(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 104852800 A
(43)申请公布日 2015.08.19

(21)申请号 201510272290.X

(22)申请日 2015.05.25

(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 葛琦 孙龙 崔恒彬

(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 9/08(2006.01)
H04L 29/06(2006.01)

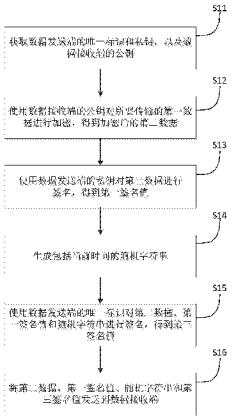
权利要求书8页 说明书28页 附图22页

(54)发明名称

数据传输方法及装置

(57)摘要

本公开是关于一种数据传输方法及装置。所述方法包括：获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；生成包括当前时间的随机字符串；使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，得到第三签名值；将所述第二数据，第一签名值、所述随机字符串和第三签名值发送到所述数据接收端。用以提高数据传输过程中数据的安全性。



CN 104852800 A

1. 一种数据传输方法，其特征在于，应用于数据发送端，所述方法包括：

获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

生成包括当前时间的随机字符串；

使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，得到第三签名值；

将所述第二数据，第一签名值、所述随机字符串和第三签名值发送到所述数据接收端。

2. 根据权利要求 1 所述的方法，其特征在于，使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，包括：

以所述数据发送端的唯一标识为密钥，对所述第二数据、第一签名值和所述随机字符串进行哈希运算消息认证码 (HMAC) 运算。

3. 根据权利要求 1 所述的方法，其特征在于，当所述数据发送端为移动终端时，所述获取数据发送端的私钥，包括：

从所述移动终端的信任区域 (TrustZone) 的回访保护存储块 (RPMB) 区域或安全文件系统 (SFS) 区域提取所述移动终端的私钥。

4. 一种数据传输方法，其特征在于，应用于数据接收端，所述方法包括：

接收数据发送端发送的数据；

获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

从所述数据发送端发送的数据中提取出第二数据，第一签名值，随机字符串和第三签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述第二数据、所述随机字符串和第一签名值进行签名得到的；

根据所述数据发送端的唯一标识对所述第三签名值进行验证；

当对所述第三签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述数据发送端的公钥对所述第一签名值进行验证；

当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

5. 一种数据传输方法，其特征在于，应用于被识别设备，所述方法包括：

获取被识别设备的唯一标识；

生成包括当前时间的随机字符串；

根据所述发送端唯一标识对所述随机字符串进行签名，得到第三签名值；

将所述随机字符串和所述第三签名值发送到识别设备。

6. 一种数据传输方法，其特征在于，应用于识别设备，所述方法包括：

接收被识别设备发送的数据；

获取所述被识别设备的唯一标识；

从所述被识别设备发送的数据中提取出随机字符串和第三签名值，所述随机字符串包括所述被识别设备生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述随机字符串进行签名得到的；

从所述随机字符串中提取所述被识别设备生成所述随机字符串的时间；

判断所述被识别设备生成所述随机字符串的时间是否在预设时间范围内；

当所述被识别设备生成所述随机字符串的时间在所述预设时间范围内时，使用所述被识别设备的唯一标识对所述第三签名值进行验证；

当对所述第三签名值的验证通过时，确定所述被识别设备为可信的。

7. 一种数据传输方法，其特征在于，应用于数据发送端，所述方法包括：

获取数据发送端的私钥；

生成包括当前时间的随机字符串；

使用所述数据发送端的私钥对所要传输的第一数据和所述随机字符串进行签名，得到第四签名值；

将所述第一数据，所述随机字符串和所述第四签名值发送到所述数据接收端。

8. 一种数据传输方法，其特征在于，应用于数据接收端，所述方法包括：

接收数据发送端发送的数据；

获取所述数据发送端的公钥；

从所述数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第四签名值为使用所述数据发送端的私钥对所述第一数据和随机字符串进行签名得到的；

根据所述数据发送端的公钥对所述第四签名值进行验证；

当对所述第四签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述第一数据。

9. 一种数据传输方法，其特征在于，应用于数据发送端，所述方法包括：

获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名，得到第二签名值；

将所述第二数据，第一签名值和第二签名值发送到所述数据接收端。

10. 一种数据传输方法，其特征在于，应用于数据接收端，所述方法包括：

接收数据发送端发送的数据；

获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

从所述数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述第二签名值为使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名得到的；

根据所述数据发送端的唯一标识对所述第二签名值进行验证；

当对所述第二签名值验证通过时，使用所述数据发送端的公钥对所述第一签名值进行验证；

当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

11. 一种数据传输装置，其特征在于，应用于数据发送端，所述装置包括：

第一获取模块，用于获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

第一加密模块，用于使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

第一签名模块，用于使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

第一生成模块，用于生成包括当前时间的随机字符串；

第二签名模块，用于使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，得到第三签名值；

第一发送模块，用于将所述第二数据，第一签名值、所述随机字符串和第三签名值发送到所述数据接收端。

12. 根据权利要求 11 所述的装置，其特征在于，所述第二签名模块，包括：

运算子模块，用于以所述数据发送端的唯一标识为密钥，对所述第二数据、第一签名值和所述随机字符串进行哈希运算消息认证码 (HMAC) 运算。

13. 根据权利要求 11 所述的装置，其特征在于，所述第一获取模块，包括：

提取子模块，用于当所述数据发送端为移动终端时，从所述移动终端的信任区域 (TrustZone) 的回访保护存储块 (RPMB) 区域或安全文件系统 (SFS) 区域提取所述移动终端的私钥。

14. 一种数据传输装置，其特征在于，应用于数据接收端，所述装置包括：

第一接收模块，用于接收数据发送端发送的数据；

第二获取模块，用于获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

第一提取模块，用于从所述数据发送端发送的数据中提取出第二数据，第一签名值，随机字符串和第三签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述第二数据、所述随机字符串和第一签名值进行签名得到的；

