(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 104243484 A
(43)申请公布日 2014.12.24

(21)申请号 201410498743.6

(22)申请日 2014.09.25

(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 林俊琦 张洋 汪晨磊

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

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

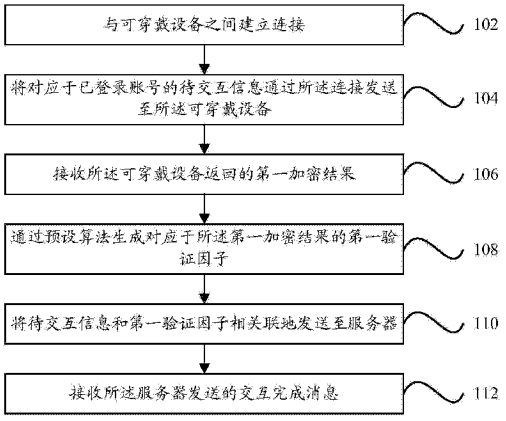
权利要求书4页 说明书16页 附图11页

(54)发明名称

信息交互方法及装置、电子设备

(57)摘要

本公开是关于信息交互方法及装置、电子设备，包括：与可穿戴设备之间建立连接；将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；接收所述可穿戴设备返回的第一加密结果；通过预设算法生成对应于所述第一加密结果的第一验证因子；将所述待交互信息和所述第一验证因子相关联地发送至服务器；接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用预存储的所述加密密钥对所述待交互信息进行加密操作，得到第二加密结果，并确定采用预设算法生成的对应于所述第二加密结果的第二验证因子与所述第一验证因子相同时发送。通过本公开的技术方案，可以基于可穿戴设备实现用户的身份验证，有助于提升信息交互效率。



CN 104243484 A

1. 一种信息交互方法，其特征在于，包括：

与可穿戴设备之间建立连接；

将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

接收所述可穿戴设备返回的第一加密结果，所述第一加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作后得到；

通过预设算法生成对应于所述第一加密结果的第一验证因子；

将所述待交互信息和所述第一验证因子相关联地发送至服务器；

接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用预存储的所述加密密钥对所述待交互信息进行加密操作，得到第二加密结果，并确定采用预设算法生成的对应于所述第二加密结果的第二验证因子与所述第一验证因子相同时发送。

2. 根据权利要求 1 所述的方法，其特征在于，还包括：

接收所述可穿戴设备发送的所述加密密钥；

将所述加密密钥发送至所述服务器，由所述服务器将所述加密密钥和所述已登录账号进行关联存储。

3. 根据权利要求 1 所述的方法，其特征在于，还包括：

接收所述服务器发送的所述加密密钥；

通过所述连接，将所述加密密钥传输至所述可穿戴设备，由所述可穿戴设备将所述加密密钥和所述已登录账号进行关联存储。

4. 一种信息交互方法，其特征在于，包括：

与可穿戴设备之间建立连接；

将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

接收所述可穿戴设备返回的加密结果，所述加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的第一密钥对所述待交互信息进行加密操作后得到；

将所述加密结果发送至所述服务器；

接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用与所述第一密钥相匹配的第二密钥对所述加密结果完成解密操作后发送。

5. 根据权利要求 4 所述的方法，其特征在于，还包括：

接收所述服务器发送的所述第一密钥；

通过所述连接，将所述第一密钥传输至所述可穿戴设备，由所述可穿戴设备将所述第一密钥和所述已登录账号进行关联存储。

6. 根据权利要求 4 所述的方法，其特征在于，还包括：

接收所述可穿戴设备发送的所述第二密钥；

将所述第二密钥传输至所述服务器，由所述服务器将所述第二密钥和所述已登录账号进行关联存储。

7. 根据权利要求 4 所述的方法，其特征在于，还包括：

通过预设算法生成对应于所述待交互信息的第一验证因子；

将所述第一验证因子与所述加密结果相关联地发送至所述服务器，由所述服务器在确定采用所述预设算法生成的对应于所述解密操作的操作结果的第二验证因子与所述第一

验证因子相同后，返回所述交互完成消息。

8. 一种信息交互方法，其特征在于，包括：

与终端之间建立连接；

接收所述终端通过所述连接发送的待交互信息，所述待交互信息对应于所述终端上的已登录账号；

采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果；

将所述加密结果通过所述连接发送至所述终端，并由所述终端将所述加密结果发送至服务器，或者由所述终端通过预设算法生成对应于所述加密结果的验证因子后，将所述验证因子和所述待交互信息相关联地发送至所述服务器。

9. 一种信息交互装置，其特征在于，包括：

建立模块，用于与可穿戴设备之间建立连接；

第一发送模块，用于将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

第一接收模块，用于接收所述可穿戴设备返回的第一加密结果，所述第一加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作后得到；

生成模块，用于通过预设算法生成对应于所述第一加密结果的第一验证因子；

第二发送模块，用于将所述待交互信息和所述第一验证因子相关联地发送至服务器；

第二接收模块，用于接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用预存储的所述加密密钥对所述待交互信息进行加密操作，得到第二加密结果，并确定采用预设算法生成的对应于所述第二加密结果的第二验证因子与所述第一验证因子相同时发送。

10. 根据权利要求 9 所述的装置，其特征在于，还包括：

第一密钥接收模块，用于接收所述可穿戴设备发送的所述加密密钥；

第一密钥传输模块，用于将所述加密密钥发送至所述服务器，由所述服务器将所述加密密钥和所述已登录账号进行关联存储。

11. 根据权利要求 9 所述的装置，其特征在于，还包括：

第二密钥接收模块，用于接收所述服务器发送的所述加密密钥；

第二密钥传输模块，用于通过所述连接，将所述加密密钥传输至所述可穿戴设备，由所述可穿戴设备将所述加密密钥和所述已登录账号进行关联存储。

12. 一种信息交互装置，其特征在于，包括：

建立模块，用于与可穿戴设备之间建立连接；

第一发送模块，用于将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

第一接收模块，用于接收所述可穿戴设备返回的加密结果，所述加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的第一密钥对所述待交互信息进行加密操作后得到；

第二发送模块，用于将所述加密结果发送至所述服务器；

第二接收模块，用于接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用与所述第一密钥相匹配的第二密钥对所述加密结果完成解密操作后发送。

13. 根据权利要求 12 所述的装置，其特征在于，还包括：

第一密钥接收模块，用于接收所述服务器发送的所述第一密钥；

第一密钥传输模块，用于通过所述连接，将所述第一密钥传输至所述可穿戴设备，由所述可穿戴设备将所述第一密钥和所述已登录账号进行关联存储。

14. 根据权利要求 12 所述的装置，其特征在于，还包括：

第二密钥接收模块，用于接收所述可穿戴设备发送的所述第二密钥；

第二密钥传输模块，用于将所述第二密钥传输至所述服务器，由所述服务器将所述第二密钥和所述已登录账号进行关联存储。

15. 根据权利要求 12 所述的装置，其特征在于，还包括：

生成模块，用于通过预设算法生成对应于所述待交互信息的第一验证因子；

第三发送模块，用于将所述第一验证因子与所述加密结果相关联地发送至所述服务器，由所述服务器在确定采用所述预设算法生成的对应于所述解密操作的操作结果的第二验证因子与所述第一验证因子相同后，返回所述交互完成消息。

16. 一种信息交互装置，其特征在于，包括：

建立模块，用于与终端之间建立连接；

接收模块，用于接收所述终端通过所述连接发送的待交互信息，所述待交互信息对应于所述终端上的已登录账号；

加密模块，用于采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果；

发送模块，用于将所述加密结果通过所述连接发送至所述终端，并由所述终端将所述加密结果发送至服务器，或者由所述终端通过预设算法生成对应于所述加密结果的验证因子后，将所述验证因子和所述待交互信息相关联地发送至所述服务器。

17. 一种电子设备，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：

与可穿戴设备之间建立连接；

将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

接收所述可穿戴设备返回的第一加密结果，所述第一加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作后得到；

通过预设算法生成对应于所述第一加密结果的第一验证因子；

将所述待交互信息和所述第一验证因子相关联地发送至所述服务器；

接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用预存储的所述加密密钥对所述待交互信息进行加密操作，得到第二加密结果，并确定采用预设算法生成的对应于所述第二加密结果的第二验证因子与所述第一验证因子相同时发送。

18. 一种电子设备，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：

与可穿戴设备之间建立连接；

将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

接收所述可穿戴设备返回的加密结果，所述加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的第一密钥对所述待交互信息进行加密操作后得到；

将所述加密结果发送至所述服务器；

接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用与所述第一密钥相匹配的第二密钥对所述加密结果完成解密操作后发送。

19. 一种电子设备，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：

与终端之间建立连接；

接收所述终端通过所述连接发送的待交互信息，所述待交互信息对应于所述终端上的已登录账号；

采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果；

将所述加密结果通过所述连接发送至所述终端，并由所述终端将所述加密结果发送至服务器，或者由所述终端通过预设算法生成对应于所述加密结果的验证因子后，将所述验证因子和所述待交互信息相关联地发送至所述服务器。

信息交互方法及装置、电子设备

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及信息交互方法及装置、电子设备。

背景技术

[0002] 通过在终端上输入已注册的用户账号和登录密码，用户可以实现账号登录，并基于该已登录账号进行信息交互。但在一些安全性要求更高的场景下，需要对用户身份执行进一步的验证，则相关技术中，往往需要用户输入相应的身份验证密码。

[0003] 然而，在输入身份验证密码时，很容易被其他人窥视，而当身份验证密码较为复杂时，不仅需要花费用户较长的输入时间，还容易发生输入错误等问题，影响信息交互效率。

发明内容

[0004] 本公开提供信息交互方法及装置、电子设备，以解决相关技术中的信息交互效率低下的技术问题。

[0005] 根据本公开实施例的第一方面，提供一种信息交互方法，包括：

[0006] 与可穿戴设备之间建立连接；

[0007] 将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

[0008] 接收所述可穿戴设备返回的第一加密结果，所述第一加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作后得到；

[0009] 通过预设算法生成对应于所述第一加密结果的第一验证因子；

[0010] 将所述待交互信息和所述第一验证因子相关联地发送至服务器；

[0011] 接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用预存储的所述加密密钥对所述待交互信息进行加密操作，得到第二加密结果，并确定采用预设算法生成的对应于所述第二加密结果的第二验证因子与所述第一验证因子相同时发送。

[0012] 可选的，还包括：

[0013] 接收所述可穿戴设备发送的所述加密密钥；

[0014] 将所述加密密钥发送至所述服务器，由所述服务器将所述加密密钥和所述已登录账号进行关联存储。

[0015] 可选的，还包括：

[0016] 接收所述服务器发送的所述加密密钥；

[0017] 通过所述连接，将所述加密密钥传输至所述可穿戴设备，以由所述可穿戴设备将所述加密密钥和所述已登录账号进行关联存储。

[0018] 根据本公开实施例的第二方面，提供一种信息交互方法，包括：

[0019] 与可穿戴设备之间建立连接；

[0020] 将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

[0021] 接收所述可穿戴设备返回的加密结果，所述加密结果由所述可穿戴设备采用预存

储的唯一对应于所述已登录账号的第一密钥对所述待交互信息进行加密操作后得到；

[0022] 将所述加密结果发送至所述服务器；

[0023] 接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用与所述第一密钥相匹配的第二密钥对所述加密结果完成解密操作后发送。

