(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105120452 B
(45)授权公告日 2018.11.23

(21)申请号 201510373613.4

(22)申请日 2015.06.30

(65)同一申请的已公布的文献号
申请公布号 CN 105120452 A

(43)申请公布日 2015.12.02

(73)专利权人 北京小米支付技术有限公司
地址 100176 北京市北京经济技术开发区科创十四街99号33幢D栋2层2243号（集中办公区）

(72)发明人 刘书文 张晓亮 于红亮

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 徐立

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/04(2009.01)

(56)对比文件
CN 104144049 A,2014.11.12,
CN 104510132 A,2015.04.22,
CN 102497465 A,2012.06.13,
CN 104243484 A,2014.12.24,
US 20130166456 A1,2013.06.27,
CN 103473514 A,2013.12.25,

审查员 董春阳

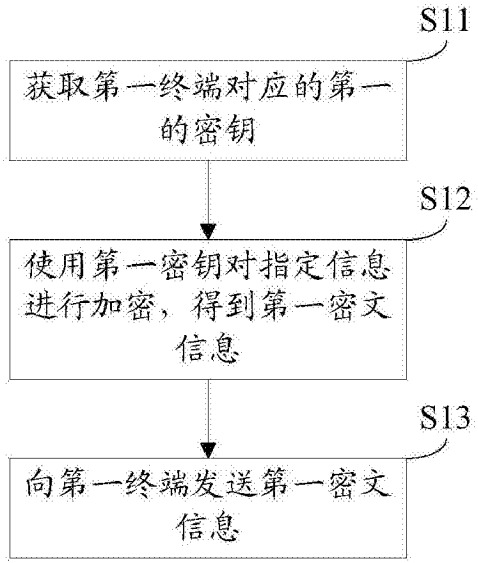
权利要求书5页 说明书21页 附图9页

(54)发明名称

传输信息的方法、装置及系统

(57)摘要

本公开是关于一种传输信息的方法、装置及系统，属于数据传输技术领域。所述方法包括：获取第一终端对应的第一密钥，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；使用所述第一密钥对指定信息进行加密，得到第一密文信息；向第一终端发送所述第一密文信息，所述第一终端用于采用所述第一可穿戴设备对所述第一密文信息进行解密。本公开通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。



CN 105120452 B

1.一种传输信息的方法，其特征在于，包括：

获取第一终端对应的第一密钥，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

使用所述第一密钥对指定信息进行加密，得到第一密文信息；

向所述第一终端发送所述第一密文信息，所述第一终端用于采用所述第一可穿戴设备对所述第一密文信息进行解密，得到所述指定信息。

2.根据权利要求1所述的方法，其特征在于，当所述方法由服务器执行时，所述获取第一终端对应的第一密钥，包括：

根据存储的终端和密钥的对应关系，获取所述第一终端对应的第一密钥。

3.根据权利要求2所述的方法，其特征在于，所述方法还包括：

接收密文形式的第二密钥，所述密文形式的第二密钥是所述第一可穿戴设备使用第三密钥对第二密钥进行加密得到的，所述第二密钥和所述第三密钥均是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥；

使用所述第一密钥对所述密文形式的第二密钥进行解密，得到所述第二密钥；

将所述第一终端对应的第一密钥更新为所述第二密钥。

4.根据权利要求1所述的方法，其特征在于，当所述方法由服务器执行时，所述方法还包括：

接收第二密文信息，所述第二密文信息是第二可穿戴设备使用第二终端对应的第四密钥对所述指定信息进行加密得到的，所述第四密钥是所述第二可穿戴设备根据所述第二可穿戴设备的标识和用户输入的密码指令生成的，所述第四密钥为对称算法中使用的密钥；

使用所述第四密钥对所述第二密文信息进行解密，得到所述指定信息。

5.根据权利要求4所述的方法，其特征在于，所述方法还包括：

接收密文形式的第五密钥，所述密文形式的第五密钥是所述第二可穿戴设备使用所述第四密钥对第五密钥进行加密得到的，所述第五密钥是所述第二可穿戴设备根据所述第二可穿戴设备的标识和用户输入的密码指令生成的；

使用所述第四密钥对所述密文形式的第五密钥进行解密，得到所述第五密钥；

将所述第二终端对应的第四密钥更新为所述第五密钥。

6.根据权利要求1所述的方法，其特征在于，当所述方法由第二终端执行时，所述获取第一终端对应的第一密钥，包括：

向服务器发送密钥请求，所述密钥请求用于获取所述第一密钥；

接收所述第一密钥，所述第一密钥是所述服务器根据存储的终端和密钥的对应关系获取的。

7.根据权利要求1所述的方法，其特征在于，当所述方法由第二终端执行时，所述使用所述第一密钥对所述指定信息进行加密，得到第一密文信息，包括：

向第二可穿戴设备发送所述第一密钥和所述指定信息；

接收所述第一密文信息，所述第一密文信息是所述第二可穿戴设备使用所述第一密钥对所述指定信息进行加密得到的。

8.一种传输信息的方法，其特征在于，包括：

接收第一密文信息，所述第一密文信息是使用第一终端对应的第一密钥对指定信息进行加密得到的，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

向所述第一可穿戴设备发送所述第一密文信息；

接收所述指定信息，所述指定信息是所述第一可穿戴设备使用第三密钥对所述第一密文信息进行解密得到的，所述第三密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

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：

接收密文形式的第二密钥，所述密文形式的第二密钥是所述第一可穿戴设备使用所述第三密钥对第二密钥进行加密得到的，所述第二密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

向服务器发送所述密文形式的第二密钥，以使所述服务器使用所述第一密钥对所述密文形式的第二密钥进行解密，得到所述第二密钥，并将所述第一终端对应的第一密钥更新为所述第二密钥。

10.一种传输信息的装置，其特征在于，包括：

密钥获取模块，用于获取第一终端对应的第一密钥，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

信息加密模块，用于使用所述第一密钥对指定信息进行加密，得到第一密文信息；

信息发送模块，用于向所述第一终端发送所述第一密文信息，所述第一终端用于采用所述第一可穿戴设备对所述第一密文信息进行解密，得到所述指定信息。

11.根据权利要求10所述的装置，其特征在于，当所述装置为服务器时，所述密钥获取模块用于，

根据存储的终端和密钥的对应关系，获取所述第一终端对应的第一密钥。

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：

第一密钥接收模块，用于接收密文形式的第二密钥，所述密文形式的第二密钥是所述第一可穿戴设备使用第三密钥对第二密钥进行加密得到的，所述第二密钥和所述第三密钥均是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥；

第一密钥解密模块，用于使用所述第一密钥对所述密文形式的第二密钥进行解密，得到所述第二密钥；

第一密钥更新模块，用于将所述第一终端对应的第一密钥更新为所述第二密钥。

13.根据权利要求10所述的装置，其特征在于，当所述装置为服务器时，所述装置还包括：

信息接收模块，用于接收第二密文信息，所述第二密文信息是第二可穿戴设备使用第二终端对应的第四密钥对所述指定信息进行加密得到的，所述第四密钥是所述第二可穿戴设备根据所述第二可穿戴设备的标识和用户输入的密码指令生成的，所述第四密钥为对称算法中使用的密钥；

信息解密模块，用于使用所述第四密钥对所述第二密文信息进行解密，得到所述指定信息。

14.根据权利要求13所述的装置，其特征在于，所述装置还包括：

第二密钥接收模块，用于接收密文形式的第五密钥，所述密文形式的第五密钥是所述第二可穿戴设备使用所述第四密钥对第五密钥进行加密得到的，所述第五密钥是所述第二可穿戴设备根据所述第二可穿戴设备的标识和用户输入的密码指令生成的；

第二密钥解密模块，用于使用所述第四密钥对所述密文形式的第五密钥进行解密，得到所述第五密钥；

第二密钥更新模块，用于将所述第二终端对应的第四密钥更新为所述第五密钥。

15.根据权利要求10所述的装置，其特征在于，当所述装置为第二终端时，所述密钥获取模块包括：

请求发送子模块，用于向服务器发送密钥请求，所述密钥请求用于获取所述第一密钥；

密钥接收子模块，用于接收所述第一密钥，所述第一密钥是所述服务器根据存储的终端和密钥的对应关系获取的。

16.根据权利要求10所述的装置，其特征在于，当所述装置为第二终端时，所述信息加密模块包括：

信息发送子模块，用于向第二可穿戴设备发送所述第一密钥和所述指定信息；

信息接收子模块，用于接收所述第一密文信息，所述第一密文信息是所述第二可穿戴设备使用所述第一密钥对所述指定信息进行加密得到的。

17.一种传输信息的装置，其特征在于，包括：

第一接收模块，用于接收第一密文信息，所述第一密文信息是使用第一终端对应的第一密钥对指定信息进行加密得到的，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

第一发送模块，用于向所述第一可穿戴设备发送所述第一密文信息；

第二接收模块，用于接收所述指定信息，所述指定信息是所述第一可穿戴设备使用第三密钥对所述第一密文信息进行解密得到的，所述第三密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

18.根据权利要求17所述的装置，其特征在于，所述装置还包括：

第三接收模块，用于接收密文形式的第二密钥，所述密文形式的第二密钥是所述第一可穿戴设备使用所述第三密钥对第二密钥进行加密得到的，所述第二密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

第二发送模块，用于向服务器发送所述密文形式的第二密钥，以使所述服务器使用所述第一密钥对所述密文形式的第二密钥进行解密，得到所述第二密钥，并将所述第一终端对应的第一密钥更新为所述第二密钥。

19.一种传输信息的装置，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：

获取第一终端对应的第一密钥，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

使用所述第一密钥对指定信息进行加密，得到第一密文信息；

向所述第一终端发送所述第一密文信息，所述第一终端用于采用所述第一可穿戴设备对所述第一密文信息进行解密，得到所述指定信息。

20.一种传输信息的装置，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：

接收第一密文信息，所述第一密文信息是使用第一终端对应的第一密钥对指定信息进行加密得到的，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

向所述第一可穿戴设备发送所述第一密文信息；

接收所述指定信息，所述指定信息是所述第一可穿戴设备使用第三密钥对所述第一密文信息进行解密得到的，所述第三密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

21.一种传输信息的系统，其特征在于，包括：

第一可穿戴设备，用于根据所述第一可穿戴设备的标识和用户输入的密码指令生成第一终端对应的第一密钥和第三密钥，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥；

服务器，用于获取所述第一密钥；使用所述第一密钥对指定信息进行加密，得到第一密文信息；向所述第一终端发送所述第一密文信息；

所述第一终端，用于接收所述第一密文信息；向所述第一可穿戴设备发送所述第一密文信息；

所述第一可穿戴设备还用于，接收所述第一密文信息；使用所述第三密钥对所述第一密文信息进行解密，得到所述指定信息；向所述第一终端发送所述指定信息；

所述第一终端还用于，接收所述指定信息。

22.一种传输信息的系统，其特征在于，包括：

第一可穿戴设备，用于根据所述第一可穿戴设备的标识和用户输入的密码指令生成第一终端对应的第一密钥和第三密钥，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥；

第二终端，用于向服务器发送密钥请求，所述密钥请求用于获取所述第一密钥；

所述服务器，用于接收所述密钥请求；根据存储的终端和密钥的对应关系，获取所述第一密钥；向所述第二终端发送所述第一密钥；

所述第二终端还用于，接收所述第一密钥；向第二可穿戴设备发送所述第一密钥；

所述第二可穿戴设备，用于接收所述第一密钥；使用所述第一密钥对指定信息进行加密，得到第一密文信息；向所述第二终端发送所述第一密文信息；

所述第二终端还用于，接收所述第一密文信息；向所述第一终端发送所述第一密文信

息；

所述第一终端，用于接收所述第一密文信息；向所述第一可穿戴设备发送所述第一密文信息；

所述第一可穿戴设备还用于，接收所述第一密文信息；使用所述第三密钥对所述第一密文信息进行解密，得到所述指定信息；向所述第一终端发送所述指定信息；

所述第一终端还用于，接收所述指定信息。

23.一种传输信息的系统，其特征在于，包括：

第一可穿戴设备，用于根据所述第一可穿戴设备的标识和用户输入的密码指令生成第一终端对应的第一密钥和第三密钥，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥；

第二可穿戴设备，用于根据所述第二可穿戴设备的标识和用户输入的密码指令生成第二终端对应的第四密钥，所述第四密钥为对称算法中使用的密钥；使用所述第四密钥对指定信息进行加密，得到第二密文信息；向所述第二终端发送所述第二密文信息；