第一验证模块，用于根据所述数据发送端的唯一标识对所述第三签名值进行验证；

第二提取模块，用于当对所述第三签名值验证通过时，从所述随机字符串中提取所述

数据发送端生成所述随机字符串的时间；

第一判断模块，用于判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

第二验证模块，用于当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述数据发送端的公钥对所述第一签名值进行验证；

第一解密模块，用于当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

15. 一种数据传输装置，其特征在于，应用于被识别设备，所述装置包括：

第三获取模块，用于获取所述被识别设备的唯一标识；

第二生成模块，用于生成包括当前时间的随机字符串；

第三签名模块，用于根据所述发送端唯一标识对所述随机字符串进行签名，得到第三签名值；

第二发送模块，用于将所述随机字符串和所述第三签名值发送到识别设备。

16. 一种数据传输装置，其特征在于，应用于识别设备，所述装置包括：

第二接收模块，用于接收被识别设备发送的数据；

第四获取模块，用于获取所述被识别设备的唯一标识；

第三提取模块，用于从所述被识别设备发送的数据中提取出随机字符串和第三签名值，所述随机字符串包括所述被识别设备生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述随机字符串进行签名得到的；

第四提取模块，用于从所述随机字符串中提取所述被识别设备生成所述随机字符串的时间；

第二判断模块，用于判断所述被识别设备生成所述随机字符串的时间是否在预设时间范围内；

第三验证模块，用于当所述被识别设备生成所述随机字符串的时间在所述预设时间范围内时，使用所述被识别设备的唯一标识对所述第三签名值进行验证；

确定模块，用于当对所述第三签名值的验证通过时，确定所述被识别设备为可信的。

17. 一种数据传输装置，其特征在于，应用于数据发送端，所述装置包括：

第五获取模块，用于获取数据发送端的私钥；

第三生成模块，用于生成包括当前时间的随机字符串；

第四签名模块，用于使用所述数据发送端的私钥对所要传输的第一数据和所述随机字符串进行签名，得到第四签名值；

第三发送模块，用于将所述第一数据，所述随机字符串和所述第四签名值发送到所述数据接收端。

18. 一种数据传输装置，其特征在于，应用于数据接收端，所述装置包括：

第三接收模块，用于接收数据发送端发送的数据；

第六获取模块，用于获取所述数据发送端的公钥；

第五提取模块，用于从所述数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第四签名值为使用所述数据发送端的私钥对所述第一数据和随机字符串进行签名得到的；

第四验证模块，用于根据所述数据发送端的公钥对所述第四签名值进行验证；

第六提取模块，用于当对所述第四签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

第三判断模块，用于判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

使用模块，用于当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述第一数据。

19. 一种数据传输装置，其特征在于，应用于数据发送端，所述装置包括：

第七获取模块，用于获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

第二加密模块，用于使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

第五签名模块，用于使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

第六签名模块，用于使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名，得到第二签名值；

第四发送模块，用于将所述第二数据，第一签名值和第二签名值发送到所述数据接收端。

20. 一种数据传输装置，其特征在于，应用于数据接收端，所述装置包括：

第四接收模块，用于接收数据发送端发送的数据；

第八获取模块，用于获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

第七提取模块，用于从所述数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述第二签名值为使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名得到的；

第五验证模块，用于根据所述数据发送端的唯一标识对所述第二签名值进行验证；

第六验证模块，用于当对所述第二签名值验证通过时，使用所述数据发送端的公钥对所述第一签名值进行验证；

第二解密模块，用于当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

21. 一种数据传输装置，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：

获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

生成包括当前时间的随机字符串；

使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，得到第三签名值；

将所述第二数据，第一签名值、所述随机字符串和第三签名值发送到所述数据接收端。

22. 一种数据传输装置，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：

接收数据发送端发送的数据；

获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

从所述数据发送端发送的数据中提取出第二数据，第一签名值，随机字符串和第三签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述第二数据、所述随机字符串和第一签名值进行签名得到的；

根据所述数据发送端的唯一标识对所述第三签名值进行验证；

当对所述第三签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述数据发送端的公钥对所述第一签名值进行验证；

当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

23. 一种数据传输装置，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：

获取被识别设备的唯一标识；

生成包括当前时间的随机字符串；

根据所述发送端唯一标识对所述随机字符串进行签名，得到第三签名值；

将所述随机字符串和所述第三签名值发送到识别设备。

24. 一种数据传输装置，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：

接收被识别设备发送的数据；

获取所述被识别设备的唯一标识；

从所述被识别设备发送的数据中提取出随机字符串和第三签名值，所述随机字符串包括所述被识别设备生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的

唯一标识对所述随机字符串进行签名得到的；

从所述随机字符串中提取所述被识别设备生成所述随机字符串的时间；

判断所述被识别设备生成所述随机字符串的时间是否在预设时间范围内；

当所述被识别设备生成所述随机字符串的时间在所述预设时间范围内时，使用所述被识别设备的唯一标识对所述第三签名值进行验证；

当对所述第三签名值的验证通过时，确定所述被识别设备为可信的。

25. 一种数据传输装置，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：

获取数据发送端的私钥；

生成包括当前时间的随机字符串；

使用所述数据发送端的私钥对所要传输的第一数据和所述随机字符串进行签名，得到第四签名值；

将所述第一数据，所述随机字符串和所述第四签名值发送到所述数据接收端。

26. 一种数据传输装置，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：

接收数据发送端发送的数据；

获取所述数据发送端的公钥；

从所述数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第四签名值为使用所述数据发送端的私钥对所述第一数据和随机字符串进行签名得到的；

根据所述数据发送端的公钥对所述第四签名值进行验证；

当对所述第四签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述第一数据。

27. 一种数据传输装置，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：

获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名，得到第二签

名值；

将所述第二数据，第一签名值和第二签名值发送到所述数据接收端。

28. 一种数据传输装置，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：

接收数据发送端发送的数据；

获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

从所述数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述第二签名值为使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名得到的；