[0024] 可选的，还包括：

[0025] 接收所述服务器发送的所述第一密钥；

[0026] 通过所述连接，将所述第一密钥传输至所述可穿戴设备，由所述可穿戴设备将所述第一密钥和所述已登录账号进行关联存储。

[0027] 可选的，还包括：

[0028] 接收所述可穿戴设备发送的所述第二密钥；

[0029] 将所述第二密钥传输至所述服务器，由所述服务器将所述第二密钥和所述已登录账号进行关联存储。

[0030] 可选的，还包括：

[0031] 通过预设算法生成对应于所述待交互信息的第一验证因子；

[0032] 将所述第一验证因子与所述加密结果相关联地发送至所述服务器，以由所述服务器在确定采用所述预设算法生成的对应于所述解密操作的操作结果的第二验证因子与所述第一验证因子相同后，返回所述交互完成消息。

[0033] 根据本公开实施例的第三方面，提供一种信息交互方法，包括：

[0034] 与终端之间建立连接；

[0035] 接收所述终端通过所述连接发送的待交互信息，所述待交互信息对应于所述终端上的已登录账号；

[0036] 采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果；

[0037] 将所述加密结果通过所述连接发送至所述终端，并由所述终端将所述加密结果发送至服务器，或者由所述终端通过预设算法生成对应于所述加密结果的验证因子后，将所述验证因子和所述待交互信息相关联地发送至所述服务器。

[0038] 根据本公开实施例的第四方面，提供一种信息交互装置，包括：

[0039] 建立模块，用于与可穿戴设备之间建立连接；

[0040] 第一发送模块，用于将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

[0041] 第一接收模块，用于接收所述可穿戴设备返回的第一加密结果，所述第一加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作后得到；

[0042] 生成模块，用于通过预设算法生成对应于所述第一加密结果的第一验证因子；

[0043] 第二发送模块，用于将所述待交互信息和所述第一验证因子相关联地发送至服务器；

[0044] 第二接收模块，用于接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用预存储的所述加密密钥对所述待交互信息进行加密操作，得到第二加密结果，并确定采用预设算法生成的对应于所述第二加密结果的第二验证因子与所述第一验证

因子相同时发送。

[0045] 可选的，还包括：

[0046] 第一密钥接收模块，用于接收所述可穿戴设备发送的所述加密密钥；

[0047] 第一密钥传输模块，用于将所述加密密钥发送至所述服务器，由所述服务器将所述加密密钥和所述已登录账号进行关联存储。

[0048] 可选的，还包括：

[0049] 第二密钥接收模块，用于接收所述服务器发送的所述加密密钥；

[0050] 第二密钥传输模块，用于通过所述连接，将所述加密密钥传输至所述可穿戴设备，由所述可穿戴设备将所述加密密钥和所述已登录账号进行关联存储。

[0051] 根据本公开实施例的第五方面，提供一种信息交互装置，包括：

[0052] 建立模块，用于与可穿戴设备之间建立连接；

[0053] 第一发送模块，用于将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

[0054] 第一接收模块，用于接收所述可穿戴设备返回的加密结果，所述加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的第一密钥对所述待交互信息进行加密操作后得到；

[0055] 第二发送模块，用于将所述加密结果发送至所述服务器；

[0056] 第二接收模块，用于接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用与所述第一密钥相匹配的第二密钥对所述加密结果完成解密操作后发送。

[0057] 可选的，还包括：

[0058] 第一密钥接收模块，用于接收所述服务器发送的所述第一密钥；

[0059] 第一密钥传输模块，用于通过所述连接，将所述第一密钥传输至所述可穿戴设备，由所述可穿戴设备将所述第一密钥和所述已登录账号进行关联存储。

[0060] 可选的，还包括：

[0061] 第二密钥接收模块，用于接收所述可穿戴设备发送的所述第二密钥；

[0062] 第二密钥传输模块，用于将所述第二密钥传输至所述服务器，由所述服务器将所述第二密钥和所述已登录账号进行关联存储。

[0063] 可选的，还包括：

[0064] 生成模块，用于通过预设算法生成对应于所述待交互信息的第一验证因子；

[0065] 第三发送模块，用于将所述第一验证因子与所述加密结果相关联地发送至所述服务器，由所述服务器在确定采用所述预设算法生成的对应于所述解密操作的操作结果的第二验证因子与所述第一验证因子相同后，返回所述交互完成消息。

[0066] 根据本公开实施例的第六方面，提供一种信息交互装置，包括：

[0067] 建立模块，用于与终端之间建立连接；

[0068] 接收模块，用于接收所述终端通过所述连接发送的待交互信息，所述待交互信息对应于所述终端上的已登录账号；

[0069] 加密模块，用于采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果；

[0070] 发送模块，用于将所述加密结果通过所述连接发送至所述终端，并由所述终端将

所述加密结果发送至服务器，或者由所述终端通过预设算法生成对应于所述加密结果的验证因子后，将所述验证因子和所述待交互信息相关联地发送至所述服务器。

[0071] 根据本公开实施例的第七方面，提供一种电子设备，包括：

[0072] 处理器；

[0073] 用于存储处理器可执行指令的存储器；

[0074] 其中，所述处理器被配置为：

[0075] 与可穿戴设备之间建立连接；

[0076] 将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

[0077] 接收所述可穿戴设备返回的第一加密结果，所述第一加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作后得到；

[0078] 通过预设算法生成对应于所述第一加密结果的第一验证因子；

[0079] 将所述待交互信息和所述第一验证因子相关联地发送至所述服务器；

[0080] 接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用预存储的所述加密密钥对所述待交互信息进行加密操作，得到第二加密结果，并确定采用预设算法生成的对应于所述第二加密结果的第二验证因子与所述第一验证因子相同时发送。

[0081] 根据本公开实施例的第八方面，提供一种电子设备，包括：

[0082] 处理器；

[0083] 用于存储处理器可执行指令的存储器；

[0084] 其中，所述处理器被配置为：

[0085] 与可穿戴设备之间建立连接；

[0086] 将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

[0087] 接收所述可穿戴设备返回的加密结果，所述加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的第一密钥对所述待交互信息进行加密操作后得到；

[0088] 将所述加密结果发送至所述服务器；

[0089] 接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用与所述第一密钥相匹配的第二密钥对所述加密结果完成解密操作后发送。

[0090] 根据本公开实施例的第九方面，提供一种电子设备，包括：

[0091] 处理器；

[0092] 用于存储处理器可执行指令的存储器；

[0093] 其中，所述处理器被配置为：

[0094] 处理器；

[0095] 用于存储处理器可执行指令的存储器；

[0096] 其中，所述处理器被配置为：

[0097] 与终端之间建立连接；

[0098] 接收所述终端通过所述连接发送的待交互信息，所述待交互信息对应于所述终端上的已登录账号；

[0099] 采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果；

[0100] 将所述加密结果通过所述连接发送至所述终端，并由所述终端将所述加密结果发送至服务器，或者由所述终端通过预设算法生成对应于所述加密结果的验证因子后，将所述验证因子和所述待交互信息相关联地发送至所述服务器。

[0101] 本公开的实施例提供的技术方案可以包括以下有益效果：

[0102] 本公开通过预先设置对应于用户账号的密钥对，并分别存储在可穿戴设备和服务器中，从而通过可穿戴设备对待交互信息的加密操作，使得服务器可以对可穿戴设备中存储的密钥进行验证，从而实现用户身份的验证，免去了用户手动输入身份验证密码的操作，有助于提升信息交互效率。

[0103] 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

[0104] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本发明的实施例，并与说明书一起用于解释本发明的原理。

[0105] 图 1A 是根据一示例性实施例示出的基于终端侧的一种信息交互方法的流程图。

[0106] 图 1B 是根据一示例性实施例示出的基于可穿戴设备侧的一种信息交互方法的流程图。

[0107] 图 2 是根据一示例性实施例示出的信息交互场景的示意图。

[0108] 图 3 是根据一示例性实施例示出的支付场景下的一种信息交互方法的流程图。

[0109] 图 4A 是根据一示例性实施例示出的基于终端侧的另一种信息交互方法的流程图。

[0110] 图 4B 是根据一示例性实施例示出的基于可穿戴设备侧的另一种信息交互方法的流程图。

[0111] 图 5 是根据一示例性实施例示出的支付场景下的另一种信息交互方法的流程图。

[0112] 图 6 是根据一示例性实施例示出的支付场景下的另一种信息交互方法的流程图。

[0113] 图 7 是根据一示例性实施例示出的基于终端侧的一种信息交互装置的框图。

[0114] 图 8 是根据一示例性实施例示出的基于终端侧的另一种信息交互装置的框图。

[0115] 图 9 是根据一示例性实施例示出的基于终端侧的另一种信息交互装置的框图。

[0116] 图 10 是根据一示例性实施例示出的基于终端侧的另一种信息交互装置的框图。

[0117] 图 11 是根据一示例性实施例示出的基于终端侧的另一种信息交互装置的框图。

[0118] 图 12 是根据一示例性实施例示出的基于终端侧的另一种信息交互装置的框图。

[0119] 图 13 是根据一示例性实施例示出的基于终端侧的另一种信息交互装置的框图。

[0120] 图 14 是根据一示例性实施例示出的基于可穿戴设备侧的另一种信息交互装置的框图。

[0121] 图 15 是根据一示例性实施例示出的一种用于信息交互的装置的结构示意图。

具体实施方式

[0122] 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发明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、本发明的一些方面相一致的装置和方法的例子。

[0123] 请参考图 1A，图 1A 是根据一示例性实施例示出的基于终端侧的一种信息交互方法的流程图，该方法用于终端中，可以包括以下步骤。

[0124] 在步骤 102 中，与可穿戴设备之间建立连接。

[0125] 在本实施例中，可穿戴设备包括可以直接穿在身上或是整合到用户的衣服、配件的便携式设备，比如智能眼镜、智能手表、智能手环、智能跑鞋等，本公开并不限制其具体类型。

[0126] 在本实施例中，终端可以通过各种方式实现与可穿戴设备之间的连接。作为一示例性实施方式，该连接可以为有线连接，比如通过 Micro USB 线进行连接；作为一示例性实施方式，该连接可以为无线连接，比如蓝牙连接、红外连接、WIFI（无线保真）连接等方式，本公开并不限制其具体形式。

[0127] 在步骤 104 中，将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备。

[0128] 在步骤 106 中，接收所述可穿戴设备返回的第一加密结果，所述第一加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作后得到。

[0129] 在本实施例中，通过在终端上登录预先注册的用户账号，用户才能够执行相应的操作，比如查看数据、启动预设功能等。在一些安全要求较高的情况下，需要对用户身份进行验证时，无需用户手动输入身份验证密码，而是在用户确定了待交互信息后，由终端将待交互信息发送至可穿戴设备中，通过可穿戴设备对待交互信息的加密操作，相当于对该待交互信息执行了数字签名。

[0130] 在本实施例中，用户仅需要确定待交互信息，而终端与可穿戴设备之间的信息传输、可穿戴设备的加密操作等对用户而言都是透明的，即在用户看来并不存在身份验证的过程，简化了用户在整个过程中的操作和行为，有助于提升用户体验、加快信息交互速度。