所述第二终端，用于接收所述第二密文信息；向服务器发送所述第二密文信息；

所述服务器，用于接收所述第二密文信息；使用所述第四密钥对所述第二密文信息进行解密，得到所述指定信息；获取所述第一密钥；使用所述第一密钥对所述指定信息进行加密，得到第一密文信息；向所述第一终端发送所述第一密文信息；

所述第一终端，用于接收所述第一密文信息；向所述第一可穿戴设备发送所述第一密文信息；

所述第一可穿戴设备还用于，接收所述第一密文信息；使用所述第三密钥对所述第一密文信息进行解密，得到所述指定信息；向所述第一终端发送所述指定信息；

所述第一终端还用于，接收所述指定信息。

传输信息的方法、装置及系统

技术领域

[0001] 本公开涉及数据传输技术领域，尤其涉及一种传输信息的方法、装置及系统。

背景技术

[0002] 随着移动互联网技术的发展，人们通过移动终端传输的数据越来越多。这些通过移动终端传输的数据中包括如付款的验证码、银行的账号和密码等敏感信息。

[0003] 相关技术中，移动终端的所有数据均采用明文传输。

[0004] 由于数据在传输的过程中存在被第三方截获的风险，当第三方截获采用明文传输的敏感信息时，即可获取到敏感信息的真实内容，造成敏感信息泄露。

发明内容

[0005] 为克服相关技术中存在的泄露用户敏感信息的问题，本公开提供一种传输信息的方法、装置及系统。

[0006] 根据本公开实施例的第一方面，提供一种传输信息的方法，包括：

[0007] 获取第一终端对应的第一密钥，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

[0008] 使用所述第一密钥对指定信息进行加密，得到第一密文信息；

[0009] 向所述第一终端发送所述第一密文信息，所述第一终端用于采用所述第一可穿戴设备对所述第一密文信息进行解密，得到所述指定信息。

[0010] 在第一方面一种可能的实现方式中，当所述方法由服务器执行时，所述获取第一终端对应的第一密钥，包括：

[0011] 根据存储的终端和密钥的对应关系，获取所述第一终端对应的第一密钥。

[0012] 可选地，所述方法还包括：

[0013] 接收密文形式的第二密钥，所述密文形式的第二密钥是所述第一可穿戴设备使用第三密钥对第二密钥进行加密得到的，所述第二密钥和所述第三密钥均是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥；

[0014] 使用所述第一密钥对所述密文形式的第二密钥进行解密，得到所述第二密钥；

[0015] 将所述第一终端对应的第一密钥更新为所述第二密钥。

[0016] 在第一方面另一种可能的实现方式中，当所述方法由服务器执行时，所述方法还包括：

[0017] 接收第二密文信息，所述第二密文信息是第二可穿戴设备使用第二终端对应的第四密钥对所述指定信息进行加密得到的，所述第四密钥是所述第二可穿戴设备根据所述第二可穿戴设备的标识和用户输入的密码指令生成的，所述第四密钥为对称算法中使用的密钥；

[0018] 使用所述第四密钥对所述第二密文信息进行解密，得到所述指定信息。

[0019] 可选地，所述方法还包括：

[0020] 接收密文形式的第五密钥，所述密文形式的第五密钥是所述第二可穿戴设备使用所述第四密钥对第五密钥进行加密得到的，所述第五密钥是所述第二可穿戴设备根据所述第二可穿戴设备的标识和用户输入的密码指令生成的；

[0021] 使用所述第四密钥对所述密文形式的第五密钥进行解密，得到所述第五密钥；

[0022] 将所述第二终端对应的第四密钥更新为所述第五密钥。

[0023] 在第一方面又一种可能的实现方式中，当所述方法由第二终端执行时，所述获取第一终端对应的第一密钥，包括：

[0024] 向服务器发送密钥请求，所述密钥请求用于获取所述第一密钥；

[0025] 接收所述第一密钥，所述第一密钥是所述服务器根据存储的终端和密钥的对应关系获取的。

[0026] 在第一方面又一种可能的实现方式中，当所述方法由第二终端执行时，所述使用所述第一密钥对所述指定信息进行加密，得到第一密文信息，包括：

[0027] 向第二可穿戴设备发送所述第一密钥和所述指定信息；

[0028] 接收所述第一密文信息，所述第一密文信息是所述第二可穿戴设备使用所述第一密钥对所述指定信息进行加密得到的。

[0029] 根据本公开实施例的第二方面，提供一种传输信息的方法，包括：

[0030] 接收第一密文信息，所述第一密文信息是使用第一终端对应的第一密钥对指定信息进行加密得到的，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

[0031] 向所述第一可穿戴设备发送所述第一密文信息；

[0032] 接收所述指定信息，所述指定信息是所述第一可穿戴设备使用第三密钥对所述第一密文信息进行解密得到的，所述第三密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0033] 在第二方面一种可能的实现方式中，所述方法还包括：

[0034] 接收密文形式的第二密钥，所述密文形式的第二密钥是所述第一可穿戴设备使用所述第三密钥对第二密钥进行加密得到的，所述第二密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

[0035] 向服务器发送所述密文形式的第二密钥，以使所述服务器使用所述第一密钥对所述密文形式的第二密钥进行解密，得到所述第二密钥，并将所述第一终端对应的第一密钥更新为所述第二密钥。

[0036] 根据本公开实施例的第三方面，提供一种传输信息的装置，包括：

[0037] 密钥获取模块，用于获取第一终端对应的第一密钥，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

[0038] 信息加密模块，用于使用所述第一密钥对指定信息进行加密，得到第一密文信息；

[0039] 信息发送模块，用于向所述第一终端发送所述第一密文信息，所述第一终端用于采用所述第一可穿戴设备对所述第一密文信息进行解密，得到所述指定信息。

[0040] 在第三方面一种可能的实现方式中，当所述装置为服务器时，所述密钥获取模块

用于，

[0041] 根据存储的终端和密钥的对应关系，获取所述第一终端对应的第一密钥。

[0042] 可选地，所述装置还包括：

[0043] 第一密钥接收模块，用于接收密文形式的第二密钥，所述密文形式的第二密钥是所述第一可穿戴设备使用第三密钥对第二密钥进行加密得到的，所述第二密钥和所述第三密钥均是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥；

[0044] 第一密钥解密模块，用于使用所述第一密钥对所述密文形式的第二密钥进行解密，得到所述第二密钥；

[0045] 第一密钥更新模块，用于将所述第一终端对应的第一密钥更新为所述第二密钥。

[0046] 在第三方面另一种可能的实现方式中，当所述装置为服务器时，所述装置还包括：

[0047] 信息接收模块，用于接收第二密文信息，所述第二密文信息是第二可穿戴设备使用第二终端对应的第四密钥对所述指定信息进行加密得到的，所述第四密钥是所述第二可穿戴设备根据所述第二可穿戴设备的标识和用户输入的密码指令生成的，所述第四密钥为对称算法中使用的密钥；

[0048] 信息解密模块，用于使用所述第四密钥对所述第二密文信息进行解密，得到所述指定信息。

[0049] 可选地，所述装置还包括：

[0050] 第二密钥接收模块，用于接收密文形式的第五密钥，所述密文形式的第五密钥是所述第二可穿戴设备使用所述第四密钥对第五密钥进行加密得到的，所述第五密钥是所述第二可穿戴设备根据所述第二可穿戴设备的标识和用户输入的密码指令生成的；

[0051] 第二密钥解密模块，用于使用所述第四密钥对所述密文形式的第五密钥进行解密，得到所述第五密钥；

[0052] 第二密钥更新模块，用于将所述第二终端对应的第四密钥更新为所述第五密钥。

[0053] 在第三方面又一种可能的实现方式中，当所述装置为第二终端时，所述信息获取模块包括：

[0054] 请求发送子模块，用于向服务器发送密钥请求，所述密钥请求用于获取所述第一密钥；

[0055] 密钥接收子模块，用于接收所述第一密钥，所述第一密钥是所述服务器根据存储的终端和密钥的对应关系获取的。

[0056] 在第三方面又一种可能的实现方式中，当所述装置为第二终端时，所述信息加密模块包括：

[0057] 信息发送子模块，用于向第二可穿戴设备发送所述第一密钥和所述指定信息；

[0058] 信息接收子模块，用于接收所述第一密文信息，所述第一密文信息是所述第二可穿戴设备使用所述第一密钥对所述指定信息进行加密得到的。

[0059] 根据本公开实施例的第四方面，提供一种传输信息的装置，包括：

[0060] 第一接收模块，用于接收第一密文信息，所述第一密文信息是使用第一终端对应的第一密钥对指定信息进行加密得到的，所述第一密钥是第一可穿戴设备根据所述第一可

穿戴设备的标识和用户输入的密码指令生成的；

[0061] 第一发送模块，用于向所述第一可穿戴设备发送所述第一密文信息；

[0062] 第二接收模块，用于接收所述指定信息，所述指定信息是所述第一可穿戴设备使用第三密钥对所述第一密文信息进行解密得到的，所述第三密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0063] 在第四方面一种可能的实现方式中，所述装置还包括：

[0064] 第三接收模块，用于接收密文形式的第二密钥，所述密文形式的第二密钥是所述第一可穿戴设备使用所述第三密钥对第二密钥进行加密得到的，所述第二密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

[0065] 第二发送模块，用于向服务器发送所述密文形式的第二密钥，以使所述服务器使用所述第一密钥对所述密文形式的第二密钥进行解密，得到所述第二密钥，并将所述第一终端对应的第一密钥更新为所述第二密钥。

[0066] 根据本公开实施例的第五方面，提供一种传输信息的装置，包括：

[0067] 处理器；

[0068] 用于存储处理器可执行指令的存储器；

[0069] 其中，所述处理器被配置为：

[0070] 获取第一终端对应的第一密钥，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

[0071] 使用所述第一密钥对指定信息进行加密，得到第一密文信息；

[0072] 向所述第一终端发送所述第一密文信息，所述第一终端用于采用所述第一可穿戴设备对所述第一密文信息进行解密，得到所述指定信息。

[0073] 根据本公开实施例的第六方面，提供一种传输信息的装置，包括：

[0074] 处理器；

[0075] 用于存储处理器可执行指令的存储器；

[0076] 其中，所述处理器被配置为：

[0077] 接收第一密文信息，所述第一密文信息是使用第一终端对应的第一密钥对指定信息进行加密得到的，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

[0078] 向所述第一可穿戴设备发送所述第一密文信息；

[0079] 接收所述指定信息，所述指定信息是所述第一可穿戴设备使用第三密钥对所述第一密文信息进行解密得到的，所述第三密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0080] 根据本公开实施例的第七方面，提供一种传输信息的系统，包括：

[0081] 第一可穿戴设备，用于根据所述第一可穿戴设备的标识和用户输入的密码指令生成第一终端对应的第一密钥和第三密钥，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥；

[0082] 服务器，用于获取所述第一密钥；使用所述第一密钥对指定信息进行加密，得到第

一密文信息;向所述第一终端发送所述第一密文信息;

[0083] 所述第一终端,用于接收所述第一密文信息;向所述第一可穿戴设备发送所述第一密文信息;

[0084] 所述第一可穿戴设备还用于,接收所述第一密文信息;使用所述第三密钥对所述第一密文信息进行解密,得到所述指定信息;向所述第一终端发送所述指定信息;

[0085] 所述第一终端还用于,接收所述指定信息。

[0086] 根据本公开实施例的第八方面,提供一种传输信息的系统,包括:

[0087] 第一可穿戴设备,用于根据所述第一可穿戴设备的标识和用户输入的密码指令生成第一终端对应的第一密钥和第三密钥,所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥;

[0088] 第二终端,用于向服务器发送密钥请求,所述密钥请求用于获取所述第一密钥;

[0089] 所述服务器,用于接收所述密钥请求;根据存储的终端和密钥的对应关系,获取所述第一密钥;向所述第二终端发送所述第一密钥;

[0090] 所述第二终端还用于,接收所述第一密钥;向第二可穿戴设备发送所述第一密钥;

[0091] 所述第二可穿戴设备,用于接收所述第一密钥;使用所述第一密钥对指定信息进行加密,得到第一密文信息;向所述第二终端发送所述第一密文信息;

[0092] 所述第二终端还用于,接收所述第一密文信息;向所述第一终端发送所述第一密文信息;

[0093] 所述第一终端,用于接收所述第一密文信息;向所述第一可穿戴设备发送所述第一密文信息;

[0094] 所述第一可穿戴设备还用于,接收所述第一密文信息;使用所述第三密钥对所述第一密文信息进行解密,得到所述指定信息;向所述第一终端发送所述指定信息;