根据所述数据发送端的唯一标识对所述第二签名值进行验证；

当对所述第二签名值验证通过时，使用所述数据发送端的公钥对所述第一签名值进行验证；

当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

数据传输方法及装置

技术领域

[0001] 本公开涉及通信技术领域，尤其涉及一种数据传输方法及装置。

背景技术

[0002] 相关技术中，手机记录了用户的各类信息，例如，联系人、照片、短信、通话记录、密保工具等，一旦丢失，就可能泄露遗失者的个人隐私，甚至威胁到遗失者的财产安全。

[0003] 为了防止手机遗失，生产商在手机中加入远程找回功能，并且为了保护遗失者的个人隐私和财产安全，加入了远程锁定、远程擦除等功能，在此过程中，需要第三方的参与，如运营商或者具有手机防遗失功能的应用提供者。

发明内容

[0004] 本公开实施例提供一种数据传输方法及装置，用以提高数据传输过程中数据的安全性。

[0005] 根据本公开实施例的第一方面，提供一种数据传输方法，所述方法包括：

[0006] 获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0007] 使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0008] 使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

[0009] 生成包括当前时间的随机字符串；

[0010] 使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，得到第三签名值；

[0011] 将所述第二数据，第一签名值、所述随机字符串和第三签名值发送到所述数据接收端。

[0012] 本公开的实施例提供的技术方案可以包括以下有益效果：通过数据接收端的公钥对第一数据进行加密，得到第二数据，再通过数据发送端的私钥对第二数据进行签名得到第一签名值，在对数据进行加密之后又对加密数据进行签名，增加了数据传输过程中数据的安全性，根据设备的唯一标识对第二数据，第一签名值进行签名，进一步增加了数据传输过程中数据的安全性。

[0013] 在一个实施例中，使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，包括：

[0014] 以所述数据发送端的唯一标识为密钥，对所述第二数据、第一签名值和所述随机字符串进行哈希运算消息认证码 (HMAC) 运算。

[0015] 本公开的实施例提供的技术方案可以包括以下有益效果：通过将数据发送端的唯一标识作为密钥，具备了采用哈希运算消息认证码运算的条件，而采用该运算方法，有第三方非法截获消息时，只能获取到 HMAC 结果，仅仅根据该结果并不能推出密钥，即无法获知数据发送端的唯一标识。保证了设备唯一标识在发送过程中的安全性，保证了验证设备合

法性的正确无误。

[0016] 在一个实施例中，当所述数据发送端为移动终端时，所述获取数据发送端的私钥，包括：

[0017] 从所述移动终端的信任区域（TrustZone）的回访保护存储块（RPMB）区域或安全文件系统（SFS）区域提取所述移动终端的私钥。

[0018] 本公开的实施例提供的技术方案可以包括以下有益效果：将私钥存储在移动终端的信任区域（TrustZone）的回访保护存储块（RPMB）区域或安全文件系统（SFS）区域，保证了私钥在本地的安全性。

[0019] 根据本公开实施例的第二方面，提供一种数据传输方法，应用于数据接收端，所述方法包括：

[0020] 接收数据发送端发送的数据；

[0021] 获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

[0022] 从所述数据发送端发送的数据中提取出第二数据，第一签名值，随机字符串和第三签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述第二数据、所述随机字符串和第一签名值进行签名得到的；

[0023] 根据所述数据发送端的唯一标识对所述第三签名值进行验证；

[0024] 当对所述第三签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

[0025] 判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

[0026] 当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述数据发送端的公钥对所述第一签名值进行验证；

[0027] 当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

[0028] 本公开的实施例提供的技术方案可以包括以下有益效果：通过数据发送端的唯一标识对第三签名进行验证，提取随机字符串中携带的时间信息，当生成随机字符串的时间在预设时间范围内时使用数据发送端的公钥对第一签名值进行验证，从而保证了数据的时效性。

[0029] 其次，由于随机数的非唯一性，以及使用随机数对签名信息加解密算法的不可确定性，不仅使签名信息的解密复杂度提高，利用随机字符串携带时间信息，还保证了时间信息的安全性，从而进一步提高了数据发送过程中数据的安全性。

[0030] 根据本公开实施例的第三方面，提供一种数据传输方法，

[0031] 应用于被识别设备，所述方法包括：

[0032] 获取所述被识别设备的唯一标识；

[0033] 生成包括当前时间的随机字符串；

[0034] 根据所述发送端唯一标识对所述随机字符串进行签名，得到第三签名值；

[0035] 将所述随机字符串和所述第三签名值发送到识别设备。

[0036] 本公开的实施例提供的技术方案可以包括以下有益效果：利用发送端的唯一标识对携带时间信息的随机字符串进行签名，使数据接收端能够通过该唯一标识验证发送端的合法性，并且根据该唯一标识对携带时间信息的随机字符串进行签名，保证了时间值的安全性，避免了时间值在传输过程中被篡改。

[0037] 根据本公开实施例的第四方面，提供一种数据传输方法，应用于识别设备，所述方法包括：

[0038] 接收被识别设备发送的数据；

[0039] 获取所述被识别设备的唯一标识；

[0040] 从所述被识别设备发送的数据中提取出随机字符串和第三签名值，所述随机字符串包括所述被识别设备生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述随机字符串进行签名得到的；

[0041] 从所述随机字符串中提取所述被识别设备生成所述随机字符串的时间；

[0042] 判断所述被识别设备生成所述随机字符串的时间是否在预设时间范围内；

[0043] 当所述被识别设备生成所述随机字符串的时间在所述预设时间范围内时，使用所述被识别设备的唯一标识对所述第三签名值进行验证；

[0044] 当对所述第三签名值的验证通过时，确定所述被识别设备为可信的。

[0045] 本公开的实施例提供的技术方案可以包括以下有益效果：利用发送端的唯一标识对携带时间信息的随机字符串进行签名，通过该唯一标识，可以验证发送端的合法性，并且，根据该唯一标识对携带时间信息的随机字符串进行签名，保证了时间值的安全性，避免了时间值在传输过程中被篡改。