[0131] 在步骤 108 中，通过预设算法生成对应于所述第一加密结果的第一验证因子。

[0132] 在本实施例中，通过预先在可穿戴设备与服务器上分别设置相同的算法，使得用户身份无误的情况下，可穿戴设备和服务器分别生成的验证因子相同，从而可以用于验证用户身份。

[0133] 在本实施例中，预设算法可以为不可逆算法，即第一验证因子是根据第一加密结果生成的，但根据第一验证因子无法推算出第一加密结果，以确保安全性。其中，预设算法可以为消息摘要生成算法，比如 MD5(Message-Digest Algorithm 5，信息摘要算法 5)、SHA(Secure Hash Algorithm，安全散列算法）等。通过生成第一验证因子，既可以用于服务器对接收到的待交互信息进行完整性检验，又可以在体现出可穿戴设备采用的加密密钥的同时，降低数据传输量，提升信息交互效率。

[0134] 在步骤 110 中，将所述待交互信息和所述第一验证因子相关联地发送至所述服务器，以由所述服务器采用预存储的所述加密密钥对所述待交互信息进行加密操作，得到第二加密结果。

[0135] 在步骤 112 中，在所述服务器确定采用预设算法生成的对应于所述第二加密结果

的第二验证因子与所述第一验证因子相同后，接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用预存储的所述加密密钥对所述待交互信息进行加密操作，得到第二加密结果，并确定采用预设算法生成的对应于所述第二加密结果的第二验证因子与所述第一验证因子相同时发送。

[0136] 在本实施例中，可穿戴设备和服务器上采用相同的加密密钥，即对称加密密钥，该加密密钥可以由服务器生成后，通过终端传输并存储在可穿戴设备中。在本实施例中，加密密钥与用户账号之间是一一对应的，因而如果第一验证因子和第二验证因子相同，就说明可穿戴设备采用的加密密钥与服务器相同，即可实现对用户的身份验证。

[0137] 与图 1A 相对应地，图 1B 是根据一示例性实施例示出的基于可穿戴设备侧的一种信息交互方法的流程图，可以包括以下步骤。

[0138] 在步骤 102’中，与终端之间建立连接。

[0139] 在步骤 104’中，接收所述终端通过所述连接发送的待交互信息，所述待交互信息对应于所述终端上的已登录账号。

[0140] 在步骤 106’中，采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果。

[0141] 在本实施例中，可穿戴设备采用的加密密钥对应于终端上的已登录账号，即用户通过该已登录账号，向可穿戴设备发送了待交互信息；同时，对应于该已登录账号，在服务器上存储有相匹配的加密密钥，且可穿戴设备和服务器上存储的相匹配的加密密钥之间为对称加密密钥。

[0142] 在步骤 108’中，将所述加密结果通过所述连接发送至所述终端，由所述终端通过预设算法生成对应于所述加密结果的验证因子后，将所述验证因子和所述待交互信息相关联地发送至所述服务器。

[0143] 在本实施例中，对应于图 1A 中的描述，则服务器在接收到终端发送的验证因子和待交互信息后，根据预存储的对应于已登录账号的加密密钥，会对待交互信息进行加密操作，得到另一加密结果，以及与终端采用相同的预设算法生成对应于该另一加密结果的另一验证因子，则当该另一验证因子与接收到的验证因子相同，则说明服务器和可穿戴设备采用了相同的加密密钥，实现了对当前用户的身份验证，且检验了服务器接收到的验证因子和待交互信息在传输过程中的数据完整性。

[0144] 由上述实施例可知，本公开通过在可穿戴设备与服务器上分别存储对应于用户账号的加密密钥，可以利用可穿戴设备与用户之间的强关联关系，即由于可穿戴设备是用于满足日常生活需求的设备，用户只会自行使用，因而通过验证可穿戴设备和服务器分别采用的对待交互信息进行加密的加密密钥是否相同，即可实现对用户身份的快速验证，无需用户手动输入身份验证密钥，有助于提升信息交互效率。

[0145] 基于本公开的技术方案，可以应用于任意场景下的信息交互过程，本公开并不限制其类型。作为一示例性实施例，图 2 示出了一典型应用场景，包括：智能手环、手机和支付服务器，其中当用户通过手机处理支付业务时，采用预先配对的智能手环，实现对用户身份的快速验证，从而在支付服务器上实现支付操作。对应于图 1 所示的处理流程，当应用于图 2 所示的支付场景时，图 3 示出了相应的信息交互方法的流程图，包括下述步骤。

[0146] 1) 配对过程

[0147] 在步骤 302 中，针对用户通过手机发起的配对请求，支付服务器生成加密密钥，该加密密钥唯一对应于用户在手机上的已登录账号。

[0148] 在本实施例中，用户可以在任意时刻发起配对请求，建立智能手环与用户账号之间的关联关系；并且，用户也可以对智能手环与用户账号之间的关联关系进行修改。

[0149] 在本实施例中，为方便用户使用，尤其是用户注册了多个用户账号，或者希望将智能手环在家人之间共享的情况下，还可以使得同一个智能手环与多个用户账号分别配对，并且将每个用户账号与相应的加密密钥相关联地存储在智能手环中。当然，用户可以对智能手环中允许存储的加密密钥数量进行限制，以提升智能手环的私密性。

[0150] 在本实施例中，以服务器生成加密密钥为例进行说明，但也可以由可穿戴设备生成对应于已登录账号的加密密钥后，将加密密钥发送至终端，并由终端转发至服务器。

[0151] 在步骤 304 中，支付服务器将生成的对应于已登录账号的加密密钥发送至手机。

[0152] 在步骤 306 中，手机将接收到的加密密钥发送至智能手环，使得智能手环将该加密密钥与已登录账号进行关联存储。

[0153] 以上基于步骤 302 至步骤 306 的操作，智能手环和服务器分别将加密密钥与用户账号进行关联存储，且对应于同一个用户账号，智能手环和服务器采用了相同且唯一对应于该用户账号的加密密钥，以便于后续的身份验证操作。

[0154] 2) 身份验证

[0155] 在步骤 308 中，基于手机上被触发的支付业务，生成相应的支付参数，比如支付对象、支付金额、支付账户等信息。

[0156] 在步骤 310 中，手机将生成的支付参数发送至智能手环中。

[0157] 在本实施例中，手机与智能手环可以基于任意方式实现无线连接，比如蓝牙、红外、近场通信等，以实现数据的无线传输。

[0158] 在步骤 312，智能手环基于预存储的加密密钥，对接收到的支付参数进行加密处理。

[0159] 在步骤 314 中，智能手环将生成的第一加密结果发送至手机。

[0160] 在步骤 316 中，手机采用 MD5 算法，生成该第一加密结果对应的第一消息摘要。

[0161] 在本实施例中，当然也可以采用其他类型的消息摘要算法，比如 SHA 算法等。

[0162] 在步骤 318 中，手机将原始的（即未经过加密等过程的处理）支付参数和第一消息摘要相关联地发送至支付服务器。

[0163] 在步骤 320 中，支付服务器采用对应于当前的已登录账号的加密密钥，对接收到的原始的支付参数进行加密操作。

[0164] 在步骤 322 中，针对生成的第二加密结果，采用与智能手环相同的消息摘要算法，如 MD5 算法，生成对应于第二加密结果的第二消息摘要。

[0165] 在步骤 324 中，比较第一消息摘要和第二消息摘要。

[0166] 在本实施例中，如果在手机与支付服务器之间的数据传输过程没有发生意外，则支付服务器和智能手环接收到的支付参数相同；因此，如果用户身份无误，则智能手环与支付服务器采用的加密密钥也应当相同，而消息摘要算法也相同，第一消息摘要和第二消息摘要就应当相同。所以，如果第一消息摘要和第二消息摘要不同，则极有可能是由于用户身份验证出错，或者也可能是传输数据出现偏差，但这些情况均表明本次支付操作的环境不

安全，应当停止本次支付操作。

[0167] 在步骤 326 中，当第一消息摘要和第二消息摘要相同时，表明用户身份验证通过，支付服务器可以根据接收到的支付参数，完成相应的支付操作。

[0168] 在步骤 328 中，支付服务器向手机发送完成支付操作时的反馈消息。

[0169] 请参考图 4，图 4 是根据一示例性实施例示出的另一种信息交互方法的流程图，该方法应用于终端上，可以包括下述步骤。

[0170] 在步骤 402 中，与可穿戴设备之间建立连接。

[0171] 在本实施例中，可穿戴设备包括可以直接穿在身上或是整合到用户的衣服、配件的便携式设备，比如智能眼镜、智能手表、智能手环、智能跑鞋等，本公开并不限制其具体类型。

[0172] 在本实施例中，终端可以通过各种方式实现与可穿戴设备之间的连接。作为一示例性实施方式，该连接可以为有线连接，比如通过 Micro USB 线进行连接；作为一示例性实施方式，该连接可以为无线连接比如蓝牙连接、红外连接、WIFI（无线保真）连接等方式，本公开并不限制其具体形式。

[0173] 在步骤 404 中，将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备。

[0174] 在步骤 406 中，接收所述可穿戴设备返回的加密结果，所述加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的第一密钥对所述待交互信息进行加密操作后得到。

[0175] 在本实施例中，通过在终端上登录预先注册的用户账号，用户才能够执行相应的操作，比如查看数据、启动预设功能等。在一些安全要求较高的情况下，需要对用户身份进行验证时，无需用户手动输入身份验证密码，而是在用户确定了待交互信息后，由终端将待交互信息发送至可穿戴设备中，通过可穿戴设备对待交互信息的加密操作，相当于对该待交互信息执行了数字签名。

[0176] 在本实施例中，用户仅需要确定待交互信息，而终端与可穿戴设备之间的信息传输、可穿戴设备的加密操作等对用户而言都是透明的，即在用户看来并不存在身份验证的过程，简化了用户在整个过程中的操作和行为，有助于提升用户体验、加快信息交互速度。

[0177] 在步骤 408 中，将所述加密结果发送至所述服务器。

[0178] 在步骤 410 中，接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用与所述第一密钥相匹配的第二密钥对所述加密结果完成解密操作后发送。

[0179] 在本实施例中，通过在可穿戴设备和服务器上采用相匹配的密钥对，即第一密钥和第二密钥，则只要服务器能够对来自终端的加密结果进行解密操作，就说明该加密结果是由第一密钥进行加密生成的，而密钥对与用户账号之间是一一对应的，从而即可实现对用户身份的验证。

[0180] 与图 4A 相对应地，图 4B 是根据一示例性实施例示出的基于可穿戴设备侧的另一种信息交互方法的流程图，可以包括以下步骤。

[0181] 在步骤 402’中，与终端之间建立连接。

[0182] 在步骤 404’中，接收所述终端通过所述连接发送的待交互信息，所述待交互信息对应于所述终端上的已登录账号。

[0183] 在步骤 406’中，采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果。

[0184] 在本实施例中，可穿戴设备采用的加密密钥对应于终端上的已登录账号，即用户通过该已登录账号，向可穿戴设备发送了待交互信息；同时，对应于该已登录账号，在服务器上存储有相匹配的加密密钥，且可穿戴设备和服务器上存储的相匹配的加密密钥之间可以为对称加密密钥或非对称加密密钥。