[0095] 所述第一终端还用于,接收所述指定信息。

[0096] 根据本公开实施例的第九方面,提供一种传输信息的系统,包括:

[0097] 第一可穿戴设备,用于根据所述第一可穿戴设备的标识和用户输入的密码指令生成第一终端对应的第一密钥和第三密钥,所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥;

[0098] 第二可穿戴设备,用于根据所述第二可穿戴设备的标识和用户输入的密码指令生成第二终端对应的第四密钥,所述第四密钥为对称算法中使用的密钥;使用所述第四密钥对指定信息进行加密,得到第二密文信息;向所述第二终端发送所述第二密文信息;

[0099] 所述第二终端,用于接收所述第二密文信息;向服务器发送所述第二密文信息;

[0100] 所述服务器,用于接收所述第二密文信息;使用所述第四密钥对所述第二密文信息进行解密,得到所述指定信息;获取所述第一密钥;使用所述第一密钥对所述指定信息进行加密,得到第一密文信息;向所述第一终端发送所述第一密文信息;

[0101] 所述第一终端,用于接收所述第一密文信息;向所述第一可穿戴设备发送所述第一密文信息;

[0102] 所述第一可穿戴设备还用于,接收所述第一密文信息;使用所述第三密钥对所述第一密文信息进行解密,得到所述指定信息;向所述第一终端发送所述指定信息;

[0103] 所述第一终端还用于,接收所述指定信息。

[0104] 本公开的实施例提供的技术方案可以包括以下有益效果：通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。

[0105] 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

[0106] 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。

[0107] 图1是根据一示例性实施例示出的一种传输信息的方法的应用场景图；

[0108] 图2是根据一示例性实施例示出的另一种传输信息的方法的应用场景图；

[0109] 图3是根据一示例性实施例示出的一种传输信息的方法的流程图；

[0110] 图4是根据一示例性实施例示出的另一种传输信息的方法的流程图；

[0111] 图5是根据一示例性实施例示出的又一种传输信息的方法的的流程图；

[0112] 图6是根据一示例性实施例示出的又一种传输信息的方法的流程图；

[0113] 图7是根据一示例性实施例示出的一种传输信息的方法的流程图；

[0114] 图8是根据一示例性实施例示出的一种传输信息的装置的框图；

[0115] 图9是根据一示例性实施例示出的另一种传输信息的装置的框图；

[0116] 图10是根据一示例性实施例示出的又一种传输信息的装置的框图；

[0117] 图11是根据一示例性实施例示出的又一种传输信息的装置的框图；

[0118] 图12是根据一示例性实施例示出的又一种传输信息的装置的框图；

[0119] 图13是根据一示例性实施例示出的又一种传输信息的装置的框图；

[0120] 图14是根据一示例性实施例示出的一种装置的框图；

[0121] 图15是根据一示例性实施例示出的一种装置的框图；

[0122] 图16是根据一示例性实施例示出的一种传输信息的系统的框图；

[0123] 图17是根据一示例性实施例示出的另一种传输信息的系统的框图；

[0124] 图18是根据一示例性实施例示出的又一种传输信息的系统的框图。

具体实施方式

[0125] 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。

[0126] 下面先结合图1和图2简单介绍一下本公开实施例提供的传输信息的方法的应用场景。

[0127] 如图1所示，服务器10与终端20连接，终端20(如小米手机)由服务器10(如小米服务器)提供服务。终端20与可穿戴设备30(如智能手环)连接，可穿戴设备30与终端20登录的系统账号相同，可穿戴设备30为终端20生成密钥，并辅助终端20实现信息的加密和解密。服

务器10将敏感信息(如验证码、登录密码等)密文传输给终端20。

[0128] 如图2所示,服务器10、终端20、终端40之间两两相互连接,终端20和终端40均由服务器10提供服务。终端20与可穿戴设备30(如智能手环)连接,可穿戴设备30与终端20登录的系统账号相同,可穿戴设备30为终端20生成密钥,并辅助终端20实现信息的加密和解密。终端40与可穿戴设备50(如智能手环)连接,可穿戴设备50与终端40登录的系统账号相同,可穿戴设备50为终端40生成密钥,并辅助终端40实现信息的加密和解密。终端40在服务器10的帮助下,将敏感信息(如验证码、登录密码等)密文传输给终端20。

[0129] 需要说明的是,上述应用场景仅为举例,本公开并不限制于此。

[0130] 图3是根据一示例性实施例示出的一种传输信息的方法的流程图,如图3所示,该传输信息的方法用于终端或服务器中,包括以下步骤。

[0131] 在步骤S11中,获取第一终端对应的第一的密钥。

[0132] 在本实施例中,第一密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。

[0133] 容易知道,各可穿戴设备的标识各不相同,可穿戴设备根据其标识生成密钥,可以避免两可穿戴设备生成相同的密钥。

[0134] 可选地,第一可穿戴设备可以为智能手环。

[0135] 需要说明的是,终端对应的密钥可以为对发送给终端的信息进行加密所使用的密钥(即对终端发送的信息进行解密所使用的密钥),也可以为对终端发送的信息进行加密所使用的密钥(即对发送给终端的信息进行解密所使用的密钥)。在本实施例中,第一密钥为对发送给第一终端的信息进行加密所使用的密钥。

[0136] 在步骤S12中,使用第一密钥对指定信息进行加密,得到第一密文信息。

[0137] 在本实施例中,指定信息为付款的验证码、银行的账号和密码等敏感信息。第一密文信息为密文形式的指定信息。

[0138] 在步骤S13中,向第一终端发送第一密文信息。

[0139] 在本实施例中,第一终端用于采用第一可穿戴设备对第一密文信息进行解密。

[0140] 本公开实施例通过获取第一终端对应的第一的密钥,使用第一密钥对指定信息进行加密,得到第一密文信息,并向第一终端发送第一密文信息,指定信息即使在传输的过程中被第三方截获,第三方也只能得到密文形式的指定信息,无法获取到真实信息,有效避免了指定信息的泄露。

[0141] 图4是根据一示例性实施例示出的另一种传输信息的方法的流程图,如图4所示,该传输信息的方法用于终端中,包括以下步骤。

[0142] 在步骤S21中,接收第一密文信息。

[0143] 在本实施例中,第一密文信息是使用第一终端对应的第一密钥对指定信息进行加密得到的,即密文形式的指定信息。第一密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。指定信息为付款的验证码、银行的账号和密码等敏感信息。

[0144] 容易知道,各可穿戴设备的标识各不相同,可穿戴设备根据其标识生成密钥,可以避免两可穿戴设备生成相同的密钥。

[0145] 可选地,第一可穿戴设备可以为智能手环。

[0146] 在步骤S22中，向第一可穿戴设备发送第一密文信息。

[0147] 在步骤S23中，接收指定信息。

[0148] 在本实施例中，指定信息是第一可穿戴设备使用第三密钥对第一密文信息进行解密得到的。第三密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0149] 需要说明的是，终端对应的密钥可以为对发送给终端的信息进行加密所使用的密钥(即对终端发送的信息进行解密所使用的密钥)，也可以为对终端发送的信息进行加密所使用的密钥(即对发送给终端的信息进行解密所使用的密钥)。在本实施例中，第一密钥为对发送给第一终端的信息进行加密所使用的密钥，第三密钥为对第一终端发送的信息进行加密所使用的密钥。

[0150] 本公开实施例通过接收第一密文信息，并通过第一可穿戴设备使用第三密钥对第一密文信息进行解密，得到指定信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。

[0151] 图5是根据一示例性实施例示出的又一种传输信息的方法的流程图，如图5所示，该传输信息的方法用于服务器传输指定信息给第一终端(如图1所示的应用场景)，包括以下步骤。

[0152] 在步骤S31中，服务器获取第一终端对应的第一密钥。

[0153] 在本实施例中，第一密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。

[0154] 可选地，第一密钥可以为非对称加密算法中使用的公开密钥，也可以为对称加密算法中使用的密钥。容易知道，当第一密钥为非对称加密算法中使用的公开密钥时，由于公开密钥加密的信息，只有对应的私有密钥才能解密，而私有密钥只存储在第一终端，不会由于传输而造成泄漏，因此只有第一终端才能使用私有密钥对公开密钥加密的信息进行解密，公开密钥加密的信息在传输过程中的安全性很高。当第一密钥为对称加密算法中使用的密钥时，由于对称加密算法中使用的是单密钥，因此使用第一密钥进行加密和解密的算法简单，计算速度快，而且对生成密钥的设备要求较低，实现成本低。

[0155] 在本实施例的一种实现方式中，该步骤S31可以包括：

[0156] 根据存储的终端和密钥的对应关系，获取第一终端对应的第一密钥。

[0157] 在实际应用中，为了管理和维护各终端和密钥之间的对应关系，服务器中会设置密钥列表，密钥列表包括多个终端和密钥的对应关系，便于使用各终端的密钥进行加密和解密。在本实施例中，服务器可以从密钥列表中获取第一终端对应的第一密钥。

[0158] 可选地，各终端对应的密钥可以修改，提升了密钥的灵活性和安全性。优选地，各终端修改其密钥时，会向服务器汇报，服务器将终端汇报的密钥替换密钥列表该终端对应的密钥，以便将来使用修改后的密钥。

[0159] 在步骤S32中，服务器使用第一密钥对指定信息进行加密，得到第一密文信息。

[0160] 在本实施例中，指定信息为付款的验证码、银行的账号和密码等敏感信息。第一密文信息为密文形式的指定信息。

[0161] 在步骤S33中，服务器向第一终端发送第一密文信息。

[0162] 在步骤S34中，第一终端向第一可穿戴设备发送第一密文信息。

[0163] 在步骤S35中，第一可穿戴设备使用第三密钥对第一密文信息进行解密，得到指定信息。

[0164] 在本实施例中，第三密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0165] 在实际应用中，采用可穿戴设备(如智能手环)作为终端加密和解密的工具时，可穿戴设备和终端登录的系统账号相同，从而使可穿戴设备和终端之间可以实现信息的互传，可穿戴设备可以生成对应终端的密钥，并为终端加密或解密信息。

[0166] 可穿戴设备在出产时可以默认设有一对非对称加密算法使用的公开密钥和私有密钥或者一个对称加密算法使用的密钥，以便于第一次传输其生成的密钥，提高密钥传输的安全性。可穿戴设备默认设有的密钥预先会存储在服务器的密钥列表中，可穿戴设备第一次生成密钥，可以使用默认的密钥对第一次生成的密钥加密后，连同可穿戴设备登录的系统账号一起发送给服务器。服务器使用密钥列表中默认的密钥进行解密，得到可穿戴设备第一次生成的密钥及该密钥对应的终端(终端与可穿戴设备登录的系统账号相同)，并将可穿戴设备第一次生成的密钥和对应的终端的标识(如登录的系统账号)存储在密钥列表中，提高密钥传输的安全性。

[0167] 可选地，该方法还可以包括：

[0168] 第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成第二密钥；

[0169] 第一可穿戴设备使用第三密钥对第二密钥进行加密，得到密文形式的第二密钥；

[0170] 第一可穿戴设备向第一终端发送密文形式的第二密钥；

[0171] 第一终端向服务器发送密文形式的第二密钥；

[0172] 服务器使用第一密钥对密文形式的第二密钥进行解密，得到第二密钥；

[0173] 服务器将第一终端对应的第一密钥更新为第二密钥。

[0174] 可以理解地，对终端对应的密钥进行修改，可以提升密钥被破解的难度，从而提升信息加密的安全性。而且对第二密钥进行加密后传输，可以防止第二密钥泄露，提高了使用第二密钥进行加密的信息传输的安全性。

[0175] 在步骤S36中，第一可穿戴设备向第一终端发送指定信息。

[0176] 需要说明的是，终端对应的密钥可以为对发送给终端的信息进行加密所使用的密钥(即对终端发送的信息进行解密所使用的密钥)，也可以为对终端发送的信息进行加密所使用的密钥(即对发送给终端的信息进行解密所使用的密钥)。在本实施例中，第一密钥为对发送给第一终端的信息进行加密所使用的密钥，第三密钥为对第一终端发送的信息进行加密所使用的密钥。

[0177] 步骤S31实现了获取第一终端对应的第一密钥，步骤S32实现了使用第一密钥对指定信息进行加密，得到第一密文信息，步骤S33和步骤S34实现了第一密文信息的发送和接收，步骤S35和步骤S36实现了使用第三密钥对第一密文信息进行解密，得到指定信息。

