于便携式设备，包括：

[0092] 处理器；

[0093] 用于存储处理器可执行指令的存储器；

[0094] 其中，所述处理器被配置为：

[0095] 将所述便携式设备的身份信息广播给外部设备；

[0096] 接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0097] 检测所述外部设备是否为预先与所述便携式设备绑定的设备；

[0098] 当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

[0099] 根据本公开实施例的第十二方面，提供一种身份授权装置，用于外部设备，包括：

[0100] 处理器；

[0101] 用于存储处理器可执行指令的存储器；

[0102] 其中，所述处理器被配置为：

[0103] 接收便携式设备的身份信息；

[0104] 向服务器发送授权请求和所述便携式设备的身份信息；

[0105] 接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0106] 将所述第二加密信息发送给所述便携式设备；

[0107] 接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

[0108] 本公开的实施例提供的技术方案可以包括以下有益效果：

[0109] 本公开的技术方案的身份认证和身份授权过程，利用便携式设备的便携性，通过便携式设备、外部设备、服务器之间一些验证和授权信息的交互，来完成便携式设备的身份认证和身份授权过程。此时，由于用户携带便携式设备，所以无需用户输入密码且无需用户进行操作便可安全、便捷的完成身份认证和身份授权过程。

[0110] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

[0111] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

[0112] 图 1 是根据一示例性实施例示出的一种身份认证方法的流程图。

[0113] 图 2 是根据一示例性实施例示出的另一种身份认证方法的流程图。

[0114] 图 3 是根据一示例性实施例示出的再一种身份认证方法的流程图

[0115] 图 4 是根据一示例性实施例示出的又一种身份认证方法的流程图

[0116] 图 5 是根据一示例性实施例一示出的身份认证方法的流程图。

[0117] 图 6 是根据一示例性实施例示出的一种身份授权方法的流程图。

[0118] 图 7 是根据一示例性实施例示出的另一种身份授权方法的流程图。

[0119] 图 8 是根据一示例性实施例二示出的身份授权方法的流程图。

[0120] 图 9 是根据一示例性实施例示出的一种身份认证装置的框图。

[0121] 图 10 是根据一示例性实施例示出的另一种身份认证装置的框图。

[0122] 图 11 是根据一示例性实施例示出的又一种身份认证装置的框图。

[0123] 图 12 是根据一示例性实施例示出的再一种身份认证装置的框图。

[0124] 图 13 是根据一示例性实施例示出的一种身份授权装置的框图。

[0125] 图 14 是根据一示例性实施例示出的另一种身份授权装置的框图。

[0126] 图 15 是根据一示例性实施例示出的一种适用于身份认证（或身份授权）装置的框图。

具体实施方式

[0127] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

[0128] 图 1 是根据一示例性实施例示出的一种身份认证方法的流程图，用于便携式设备，便携式设备可以是手机、智能可穿戴设备、掌上电脑等方便用户携带的智能终端设备。如图 1 所示，该方法包括以下步骤 S101-S103：

[0129] 在步骤 S101 中，将便携式设备的身份信息广播给外部设备。

[0130] 在一个实施例中，便携式设备的身份信息可以是便携式设备自身的设备 ID，或者其它能唯一标识便携式设备身份的标识信息。

[0131] 在步骤 S102 中，接收外部设备发送的第一信息。

[0132] 在一个实施例中，外部设备发送的第一信息可以是外部设备生成的一个随机码 S，也可以是外部设备预先设定的一信息。

[0133] 在步骤 S103 中，利用便携式设备与服务器预先约定的第一加密密钥对第一信息加密，生成第一加密后信息并发送给外部设备，由外部设备将便携式设备的身份信息和第一加密后信息发送给服务器，由服务器根据便携式设备与服务器预先约定的第一解密密钥和第一加密后信息验证便携式设备身份的合法性，并由服务器验证便携式设备的身份为合法之后向外部设备发送身份认证通过信息。

[0134] 其中，外部设备将便携式设备的身份信息和第一加密后信息发送给服务器之后，服务器可以根据该便携式设备的身份信息在自身存储的密钥中，查找到便携式设备与服务器预先约定的第一解密密钥，即，服务器中可以将便携式设备的身份信息、与便携式设备与服务器预先约定的第一解密密钥对应存储。

[0135] 本公开技术方案可以基于一种非对称加密算法（例如公钥加密算法），便携式设备在初始化时，需要写入第一加密密钥，并在服务器存储与第一加密密钥对应的第一解密密钥。例如第一加密密钥可以是私钥 A，第一解密密钥可以是公钥 A，公私钥对是唯一匹配的。

[0136] 本公开实施例提供的上述身份认证方法，利用便携式设备的便携性，通过便携式设备、外部设备、服务器之间一些验证信息的交互，来完成便携式设备的身份认证过程，从而验证便携式设备为合法设备，能够代表用户身份。此时，由于用户携带便携式设备，所以无需用户输入密码且无需用户进行操作便可安全、便捷的完成身份认证过程。

[0137] 在完成便携式设备的身份认证后，可以利用便携式设备提供的验证功能，提供额外的授权，授权外部设备实现一些功能（比如支付功能）。在一个实施例中，如图 2 所示，对便携式设备完成身份认证之后，上述方法还可包括以下步骤 S104-S106：

[0138] 在步骤 S104 中，接收外部设备发送的第二加密信息，第二加密信息是由外部设备将便携式设备的身份信息和授权请求发送给服务器后，由服务器根据便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成。

[0139] 其中，便携式设备的身份信息可以是便携式设备的设备 ID，或者其它能唯一标识便携式设备身份的标识信息。第二加密密钥可以是便携式设备与服务器预先约定并存储在服务器端的公钥 B。

[0140] 在步骤 S105 中，检测外部设备是否为预先与便携式设备绑定的设备。

[0141] 其中，预进行身份授权的外部设备需预先与便携式设备绑定，绑定后，外部设备为合法的外部设备。可以避免非绑定的外部设备通过窃取密钥来完成身份授权，提高安全性。

[0142] 在步骤 S106 中，当检测到外部设备为预先与便携式设备绑定的设备时，利用便携

式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密，得到授权码，将授权码发送给外部设备。

[0143] 本公开技术方案可基于一种非对称加密算法（例如公钥加密算法），便携式设备在初始化时，需要写入第二加密密钥，并在服务器存储与第二加密密钥对应的第二解密密钥。其中，第二解密密钥可以是便携式设备与服务器预先约定并存储在便携式设备内的私钥 B，公钥 B 和私钥 B 是唯一匹配的。

[0144] 本公开实施例提供的上述身份认证方法，利用便携式设备的便携性，通过便携式设备、外部设备、服务器之间一些验证信息的交互，来完成便携式设备的身份认证过程，从而验证便携式设备为合法设备，能够代表用户身份。此时，由于用户携带便携式设备，所以无需用户输入密码且无需用户进行操作便可安全、便捷的完成身份认证过程。

[0145] 对应前述用于便携式设备的身份认证方法，图 3 是根据一示例性实施例示出的另一种身份认证方法的流程图，用于外部设备，外部设备可以是门禁系统、手机、掌上电脑、身份验证系统等终端设备。如图 3 所示，该方法包括以下步骤 S201-S206：

[0146] 在步骤 S201 中，接收便携式设备的身份信息。

[0147] 在一个实施例中，便携式设备的身份信息可以是便携式设备自身的设备 ID，或者其它能唯一标识便携式设备身份的标识信息。

[0148] 在步骤 S202 中，向便携式设备发送第一信息。

[0149] 在一个实施例中，外部设备发送的第一信息可以是外部设备生成的一个随机码 S，也可以是外部设备预先设定的一信息。

[0150] 在步骤 S203 中，接收便携式设备发送的第一加密后信息，第一加密后信息由便携式设备利用便携式设备与服务器预先约定的第一加密密钥对第一信息加密后生成。

[0151] 在一个实施例中，第一信息为外部设备生成的随机码 S 时，第一加密密钥对该随机码 S 加密，记为 S’。S’为第一加密后信息。

[0152] 在步骤 S204 中，向服务器发送便携式设备的身份信息和第一加密后信息，由服务器根据便携式设备与服务器预先约定的第一解密密钥和第一加密后信息验证便携式设备身份的合法性。

[0153] 在一个实施例中，外部设备向服务器发送便携式设备的身份信息和第一加密后信息 S’，服务器使用与第一加密密钥唯一配对的第一解密密钥对第一加密后信息 S’解密，得到随机码 S，便对便携式设备完成了身份确认，确认便携式设备为合法设备。

[0154] 本公开技术方案可基于一种非对称加密算法（例如公钥加密算法），便携式设备在初始化时，需要写入第一加密密钥，并在服务器存储与第一加密密钥唯一匹配的第一解密密钥。例如第一加密密钥可以是私钥 A，第一解密密钥可以是公钥 A，公私钥对是唯一匹配的。

[0155] 在步骤 S205 中，接收服务器验证便携式设备的身份为合法之后返回的身份认证通过信息。

[0156] 服务器解密成功之后，说明便携式设备的身份为合法，向外部设备返回便携式设备的身份认证通过信息，外部设备接收便携式设备的身份认证通过信息，校验正确，完成身份认证。

[0157] 步骤 S201-S205 是对便携式设备的身份认证过程。在完成便携式设备的身份认

证后，便携式设备可以代表用户身份，利用便携式设备提供的验证功能，可以提供额外的授权，授权外部设备实现一些功能（比如支付功能）。在一个实施例中，如图 4 所示，对便携式设备完成身份认证之后，上述方法还可包括以下步骤 S206-S209 ：