[0046] 根据本公开实施例的第五方面，提供一种数据传输方法，应用于数据发送端，所述方法包括：

[0047] 获取数据发送端的私钥；

[0048] 生成包括当前时间的随机字符串；

[0049] 使用所述数据发送端的私钥对所要传输的第一数据和所述随机字符串进行签名，得到第四签名值；

[0050] 将所述第一数据，所述随机字符串和所述第四签名值发送到所述数据接收端。

[0051] 本公开的实施例提供的技术方案可以包括以下有益效果：利用数据发送端自身的私钥对要传送的数据和包含时间信息的随机字符串进行签名，这样的签名方式，无需获知数据接收端的公钥，在保证数据发送过程安全的基础上，可实现对多个存储有该数据发送端私钥的数据接收端发送数据。

[0052] 根据本公开实施例的第六方面，提供一种数据传输方法，其特征在于，应用于数据接收端，所述方法包括：

[0053] 接收数据发送端发送的数据；

[0054] 获取所述数据发送端的公钥；

[0055] 从所述数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第四签名值为使用所述数据发送端的私钥对所述第一数据和随机字符串进行签名得到的；

[0056] 根据所述数据发送端的公钥对所述第四签名值进行验证；

[0057] 当对所述第四签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

[0058] 判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

[0059] 当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述第一数据。

[0060] 本公开的实施例提供的技术方案可以包括以下有益效果：由于第四签名值为使用所述数据发送端的私钥对所述第一数据和随机字符串进行签名得到的，因此，仅需存储有数据发送端的公钥，就可以通过验证第四签名值得到生成该随机字符串的时间信息，简化了数据验证操作。

[0061] 根据本公开实施例的第七方面，提供一种数据传输方法，应用于数据发送端，所述方法包括：

[0062] 获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0063] 使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0064] 使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

[0065] 使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名，得到第二签名值；

[0066] 将所述第二数据，第一签名值和第二签名值发送到所述数据接收端。

[0067] 本公开的实施例提供的技术方案可以包括以下有益效果：在对数据进行加密之后又对加密数据进行签名，增加了数据传输过程中数据的安全性。

[0068] 根据本公开实施例的第八方面，提供一种数据传输方法，应用于数据接收端，所述方法包括：

[0069] 接收数据发送端发送的数据；

[0070] 获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

[0071] 从所述数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述第二签名值为使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名得到的；

[0072] 根据所述数据发送端的唯一标识对所述第二签名值进行验证；

[0073] 当对所述第二签名值验证通过时，使用所述数据发送端的公钥对所述第一签名值进行验证；

[0074] 当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

[0075] 本公开的实施例提供的技术方案可以包括以下有益效果：通过数据发送端的唯一标识，可以验证发送端的合法性，该唯一标识和数据发送端的公钥是预先存储在数据接收端的，并不携带在上下行的数据中，因此即使数据发送端发送的数据被第三方截获，第三方也无法得到未加密的第一数据。

[0076] 根据本公开实施例的第九方面，提供一种数据传输装置，应用于数据发送端，所述装置包括：

[0077] 第一获取模块，用于获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0078] 第一加密模块，用于使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0079] 第一签名模块，用于使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

[0080] 第一生成模块，用于生成包括当前时间的随机字符串；

[0081] 第二签名模块，用于使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，得到第三签名值；

[0082] 第一发送模块，用于将所述第二数据，第一签名值、所述随机字符串和第三签名值发送到所述数据接收端。

[0083] 在一个实施例中，所述第二签名模块，包括：

[0084] 运算子模块，用于以所述数据发送端的唯一标识为密钥，对所述第二数据、第一签名值和所述随机字符串进行哈希运算消息认证码 (HMAC) 运算。

[0085] 在一个实施例中，所述第一获取模块，包括：

[0086] 提取子模块，用于当所述数据发送端为移动终端时，从所述移动终端的信任区域 (TrustZone) 的回访保护存储块 (RPMB) 区域或安全文件系统 (SFS) 区域提取所述移动终端的私钥。

[0087] 根据本公开实施例的第十方面，提供一种数据传输装置，应用于数据接收端，所述装置包括：

[0088] 第一接收模块，用于接收数据发送端发送的数据；

[0089] 第二获取模块，用于获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

[0090] 第一提取模块，用于从所述数据发送端发送的数据中提取出第二数据，第一签名值，随机字符串和第三签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述第二数据、所述随机字符串和第一签名值进行签名得到的；

[0091] 第一验证模块，用于根据所述数据发送端的唯一标识对所述第三签名值进行验证；

[0092] 第二提取模块，用于当对所述第三签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

[0093] 第一判断模块，用于判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

[0094] 第二验证模块，用于当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述数据发送端的公钥对所述第一签名值进行验证；

[0095] 第一解密模块，用于当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

[0096] 根据本公开实施例的第十一方面，提供一种数据传输装置，应用于被识别设备，所述装置包括：

[0097] 第三获取模块，用于获取所述被识别设备的唯一标识；

[0098] 第二生成模块，用于生成包括当前时间的随机字符串；

[0099] 第三签名模块，用于根据所述发送端唯一标识对所述随机字符串进行签名，得到第三签名值；

[0100] 第二发送模块，用于将所述随机字符串和所述第三签名值发送到识别设备。

[0101] 根据本公开实施例的第十二方面，提供一种数据传输装置，应用于识别设备，所述装置包括：

[0102] 第二接收模块，用于接收被识别设备发送的数据；

[0103] 第四获取模块，用于获取所述被识别设备的唯一标识；

[0104] 第三提取模块，用于从所述被识别设备发送的数据中提取出随机字符串和第三签名值，所述随机字符串包括所述被识别设备生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述随机字符串进行签名得到的；