[0178] 本公开实施例通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程

中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0179] 图6是根据一示例性实施例示出的又一种传输信息的方法的流程图，如图6所示，该传输信息的方法用于第二终端传输指定信息给第一终端(如图2所示的应用场景)，且第一终端使用一对非对称加密算法的公开密钥和私有密钥，包括以下步骤。

[0180] 在步骤S41中，第二终端获取第一终端对应的第一密钥。

[0181] 在本实施例中，第一密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。

[0182] 在本实施例的一种实现方式中，该步骤S41可以包括：

[0183] 第二终端向服务器发送密钥请求，密钥请求用于获取第一密钥；

[0184] 服务器根据存储的终端和密钥的对应关系，获取第一密钥；

[0185] 服务器向第二终端发送第一密钥。

[0186] 在实际应用中，为了管理和维护各终端和密钥之间的对应关系，服务器中会设置密钥列表，密钥列表包括多个终端和密钥的对应关系，便于使用各终端的密钥进行加密和解密。在本实施例中，服务器可以从密钥列表中获取第一终端对应的第一密钥。

[0187] 在步骤S42中，第二终端向第二可穿戴设备发送第一密钥。

[0188] 在步骤S43中，第二可穿戴设备使用第一密钥对指定信息进行加密，得到第一密文信息。

[0189] 在本实施例中，指定信息为付款的验证码、银行的账号和密码等敏感信息。第一密文信息为密文形式的指定信息。

[0190] 可选地，指定信息可以由第二终端发送给第二可穿戴设备，也可以由用户输入第二可穿戴设备，本公开对此不作限制。

[0191] 在实际应用中，采用可穿戴设备(如智能手环)作为终端加密和解密的工具时，可穿戴设备和终端登录的系统账号相同，从而使可穿戴设备和终端之间可以实现信息的互传，可穿戴设备可以生成对应终端的密钥，并为终端加密或解密信息。

[0192] 在步骤S44中，第二可穿戴设备向第二终端发送第一密文信息。

[0193] 在步骤S45中，第二终端向第一终端发送第一密文信息。

[0194] 在步骤S46中，第一终端向第一可穿戴设备发送第一密文信息。

[0195] 可选地，该步骤S46可以与步骤S34相同，在此不再详述。

[0196] 在步骤S47中，第一可穿戴设备使用第三密钥对第一密文信息进行解密，得到指定信息。

[0197] 可选地，该步骤S47可以与步骤S35相同，在此不再详述。

[0198] 在步骤S48中，第一可穿戴设备向第一终端发送指定信息。

[0199] 可选地，该步骤S48可以与步骤S36相同，在此不再详述。

[0200] 需要说明的是，终端对应的密钥可以为对发送给终端的信息进行加密所使用的密钥(即对终端发送的信息进行解密所使用的密钥)，也可以为对终端发送的信息进行加密所使用的密钥(即对发送给终端的信息进行解密所使用的密钥)。在本实施例中，第一密钥和

第二密钥为对发送给第一终端的信息进行加密所使用的密钥，第三密钥为对第一终端发送的信息进行加密所使用的密钥。

[0201] 步骤S41实现了获取第一终端对应的第一密钥，步骤S42和步骤S43实现了使用第一密钥对指定信息进行加密，得到第一密文信息，步骤S44、步骤S45、以及步骤S46实现了第一密文信息的发送和接收，步骤S47和步骤S48实现了使用第三密钥对第一密文信息进行解密，得到指定信息。

[0202] 本公开实施例通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0203] 图7是根据一示例性实施例示出的又一种传输信息的方法的流程图，如图7所示，该传输信息的方法用于第二终端传输指定信息给第一终端(如图2所示的应用场景)，且第一终端使用一个对称加密算法的密钥，包括以下步骤。

[0204] 在步骤S51中，第二可穿戴设备使用第二终端对应的第四密钥对指定信息进行加密，得到第二密文信息。

[0205] 在本实施例中，第四密钥是第二可穿戴设备根据第二智能手环的标识和用户输入的密码指令生成的。第四密钥为对称算法中使用的密钥。指定信息为付款的验证码、银行的账号和密码等敏感信息。第二密文信息为密文形式的指定信息。

[0206] 可选地，指定信息可以由第二终端发送给第二可穿戴设备，也可以由用户输入第二可穿戴设备，本公开对此不作限制。

[0207] 在实际应用中，采用可穿戴设备(如智能手环)作为终端加密和解密的工具时，可穿戴设备和终端登录的系统账号相同，从而使可穿戴设备和终端之间可以实现信息的互传，可穿戴设备可以生成对应终端的密钥，并为终端加密或解密信息。

[0208] 为了管理和维护各终端和密钥之间的对应关系，服务器中会设置密钥列表，密钥列表包括多个终端和密钥的对应关系，便于使用各终端的密钥进行加密和解密。

[0209] 可选地，各终端对应的密钥可以修改，提升了密钥的灵活性和安全性。优选地，各终端修改其密钥时，会向服务器汇报，服务器将终端汇报的密钥替换密钥列表该终端对应的密钥，以便将来使用修改后的密钥。

[0210] 可选地，该方法还可以包括：

[0211] 第二可穿戴设备根据第二可穿戴设备的标识和用户输入的密码指令生成第五密钥；

[0212] 第二可穿戴设备使用第四密钥对第五密钥进行加密，得到密文形式的第五密钥；

[0213] 第二可穿戴设备向第二终端发送密文形式的第五密钥；

[0214] 第二终端向服务器发送密文形式的第五密钥；

[0215] 服务器使用第四密钥对密文形式的第五密钥进行解密，得到第五密钥；

[0216] 服务器将第二终端对应的第四密钥更新为第五密钥。

[0217] 可以理解地，对终端对应的密钥进行修改，可以提升密钥被破解的难度，从而提升

信息加密的安全性。而且对第五密钥进行加密后传输，可以防止第五密钥泄露，提高了使用第五密钥进行加密的信息传输的安全性。

[0218] 在步骤S52中，第二可穿戴设备向第二终端发送第二密文信息。

[0219] 在步骤S53中，第二终端向服务器发送第二密文信息。

[0220] 在步骤S54中，服务器获取第四密钥，并使用第四密钥对第二密文信息进行解密，得到指定信息。

[0221] 在步骤S55中，服务器获取第一终端对应的第一密钥，并使用第一终端对应的第一密钥对指定信息进行加密，得到第一密文信息。

[0222] 可选地，获取第一终端对应的第一密钥可以与步骤S31相同，使用第一终端对应的第一密钥对指定信息进行加密，得到第一密文信息可以与步骤S32相同，在此不再详述。

[0223] 在步骤S56中，服务器向第一终端发送第一密文信息。

[0224] 可选地，该步骤S56可以与步骤S33相同，在此不再详述。

[0225] 在步骤S57中，第一终端向第一可穿戴设备发送第一密文信息。

[0226] 可选地，该步骤S57可以与步骤S34相同，在此不再详述。

[0227] 在步骤S58中，第一可穿戴设备使用第三密钥对第一密文信息进行解密，得到指定信息。

[0228] 可选地，该步骤S58可以与步骤S35相同，在此不再详述。

[0229] 在步骤S59中，第一可穿戴设备向第一终端发送指定信息。

[0230] 可选地，该步骤S59可以与步骤S36相同，在此不再详述。

[0231] 需要说明的是，终端对应的密钥可以为对发送给终端的信息进行加密所使用的密钥(即对终端发送的信息进行解密所使用的密钥)，也可以为对终端发送的信息进行加密所使用的密钥(即对发送给终端的信息进行解密所使用的密钥)。在本实施例中，第一密钥和第二密钥为对发送给第一终端的信息进行加密所使用的密钥，第三密钥为对第一终端发送的信息进行加密所使用的密钥，第四密钥和第五密钥为对发送给第二终端的信息进行加密、对第二终端发送的信息进行加密所所使用的密钥。

[0232] 步骤S55实现了获取第一终端对应的第一的密钥、以及使用第一密钥对指定信息进行加密，得到第一密文信息，步骤S56和步骤S57实现了第一密文信息的发送和接收，步骤S58和步骤S59实现了使用第三密钥对第一密文信息进行解密，得到指定信息。

[0233] 本公开实施例通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0234] 图8是根据一示例性实施例示出的一种传输信息的装置的框图，参照图8，该传输信息的装置包括密钥获取模块601、信息加密模块602和信息发送模块603。

[0235] 该密钥获取模块601被配置为获取第一终端对应的第一密钥，第一密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。

[0236] 该信息加密模块602被配置为使用第一密钥对指定信息进行加密，得到第一密文

信息。

[0237] 该信息发送模块603被配置为向第一终端发送第一密文信息，第一终端用于采用第一可穿戴设备对第一密文信息进行解密。

[0238] 本公开实施例通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0239] 图9是根据一示例性实施例示出的另一种传输信息的装置的框图，参照图9，该传输信息的装置包括密钥获取模块701、信息加密模块702和信息发送模块703。

[0240] 该密钥获取模块701被配置为获取第一终端对应的第一密钥，第一密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。

[0241] 该信息加密模块702被配置为使用第一密钥对指定信息进行加密，得到第一密文信息。

[0242] 该信息发送模块703被配置为向第一终端发送第一密文信息，第一终端用于采用第一可穿戴设备对第一密文信息进行解密。

[0243] 在本实施例的一种实现方式中，当该装置为服务器时，该密钥获取模块701可以被配置为根据存储的终端和密钥的对应关系，获取第一终端对应的第一密钥。

[0244] 可选地，该装置可以还包括第一密钥接收模块704、第一密钥解密模块705和第一密钥更新模块706。

[0245] 该第一密钥接收模块704被配置为接收密文形式的第二密钥，密文形式的第二密钥是第一可穿戴设备使用第三密钥对第二密钥进行加密得到的，第二密钥和第三密钥均是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的，第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0246] 该第一密钥解密模块705被配置为使用第一密钥对密文形式的第二密钥进行解密，得到第二密钥。

[0247] 该第一密钥更新模块706被配置为将第一终端对应的第一密钥更新为第二密钥。

[0248] 本公开实施例通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0249] 图10是根据一示例性实施例示出的又一种传输信息的装置的框图，参照图10，该传输信息的装置包括密钥获取模块801、信息加密模块802和信息发送模块803。

[0250] 该密钥获取模块801被配置为获取第一终端对应的第一密钥，第一密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。

[0251] 该信息加密模块802被配置为使用第一密钥对指定信息进行加密，得到第一密文

信息。

[0252] 该信息发送模块803被配置为向第一终端发送第一密文信息，第一终端用于采用第一可穿戴设备对第一密文信息进行解密。

[0253] 在本实施例的一种实现方式中，当该装置为服务器时，该装置还可以包括信息接收模块804和信息解密模块805。

[0254] 该信息接收模块804被配置为接收第二密文信息，第二密文信息是第二可穿戴设备使用第二终端对应的第四密钥对指定信息进行加密得到的，第四密钥是第二可穿戴设备根据第二智能手环的标识和用户输入的密码指令生成的，第四密钥为对称算法中使用的密钥。

[0255] 该信息解密模块805被配置为使用第四密钥对第二密文信息进行解密，得到指定信息。

[0256] 可选地，该装置还可以包括第二密钥接收模块806、第二密钥解密模块807和第二密钥更新模块808。

[0257] 该第二密钥接收模块806被配置为接收密文形式的第五密钥，密文形式的第五密钥是第二可穿戴设备使用第四密钥对第五密钥进行加密得到的，第五密钥是第二可穿戴设备根据第二可穿戴设备的标识和用户输入的密码指令生成的。

[0258] 该第二密钥解密模块807被配置为使用第四密钥对密文形式的第五密钥进行解密，得到第五密钥。

[0259] 该第二密钥更新模块808被配置为将第二终端对应的第四密钥更新为第五密钥。

[0260] 在本实施例的另一种实现方式中，该装置可以还包括第一密钥接收模块、第一密钥解密模块和第一密钥更新模块。

[0261] 该第一密钥接收模块被配置为接收密文形式的第二密钥，密文形式的第二密钥是第一可穿戴设备使用第三密钥对第二密钥进行加密得到的，第二密钥和第三密钥均是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的，第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0262] 该第一密钥解密模块被配置为使用第一密钥对密文形式的第二密钥进行解密，得到第二密钥。

[0263] 该第一密钥更新模块被配置为将第一终端对应的第一密钥更新为第二密钥。

[0264] 本公开实施例通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0265] 图11是根据一示例性实施例示出的又一种传输信息的装置的框图，参照图11，该传输信息的装置包括密钥获取模块901、信息加密模块902和信息发送模块903。

[0266] 该密钥获取模块901被配置为获取第一终端对应的第一密钥，第一密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。