[0185] 在步骤 408’中，将所述加密结果通过所述连接发送至所述终端，并由所述终端将所述加密结果发送至服务器。

[0186] 在本实施例中，对应于图 4A 中的描述，则服务器在接收到终端发送的加密结果后，根据预存储的对应于已登录账号的加密密钥，可以尝试性地对该加密结果进行解密操作。如果当前用户的身份无误，则服务器选取的对应于已登录账号的加密密钥与可穿戴设备上采用的加密密钥之间是相匹配的，使得服务器能够成功完成解密操作，得到相应的待交互信息。

[0187] 由上述实施例可知，本公开通过在可穿戴设备与服务器上分别存储相匹配且对应于用户账号的密钥，可以利用可穿戴设备与用户之间的强关联关系，即由于可穿戴设备是用于满足日常生活需求的设备，用户只会自行使用，因而通过验证可穿戴设备对待交互信息进行加密的第一密钥与服务器进行解密的第二密钥是否匹配，即可实现对用户身份的快速验证，无需用户手动输入身份验证密钥，有助于提升信息交互效率。

[0188] 与图 1 所示的实施例相类似地，本实施例同样可以应用于任意场景下的信息交互过程，本公开并不限制其类型。对应于图 4 所示的处理流程，当应用于图 2 所示的支付场景时，图 5 示出了一种实施方式的信息交互方法的流程图，包括下述步骤。

[0189] 1) 配对过程

[0190] 在步骤 502 中，由智能手环生成用于信息加密的密钥对。

[0191] 在本实施例中，智能手环可以在任意时刻生成密钥对，比如在激活使用后自动生成，或者基于用户发起的配对请求而生成。

[0192] 在本实施例中，由智能手环生成的密钥对可以为非对称加密密钥，其中存储在智能手环中的第一密钥为私钥、存储在支付服务器中的第二密钥为公钥。

[0193] 当然，作为一示例性实施方式，也可以采用对称加密密钥，则可以由服务器生成对称的第一密钥和第二密钥（即第一密钥与和第二密钥相同），然后服务器将第一密钥发送至手机，由手机将第一密钥转发至智能手环，并存储在智能手环中。

[0194] 在步骤 504 中，智能手环对密钥对中的第一密钥进行存储。

[0195] 在步骤 506 中，手机接收智能手环发送的所述密钥对中的第二密钥，其中第一密钥与第二密钥相匹配。

[0196] 在本实施例中，可以针对用户通过手机发起的配对请求，使得智能手环将第二密钥发送至手机；其中，当手机发起配对请求时，可以将当前的已登录账号发送至智能手环，从而在该已登录账号与第一密钥、第二密钥之间建立关联，即实际上是在拥有该已登录账号的用户与密钥对之间建立关联关系。

[0197] 在步骤 508 中，手机将第二密钥发送至支付服务器，使得支付服务器对第二密钥进行存储。

[0198] 在本实施例中，手机可以向支付服务器发起配对请求，即用户通过当前的已登录账号发起相应的配对请求，从而使得支付服务器将接收到的第二密钥与当前的已登录账号之间进行关联存储。

[0199] 2) 身份验证

[0200] 在步骤 510 中，基于手机上被触发的支付业务，生成相应的支付参数，比如支付对象、支付金额、支付账户等信息。

[0201] 在步骤 512 中，手机将生成的支付参数发送至智能手环中。

[0202] 在本实施例中，手机与智能手环可以基于任意方式实现无线连接，比如蓝牙、红外、近场通信等，以实现数据的无线传输。

[0203] 在步骤 514 中，智能手环基于预存储的第一密钥，对接收到的支付参数进行加密处理。

[0204] 在步骤 516 中，智能手环将生成的加密结果发送至手机。

[0205] 在步骤 518 中，手机将加密结果发送至支付服务器。

[0206] 在步骤 520 中，基于当前的已登录账号，支付服务器采用对应的第二密钥对该加密结果进行解密操作。

[0207] 在步骤 522 中，若成功完成对加密结果的解密操作，则说明第二密钥与智能手环采用的第一密钥之间相匹配，所以完成了对当前已登录账号的身份验证且验证通过，完成相应的支付操作。

[0208] 在步骤 524 中，支付服务器向手机发送完成支付操作时的反馈消息。

[0209] 对应于图 4 所示的处理流程，针对图 2 所示的支付场景时，图 6 示出了另一种实施方式的信息交互方法的流程图，该流程中从 1) 配对过程中的智能手环生成密钥对，直至 2) 身份验证中的智能手环对支付参数进行加密并返回加密结果，与图 5 所示的步骤 502 至步骤 516 相同，而不同之处在于下述处理流程。

[0210] 在步骤 602 中，基于生成的原始的支付参数，手机通过预设算法生成对应的第一消息摘要，该预设算法可以为 MD5 算法、SHA 算法等。

[0211] 在本实施例中，手机和智能手环分别生成第一消息摘要和加密结果，两者之间并没有确定的生成顺序，且具体顺序不会对处理结果造成不同影响。

[0212] 在步骤 604 中，手机将加密结果和第一消息摘要相关联地发送至支付服务器。

[0213] 在步骤 606 中，支付服务器根据当前的已登录账号，采用对应的第二密钥对接收到的加密结果进行解密操作，若能够成功解密，说明第二密钥与智能手环采用的第一密钥之间相匹配，实现了对用户身份的验证。

[0214] 在步骤 608 中，支付服务器采用预设算法，生成对应于解密得到的支付参数的第二消息摘要。

[0215] 在步骤 610 中，对接收到的第一消息摘要和生成的第二消息摘要进行比较，以验证步骤 604 的传输过程中，对加密结果的传输完整性。

[0216] 在步骤 612 中，若用户身份验证完成且数据传输完整，则说明当前的支付环境安全，完成相应的支付操作。

[0217] 在步骤 614 中，支付服务器向手机发送完成支付操作时的反馈消息。

[0218] 与图 1A 所示的信息交互方法的实施例相对应，本公开还提供了信息交互装置的

实施例。

[0219] 图 7 是根据一示例性实施例示出的基于终端侧的一种信息交互装置框图。请参考图 7，该装置可以包括建立模块 701、第一发送模块 702、第一接收模块 703、生成模块 704、第二发送模块 705 和第二接收模块 706。

[0220] 其中，建立模块 701，被配置为与可穿戴设备之间建立连接；

[0221] 第一发送模块 702，被配置为将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备；

[0222] 第一接收模块 703，被配置为接收所述可穿戴设备返回的第一加密结果，所述第一加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作后得到；

[0223] 生成模块 704，被配置为通过预设算法生成对应于所述第一加密结果的第一验证因子；

[0224] 第二发送模块 705，被配置为将所述待交互信息和所述第一验证因子相关联地发送至服务器；

[0225] 第二接收模块 706，被配置为接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用预存储的所述加密密钥对所述待交互信息进行加密操作，得到第二加密结果，并确定采用预设算法生成的对应于所述第二加密结果的第二验证因子与所述第一验证因子相同时发送。

[0226] 在上述实施例中，通过预先设置对应于用户账号的密钥对，并分别存储在可穿戴设备和服务器中，从而通过可穿戴设备对待交互信息的加密操作，使得服务器可以对可穿戴设备中存储的密钥进行验证，从而实现用户身份的验证，免去了用户手动输入身份验证密码的操作，有助于提升信息交互效率。

[0227] 可选的，所述预设算法包括消息摘要生成算法。

[0228] 如图 8 所示，图 8 是根据一示例性实施例示出的基于终端侧的另一种信息交互装置的框图，该实施例在前述图 7 所示实施例的基础上，还可以包括：第一密钥接收模块 707 和第二密钥传输模块 708。

[0229] 其中，第一密钥接收模块，被配置为接收所述可穿戴设备发送的所述加密密钥；

[0230] 第一密钥传输模块，被配置为将所述加密密钥发送至所述服务器，由所述服务器将所述加密密钥和所述已登录账号进行关联存储。

[0231] 在上述实施例中，可以由可穿戴设备生成加密密钥，并通过终端将加密密钥发送至服务器，使得可穿戴设备和服务器上分别存储了相匹配的加密密钥，且该加密密钥对唯一对应于已登录账号。

[0232] 如图 9 所示，图 9 是根据一示例性实施例示出的基于终端侧的另一种信息交互装置的框图，该实施例在前述图 7 所示实施例的基础上，还可以包括：第二密钥接收模块 709 和第二密钥传输模块 710。

[0233] 其中，密钥接收模块 709，接收所述服务器发送的所述加密密钥；

[0234] 密钥传输模块 710，被配置为通过所述连接，将所述加密密钥传输至所述可穿戴设备，由所述可穿戴设备将所述加密密钥和所述已登录账号进行关联存储。

[0235] 在本实施例中，可以由服务器生成加密密钥，并通过终端将加密密钥发送至可穿

戴设备，使得可穿戴设备和服务器上分别存储了相匹配的加密密钥，且该加密密钥对唯一对应于已登录账号。

[0236] 在图 8 和图 9 所示的实施例中，在采用的密钥对为对称加密密钥时，通过生成对应于加密结果的消息摘要，并向服务器发送消息摘要和待交互信息，既能够降低传输的数据量，又能够对服务器接收到的待交互信息进行完整性检验，有助于提升数据安全性。

[0237] 与图 4A 所示的信息交互方法的实施例相对应，本公开还提供了信息交互装置的实施例。

[0238] 图 10 是根据一示例性实施例示出的基于终端侧的一种信息交互装置框图。请参考图 10，该装置可以包括建立模块 901、第一发送模块 902、第一接收模块 903、第二发送模块 904 和第二接收模块 905。

[0239] 其中，建立模块 901，被配置为与可穿戴设备之间建立连接；

[0240] 第一发送模块 902，被配置为将对应于已登录账号的待交互信息通过所述无线连接发送至所述可穿戴设备；

[0241] 第一接收模块 903，被配置为接收所述可穿戴设备返回的加密结果，所述加密结果由所述可穿戴设备采用预存储的唯一对应于所述已登录账号的第一密钥对所述待交互信息进行加密操作后得到；

[0242] 第二发送模块 904，被配置为将所述加密结果发送至所述服务器；

[0243] 第二接收模块 905，被配置为接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用与所述第一密钥相匹配的第二密钥对所述加密结果完成解密操作后发送。

[0244] 在上述实施例中，通过预先设置对应于用户账号的密钥对，并分别存储在可穿戴设备和服务器中，从而通过可穿戴设备对待交互信息的加密操作，使得服务器可以对可穿戴设备中存储的密钥进行验证，从而实现用户身份的验证，免去了用户手动输入身份验证密码的操作，有助于提升信息交互效率。

[0245] 如图 11 所示，图 11 是根据一示例性实施例示出的基于终端侧的另一种信息交互装置的框图，该实施例在前述图 10 所示实施例的基础上，还可以包括：第一密钥接收模块 906 和第一密钥传输模块 907。

[0246] 第一密钥接收模块 906，接收所述服务器发送的所述第一密钥；

[0247] 第一密钥传输模块 907，被配置为通过所述连接，将所述第一密钥传输至所述可穿戴设备，由所述可穿戴设备将所述第一密钥和所述已登录账号进行关联存储。

[0248] 可选的，所述第一密钥和所述第二密钥为对称加密密钥。

[0249] 在上述实施例中，在采用的密钥对为对称加密密钥时，通过直接向服务器发送加密结果，使得服务器可以基于对接收到的加密结果的解密情况，确定可穿戴设备中存储的密钥与当前的已登录用户是否匹配，从而完成对用户的身份验证操作。