[0105] 第四提取模块，用于从所述随机字符串中提取所述被识别设备生成所述随机字符串的时间；

[0106] 第二判断模块，用于判断所述被识别设备生成所述随机字符串的时间是否在预设时间范围内；

[0107] 第三验证模块，用于当所述被识别设备生成所述随机字符串的时间在所述预设时间范围内时，使用所述被识别设备的唯一标识对所述第三签名值进行验证；

[0108] 确定模块，用于当对所述第三签名值的验证通过时，确定所述被识别设备为可信的。

[0109] 根据本公开实施例的第十三方面，提供一种数据传输装置，应用于数据发送端，所述装置包括：

[0110] 第五获取模块，用于获取数据发送端的私钥；

[0111] 第三生成模块，用于生成包括当前时间的随机字符串；

[0112] 第四签名模块，用于使用所述数据发送端的私钥对所要传输的第一数据和所述随机字符串进行签名，得到第四签名值；

[0113] 第三发送模块，用于将所述第一数据，所述随机字符串和所述第四签名值发送到所述数据接收端。

[0114] 根据本公开实施例的第十四方面，提供一种数据传输装置，应用于数据接收端，所述装置包括：

[0115] 第三接收模块，用于接收数据发送端发送的数据；

[0116] 第六获取模块，用于获取所述数据发送端的公钥；

[0117] 第五提取模块，用于从所述数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第四签名值为使用所述数据发送端的私钥对所述第一数据和随机字符串进行签名得到的；

[0118] 第四验证模块，用于根据所述数据发送端的公钥对所述第四签名值进行验证；

[0119] 第六提取模块，用于当对所述第四签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

[0120] 第三判断模块，用于判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

[0121] 使用模块，用于当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述第一数据。

[0122] 根据本公开实施例的第十五方面，提供一种数据传输装置，应用于数据发送端，所述装置包括：

[0123] 第七获取模块，用于获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0124] 第二加密模块，用于使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0125] 第五签名模块，用于使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

[0126] 第六签名模块，用于使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名，得到第二签名值；

[0127] 第四发送模块，用于将所述第二数据，第一签名值和第二签名值发送到所述数据接收端。

[0128] 根据本公开实施例的第十六方面，提供一种数据传输装置，应用于数据接收端，所述装置包括：

[0129] 第四接收模块，用于接收数据发送端发送的数据；

[0130] 第八获取模块，用于获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

[0131] 第七提取模块，用于从所述数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述第二签名值为使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名得到的；

[0132] 第五验证模块，用于根据所述数据发送端的唯一标识对所述第二签名值进行验证；

[0133] 第六验证模块，用于当对所述第二签名值验证通过时，使用所述数据发送端的公钥对所述第一签名值进行验证；

[0134] 第二解密模块，用于当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

[0135] 根据本公开实施例的第十七方面，提供一种数据传输装置，包括：

[0136] 处理器；

[0137] 用于存储处理器可执行指令的存储器；

[0138] 其中，所述处理器被配置为：

[0139] 获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0140] 使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0141] 使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

[0142] 生成包括当前时间的随机字符串；

[0143] 使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，得到第三签名值；

[0144] 将所述第二数据，第一签名值、所述随机字符串和第三签名值发送到所述数据接收端。

[0145] 根据本公开实施例的第十八方面，提供一种数据传输装置，包括：

[0146] 处理器；

[0147] 用于存储处理器可执行指令的存储器；

[0148] 其中，所述处理器被配置为：

[0149] 接收数据发送端发送的数据；

[0150] 获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

[0151] 从所述数据发送端发送的数据中提取出第二数据，第一签名值，随机字符串和第三签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述第二数据、所述随机字符串和第一签名值进行签名得到的；

[0152] 根据所述数据发送端的唯一标识对所述第三签名值进行验证；

[0153] 当对所述第三签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

[0154] 判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

[0155] 当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述数据发送端的公钥对所述第一签名值进行验证；

[0156] 当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

[0157] 根据本公开实施例的第十九方面，提供一种数据传输装置，包括：

[0158] 处理器；

[0159] 用于存储处理器可执行指令的存储器；

[0160] 其中，所述处理器被配置为：

[0161] 获取被识别设备的唯一标识；

[0162] 生成包括当前时间的随机字符串；

[0163] 根据所述发送端唯一标识对所述随机字符串进行签名，得到第三签名值；

[0164] 将所述随机字符串和所述第三签名值发送到识别设备。

[0165] 根据本公开实施例的第二十方面，提供一种数据传输装置，包括：

[0166] 处理器；

[0167] 用于存储处理器可执行指令的存储器；

[0168] 其中，所述处理器被配置为：

[0169] 接收被识别设备发送的数据；

[0170] 获取所述被识别设备的唯一标识；

[0171] 从所述被识别设备发送的数据中提取出随机字符串和第三签名值，所述随机字符串包括所述被识别设备生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述随机字符串进行签名得到的；

[0172] 从所述随机字符串中提取所述被识别设备生成所述随机字符串的时间；

[0173] 判断所述被识别设备生成所述随机字符串的时间是否在预设时间范围内；

[0174] 当所述被识别设备生成所述随机字符串的时间在所述预设时间范围内时，使用所述被识别设备的唯一标识对所述第三签名值进行验证；

[0175] 当对所述第三签名值的验证通过时，确定所述被识别设备为可信的。

[0176] 根据本公开实施例的第二十一方面，提供一种数据传输装置，包括：

[0177] 处理器；

[0178] 用于存储处理器可执行指令的存储器；

[0179] 其中，所述处理器被配置为：

[0180] 获取数据发送端的私钥；

[0181] 生成包括当前时间的随机字符串；

[0182] 使用所述数据发送端的私钥对所要传输的第一数据和所述随机字符串进行签名，得到第四签名值；

[0183] 将所述第一数据，所述随机字符串和所述第四签名值发送到所述数据接收端。

[0184] 根据本公开实施例的第二十二方面，提供一种数据传输装置，包括：

[0185] 处理器；

[0186] 用于存储处理器可执行指令的存储器；

[0187] 其中，所述处理器被配置为：

[0188] 接收数据发送端发送的数据；

[0189] 获取所述数据发送端的公钥；

[0190] 从所述数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第四签名值为使用所述数据发送端的私钥对所述第一数据和随机字符串进行签名得到的；

[0191] 根据所述数据发送端的公钥对所述第四签名值进行验证；

[0192] 当对所述第四签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

[0193] 判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

[0194] 当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述第一数据。

[0195] 根据本公开实施例的第二十三方面，提供一种数据传输装置，包括：

[0196] 处理器；

[0197] 用于存储处理器可执行指令的存储器；

[0198] 其中，所述处理器被配置为：

[0199] 获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0200] 使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0201] 使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