[0267] 该信息加密模块902被配置为使用第一密钥对指定信息进行加密，得到第一密文

信息。

[0268] 该信息发送模块903被配置为向第一终端发送第一密文信息，第一终端用于采用第一可穿戴设备对第一密文信息进行解密。

[0269] 在本实施例的一种实现方式中，当该装置为第二终端时，该密钥获取模块901可以包括请求发送子模块901a和密钥接收子模块901b。

[0270] 该请求发送子模块901a被配置为向服务器发送密钥请求，密钥请求用于获取第一密钥。

[0271] 该密钥接收子模块901b被配置为接收第一密钥，第一密钥是服务器根据存储的终端和密钥的对应关系获取的。

[0272] 在本实施例的另一种实现方式中，当该装置为第二终端时，该信息加密模块902可以包括信息发送子模块902a和信息接收子模块902b。

[0273] 该信息发送子模块902a被配置为向第二可穿戴设备发送第一密钥。

[0274] 该信息接收子模块902b被配置为接收第一密文信息，第一密文信息是第二可穿戴设备使用第一密钥对指定信息进行加密得到的。

[0275] 在本实施例的又一种实现方式中，该装置可以还包括第一密钥接收模块、第一密钥解密模块和第一密钥更新模块。

[0276] 该第一密钥接收模块被配置为接收密文形式的第二密钥，密文形式的第二密钥是第一可穿戴设备使用第三密钥对第二密钥进行加密得到的，第二密钥和第三密钥均是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的，第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0277] 该第一密钥解密模块被配置为使用第一密钥对密文形式的第二密钥进行解密，得到第二密钥。

[0278] 该第一密钥更新模块被配置为将第一终端对应的第一密钥更新为第二密钥。

[0279] 本公开实施例通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0280] 图12是根据一示例性实施例示出的又一种传输信息的装置的框图，参照图12，该传输信息的装置包括第一接收模块1001、第一发送模块1002和第二接收模块1003。

[0281] 该第一接收模块1001被配置为接收第一密文信息，第一密文信息是使用第一终端对应的第一密钥对指定信息进行加密得到的，第一密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。

[0282] 该第一发送模块1002被配置为向第一可穿戴设备发送第一密文信息。

[0283] 该第二接收模块1003被配置为接收指定信息，指定信息是第一可穿戴设备使用第三密钥对第一密文信息进行解密得到的，第三密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的，第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0284] 本公开实施例通过接收第一密文信息，并通过第一可穿戴设备使用第三密钥对第一密文信息进行解密，得到指定信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0285] 图13是根据一示例性实施例示出的又一种传输信息的装置的框图，参照图13，该传输信息的装置包括第一接收模块1101、第一发送模块1102和第二接收模块1103。

[0286] 该第一接收模块1101被配置为接收第一密文信息，第一密文信息是使用第一终端对应的第一密钥对指定信息进行加密得到的，第一密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。

[0287] 该第一发送模块1102被配置为向第一可穿戴设备发送第一密文信息。

[0288] 该第二接收模块1103被配置为接收指定信息，指定信息是第一可穿戴设备使用第三密钥对第一密文信息进行解密得到的，第三密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的，第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0289] 在本实施例的一种实现方式中，该装置还可以包括第三接收模块1104和第二发送模块1105。

[0290] 该第三接收模块1104被配置为接收密文形式的第二密钥，密文形式的第二密钥是第一可穿戴设备使用第三密钥对第二密钥进行加密得到的，第二密钥是第一可穿戴设备根据第一可穿戴设备的标识和用户输入的密码指令生成的。

[0291] 该第二发送模块1105被配置为向服务器发送密文形式的第二密钥，以使服务器使用第一密钥对密文形式的第二密钥进行解密，得到第二密钥，并将第一终端对应的第一密钥更新为第二密钥。

[0292] 本公开实施例通过接收第一密文信息，并通过第一可穿戴设备使用第三密钥对第一密文信息进行解密，得到指定信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0293] 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。

[0294] 图14是根据一示例性实施例示出的一种用于传输信息的装置1400的框图。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。

[0295] 参照图14，装置1400可以包括以下一个或多个组件：处理组件1402，存储器1404，电力组件1406，多媒体组件1408，音频组件1410，输入/输出(I/O)的接口1412，传感器组件1414，以及通信组件1416。

[0296] 处理组件1402通常控制装置1400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1402可以包括一个或多个处理器1420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1402可以包括一个或多个模块，便于处理组件1402和其他组件之间的交互。例如，处理组件1402可以包括多媒体模块，以方便多媒体组件1408和处理组件1402之间的交互。

[0297] 存储器1404被配置为存储各种类型的数据以支持在设备1400的操作。这些数据的示例包括用于在装置1400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1404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。

[0298] 电力组件1406为装置1400的各种组件提供电力。电力组件1406可以包括电源管理系统，一个或多个电源，及其他与为装置1400生成、管理和分配电力相关联的组件。

[0299] 多媒体组件1408包括在所述装置1400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1408包括一个前置摄像头和/或后置摄像头。当设备1400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。

[0300] 音频组件1410被配置为输出和/或输入音频信号。例如，音频组件1410包括一个麦克风(MIC)，当装置1400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1404或经由通信组件1416发送。在一些实施例中，音频组件1410还包括一个扬声器，用于输出音频信号。

[0301] I/O接口1412为处理组件1402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。

[0302] 传感器组件1414包括一个或多个传感器，用于为装置1400提供各个方面的状态评估。例如，传感器组件1414可以检测到设备1400的打开/关闭状态，组件的相对定位，例如所述组件为装置1400的显示器和小键盘，传感器组件1414还可以检测装置1400或装置1400一个组件的位置改变，用户与装置1400接触的存在或不存在，装置1400方位或加速/减速和装置1400的温度变化。传感器组件1414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1414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1414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。

[0303] 通信组件1416被配置为便于装置1400和其他设备之间有线或无线方式的通信。装置1400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1416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1416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。

[0304] 在示例性实施例中，装置1400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。

[0305] 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1404，上述指令可由装置1400的处理器1420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。

[0306] 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传输信息的方法，所述方法包括：

[0307] 获取第一终端对应的第一密钥，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

[0308] 使用所述第一密钥对指定信息进行加密，得到第一密文信息；

[0309] 向第一终端发送所述第一密文信息，所述第一终端用于采用所述第一可穿戴设备对所述第一密文信息进行解密。

[0310] 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传输信息的方法，所述方法包括：

[0311] 接收第一密文信息，所述第一密文信息是使用第一终端对应的第一密钥对指定信息进行加密得到的，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

[0312] 向所述第一可穿戴设备发送所述第一密文信息；

[0313] 接收所述指定信息，所述指定信息是所述第一可穿戴设备使用第三密钥对所述第一密文信息进行解密得到的，所述第三密钥是所述第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的，所述第三密钥与所述第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0314] 图15是根据一示例性实施例示出的一种用于传输信息的装置1500的框图。例如，装置1500可以被提供为一服务器。参照图15，装置1500包括处理组件1522，其进一步包括一个或多个处理器，以及由存储器1532所代表的存储器资源，用于存储可由处理组件1522的执行的指令，例如应用程序。存储器1532中存储的应用程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外，处理组件1522被配置为执行指令，以执行上述方法，所述方法包括：

[0315] 获取第一终端对应的第一密钥，所述第一密钥是第一可穿戴设备根据所述第一可穿戴设备的标识和用户输入的密码指令生成的；

[0316] 使用所述第一密钥对指定信息进行加密，得到第一密文信息；

[0317] 向第一终端发送所述第一密文信息，所述第一终端用于采用所述第一可穿戴设备对所述第一密文信息进行解密。

[0318] 装置1500还可以包括一个电源组件1526被配置为执行装置1500的电源管理，一个有线或无线网络接口1550被配置为将装置1500连接到网络，和一个输入输出(I/O)接口

1558。装置1500可以操作基于存储在存储器1532的操作系统，例如Windows ServerTM，Mac OS XTM，UnixTM，LinuxTM，FreeBSDTM或类似。

[0319] 图16是根据一示例性实施例示出的一种传输信息的系统的框图，参照图16，该传输信息的系统包括第一可穿戴设备1601、第一终端1602和服务器1603。

[0320] 该第一可穿戴设备1601被配置为根据第一可穿戴设备1601的标识和用户输入的密码指令生成第一终端1602对应的第一密钥和第三密钥，第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0321] 该服务器1603被配置为获取第一密钥；使用第一密钥对指定信息进行加密，得到第一密文信息；向第一终端1602发送第一密文信息。

[0322] 该第一终端1602被配置为接收第一密文信息；向第一可穿戴设备1601发送第一密文信息。

[0323] 该第一可穿戴设备1601还被配置为接收第一密文信息；使用第三密钥对第一密文信息进行解密，得到指定信息；向第一终端1602发送指定信息。

[0324] 该第一终端1602还被配置为接收指定信息。

[0325] 在本实施例的一种实现方式中，该服务器1603可以被配置为根据存储的终端和密钥的对应关系，获取第一终端对应的第一密钥。

[0326] 在本实施例的另一种实现方式中，该第一可穿戴设备1601还可以被配置为根据第一可穿戴设备1601的标识和用户输入的密码指令生成第二密钥；使用第三密钥对第二密钥进行加密，得到密文形式的第二密钥，第三密钥是第一可穿戴设备1601根据第一可穿戴设备1601的标识和用户输入的密码指令生成的，第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥；向第一终端1602发送密文形式的第二密钥。

[0327] 该第一终端1602还被配置为接收密文形式的第二密钥；向服务器1603发送密文形式的第二密钥。

[0328] 该服务器1603还被配置为接收密文形式的第二密钥；使用第一密钥对密文形式的第二密钥进行解密，得到第二密钥；将第一终端1602对应的第一密钥更新为第二密钥。

[0329] 本公开实施例通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0330] 图17是根据一示例性实施例示出的另一种传输信息的系统的框图，参照图17，该传输信息的系统包括第一可穿戴设备1701、第一终端1702、服务器1703、第二终端1704和第二可穿戴设备1705。

[0331] 该第一可穿戴设备1701被配置为根据第一可穿戴设备1701的标识和用户输入的密码指令生成第一终端1702对应的第一密钥和第三密钥，第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0332] 该第二终端1704被配置为向服务器1703发送密钥请求，密钥请求用于获取第一密

钥。

[0333] 该服务器1703被配置为接收密钥请求；根据存储的终端和密钥的对应关系，获取第一密钥；向第二终端1704发送第一密钥。

[0334] 该第二终端1704还被配置为接收第一密钥；向第二可穿戴设备1705发送第一密钥。

[0335] 该第二可穿戴设备1705被配置为接收第一密钥；使用第一密钥对指定信息进行加密，得到第一密文信息；向第二终端1704发送第一密文信息。

[0336] 该第二终端1704还被配置为接收第一密文信息；向第一终端1702发送第一密文信息。

[0337] 该第一终端1702被配置为接收第一密文信息；向第一可穿戴设备发送第一密文信息。

[0338] 该第一可穿戴设备1701还被配置为接收第一密文信息；使用第三密钥对第一密文信息进行解密，得到指定信息；向第一终端发送指定信息。

[0339] 该第一终端1702还被配置为接收指定信息。

[0340] 在本实施例的一种实现方式中，该第一可穿戴设备1701还可以被配置为根据第一可穿戴设备1701的标识和用户输入的密码指令生成第二密钥；使用第三密钥对第二密钥进行加密，得到密文形式的第二密钥，第三密钥是第一可穿戴设备1701根据第一可穿戴设备1701的标识和用户输入的密码指令生成的，第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥；向第一终端1702发送密文形式的第二密钥。

[0341] 该第一终端1702还被配置为接收密文形式的第二密钥；向服务器1703发送密文形式的第二密钥。

[0342] 该服务器1703还被配置为接收密文形式的第二密钥；使用第一密钥对密文形式的第二密钥进行解密，得到第二密钥；将第一终端1702对应的第一密钥更新为第二密钥。

[0343] 本公开实施例通过获取第一终端对应的第一的密钥，使用第一密钥对指定信息进行加密，得到第一密文信息，并向第一终端发送第一密文信息，指定信息即使在传输的过程中被第三方截获，第三方也只能得到密文形式的指定信息，无法获取到真实信息，有效避免了指定信息的泄露。由于可穿戴设备与终端相比，受到黑客攻击的可能性低，因此第一密钥是第一可穿戴设备生成的，第一终端也采用第一可穿戴设备对第一密文信息进行解密，可以提高密钥及信息的安全性，进一步有效避免了指定信息的泄露。