[0158] 在步骤 S206 中，向服务器发送授权请求和便携式设备的身份信息。

[0159] 在一个实施例中，便携式设备的身份信息可以是便携式设备自身的设备 ID，或者其它能唯一标识便携式设备身份的标识信息。

[0160] 在步骤 S207 中，接收服务器发送的第二加密信息，第二加密信息由服务器根据便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成。

[0161] 在一个实施例中，授权码可以是外部设备预先设定的一信息。第二加密密钥可以是便携式设备与服务器预先约定并存储在服务器端的公钥 B。公钥 B 对授权码 T 加密生成第二加密信息 T’。

[0162] 在步骤 S208 中，将第二加密信息发送给便携式设备。

[0163] 在步骤 S209 中，接收便携式设备发送的授权码，授权码是由便携式设备检测到外部设备为预先与便携式设备绑定的设备后，利用便携式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密后得到。

[0164] 其中，预进行身份授权的外部设备需预先与便携式设备绑定，绑定后，外部设备为合法的外部设备。可以避免非绑定的外部设备通过窃取密钥来完成身份授权。第二解密密钥与第二加密密钥唯一配对，第二解密密钥对第二加密信息 T’ 解密得到授权码 T。

[0165] 下面以具体实施例来说明本公开实施例提供的上述技术方案。

[0166] 实施例一

[0167] 实施例一利用本公开实施例提供的身份认证方法，用于便携式设备，其中便携式设备为智能手环，外部设备为门禁系统，便携式设备的身份信息为智能手环的 ID，第一信息为门禁系统生成的随机码，第一加密密钥为私钥 A，第一解密密钥为公钥 A。其应用场景为，用户佩戴智能手环，欲通过智能手环来打开门禁系统，如图 5 所示，智能手环接下来进行如下操作 ：

[0168] 在步骤 S301 中，智能手环将自身 ID 广播给门禁系统。

[0169] 在步骤 S302 中，智能手环接收门禁系统发送的随机码 S。

[0170] 在步骤 S303 中，智能手环使用初始化时存入的私钥 A 对随机码 S 加密，生成 S’，并将 S’ 发送给门禁系统，由门禁系统将智能手环的 ID 和 S’ 发送给服务器，由服务器使用与私钥 A 唯一配对的公钥 A 对 S’解密，获得随机码 S。即验证了智能手环的身份合法，由服务器向门禁系统发送智能手环身份认证通过信息。

[0171] 在步骤 S304 中，由门禁系统接收智能手环身份认证通过信息，完成智能手环的身份认证，门禁自动打开。

[0172] 实施例一，利用智能手环的便携性，对智能手环进行身份认证，由于用户佩戴智能手环，所以无需用户输入密码且无需用户进行操作便可安全、便捷的完成身份认证过程。

[0173] 通过私钥对随机码进行加密，并在服务器端利用公钥对其解密来完成智能手环的身份认证过程，该方法无需广播智能手环的密钥，避免了因为广播密钥产生的安全问题，提高了安全性。

[0174] 图 6 是根据一示例性实施例示出的另一种身份授权方法的流程图，用于便携式设

备，便携式设备可以是手机、智能可穿戴设备、掌上电脑等便于携带的终端设备。如图 6 所示，该方法包括以下步骤 S401-S404 ：

[0175] 在步骤 S401 中，将便携式设备的身份信息广播给外部设备。

[0176] 在步骤 S402 中，接收外部设备发送的第二加密信息，第二加密信息是由外部设备将便携式设备的便携式设备的身份信息和授权请求发送给服务器后，由服务器根据便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成。

[0177] 在步骤 S403 中，检测外部设备是否为预先与便携式设备绑定的设备。

[0178] 在步骤 S404 中，当检测到外部设备为预先与便携式设备绑定的设备时，利用便携式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密，得到授权码，将授权码发送给外部设备。

[0179] 图 7 是根据一示例性实施例示出的另一种身份授权方法的流程图，用于外部设备，外部设备可以是门禁系统、手机、掌上电脑、身份验证系统等终端设备。如图 7 所示，该方法包括以下步骤 S501-S505 ：

[0180] 在步骤 S501 中，接收便携式设备的身份信息。

[0181] 在步骤 S502 中，向服务器发送授权请求和便携式设备的便携式设备的身份信息。

[0182] 在步骤 S503 中，接收服务器发送的第二加密信息，第二加密信息由服务器根据便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成。

[0183] 在步骤 S504 中，将第二加密信息发送给便携式设备。

[0184] 在步骤 S505 中，接收便携式设备发送的授权码，授权码是由便携式设备检测到外部设备为预先与便携式设备绑定的设备后，利用便携式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密后得到。

[0185] 下面以具体实施例来说明本公开实施例提供的上述技术方案。

[0186] 实施例二

[0187] 实施例二利用本公开实施例提供的身份授权方法，用于便携式设备，其中，便携式设备为智能手表，外部设备为手机，便携式设备的身份信息智能手表的 ID 为，第二加密密钥为公钥 B，第二解密密钥为私钥 B。其应用场景为，智能手表已利用步骤 S101-S103 的方法完成了身份认证，现利用智能手表对手机进行授权，允许其在手机上进行支付操作。如图 8 所示，该方法包括如下步骤 S601-S605 ：

[0188] 在步骤 S601 中，智能手表将自身 ID 广播给手机。

[0189] 在步骤 S602 中，智能手表接收手机发送的第二加密信息，第二加密信息是由手机将智能手表的 ID 和授权请求发送给服务器后，由服务器根据智能手表与服务器预先约定的公钥 B 对授权码 T 加密后生成。

[0190] 在步骤 S603 中，智能手表检测手机是否为预先与智能手表绑定的设备。

[0191] 在步骤 S604 中，当检测到手机为与智能手表绑定的设备时，利用智能手表与服务器预先约定的私钥 B 对第二加密信息进行解密，得到授权码 T，将授权码 T 发送给手机。

[0192] 在步骤 S605 中，手机使用授权码进行相关操作（例如用手机进行支付）。

[0193] 实施例二，通过在服务器利用公钥对授权码进行加密，在智能手表中利用私钥对其解密来完成对手机的授权操作，由于用户佩戴智能手表，所以无需用户输入密码且无需用户进行操作便可安全、便捷的完成身份认证过程。

[0194] 图 9 是根据一示例性实施例示出的一种身份认证装置的框图，用于便携式设备，如图 9 所示，上述装置包括：

[0195] 广播模块 91，用于将便携式设备的身份信息广播给外部设备。

[0196] 第一接收模块 92，用于接收外部设备发送的第一信息。

[0197] 加密模块 93，用于利用便携式设备与服务器预先约定的第一加密密钥对第一信息加密，生成第一加密后信息并发送给外部设备，由外部设备将便携式设备的身份信息和第一加密后信息发送给服务器，由服务器根据便携式设备与服务器预先约定的第一解密密钥和第一加密后信息验证便携式设备身份的合法性，并由服务器验证便携式设备的身份为合法之后向外部设备发送身份认证通过信息。

[0198] 在一个实施例中，如图 10 所示，上述装置还可包括：

[0199] 第二接收模块 94，用于在所述广播模块将所述便携式设备的身份信息广播给外部设备之后，接收外部设备发送的第二加密信息，第二加密信息是由外部设备将便携式设备的身份信息和授权请求发送给服务器后，由服务器根据便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0200] 检测模块 95，用于检测外部设备是否为预先与便携式设备绑定的设备；

[0201] 解密模块 96，用于当检测到外部设备为预先与便携式设备绑定的设备时，利用便携式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密，得到授权码，将授权码发送给外部设备。

[0202] 图 11 是根据一示例性实施例示出的一种身份认证装置的框图，用于外部设备，如图 11 所示，上述装置包括：

[0203] 第一接收模块 111，用于接收便携式设备的身份信息。

[0204] 第一发送模块 112，用于向便携式设备发送第一信息。

[0205] 第二接收模块 113，用于接收便携式设备发送的第一加密后信息，第一加密后信息由便携式设备利用便携式设备与服务器预先约定的第一加密密钥对第一信息加密后生成。

[0206] 第二发送模块 114，用于向服务器发送便携式设备的身份信息和第一加密后信息，由服务器根据便携式设备与服务器预先约定的第一解密密钥和第一加密后信息验证便携式设备身份的合法性。

[0207] 第三接收模块 115，用于接收服务器验证便携式设备的身份为合法之后返回的身份认证通过信息。

[0208] 在一个实施例中，第一信息可以为外部设备生成的随机码。

[0209] 在一个实施例中，如图 12 所示，上述装置还可包括：

[0210] 第三发送模块 116，用于在所述第一接收模块接收便携式设备的身份信息之后，向服务器发送授权请求和便携式设备的身份信息；

[0211] 第四接收模块 117，用于接收服务器发送的第二加密信息，第二加密信息由服务器根据便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0212] 第四发送模块 118，用于将第二加密信息发送给便携式设备；

[0213] 第五接收模块 119，用于接收便携式设备发送的授权码，授权码是由便携式设备检测到外部设备为预先与便携式设备绑定的设备后，利用便携式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密后得到。

[0214] 图 13 是根据一示例性实施例示出的一种身份授权装置的框图，用于便携式设备，如图 13 所示，上述装置包括：

[0215] 广播模块 131，用于将便携式设备的身份信息广播给外部设备；

[0216] 接收模块 132，用于接收外部设备发送的第二加密信息，第二加密信息是由外部设备将便携式设备的身份信息和授权请求发送给服务器后，由服务器根据便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0217] 检测模块 133，用于检测外部设备是否为预先与便携式设备绑定的设备；