[0250] 如图 12 所示，图 12 是根据一示例性实施例示出的基于终端侧的另一种信息交互装置的框图，该实施例在前述图 10 所示实施例的基础上，还可以包括：第二密钥接收模块 908 和第二密钥传输模块 909。

[0251] 其中，第二密钥接收模块 908，被配置为接收所述可穿戴设备发送的所述第二密钥；

[0252] 第二密钥传输模块 909，被配置为将所述第二密钥传输至所述服务器，由所述服务器将所述第二密钥和所述已登录账号进行关联存储。

[0253] 可选的，所述第一密钥和所述第二密钥为非对称加密密钥，其中所述第一密钥为私钥、所述第二密钥为公钥。

[0254] 在上述实施例中，在采用的密钥对为非对称加密密钥时，通过直接向服务器发送加密结果，使得服务器可以基于对接收到的加密结果的解密情况，确定可穿戴设备中存储的密钥与当前的已登录用户是否匹配，从而完成对用户的身份验证操作。

[0255] 如图 13 所示，图 13 是根据一示例性实施例示出的另一种信息交互装置的框图，该实施例在前述图 10 所示实施例的基础上，还可以包括：生成模块 910 和第三发送模块 911。

[0256] 其中，生成模块 910，被配置为通过预设算法生成对应于所述待交互信息的第一验证因子；

[0257] 第三发送模块 911，被配置为将所述第一验证因子与所述加密结果相关联地发送至所述服务器，由所述服务器在确定采用所述预设算法生成的对应于所述解密操作的操作结果的第二验证因子与所述第一验证因子相同后，返回所述交互完成消息。

[0258] 在上述实施例中，通过生成对应于待交互信息的消息摘要，使得服务器在对可穿戴设备中存储的密钥进行验证的同时，还可以对解密操作的解密结果进行完整性检验，有助于提升数据安全性。

[0259] 需要说明的是，上述图 12 所示的装置实施例中的生成模块 910 和第三发送模块 911 的结构也可以包含在前述图 9 至图 11 的装置实施例中，对此本公开不进行限制。

[0260] 可选的，在图 9 至图 12 的装置实施例中，所述预设算法包括消息摘要生成算法。

[0261] 与图 1B 和图 4B 所示的信息交互方法的实施例相对应，本公开还提供了信息交互装置的实施例。

[0262] 图 14 是根据一示例性实施例示出的基于可穿戴设备侧的一种信息交互装置框图。请参考图 14，该装置可以包括建立模块 141、接收模块 142、加密模块 143 和发送模块 144。

[0263] 其中，建立模块，被配置为与终端之间建立连接；

[0264] 接收模块，被配置为接收所述终端通过所述连接发送的待交互信息，该待交互信息对应于所述终端上的已登录账号；

[0265] 加密模块，被配置为采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果；

[0266] 发送模块，被配置为将所述加密结果通过所述连接发送至所述终端，并由所述终端将所述加密结果发送至服务器，或者由所述终端通过预设算法生成对应于所述加密结果的验证因子后，将所述验证因子和所述待交互信息相关联地发送至所述服务器。

[0267] 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。

[0268] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中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模块来实现本公开方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0269] 图 15 是根据一示例性实施例示出的一种用于信息交互的装置 1500 的框图。例如，装置 1500 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。

[0270] 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。

[0271] 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。处理组件 1502 可以包括一个或多个处理器 1520 来执行指令，以完成上述终端侧的方法的全部或部分步骤，或完成上述可穿戴设备侧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，处理组件 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。

[0272] 存储器 1504 被配置为存储各种类型的数据以支持在装置 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。

[0273] 电源组件 1506 为装置 1500 的各种组件提供电力。电源组件 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。

[0274] 多媒体组件 1508 包括在所述装置 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。当装置 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。

[0275] 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。

[0276] 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。

[0277] 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 可以检测到装置 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。

[0278] 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，通信组件 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，所述通信组件 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。

[0279] 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。

[0280] 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 1520 执行以完成上述终端侧的方法，或完成上述可穿戴设备侧的方法。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。

[0281] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本发明的其它实施方案。本申请旨在涵盖本发明的任何变型、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发明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，本发明的真正范围和精神由下面的权利要求指出。

[0282] 应当理解的是，本发明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。本发明的范围仅由所附的权利要求来限制。

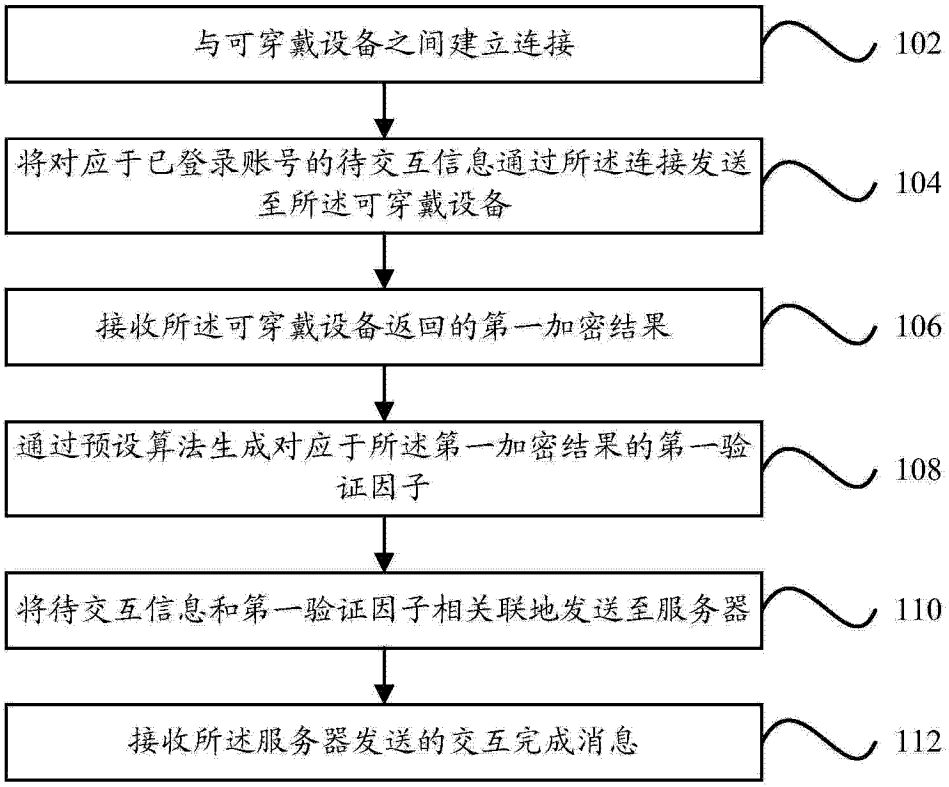

与可穿戴设备之间建立连接
102
将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备
104
接收所述可穿戴设备返回的第一加密结果
106
通过预设算法生成对应于所述第一加密结果的第一验证因子
108
将待交互信息和第一验证因子相关联地发送至服务器
110
接收所述服务器发送的交互完成消息
112

图 1A

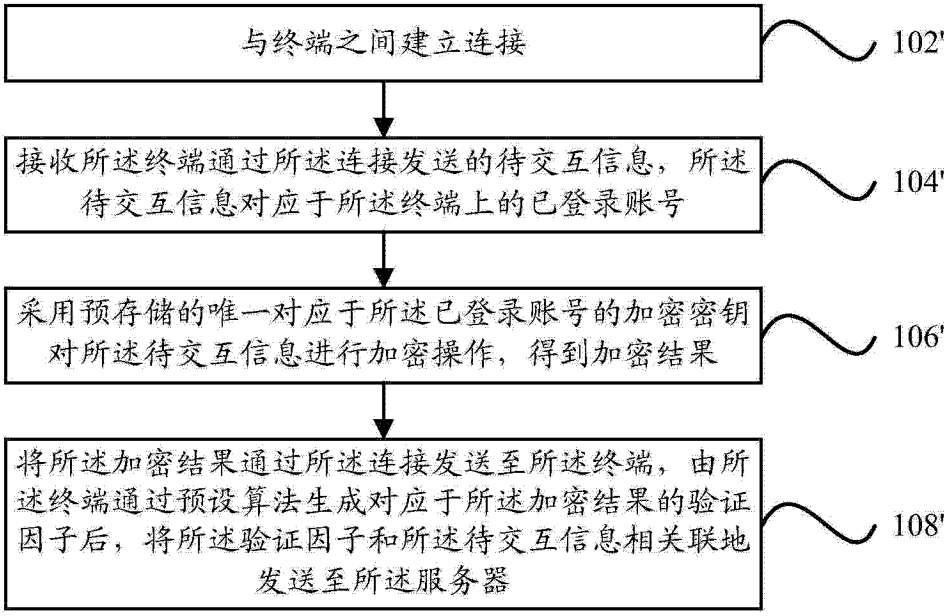

与终端之间建立连接
102'
接收所述终端通过所述连接发送的待交互信息，所述待交互信息对应于所述终端上的已登录账号
104'
采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果
106'
将所述加密结果通过所述连接发送至所述终端，由所述终端通过预设算法生成对应于所述加密结果的验证因子后，将所述验证因子和所述待交互信息相关联地发送至所述服务器
108'