[0344] 图18是根据一示例性实施例示出的又一种传输信息的系统的框图，参照图18，该传输信息的系统包括第一可穿戴设备1801、第一终端1802、服务器1803、第二终端1804和第二可穿戴设备1805。

[0345] 该第一可穿戴设备1801被配置为根据第一可穿戴设备1801的标识和用户输入的密码指令生成第一终端1802对应的第一密钥和第三密钥，第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥。

[0346] 该第二可穿戴设备1805被配置为根据第二可穿戴设备1805的标识和用户输入的密码指令生成第二终端1804对应的第四密钥，第四密钥为对称算法中使用的密钥；使用第四密钥对指定信息进行加密，得到第二密文信息；向第二终端1804发送第二密文信息。

[0347] 该第二终端1804被配置为接收第二密文信息;向服务器1803发送第二密文信息。

[0348] 该服务器1803被配置为接收第二密文信息;使用第四密钥对第二密文信息进行解密,得到指定信息;获取第一密钥;使用第一密钥对指定信息进行加密,得到第一密文信息;向第一终端1802发送第一密文信息。

[0349] 该第一终端1802被配置为接收第一密文信息;向第一可穿戴设备1801发送第一密文信息。

[0350] 该第一可穿戴设备1801还被配置为接收第一密文信息;使用第三密钥对第一密文信息进行解密,得到指定信息;向第一终端1802发送指定信息。

[0351] 该第一终端1802还被配置为接收指定信息。

[0352] 在本实施例的一种实现方式中,该第二可穿戴设备1805还可以被配置为根据第二可穿戴设备1805的标识和用户输入的密码指令生成第五密钥;使用第四密钥对第五密钥进行加密,得到密文形式的第五密钥;向第二终端1804发送密文形式的第五密钥。

[0353] 该第一终端1802还被配置为接收密文形式的第五密钥;向服务器1803发送密文形式的第五密钥。

[0354] 该服务器1803还被配置为接收密文形式的第五密钥;使用第四密钥对密文形式的第五密钥进行解密,得到第五密钥;将第二终端1804对应的第四密钥更新为第五密钥。

[0355] 在本实施例的另一种实现方式中,该第一可穿戴设备1801还可以被配置为根据第一可穿戴设备1801的标识和用户输入的密码指令生成第二密钥;使用第三密钥对第二密钥进行加密,得到密文形式的第二密钥,第三密钥是第一可穿戴设备1801根据第一可穿戴设备1801的标识和用户输入的密码指令生成的,第三密钥与第一密钥为非对称加密算法中使用的一对密钥或者对称加密算法中使用的同一个密钥;向第一终端1802发送密文形式的第二密钥。

[0356] 该第一终端1802还被配置为接收密文形式的第二密钥;向服务器1803发送密文形式的第二密钥。

[0357] 该服务器1803还被配置为接收密文形式的第二密钥;使用第一密钥对密文形式的第二密钥进行解密,得到第二密钥;将第一终端1802对应的第一密钥更新为第二密钥。

[0358] 本公开实施例通过获取第一终端对应的第一的密钥,使用第一密钥对指定信息进行加密,得到第一密文信息,并向第一终端发送第一密文信息,指定信息即使在传输的过程中被第三方截获,第三方也只能得到密文形式的指定信息,无法获取到真实信息,有效避免了指定信息的泄露。由于可穿戴设备与终端相比,受到黑客攻击的可能性低,因此第一密钥是第一可穿戴设备生成的,第一终端也采用第一可穿戴设备对第一密文信息进行解密,可以提高密钥及信息的安全性,进一步有效避免了指定信息的泄露。

[0359] 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。

[0360] 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。

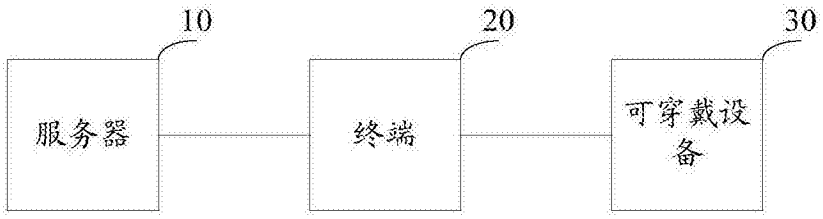

10
20
30
服务器
终端
可穿戴设备

图1

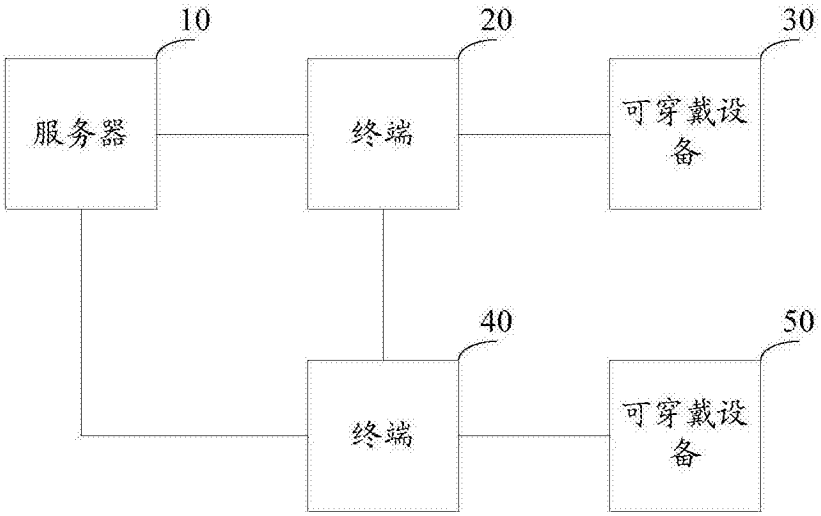

10
20
30
服务器
终端
可穿戴设备
40
50
终端
可穿戴设备

图2

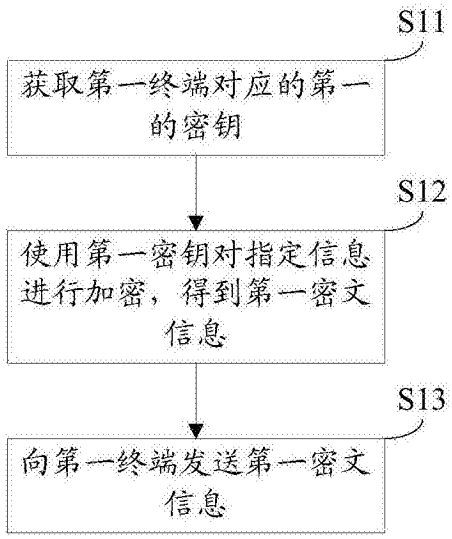

S11
获取第一终端对应的第一的密钥
S12
使用第一密钥对指定信息进行加密，得到第一密文信息
S13
向第一终端发送第一密文信息

图3

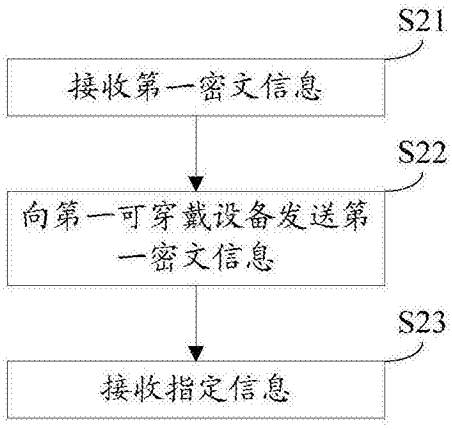

S21
接收第一密文信息
S22
向第一可穿戴设备发送第一密文信息
S23
接收指定信息

图4

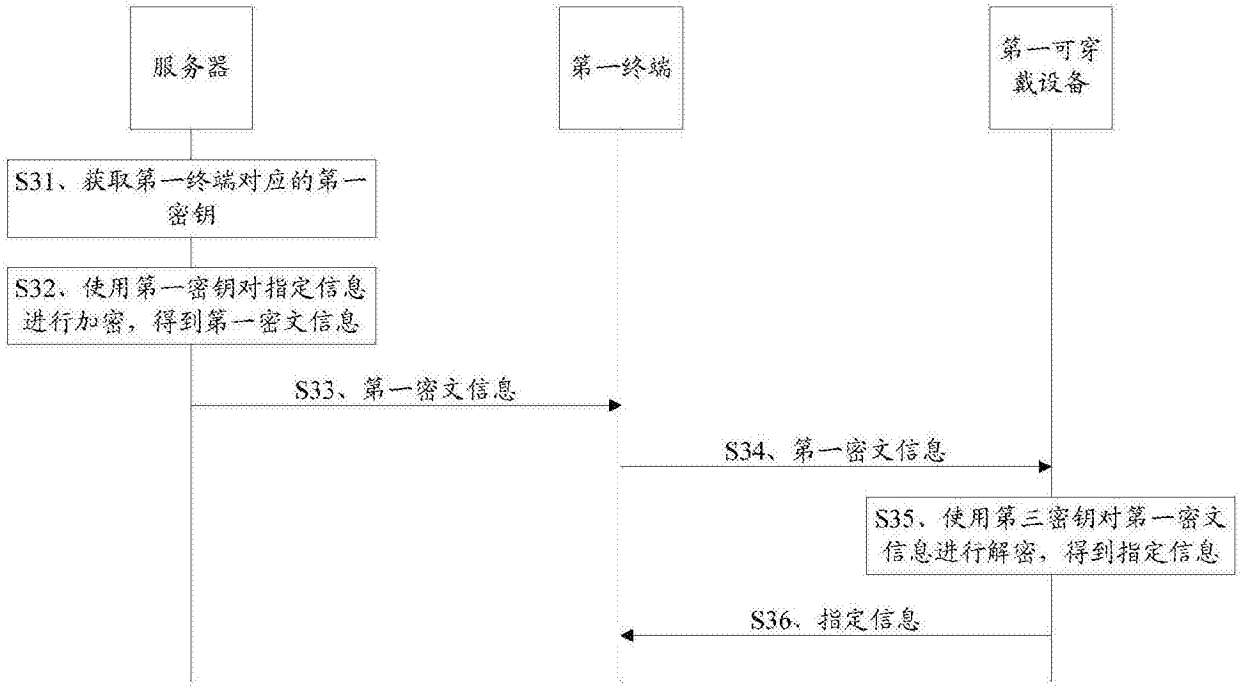

服务器
第一终端
第一可穿戴设备
S31、获取第一终端对应的第一密钥
S32、使用第一密钥对指定信息进行加密，得到第一密文信息
S33、第一密文信息
S34、第一密文信息
S35、使用第三密钥对第一密文信息进行解密，得到指定信息
S36、指定信息