[0218] 解密模块 134，用于当检测到外部设备为预先与便携式设备绑定的设备时，利用便携式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密，得到授权码，将授权码发送给外部设备。

[0219] 图 14 是根据一示例性实施例示出的另一种身份授权装置的框图，用于外部设备，如图 14 所示，上述装置包括：

[0220] 第一接收模块 141，用于接收便携式设备的身份信息；

[0221] 第一发送模块 142，用于向服务器发送授权请求和便携式设备的身份信息；

[0222] 第二接收模块 143，用于接收服务器发送的第二加密信息，第二加密信息由服务器根据便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0223] 第二发送模块 144，用于将第二加密信息发送给便携式设备；

[0224] 第三接收模块 145，用于接收便携式设备发送的授权码，授权码是由便携式设备检测到外部设备为预先与便携式设备绑定的设备后，利用便携式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密后得到。

[0225] 本公开实施例提供的上述身份认证及身份授权装置，利用便携式设备的便携性，通过便携式设备、外部设备、服务器之间一些验证信息的交互，来完成便携式设备的身份认证过程，从而验证便携式设备为合法设备，能够代表用户身份。此时，由于用户携带便携式设备，所以无需用户输入密码且无需用户进行操作便可安全、便捷的完成身份认证过程。

[0226] 关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

[0227] 图 15 是根据一示例性实施例示出的一种用于身份认证（或身份授权）装置 1400 的框图，该装置适用于终端设备。例如，装置 1400 可以是移动电话，计算机，数字广播终端，消息收发设备，游戏控制台，平板设备，医疗设备，健身设备，个人数字助理等。

[0228] 参照图 15，装置 1500 可以包括以下一个或多个组件：处理组件 1502，存储器 1504，电源组件 1506，多媒体组件 1508，音频组件 1510，输入 / 输出 (I/O) 的接口 1512，传感器组件 1514，以及通信组件 1516。

[0229] 处理组件 1502 通常控制装置 1500 的整体操作，诸如与显示，电话呼叫，数据通信，相机操作和记录操作相关联的操作。处理元件 1502 可以包括一个或多个处理器 1520 来执行指令，以完成上述的方法的全部或部分步骤。此外，处理组件 1502 可以包括一个或多个模块，便于处理组件 1502 和其他组件之间的交互。例如，处理部件 1502 可以包括多媒体模块，以方便多媒体组件 1508 和处理组件 1502 之间的交互。

[0230] 存储器 1504 被配置为存储各种类型的数据以支持在设备 1500 的操作。这些数据的示例包括用于在装置 1500 上操作的任何应用程序或方法的指令，联系人数据，电话簿数

据，消息，图片，视频等。存储器 1504 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器 (SRAM)，电可擦除可编程只读存储器 (EEPROM)，可擦除可编程只读存储器 (EPROM)，可编程只读存储器 (PROM)，只读存储器 (ROM)，磁存储器，快闪存储器，磁盘或光盘。

[0231] 电力组件 1506 为装置 1500 的各种组件提供电力。电力组件 1506 可以包括电源管理系统，一个或多个电源，及其他与为装置 1500 生成、管理和分配电力相关联的组件。

[0232] 多媒体组件 1508 包括在装置 1500 和用户之间的提供一个输出接口的屏幕。在一些实施例中，屏幕可以包括液晶显示器 (LCD) 和触摸面板 (TP)。如果屏幕包括触摸面板，屏幕可以被实现为触摸屏，以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界，而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中，多媒体组件 1508 包括一个前置摄像头和 / 或后置摄像头。当设备 1500 处于操作模式，如拍摄模式或视频模式时，前置摄像头和 / 或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

[0233] 音频组件 1510 被配置为输出和 / 或输入音频信号。例如，音频组件 1510 包括一个麦克风 (MIC)，当装置 1500 处于操作模式，如呼叫模式、记录模式和语音识别模式时，麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 1504 或经由通信组件 1516 发送。在一些实施例中，音频组件 1510 还包括一个扬声器，用于输出音频信号。

[0234] I/O 接口 1512 为处理组件 1502 和外围接口模块之间提供接口，上述外围接口模块可以是键盘，点击轮，按钮等。这些按钮可包括但不限于 :主页按钮、音量按钮、启动按钮和锁定按钮。

[0235] 传感器组件 1514 包括一个或多个传感器，用于为装置 1500 提供各个方面的状态评估。例如，传感器组件 1514 可以检测到设备 1500 的打开 / 关闭状态，组件的相对定位，例如所述组件为装置 1500 的显示器和小键盘，传感器组件 1514 还可以检测装置 1500 或装置 1500 一个组件的位置改变，用户与装置 1500 接触的存在或不存在，装置 1500 方位或加速 / 减速和装置 1500 的温度变化。传感器组件 1514 可以包括接近传感器，被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件 1514 还可以包括光传感器，如 CMOS 或 CCD 图像传感器，用于在成像应用中使用。在一些实施例中，该传感器组件 1514 还可以包括加速度传感器，陀螺仪传感器，磁传感器，压力传感器或温度传感器。

[0236] 通信组件 1516 被配置为便于装置 1500 和其他设备之间有线或无线方式的通信。装置 1500 可以接入基于通信标准的无线网络，如 WiFi，2G 或 3G，或它们的组合。在一个示例性实施例中，通信部件 1516 经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信部件 1516 还包括近场通信 (NFC) 模块，以促进短程通信。例如，在 NFC 模块可基于射频识别 (RFID) 技术，红外数据协会 (IrDA) 技术，超宽带 (UWB) 技术，蓝牙 (BT) 技术和其他技术来实现。

[0237] 在示例性实施例中，装置 1500 可以被一个或多个应用专用集成电路 (ASIC)、数字信号处理器 (DSP)、数字信号处理设备 (DSPD)、可编程逻辑器件 (PLD)、现场可编程门阵列 (FPGA)、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述方法。

[0238] 在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器1504，上述指令可由装置1500的处理器820执行以完成上述方法。例如，所述非临时性计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0239] 一种身份认证装置，包括：

[0240] 处理器；

[0241] 用于存储处理器可执行指令的存储器；

[0242] 其中，所述处理器被配置为：

[0243] 将所述便携式设备的身份信息广播给外部设备；

[0244] 接收所述外部设备发送的第一信息；

[0245] 利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密，生成第一加密后信息并发送给所述外部设备，由所述外部设备将所述便携式设备的身份信息和第一加密后信息发送给所述服务器，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性，并由所述服务器验证所述便携式设备的身份为合法之后向所述外部设备发送身份认证通过信息。

[0246] 该处理器还被配置为：所述第一信息可以为所述外部设备生成的随机码。

[0247] 该处理器还被配置为：所述将所述便携式设备的身份信息广播给外部设备之后，所述方法还可包括：

[0248] 接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0249] 检测所述外部设备是否为预先与所述便携式设备绑定的设备；

[0250] 当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

[0251] 一种身份认证装置，包括：

[0252] 处理器；

[0253] 用于存储处理器可执行指令的存储器；

[0254] 其中，所述处理器被配置为：

[0255] 接收便携式设备的身份信息；

[0256] 向所述便携式设备发送第一信息；

[0257] 接收所述便携式设备发送的第一加密后信息，所述第一加密后信息由所述便携式设备利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密后生成；

[0258] 向所述服务器发送所述便携式设备的身份信息和所述第一加密后信息，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性；

[0259] 接收所述服务器验证所述便携式设备的身份为合法之后返回的身份认证通过信息。

[0260] 该处理器还被配置为：所述第一信息可以为所述外部设备生成的随机码。

[0261] 该处理器还被配置为：所述接收便携式设备的身份信息之后，所述方法还可包括：

[0262] 向服务器发送授权请求和所述便携式设备的身份信息；

[0263] 接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0264] 将所述第二加密信息发送给所述便携式设备；

[0265] 接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

[0266] 一种身份授权装置，包括：

[0267] 处理器；

[0268] 用于存储处理器可执行指令的存储器；

[0269] 其中，所述处理器被配置为：

[0270] 将所述便携式设备的身份信息广播给外部设备；

[0271] 接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0272] 检测所述外部设备是否为预先与所述便携式设备绑定的设备；

[0273] 当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

[0274] 一种身份授权装置，包括：

[0275] 处理器；

[0276] 用于存储处理器可执行指令的存储器；

[0277] 其中，所述处理器被配置为：

[0278] 接收便携式设备的身份信息；

[0279] 向服务器发送授权请求和所述便携式设备的身份信息；

[0280] 接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0281] 将所述第二加密信息发送给所述便携式设备；

[0282] 接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

[0283] 一种非临时性计算机可读存储介质，当所述存储介质中的指令由移动终端的处理器执行时，使得移动终端能够执行一种身份认证方法，所述方法包括：

[0284] 将所述便携式设备的身份信息广播给外部设备；

[0285] 接收所述外部设备发送的第一信息；

[0286] 利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密，生

成第一加密后信息并发送给所述外部设备，由所述外部设备将所述便携式设备的身份信息和第一加密后信息发送给所述服务器，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性，并由所述服务器验证所述便携式设备的身份为合法之后向所述外部设备发送身份认证通过信息。

[0287] 所述第一信息可以为所述外部设备生成的随机码。

[0288] 所述将所述便携式设备的身份信息广播给外部设备之后，所述方法还可包括：

[0289] 接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0290] 检测所述外部设备是否为预先与所述便携式设备绑定的设备；