[0202] 使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名，得到第二签名值；

[0203] 将所述第二数据，第一签名值和第二签名值发送到所述数据接收端。

[0204] 根据本公开实施例的第二十四方面，提供一种数据传输装置，包括：

[0205] 处理器；

[0206] 用于存储处理器可执行指令的存储器；

[0207] 其中，所述处理器被配置为：

[0208] 接收数据发送端发送的数据；

[0209] 获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

[0210] 从所述数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述第二签名值为使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名得到的；

[0211] 根据所述数据发送端的唯一标识对所述第二签名值进行验证；

[0212] 当对所述第二签名值验证通过时，使用所述数据发送端的公钥对所述第一签名值进行验证；

[0213] 当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

[0214] 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

[0215] 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。

[0216] 图 1 是根据一示例性实施例示出的一种数据传输方法的流程图；

[0217] 图 2 是根据一示例性实施例示出的一种数据传输方法的流程图；

[0218] 图 3 是根据一示例性实施例示出的一种数据传输方法的流程图；

[0219] 图 4 是根据一示例性实施例示出的一种数据传输方法的流程图；

[0220] 图 5 是根据一示例性实施例示出的一种数据传输方法的流程图；

[0221] 图 6 是根据一示例性实施例示出的一种数据传输方法的流程图；

[0222] 图 7 是根据一示例性实施例示出的一种数据传输方法的流程图；

[0223] 图 8 是根据一示例性实施例示出的一种数据传输方法的流程图；

[0224] 图 9 是根据一示例性实施例示出的一种数据传输方法的流程图；

[0225] 图 10 是根据一示例性实施例示出的一种数据传输方法的流程图；

[0226] 图 11 是根据一示例性实施例示出的一种数据传输装置的框图。

[0227] 图 12 是根据一示例性实施例示出的一种数据传输装置的框图。

[0228] 图 13 是根据一示例性实施例示出的一种数据传输装置的框图。

[0229] 图 14 是根据一示例性实施例示出的一种数据传输装置的框图。

[0230] 图 15 是根据一示例性实施例示出的一种数据传输装置的框图。

[0231] 图 16 是根据一示例性实施例示出的一种数据传输装置的框图。

[0232] 图 17 是根据一示例性实施例示出的一种数据传输装置的框图。

[0233] 图 18 是根据一示例性实施例示出的一种数据传输装置的框图。

[0234] 图 19 是根据一示例性实施例示出的一种数据传输装置的框图。

[0235] 图 20 是根据一示例性实施例示出的一种数据传输装置的框图。

[0236] 图 21 是根据一示例性实施例示出的一种数据传输的装置 2100 的框图。

[0237] 图 22 是根据一示例性实施例示出的一种数据传输的装置 2200 的框图。

具体实施方式

[0238] 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。

[0239] 图 1 是根据一示例性实施例示出的一种数据传输方法的流程图，如图 1 所示，该数据传输方法用于终端或服务器，包括以下步骤：

[0240] 在步骤 S11 中，获取数据发送端的唯一标识和私钥，以及数据接收端的公钥。

[0241] 在步骤 S12 中，使用数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据。

[0242] 在步骤 S13 中，使用数据发送端的私钥对第二数据进行签名，得到第一签名值。

[0243] 在步骤 S14 中，生成包括当前时间的随机字符串。

[0244] 在步骤 S15 中，使用数据发送端的唯一标识对第二数据、第一签名值和随机字符串进行签名，得到第三签名值。

[0245] 在步骤 S16 中，将第二数据，第一签名值、随机字符串和第三签名值发送到数据接收端。

[0246] 例如，数据发送端为手机，数据接收端为手机安装的某个应用的后台服务器，手机要发送加密数据给服务器时，先根据预先保存的服务器的公钥对要传输的数据进行加密，得到加密后的数据 C，再利用手机的私钥对加密后的数据进行签名，得到签名值 DS。随机生成一个随机字符串 TR，TR 中包含其生成时间，根据手机的唯一标识对 C、DS 和 TR 进行签名，得到第三签名值 S。然后将 C、DS、TR 和 S 发送给服务器。

[0247] 又例如，数据发送端为手机安装的某个应用的后台服务器，数据接收端为手机，服务器要发送加密数据给手机时，先根据预先保存的手机的公钥对要传输的数据进行加密，得到加密后的数据，再利用服务器的私钥对加密后的数据进行签名，得到第五签名值。随机生成一个包含其生成时间的随机字符串，根据服务器的唯一标识对加密后的数据、第五签名值和随机字符串进行签名，得到第六签名值。然后将加密后的数据、第五签名值、随机字符串和第六签名值发送给手机。

[0248] 需要说明的是，当数据发送端为手机时，该唯一标识可以是通过将手机CPU(Central Processing Unit，中央处理器)的唯一标识符、IMEI(International Mobile Equipment Identity，移动设备国际身份码)和可选的随机字符组成的长字符串，三者进行哈希计算所得到的结果作为设备的唯一标识符。

[0249] 当数据发送端为服务器时，该唯一标识是通过将服务器CPU的唯一标识符和可选的随机字符组成的长字符串二者进行哈希计算所得到的结果作为设备的唯一标识符。

[0250] 本公开的实施例提供的技术方案可以包括以下有益效果：通过数据接收端的公钥对第一数据进行加密，得到第二数据，再通过数据发送端的私钥对第二数据进行签名得到第一签名值，在对数据进行加密之后又对加密数据进行签名，增加了数据传输过程中数据的安全性，根据设备的唯一标识对第二数据，第一签名值进行签名，进一步增加了数据传输过程中数据的安全性。