图5

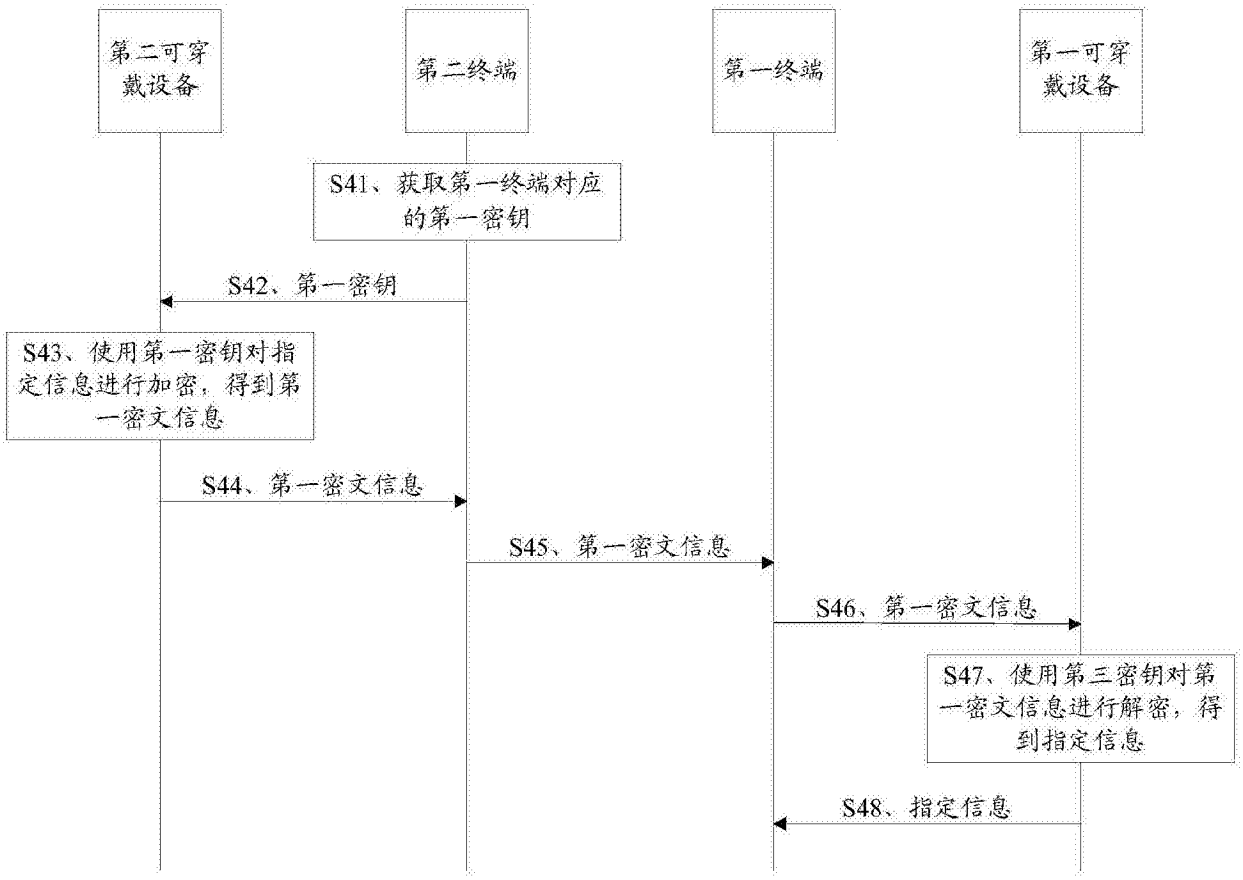

第二可穿戴设备
第二终端
第一终端
第一可穿戴设备
S41、获取第一终端对应的第一密钥
S42、第一密钥
S43、使用第一密钥对指定信息进行加密，得到第一密文信息
S44、第一密文信息
S45、第一密文信息
S46、第一密文信息
S47、使用第三密钥对第一密文信息进行解密，得到指定信息
S48、指定信息

图6

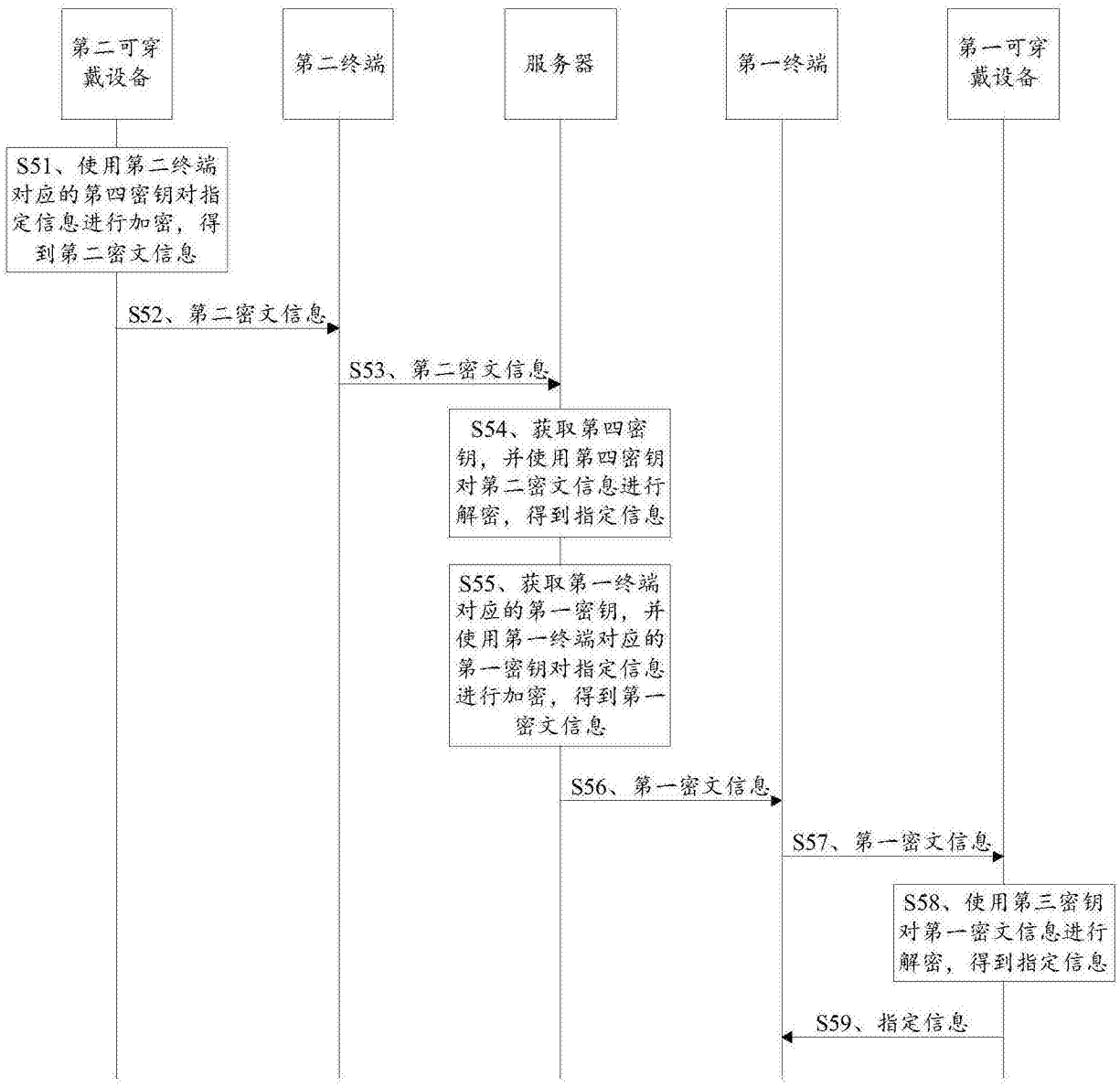

第二可穿戴设备
第二终端
服务器
第一终端
第一可穿戴设备
S51、使用第二终端对应的第四密钥对指定信息进行加密，得到第二密文信息
S52、第二密文信息
S53、第二密文信息
S54、获取第四密钥，并使用第四密钥对第二密文信息进行解密，得到指定信息
S55、获取第一终端对应的第一密钥，并使用第一终端对应的第一密钥对指定信息进行加密，得到第一密文信息
S56、第一密文信息
S57、第一密文信息
S58、使用第三密钥对第一密文信息进行解密，得到指定信息
S59、指定信息

图7

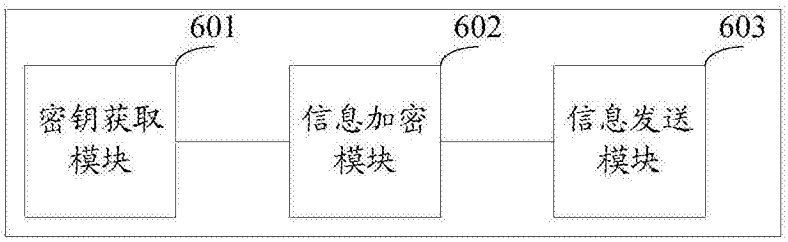

601
602
603
密钥获取模块
信息加密模块
信息发送模块

图8

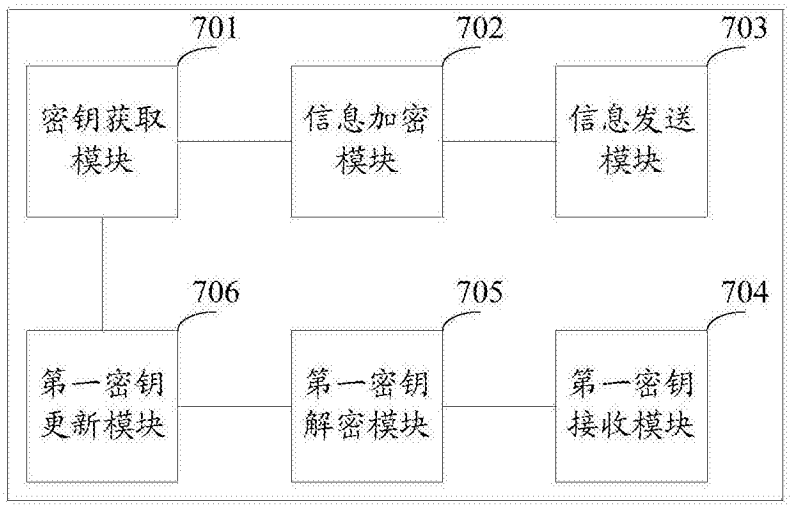

701
密钥获取模块
702
信息加密模块
703
信息发送模块
706
第一密钥更新模块
705
第一密钥解密模块
704
第一密钥接收模块

图9

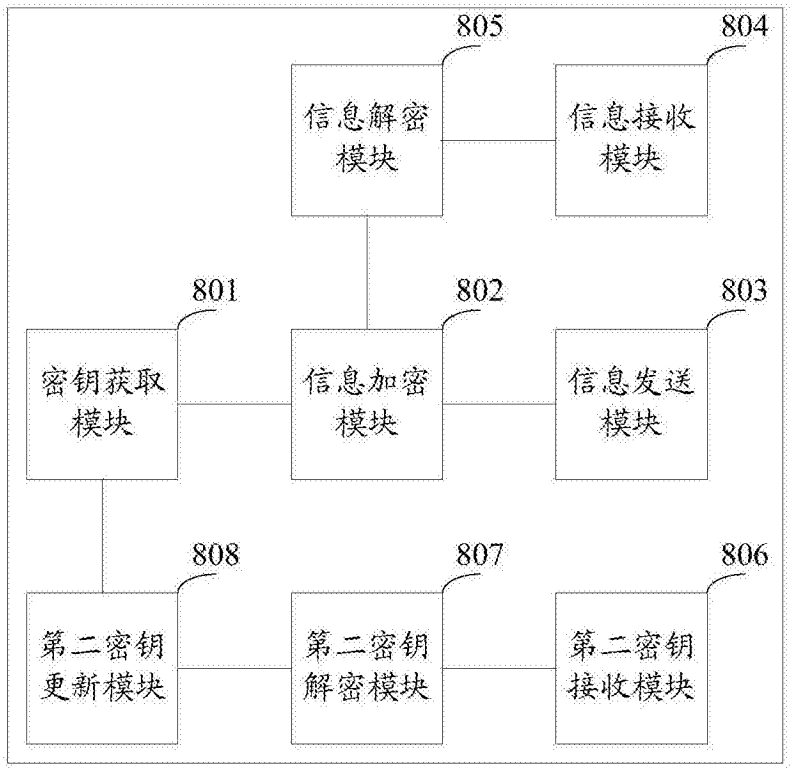

805
信息解密模块
804
信息接收模块
801
密钥获取模块
802
信息加密模块
803
信息发送模块
808
第二密钥更新模块
807
第二密钥解密模块
806
第二密钥接收模块