[0291] 当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

[0292] 一种非临时性计算机可读存储介质，当所述存储介质中的指令由移动终端的处理器执行时，使得移动终端能够执行一种身份认证方法，所述方法包括：

[0293] 接收便携式设备的身份信息；

[0294] 向所述便携式设备发送第一信息；

[0295] 接收所述便携式设备发送的第一加密后信息，所述第一加密后信息由所述便携式设备利用所述便携式设备与服务器预先约定的第一加密密钥对所述第一信息加密后生成；

[0296] 向所述服务器发送所述便携式设备的身份信息和所述第一加密后信息，由所述服务器根据所述便携式设备与所述服务器预先约定的第一解密密钥和第一加密后信息验证所述便携式设备身份的合法性；

[0297] 接收所述服务器验证所述便携式设备的身份为合法之后返回的身份认证通过信息。

[0298] 所述第一信息可以为所述外部设备生成的随机码。

[0299] 所述接收便携式设备的身份信息之后，所述方法还可包括：

[0300] 向服务器发送授权请求和所述便携式设备的身份信息；

[0301] 接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0302] 将所述第二加密信息发送给所述便携式设备；

[0303] 接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

[0304] 一种非临时性计算机可读存储介质，当所述存储介质中的指令由移动终端的处理器执行时，使得移动终端能够执行一种身份授权方法，所述方法包括：

[0305] 将所述便携式设备的身份信息广播给外部设备；

[0306] 接收外部设备发送的第二加密信息，所述第二加密信息是由所述外部设备将所述便携式设备的身份信息和授权请求发送给服务器后，由所述服务器根据所述便携式设备与

服务器预先约定的第二加密密钥对授权码加密后生成；

[0307] 检测所述外部设备是否为预先与所述便携式设备绑定的设备；

[0308] 当检测到所述外部设备为预先与所述便携式设备绑定的设备时，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密，得到授权码，将所述授权码发送给所述外部设备。

[0309] 一种非临时性计算机可读存储介质，当所述存储介质中的指令由移动终端的处理器执行时，使得移动终端能够执行一种身份授权方法，所述方法包括：

[0310] 接收便携式设备的身份信息；

[0311] 向服务器发送授权请求和所述便携式设备的身份信息；

[0312] 接收所述服务器发送的第二加密信息，所述第二加密信息由所述服务器根据所述便携式设备与服务器预先约定的第二加密密钥对授权码加密后生成；

[0313] 将所述第二加密信息发送给所述便携式设备；

[0314] 接收所述便携式设备发送的授权码，所述授权码是由所述便携式设备检测到所述外部设备为预先与所述便携式设备绑定的设备后，利用所述便携式设备与服务器预先约定的第二解密密钥对所述第二加密信息进行解密后得到。

[0315] 本领域技术人员在考虑说明书及实践这里公开的公开后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

[0316] 应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

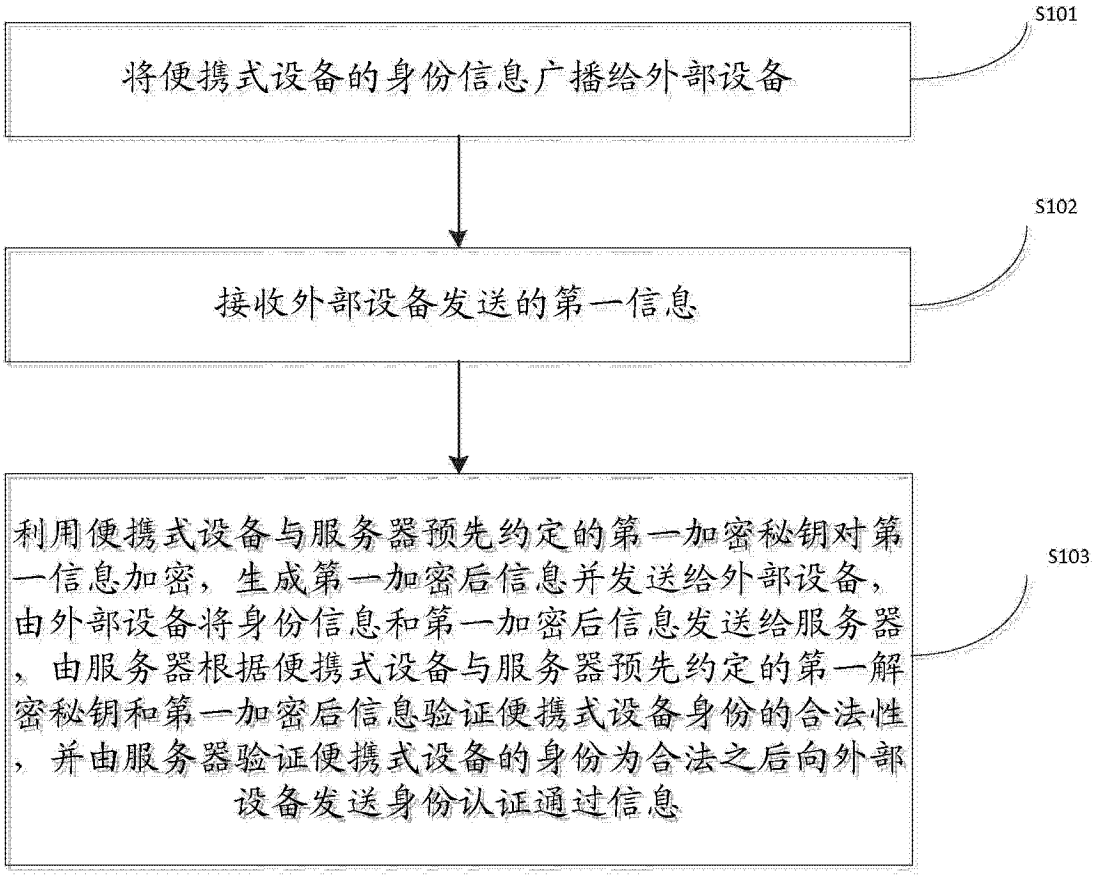

S101
将便携式设备的身份信息广播给外部设备
S102
接收外部设备发送的第一信息
S103
利用便携式设备与服务器预先约定的第一加密秘钥对第一信息加密，生成第一加密后信息并发送给外部设备，由外部设备将身份信息和第一加密后信息发送给服务器，由服务器根据便携式设备与服务器预先约定的第一解密秘钥和第一加密后信息验证便携式设备身份的合法性，并由服务器验证便携式设备的身份为合法之后向外部设备发送身份认证通过信息