[0251] 图2是根据另一示例性实施例示出的一种数据传输方法的流程图，如图2所示，步骤S15可包括步骤S21：

[0252] 在步骤S21中：以数据发送端的唯一标识为密钥，对第二数据、第一签名值和随机字符串进行哈希运算消息认证码(HMAC)运算。

[0253] 本公开的实施例提供的技术方案可以包括以下有益效果：通过将数据发送端的唯一标识作为密钥，具备了采用哈希运算消息认证码运算的条件，而采用该运算方法，有第三方非法截获消息时，只能获取到HMAC结果，仅仅根据该结果并不能推出密钥，即无法获知数据发送端的唯一标识。保证了设备唯一标识在发送过程中的安全性，保证了验证设备合法性的正确无误。

[0254] 图3是根据另一示例性实施例示出的一种数据传输方法的流程图，如图3所示，当数据发送端为移动终端时，步骤S11中，获取数据发送端的私钥可包括步骤S31：

[0255] 在步骤S31中：从移动终端的信任区域(TrustZone)的回访保护存储块(RPMB)区域或安全文件系统(SFS)区域提取移动终端的私钥。

[0256] 本公开的实施例提供的技术方案可以包括以下有益效果：将私钥存储在移动终端的信任区域(TrustZone)的回访保护存储块(RPMB)区域或安全文件系统(SFS)区域，保证了私钥在本地的安全性。

[0257] 图4是根据一示例性实施例示出的一种数据传输方法的流程图，如图4所示，该数据传输方法用于服务器，包括以下步骤：

[0258] 在步骤S41中，接收数据发送端发送的数据；

[0259] 在步骤S42中，获取数据接收端的私钥，数据发送端的唯一标识和公钥；

[0260] 在步骤S43中，从数据发送端发送的数据中提取出第二数据，第一签名值，随机字符串和第三签名值，第二数据为使用数据接收端的公钥对所要传输的第一数据进行加密后得到的，第一签名值为使用数据发送端的私钥对第二数据进行签名得到的，随机字符串包括数据发送端生成随机字符串的时间，第三签名值为使用数据发送端的唯一标识对第二数据、随机字符串和第一签名值进行签名得到的；

[0261] 在步骤S44中，根据数据发送端的唯一标识对第三签名值进行验证；

[0262] 在步骤S45中，当对第三签名值验证通过时，从随机字符串中提取数据发送端生成随机字符串的时间；

[0263] 在步骤 S46 中，判断数据发送端生成随机字符串的时间是否在预设时间范围内；

[0264] 在步骤 S47 中，当数据发送端生成随机字符串的时间在预设时间范围内时，使用数据发送端的公钥对第一签名值进行验证；

[0265] 在步骤 S48 中，当对第一签名值验证通过时，使用数据接收端的私钥对第二数据进行解密，得到第一数据。

[0266] 例如，数据发送端为手机，数据接收端为手机安装的某个应用的后台服务器，或者手机生产厂家的服务器。在服务器与手机进行数据交互之前，首先需要在本身的数据库中存储该手机的公钥信息和唯一标识符信息。服务器接收到手机发送的加密后的数据 C、对加密数据进行签名后的第一签名值 DS、包含其生成时间的随机字符串 TR 和根据手机的唯一标识对 C、DS、TR 进行签名后的第三签名值 S 之后，再将加密后的数据 C、第一签名值 DS、随机字符串 TR 和第三签名值 S 提取出来。根据服务器中预先存储的服务器的唯一标识对第三签名值 S 进行验证，验证通过后，提取随机字符串 TR 中包含的时间信息，由于随机字符串生成之后很短的时间之内就进行数据发送，该随机字符串的生成时间几乎和数据的发送时间是一致的，因此，得到该随机字符串的生成时间就相当于得到了数据发送时间。判断生成时间是否在预设时间范围内，相当于判断数据发送时间是否在预设时间范围之内。当手机生成随机字符串的时间在预设时间范围内时，使用预先存储在服务器中的手机的公钥对第一签名值 DS 进行验证；验证通过后得到加密后的数据 C，再根据服务器自身的私钥对该加密后的数据 C 进行解密，得到原始数据。该预设时间范围通常根据数据时效性情况进行设置。

[0267] 又例如，数据发送端为服务器，数据接收端为手机。在手机与服务器进行数据交互之前，首先需要在本身的数据库中存储该手机的公钥信息和唯一标识符信息。手机接收到服务器发送的加密后的数据、对加密数据进行签名后的第五签名值、包含其生成时间的随机字符串和第六签名值之后，再将加密后的数据、第五签名值、随机字符串和第六签名值提取出来。根据手机中预先存储的服务器的唯一标识对第六签名值进行验证，验证通过后，提取随机字符串中包含的时间信息，生成随机字符串的时间与当前时间的间隔在预设时间范围内时，使用预先存储在服务器中的服务器的公钥对第五签名值进行验证；验证通过后得到加密后的数据，再根据手机自身的私钥对该加密后的数据进行解密，得到原始数据。

[0268] 本公开的实施例提供的技术方案可以包括以下有益效果：通过数据发送端的唯一标识对第三签名进行验证，提取随机字符串中携带的时间信息，当生成随机字符串的时间在预设时间范围内时使用数据发送端的公钥对第一签名值进行验证，从而保证了数据的时效性。

[0269] 其次，由于随机数的非唯一性，以及使用随机数对签名信息加解密算法的不可确定性，不仅使签名信息的解密复杂度提高，利用随机字符串携带时间信息，还保证了时间信息的安全性，从而进一步提高了数据发送过程中数据的安全性。

[0270] 图 5 是根据一示例性实施例示出的一种数据传输方法的流程图，如图 5 所示，该数据传输方法用于需要被识别手机，包括以下步骤：

[0271] 在步骤 S51 中，获取被识别设备的唯一标识；

[0272] 在步骤 S52 中，生成包括当前时间的随机字符串；

[0273] 在步骤 S53 中，根据发送端唯一标识对随机字符串进行签名，得到第三签名值；

[0274] 在步骤 S54 中，将随机字符串和第三签名值发送到识别设备。

[0275] 例如，发送验证信息给服务器。当用户根据相应的验证入口发送验证请求时，手机根据自身 CPU(Central Processing Unit，中央处理器）的唯一标识符、IMEI(International Mobile Equipment Identity，移动设备国际身份码）和可选的随机字符组成的长字符串，三者进行哈希计算，将计算得到的结果作为手机的唯一标识符，并生成包括其生成时间的随机字符串，根据唯一标识符对随机字符串进行签名，并将随机字符串和对该随机字符串进行签名的签名值发送给上述服务器中。