图10

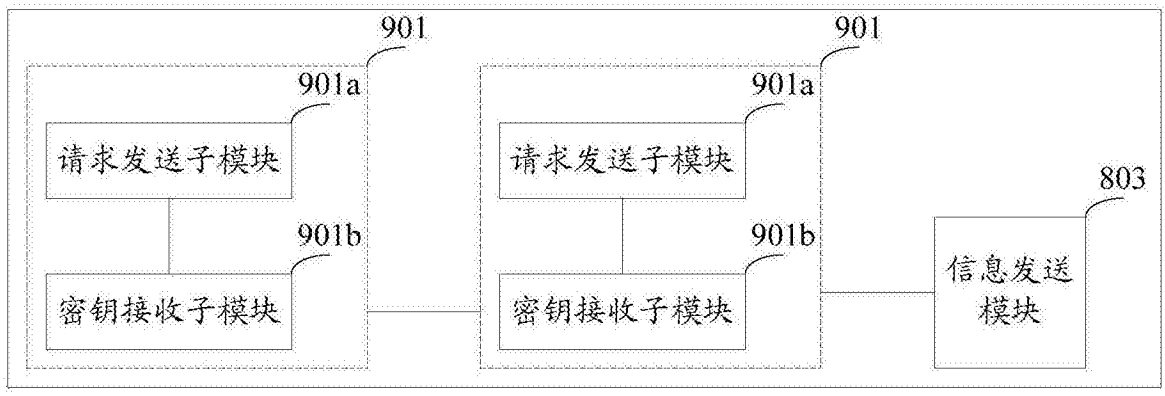

901
901a
请求发送子模块
901b
密钥接收子模块
901
901a
请求发送子模块
901b
密钥接收子模块
803
信息发送模块

图11

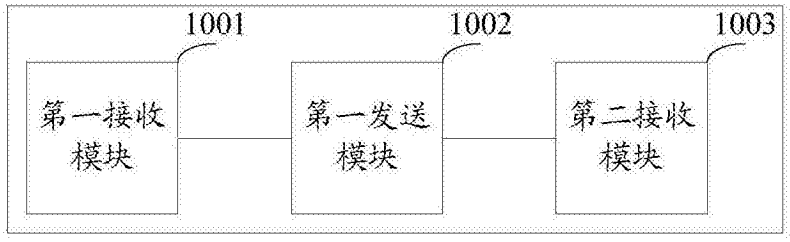

1001
第一接收模块
1002
第一发送模块
1003
第二接收模块

图12

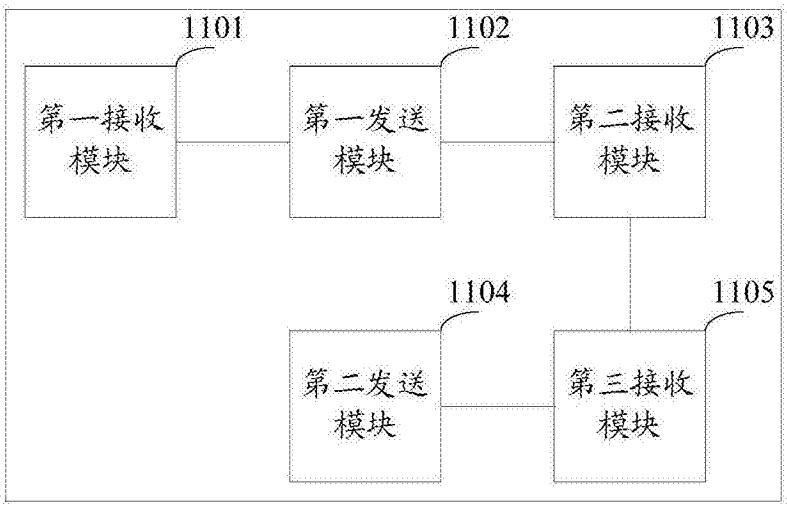

1101
第一接收模块
1102
第一发送模块
1103
第二接收模块
1104
第二发送模块
1105
第三接收模块

图13

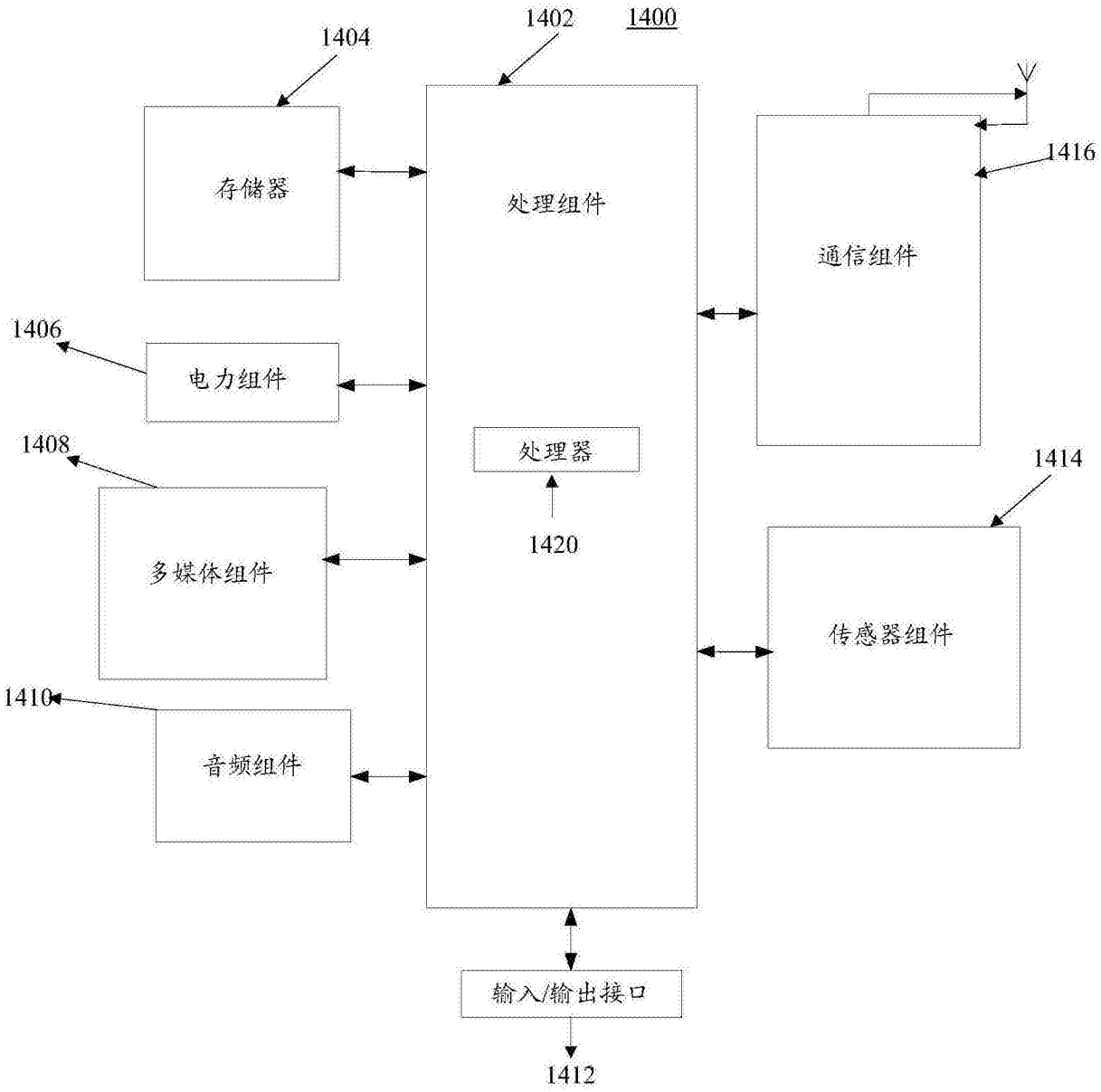

1402
1400
1404
存储器
处理组件
通信组件
1416
1406
电力组件
处理器
1408
1420
1414
多媒体组件
传感器组件
1410
音频组件
输入/输出接口
1412

图14

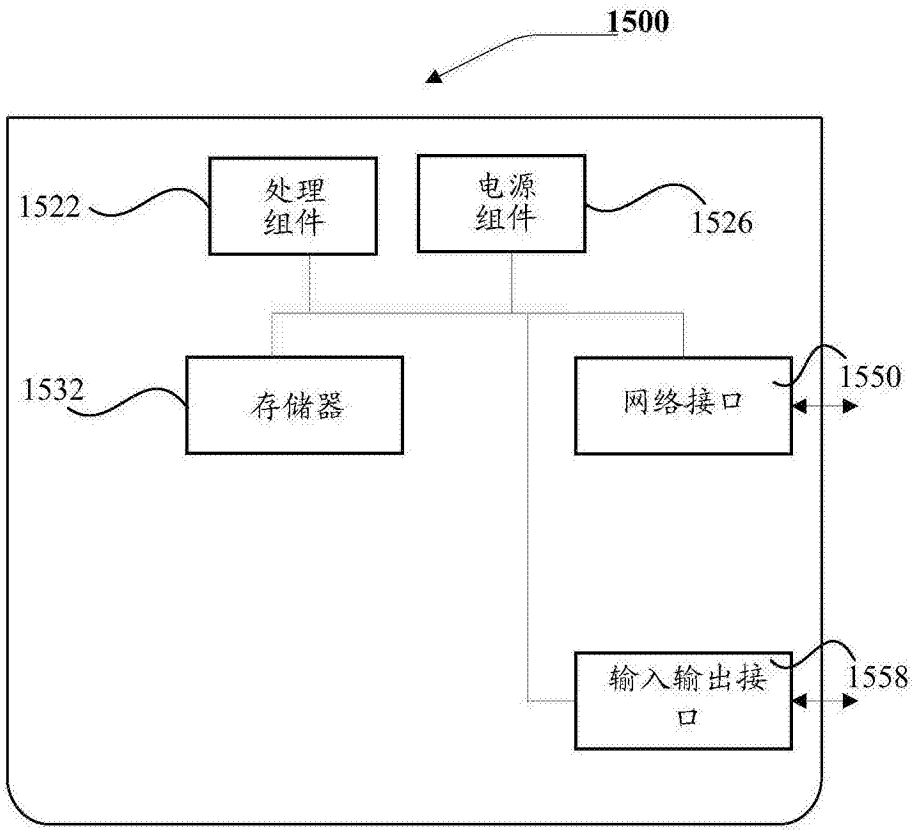

1500
1522
处理组件
电源组件
1526
1532
存储器
网络接口
1550
输入输出接口
1558

图15

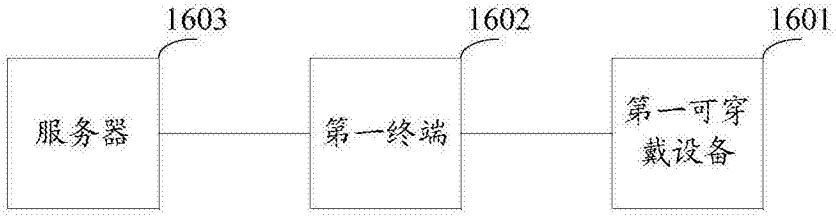

1603
1602
1601
服务器
第一终端
第一可穿戴设备

图16

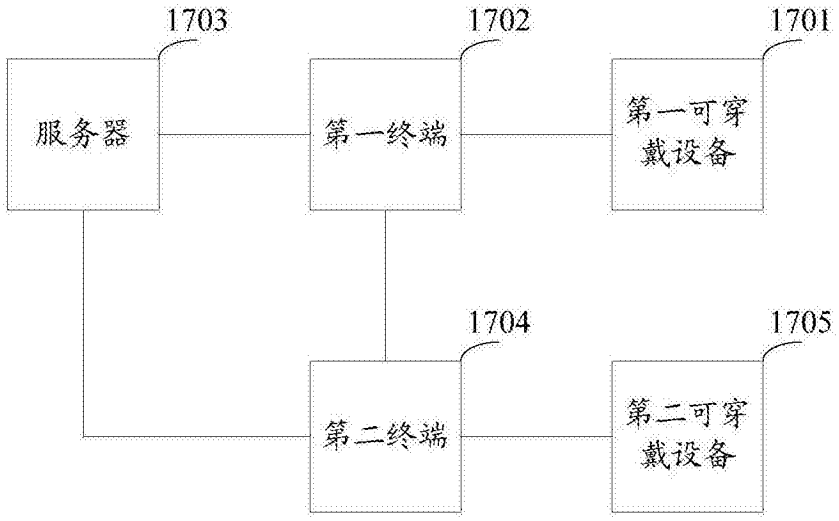

1703
1702
1701
服务器
第一终端
第一可穿戴设备
1704
1705
第二终端
第二可穿戴设备

图17

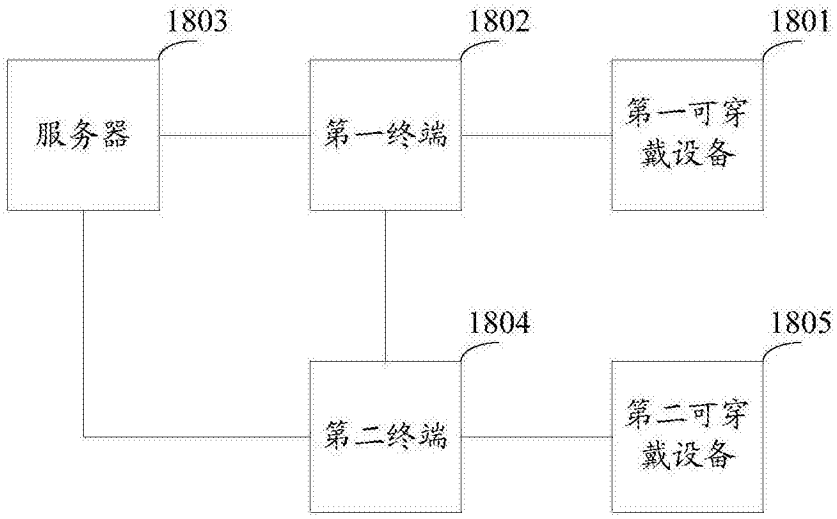

1803
1802
1801
服务器
第一终端
第一可穿戴设备
1804
1805
第二终端
第二可穿戴设备

图18