图 1B

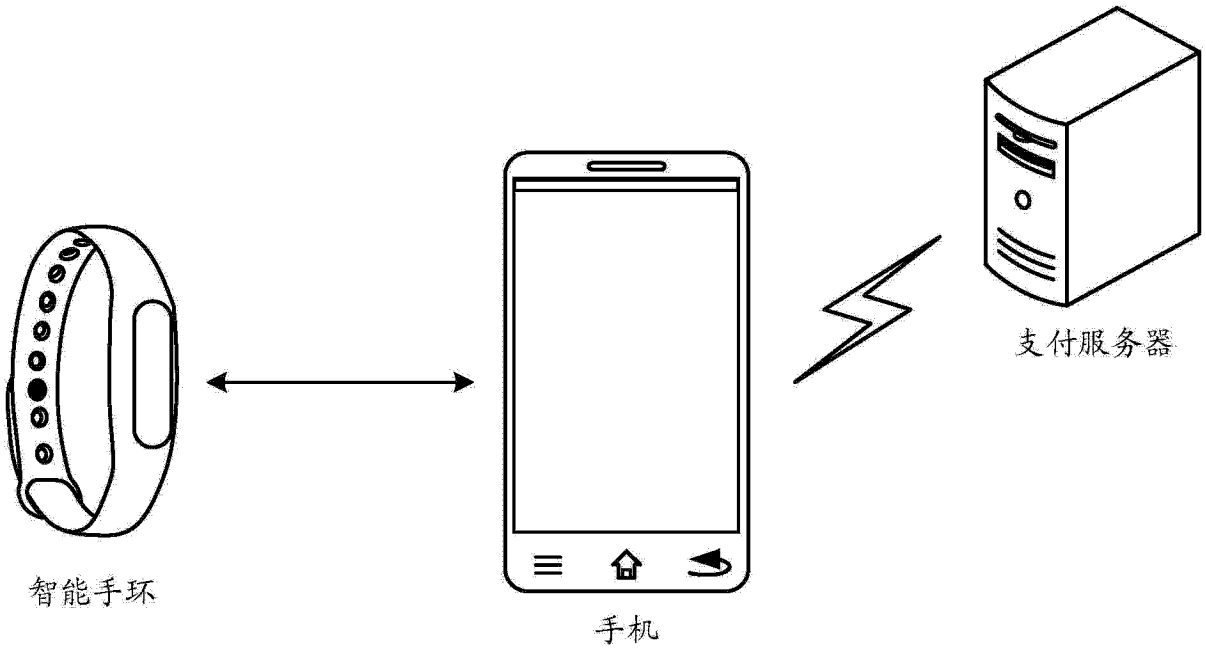


图 2

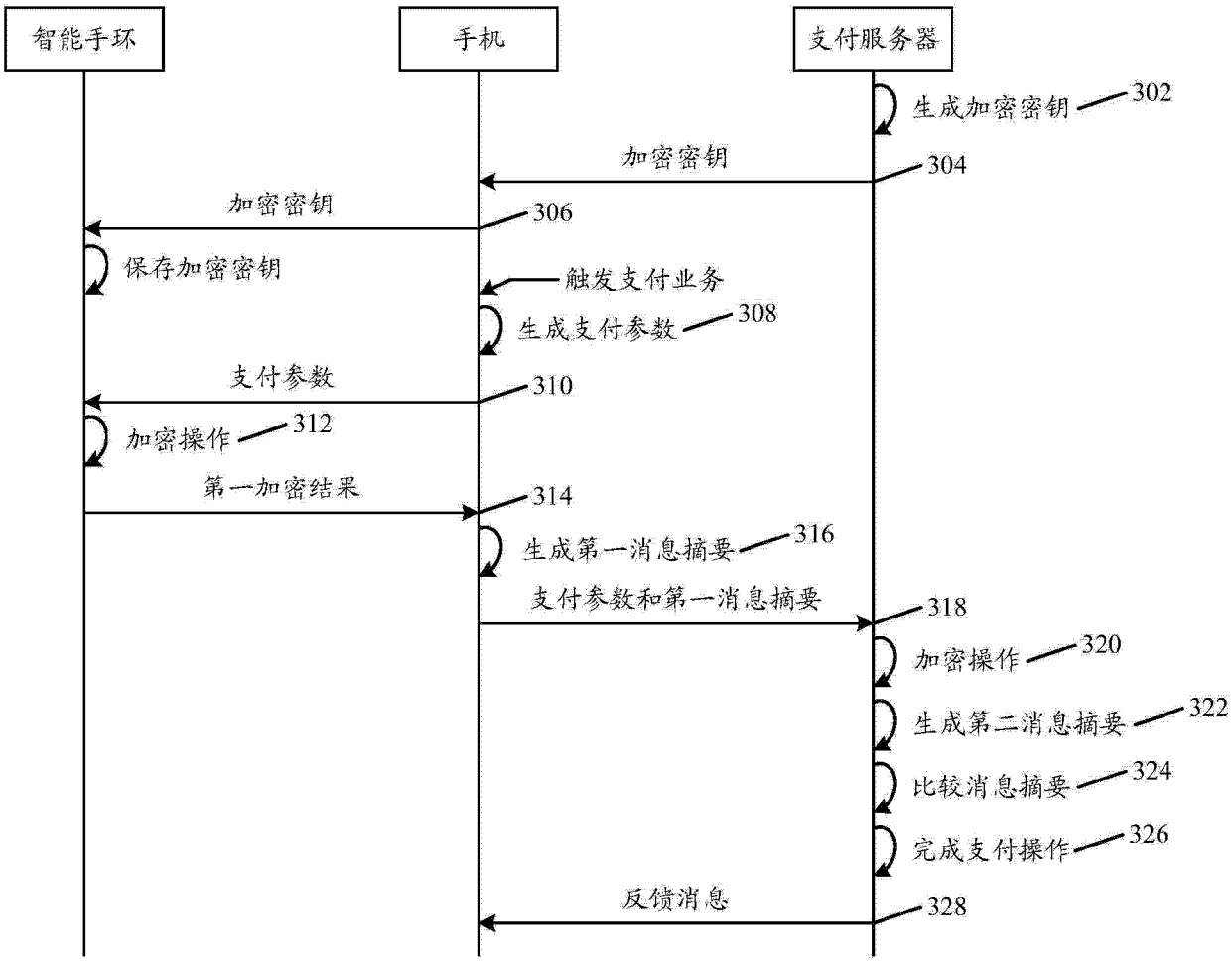

智能手环
手机
支付服务器
生成加密密钥
302
加密密钥
304
加密密钥
306
保存加密密钥
触发支付业务
生成支付参数
308
支付参数
310
加密操作
312
第一加密结果
314
生成第一消息摘要
316
支付参数和第一消息摘要
318
加密操作
320
生成第二消息摘要
322
比较消息摘要
324
完成支付操作
326
反馈消息
328

图 3

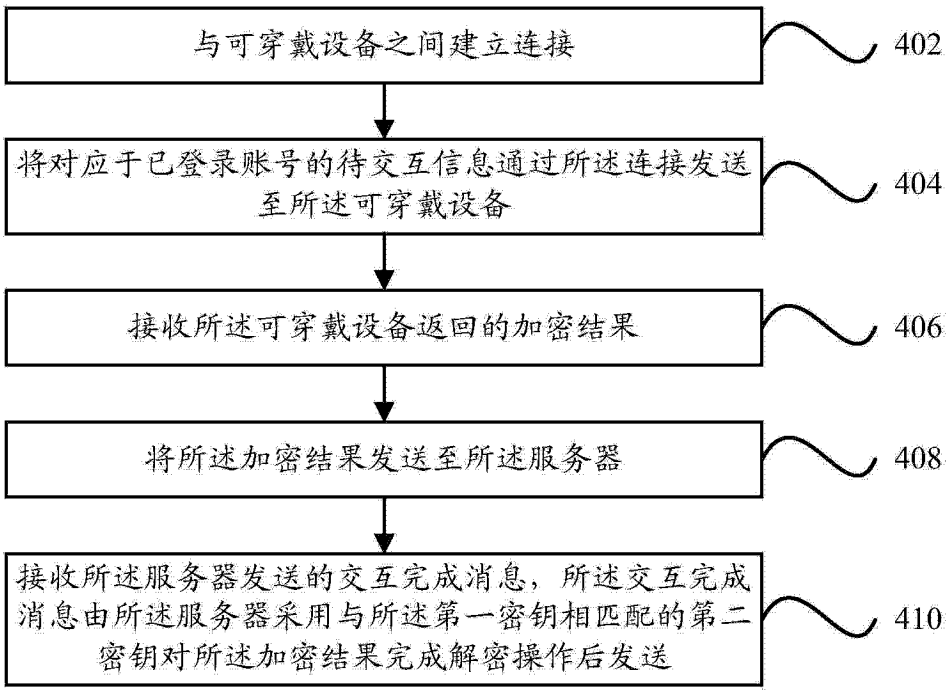

与可穿戴设备之间建立连接
402
将对应于已登录账号的待交互信息通过所述连接发送至所述可穿戴设备
404
接收所述可穿戴设备返回的加密结果
406
将所述加密结果发送至所述服务器
408
接收所述服务器发送的交互完成消息，所述交互完成消息由所述服务器采用与所述第一密钥相匹配的第二密钥对所述加密结果完成解密操作后发送
410

图 4A

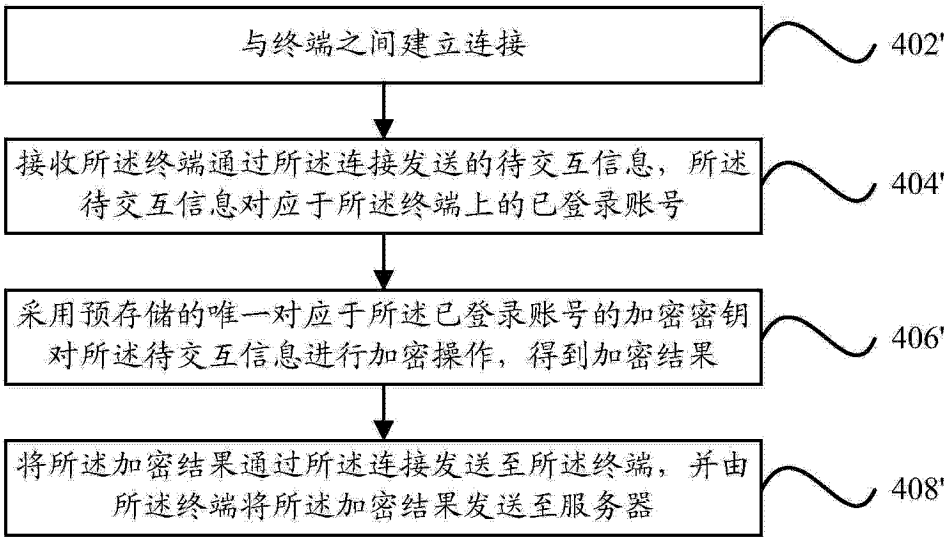

与终端之间建立连接
402'
接收所述终端通过所述连接发送的待交互信息，所述待交互信息对应于所述终端上的已登录账号
404'
采用预存储的唯一对应于所述已登录账号的加密密钥对所述待交互信息进行加密操作，得到加密结果
406'
将所述加密结果通过所述连接发送至所述终端，并由所述终端将所述加密结果发送至服务器
408'