图 1

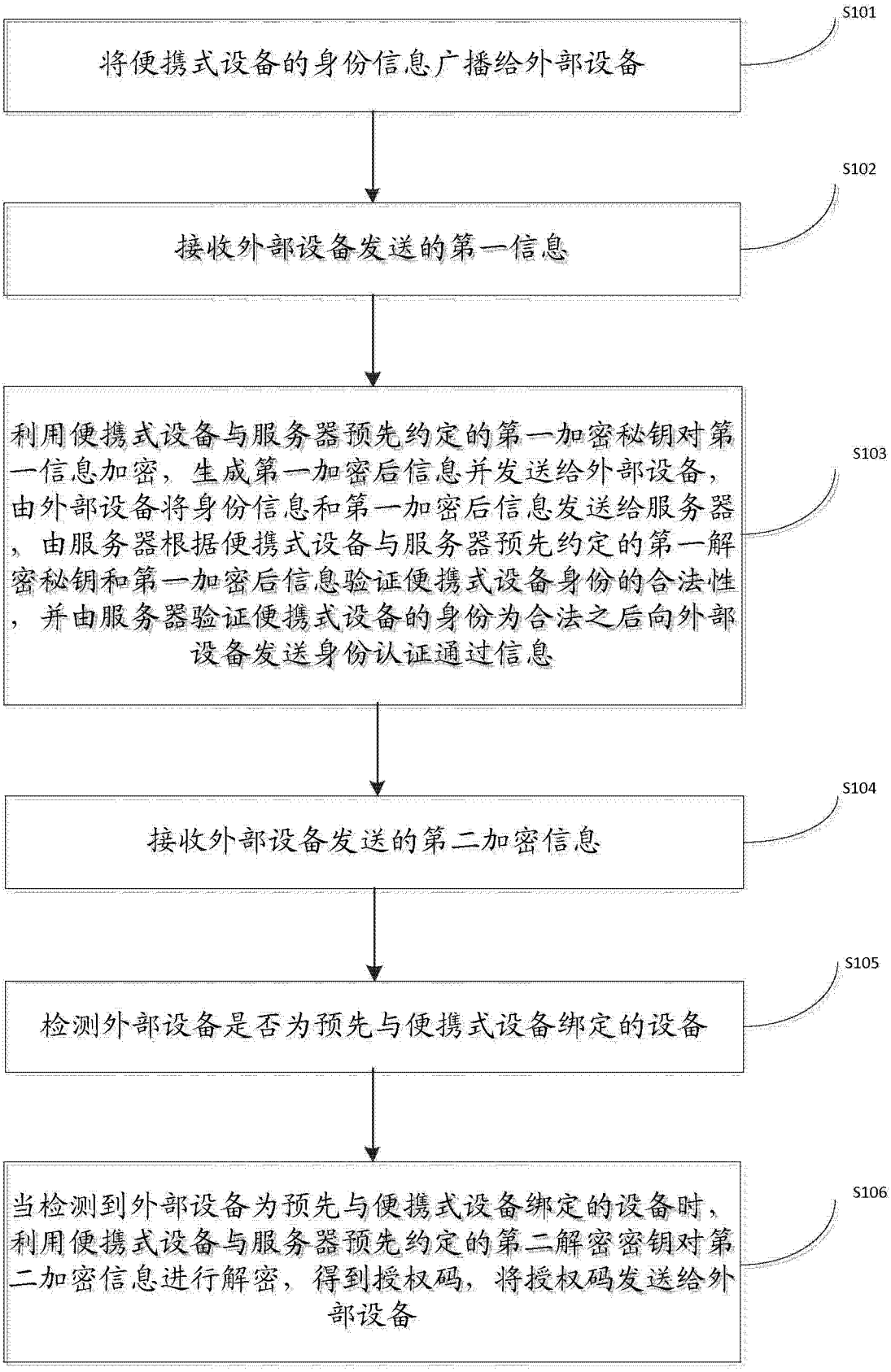

S101
将便携式设备的身份信息广播给外部设备
S102
接收外部设备发送的第一信息
S103
利用便携式设备与服务器预先约定的第一加密秘钥对第一信息加密，生成第一加密后信息并发送给外部设备，由外部设备将身份信息和第一加密后信息发送给服务器，由服务器根据便携式设备与服务器预先约定的第一解密秘钥和第一加密后信息验证便携式设备身份的合法性，并由服务器验证便携式设备的身份为合法之后向外部设备发送身份认证通过信息
S104
接收外部设备发送的第二加密信息
S105
检测外部设备是否为预先与便携式设备绑定的设备
S106
当检测到外部设备为预先与便携式设备绑定的设备时，利用便携式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密，得到授权码，将授权码发送给外部设备

图 2

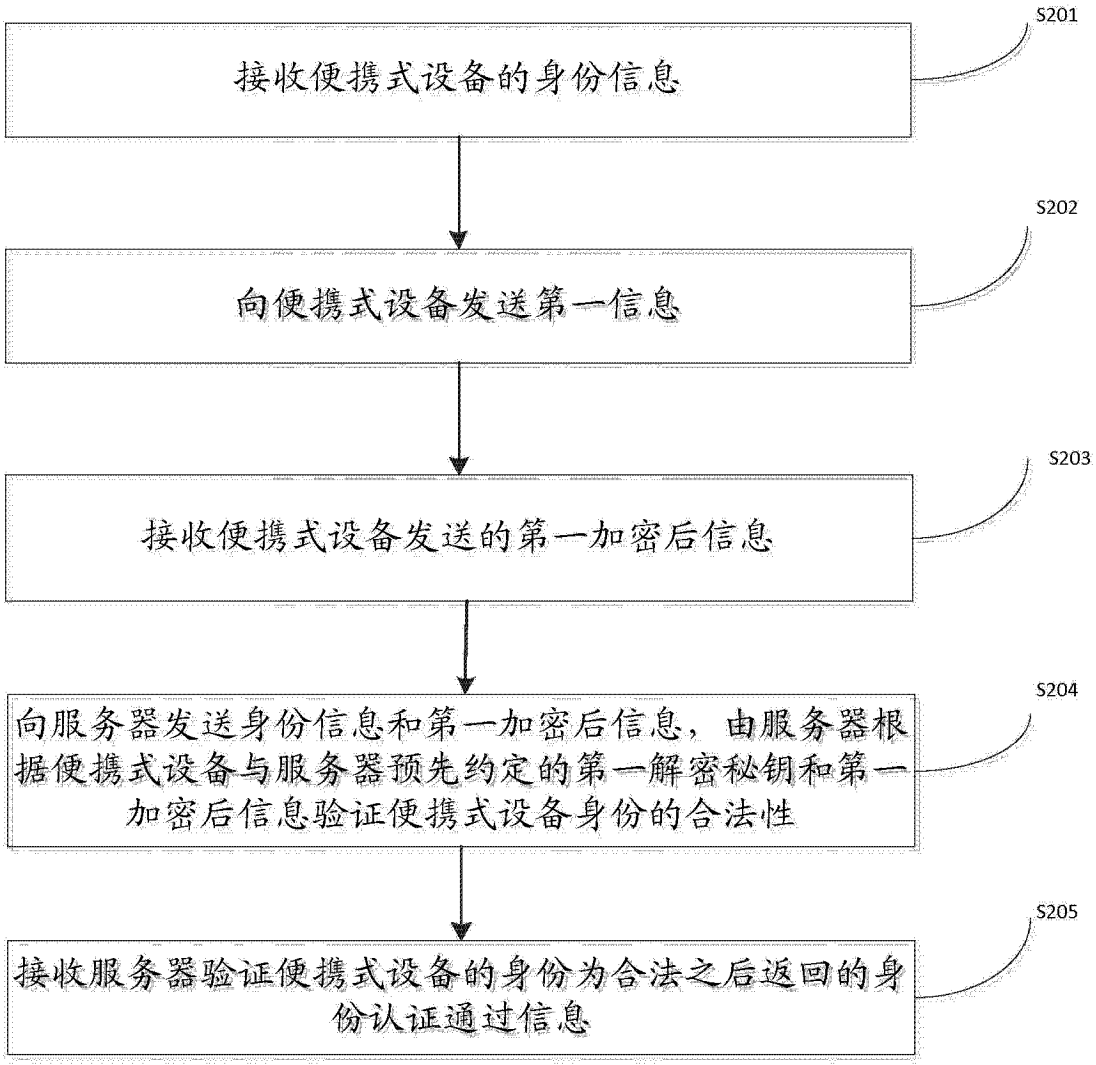

S201
接收便携式设备的身份信息
S202
向便携式设备发送第一信息
S203
接收便携式设备发送的第一加密后信息
S204
向服务器发送身份信息和第一加密后信息，由服务器根据便携式设备与服务器预先约定的第一解密秘钥和第一加密后信息验证便携式设备身份的合法性
S205
接收服务器验证便携式设备的身份为合法之后返回的身份认证通过信息

图 3

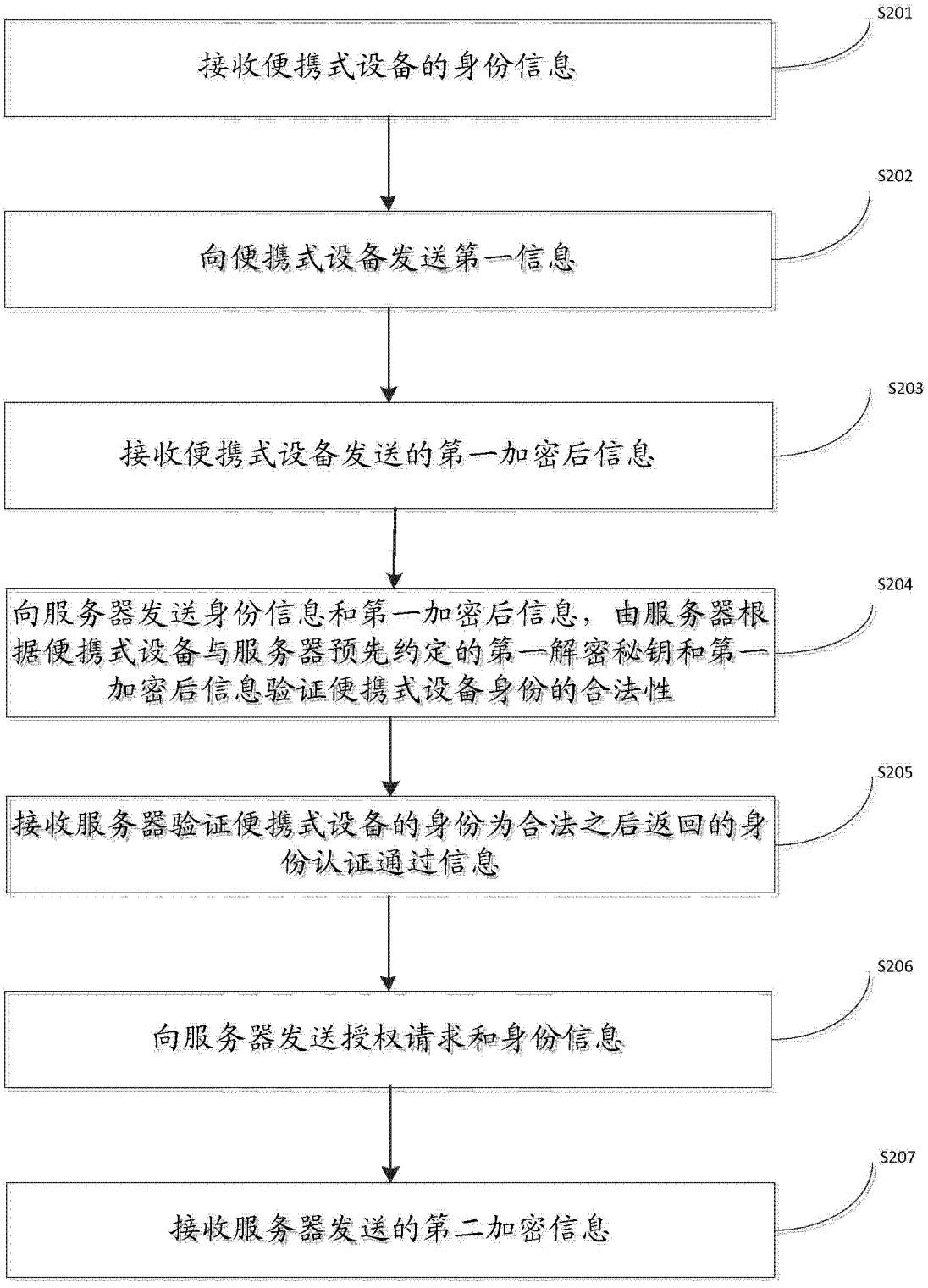

S201
接收便携式设备的身份信息
S202
向便携式设备发送第一信息
S203
接收便携式设备发送的第一加密后信息
S204
向服务器发送身份信息和第一加密后信息，由服务器根据便携式设备与服务器预先约定的第一解密秘钥和第一加密后信息验证便携式设备身份的合法性
S205
接收服务器验证便携式设备的身份为合法之后返回的身份认证通过信息
S206
向服务器发送授权请求和身份信息
S207
接收服务器发送的第二加密信息

图 4

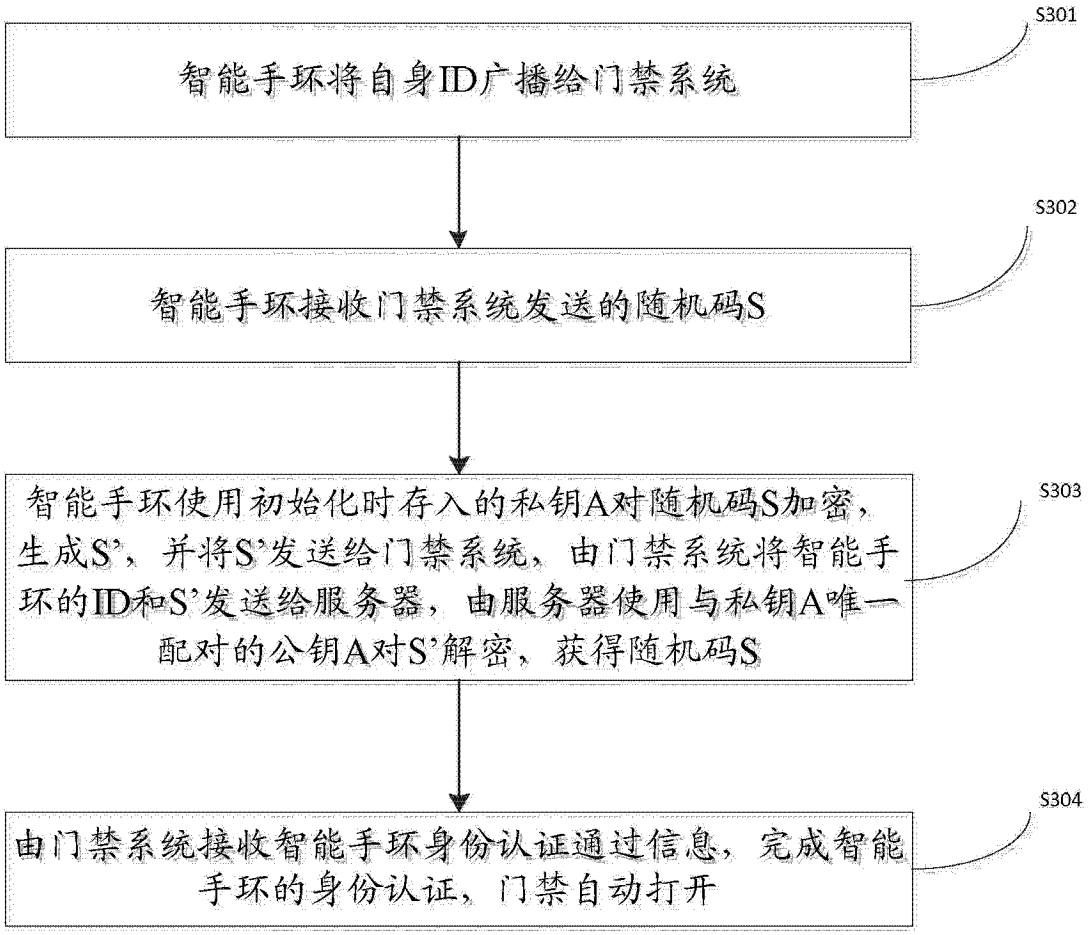

S301
智能手环将自身ID广播给门禁系统
S302
智能手环接收门禁系统发送的随机码S
S303
智能手环使用初始化时存入的私钥A对随机码S加密，生成S'，并将S'发送给门禁系统，由门禁系统将智能手环的ID和S'发送给服务器，由服务器使用与私钥A唯一配对的公钥A对S'解密，获得随机码S
S304
由门禁系统接收智能手环身份认证通过信息，完成智能手环的身份认证，门禁自动打开

图 5

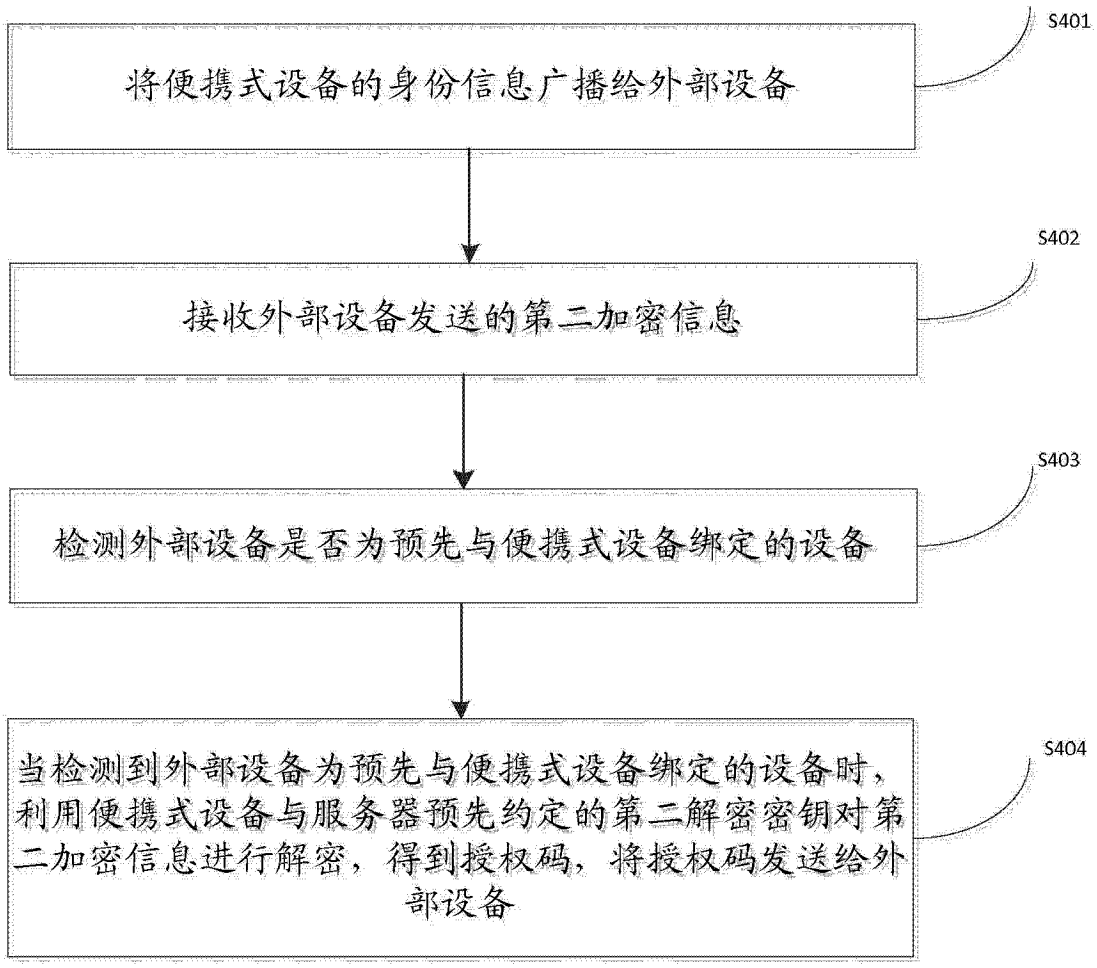

S401
将便携式设备的身份信息广播给外部设备
S402
接收外部设备发送的第二加密信息
S403
检测外部设备是否为预先与便携式设备绑定的设备
S404
当检测到外部设备为预先与便携式设备绑定的设备时，利用便携式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密，得到授权码，将授权码发送给外部设备