图 4B

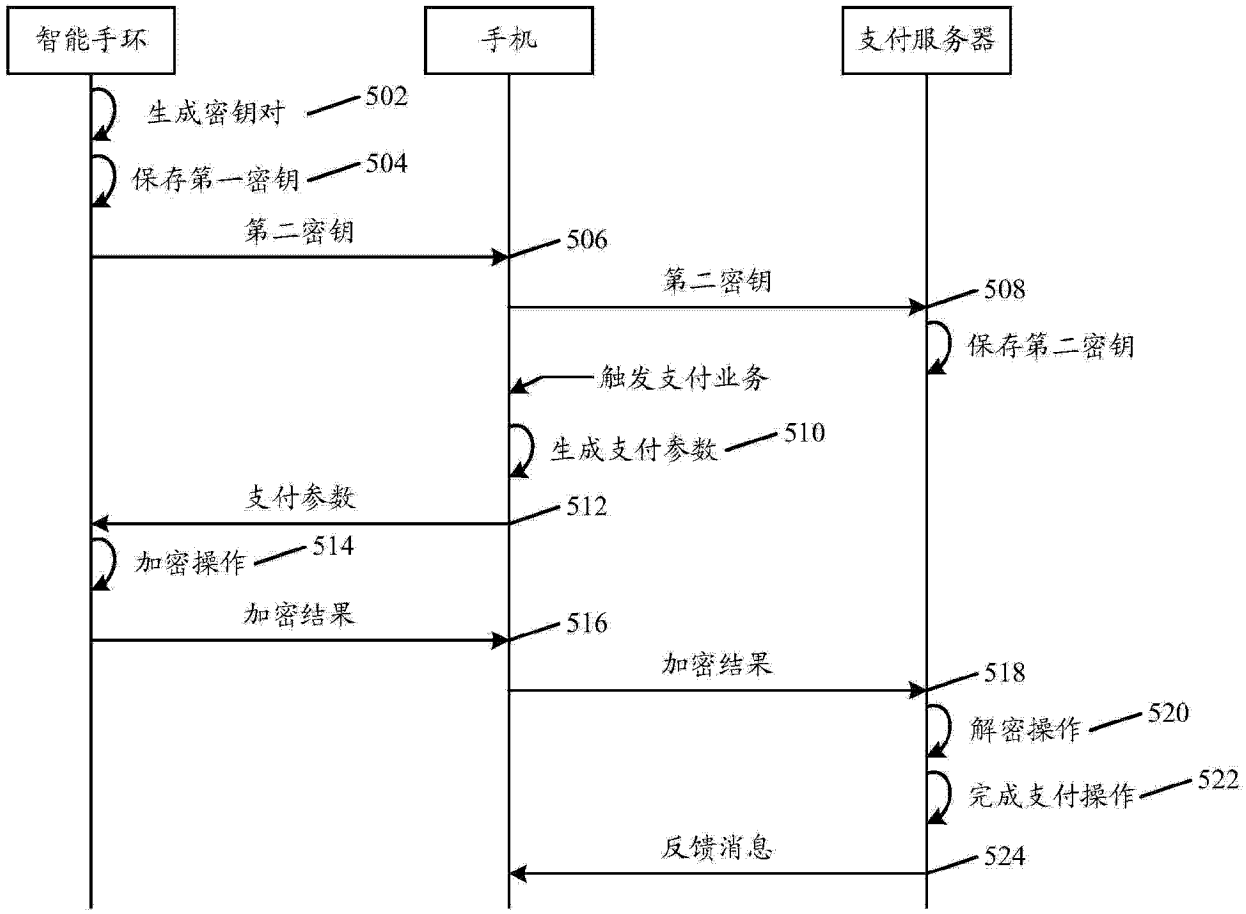

智能手环
手机
支付服务器
生成密钥对
502
保存第一密钥
504
第二密钥
506
第二密钥
508
保存第二密钥
触发支付业务
生成支付参数
510
支付参数
512
加密操作
514
加密结果
516
加密结果
518
解密操作
520
完成支付操作
522
反馈消息
524

图 5

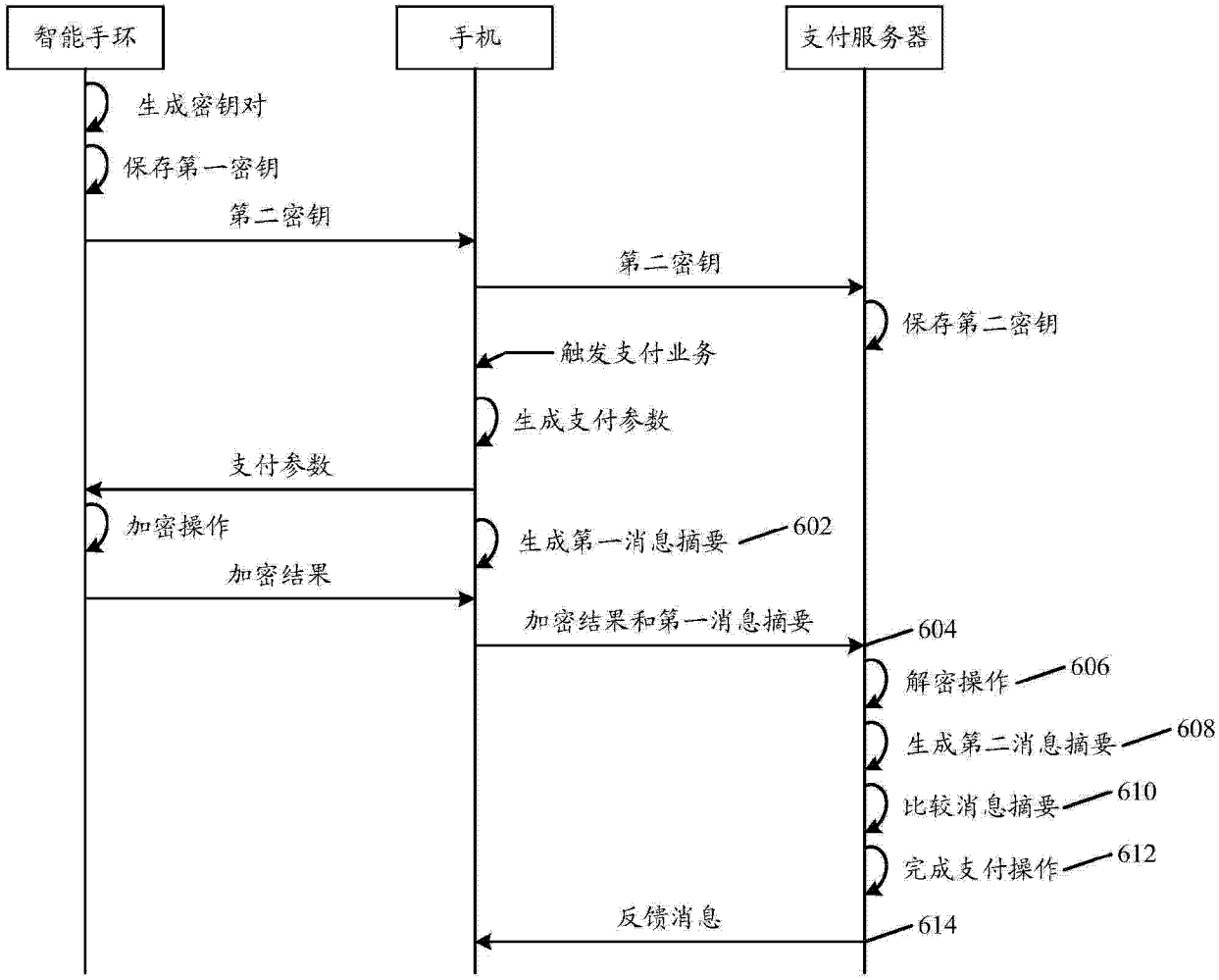

智能手环
手机
支付服务器
生成密钥对
保存第一密钥
第二密钥
第二密钥
保存第二密钥
触发支付业务
生成支付参数
支付参数
加密操作
生成第一消息摘要
602
加密结果
加密结果和第一消息摘要
604
解密操作
606
生成第二消息摘要
608
比较消息摘要
610
完成支付操作
612
反馈消息
614

图 6

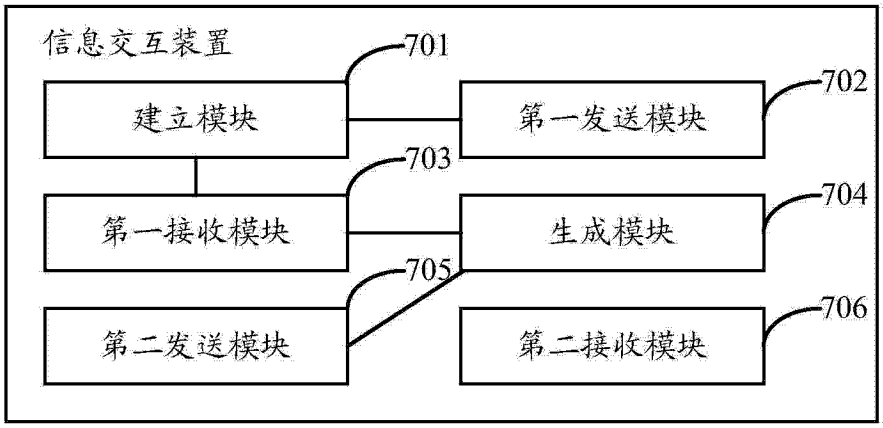

信息交互装置
701
建立模块
第一发送模块
702
703
第一接收模块
生成模块
704
705
第二发送模块
第二接收模块
706

图 7

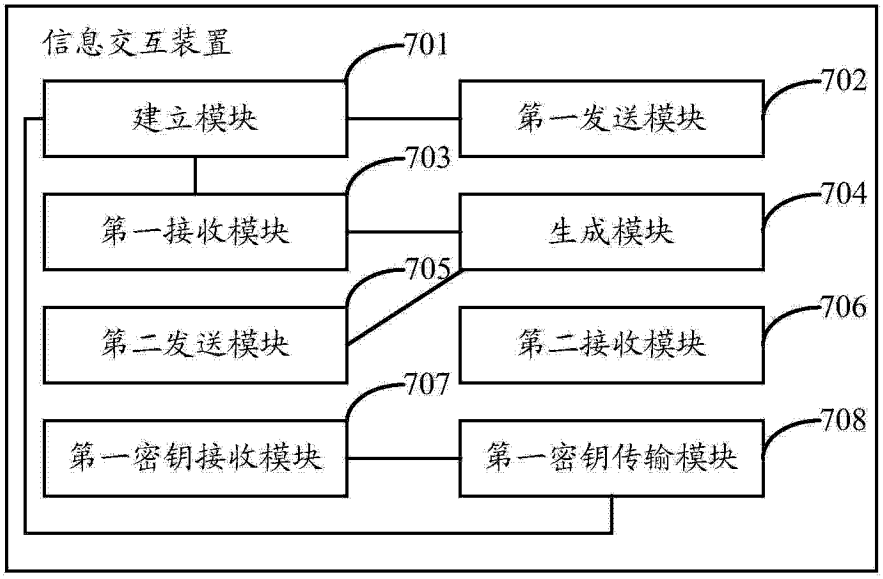

信息交互装置
701
建立模块
702
第一发送模块
703
第一接收模块
704
生成模块
705
第二发送模块
706
第二接收模块
707
第一密钥接收模块
708
第一密钥传输模块

图 8

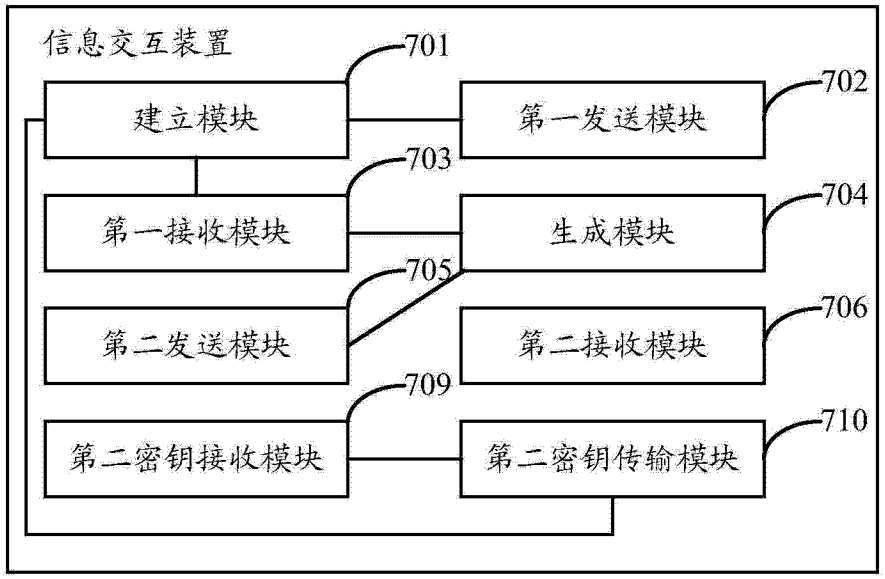

信息交互装置
701
建立模块
702
第一发送模块
703
第一接收模块
704
生成模块
705
第二发送模块
706
第二接收模块
709
第二密钥接收模块
710
第二密钥传输模块

图 9

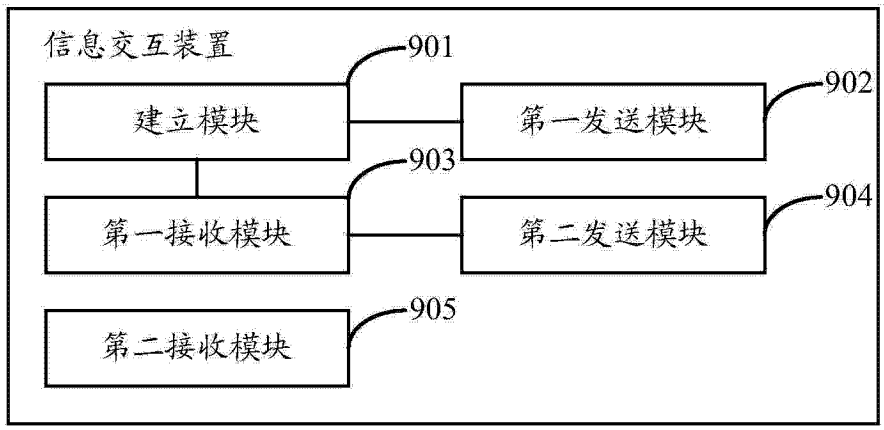

信息交互装置
901
建立模块
902
第一发送模块
903
第一接收模块
904
第二发送模块
905
第二接收模块

图 10

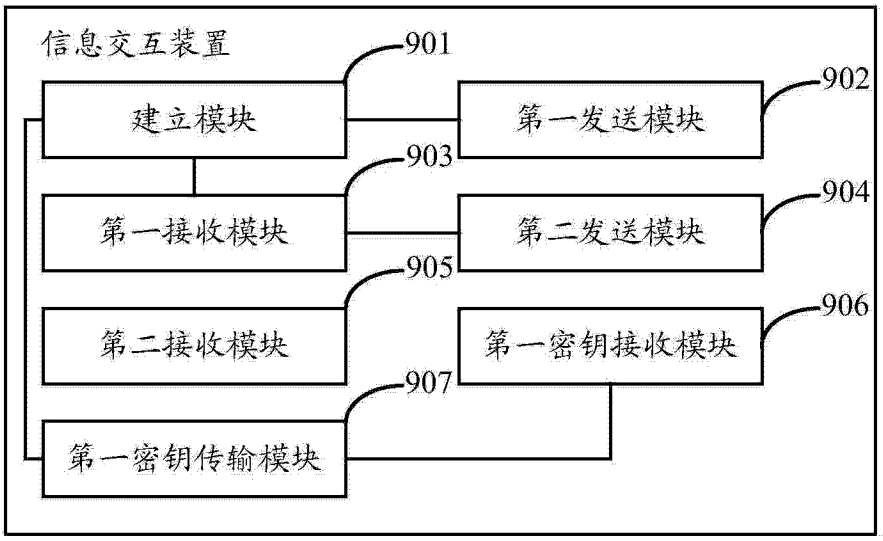

信息交互装置
901
建立模块
902
第一发送模块
903
第一接收模块
904
第二发送模块
905
第二接收模块
906
第一密钥接收模块
907
第一密钥传输模块

图 11

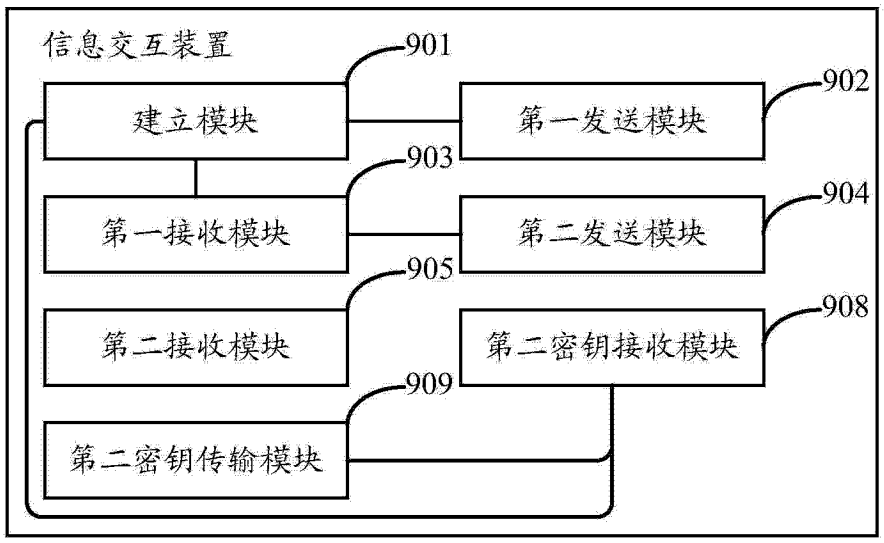

信息交互装置
901
建立模块
902
第一发送模块
903
第一接收模块
904
第二发送模块
905
第二接收模块
908
第二密钥接收模块
909
第二密钥传输模块

图 12

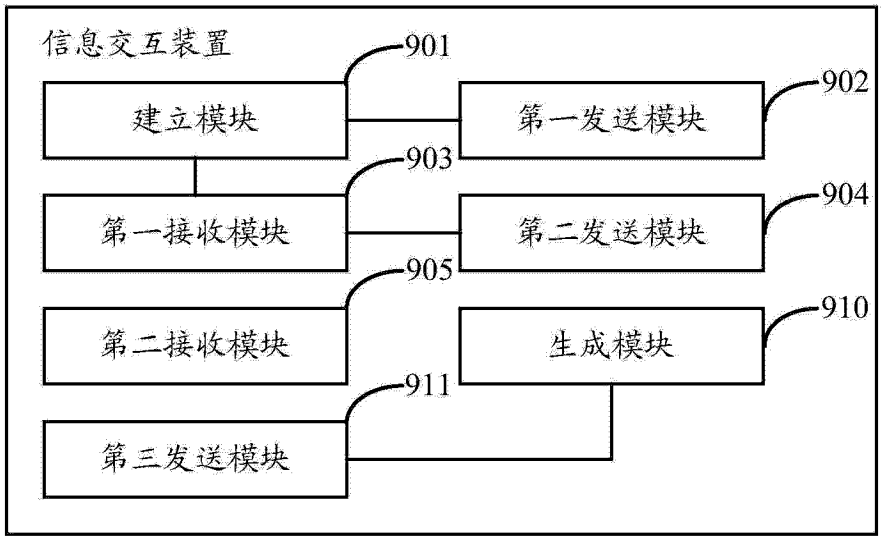

信息交互装置
901
建立模块
902
第一发送模块
903
第一接收模块
904
第二发送模块
905
第二接收模块
910
生成模块
911
第三发送模块

图 13

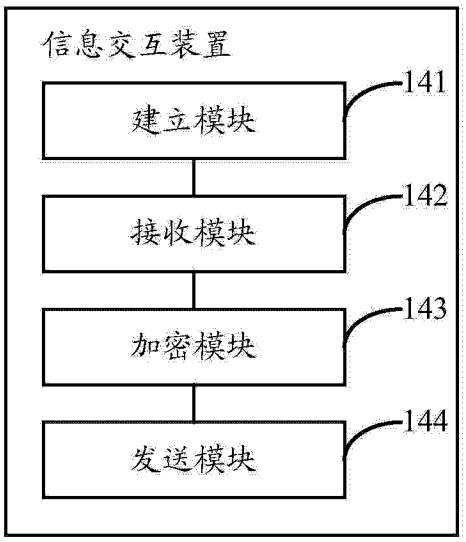


图 14

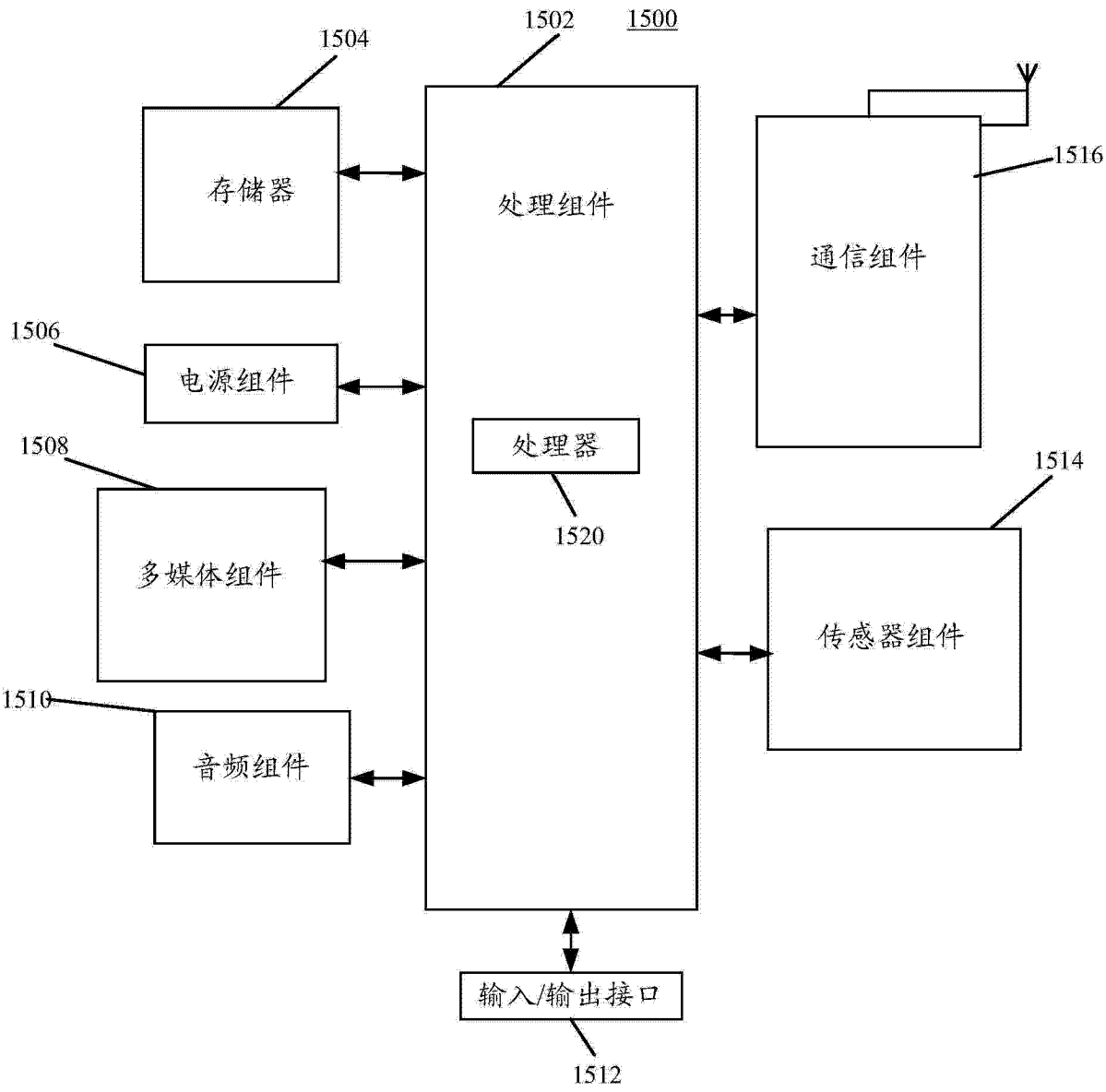

1502
1500
1504
存储器
处理组件
通信组件
1516
1506
电源组件
处理器
1520
1508
多媒体组件
1514
传感器组件
1510
音频组件
输入/输出接口
1512

图 15