图 6

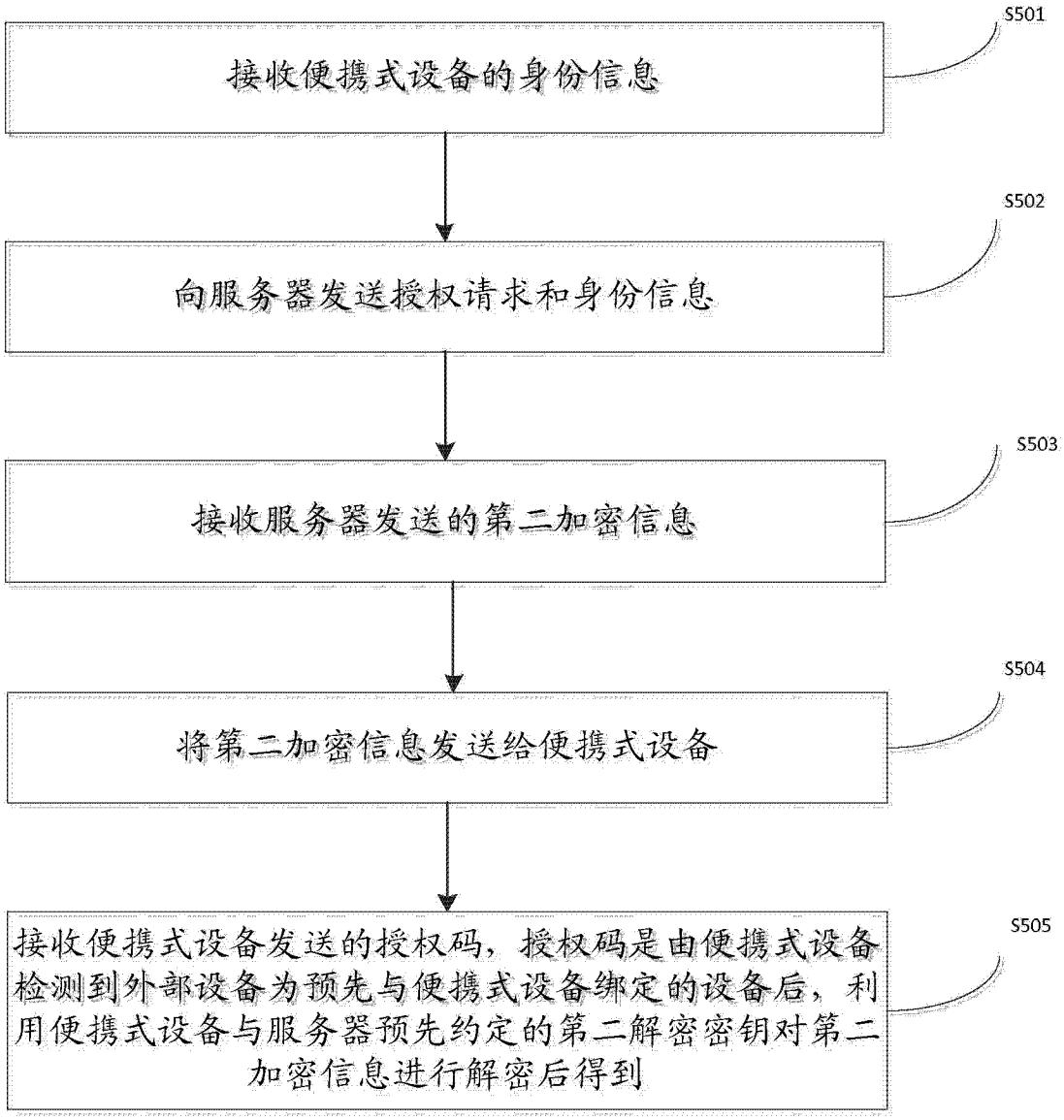

S501
接收便携式设备的身份信息
S502
向服务器发送授权请求和身份信息
S503
接收服务器发送的第二加密信息
S504
将第二加密信息发送给便携式设备
S505
接收便携式设备发送的授权码，授权码是由便携式设备检测到外部设备为预先与便携式设备绑定的设备后，利用便携式设备与服务器预先约定的第二解密密钥对第二加密信息进行解密后得到

图 7

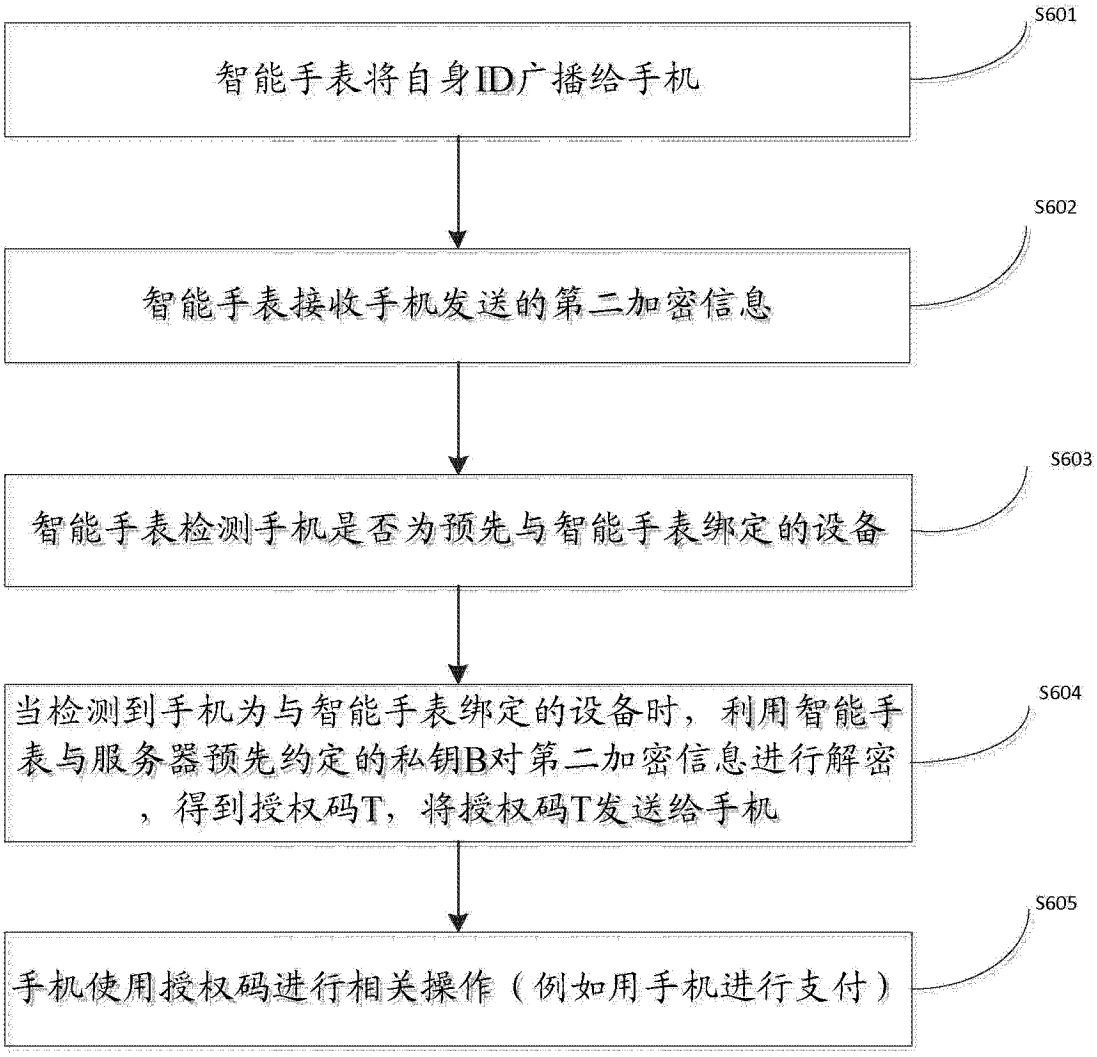

S601
智能手表将自身ID广播给手机
S602
智能手表接收手机发送的第二加密信息
S603
智能手表检测手机是否为预先与智能手表绑定的设备
S604
当检测到手机为与智能手表绑定的设备时，利用智能手表与服务器预先约定的私钥B对第二加密信息进行解密，得到授权码T，将授权码T发送给手机
S605
手机使用授权码进行相关操作（例如用手机进行支付）

图 8

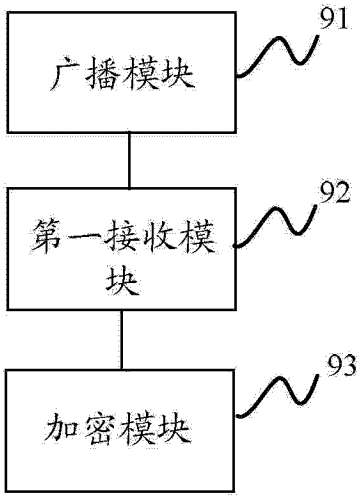

91
广播模块
92
第一接收模块
93
加密模块

图 9

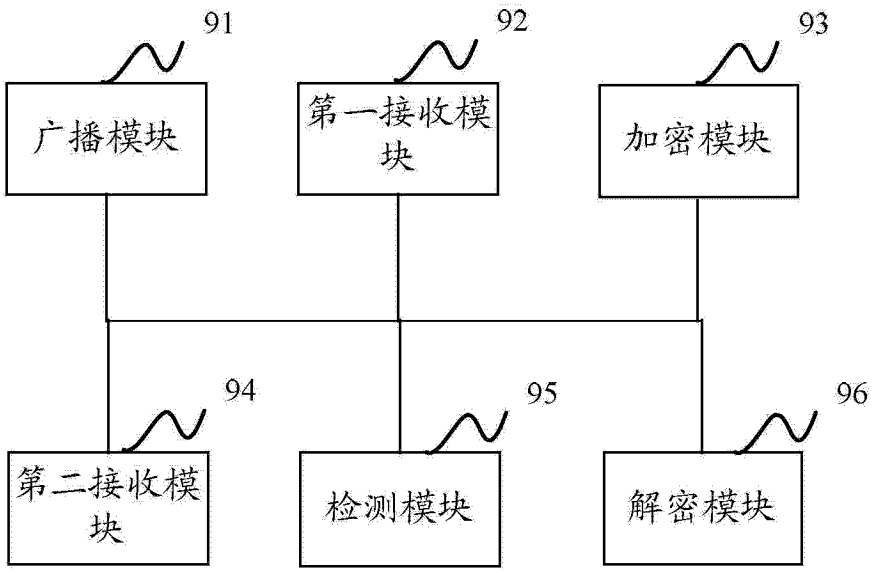

91
92
93
广播模块
第一接收模块
加密模块
94
95
96
第二接收模块
检测模块
解密模块

图 10

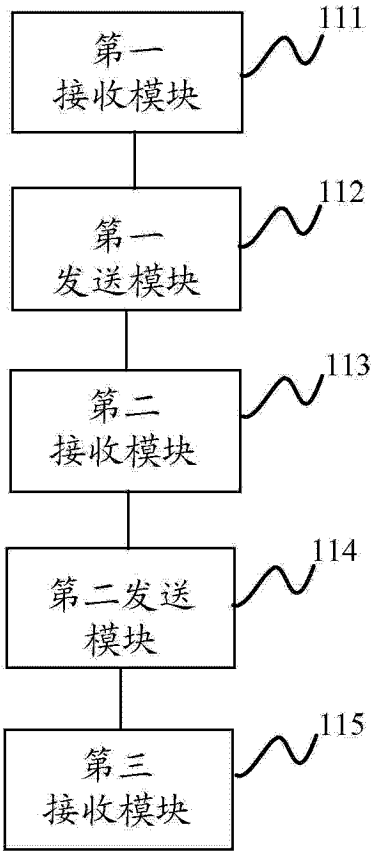

111
第一接收模块
112
第一发送模块
113
第二接收模块
114
第二发送模块
115
第三接收模块

图 11

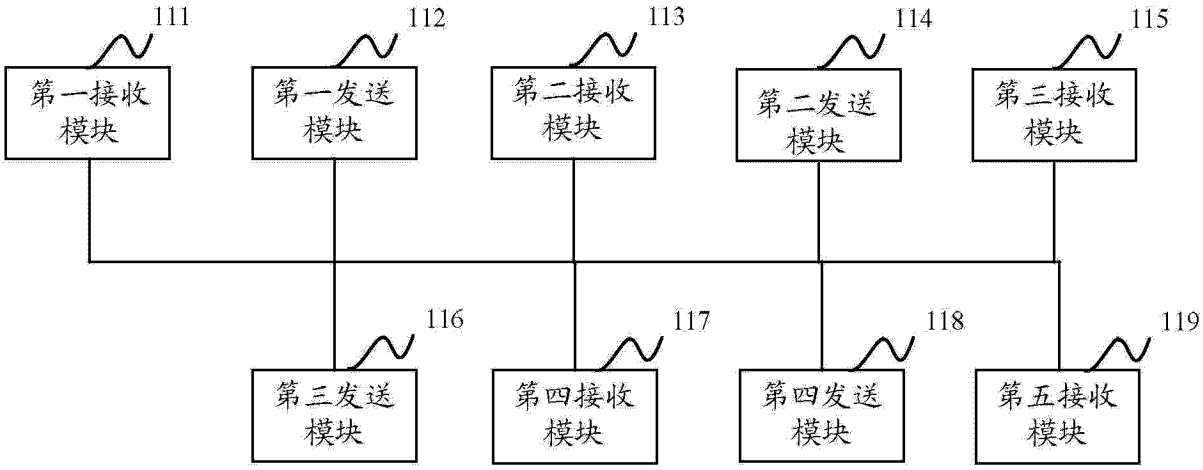

111
第一接收模块
112
第一发送模块
113
第二接收模块
114
第二发送模块
115
第三接收模块
116
第三发送模块
117
第四接收模块
118
第四发送模块
119
第五接收模块

图 12

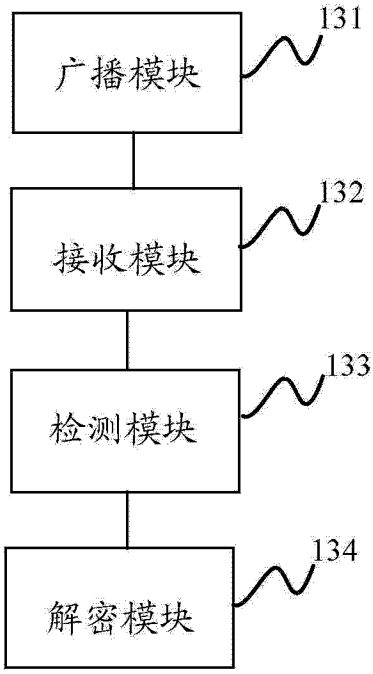

131
广播模块
132
接收模块
133
检测模块
134
解密模块

图 13

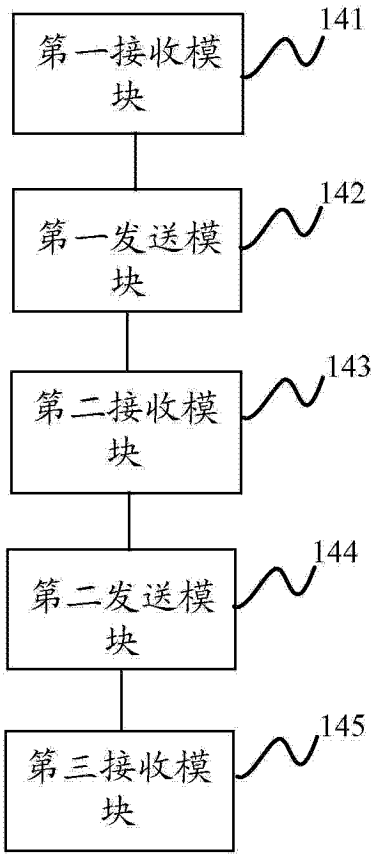

141
第一接收模块
142
第一发送模块
143
第二接收模块
144
第二发送模块
145
第三接收模块

图 14

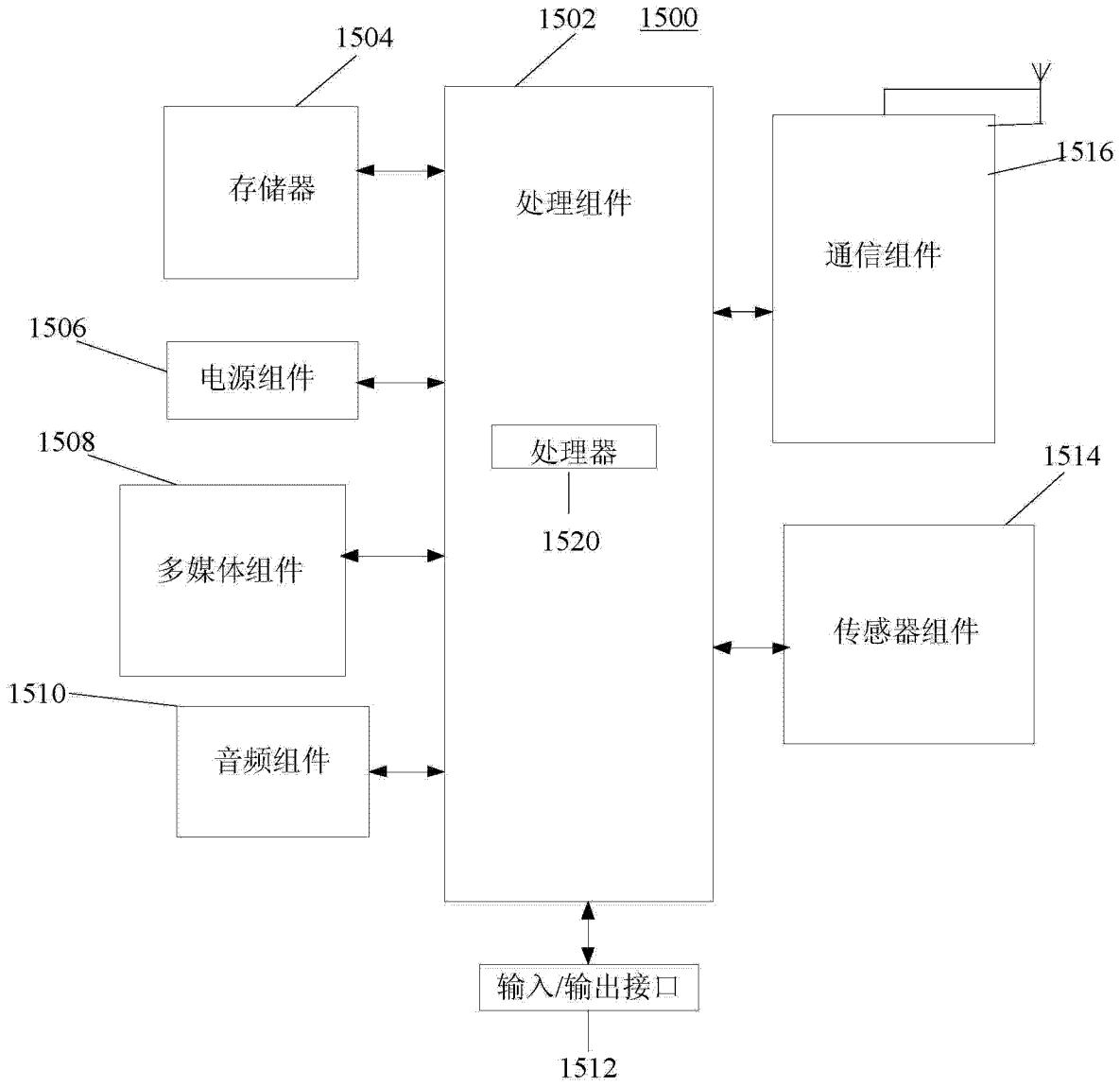

1504
1502
1500
存储器
处理组件
通信组件
1516
1506
电源组件
处理器
1520
1508
多媒体组件
1514
传感器组件
1510
音频组件
输入/输出接口
1512

图 15