[0276] 本公开的实施例提供的技术方案可以包括以下有益效果：利用发送端的唯一标识对携带时间信息的随机字符串进行签名，使数据接收端能够通过该唯一标识验证发送端的合法性，并且根据该唯一标识对携带时间信息的随机字符串进行签名，保证了时间值的安全性，避免了时间值在传输过程中被篡改。

[0277] 图 6 是根据一示例性实施例示出的一种数据传输方法的流程图，如图 6 所示，该数据传输方法用于提供手机识别服务的服务器中，包括以下步骤：

[0278] 在步骤 S61 中，接收被识别设备发送的数据；

[0279] 在步骤 S62 中，获取被识别设备的唯一标识；

[0280] 在步骤 S63 中，从被识别设备发送的数据中提取出随机字符串和第三签名值，随机字符串包括被识别设备生成随机字符串的时间，第三签名值为使用数据发送端的唯一标识对随机字符串进行签名得到的；

[0281] 在步骤 S64 中，从随机字符串中提取被识别设备生成随机字符串的时间；

[0282] 在步骤 S65 中，判断被识别设备生成随机字符串的时间是否在预设时间范围内；

[0283] 在步骤 S66 中，当被识别设备生成随机字符串的时间在预设时间范围内时，使用被识别设备的唯一标识对第三签名值进行验证；

[0284] 在步骤 S67 中，当对第三签名值的验证通过时，确定被识别设备为可信的。

[0285] 例如，识别设备为提供手机识别服务的服务器。在服务器与手机进行数据交互之前，首先需要在本身的数据库中存储该手机的唯一标识符信息。服务器接收到手机发送的数据后，从数据中提取出随机字符串和第三签名值，判断随机字符串中的时间信息是否在预设时间范围内，当随机字符串中的时间信息在预设时间范围内时，使用被设别设备的唯一标识对第三签名值进行验证，验证通过事，说明该手机为可信的。

[0286] 本公开的实施例提供的技术方案可以包括以下有益效果：利用发送端的唯一标识对携带时间信息的随机字符串进行签名，通过该唯一标识，可以验证发送端的合法性，并且，根据该唯一标识对携带时间信息的随机字符串进行签名，保证了时间值的安全性，避免了时间值在传输过程中被篡改。

[0287] 图 7 是根据一示例性实施例示出的一种数据传输方法的流程图，如图 7 所示，该数据传输方法用于对多台手机发送数据的服务器中，包括以下步骤：

[0288] 在步骤 S71 中，获取数据发送端的私钥；

[0289] 在步骤 S72 中，生成包括当前时间的随机字符串；

[0290] 在步骤 S73 中，使用数据发送端的私钥对所要传输的第一数据和随机字符串进行签名，得到第四签名值；

[0291] 在步骤 S74 中，将第一数据，随机字符串和第四签名值发送到数据接收端。

[0292] 例如，数据发送端为向多台手机发送数据的服务器。首先，生成一个包含当前时间的随机字符串 TR，利用服务器自身的私钥对要发送的数据 P 和上述随机字符串 TR 进行签名，得到第四签名值 S，并将要发送的数据 P、随机字符串 TR 和第四签名值 S 发送给多台手机。

[0293] 另外，需要说明的是，当服务器希望给一台手机发送数据时，可以获取存储在数据库中的该手机的公钥，利用该公钥对要发送的数据加密，得到加密后的数据，并利用自身的私钥对数据进行签名，得到第五签名值，再生成一个包含当前时间的随机字符串，对加密后的数据进行 HMAC 签名，得到第六签名值，

[0294] 本公开的实施例提供的技术方案可以包括以下有益效果：利用服务器自身的私钥对要传送的数据和包含时间信息的随机字符串进行签名，这样的签名方式，无需获知接收数据的手机的公钥，在保证数据发送过程安全的基础上，实现对多个存储有该数据发送端私钥的手机发送数据。

[0295] 图 8 是根据一示例性实施例示出的一种数据传输方法的流程图，如图 8 所示，该数据传输方法用于存储有服务器公钥的手机中，包括以下步骤：

[0296] 在步骤 S81 中，接收数据发送端发送的数据；

[0297] 在步骤 S82 中，获取数据发送端的公钥；

[0298] 在步骤 S83 中，从数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值，随机字符串包括数据发送端生成随机字符串的时间，第四签名值为使用数据发送端的私钥对第一数据和随机字符串进行签名得到的；

[0299] 在步骤 S84 中，根据数据发送端的公钥对第四签名值进行验证；

[0300] 在步骤 S85 中，当对第四签名值验证通过时，从随机字符串中提取数据发送端生成随机字符串的时间；

[0301] 在步骤 S86 中，判断数据发送端生成随机字符串的时间是否在预设时间范围内；

[0302] 在步骤 S87 中，当数据发送端生成随机字符串的时间在预设时间范围内时，使用第一数据。

[0303] 例如，数据接收端为手机。在与服务器进行数据交互之前，需要存储服务器的公钥，当接收到服务器发送的数据时，获取预先存储的服务器的公钥，利用服务器的公钥对第四签名值 S 进行验证，验证通过后，提取随机字符串 TR 中包含的时间信息，由于随机字符串生成之后很短的时间之内就进行数据发送，该随机字符串的生成时间几乎和数据的发送时间是一致的，因此，得到该随机字符串的生成时间就相当于得到了数据发送时间。判断生成时间是否在预设时间范围内，相当于判断数据发送时间是否在预设时间范围之内。当生成字符串的时间在预设时间范围内时，说明该数据是有效的，可以使用。

[0304] 本公开的实施例提供的技术方案可以包括以下有益效果：由于第四签名值为使用服务器的私钥对数据和随机字符串进行签名得到的，因此，仅需存储有服务器的公钥，就可以通过验证第四签名值得到生成该随机字符串的时间信息，简化了数据验证操作。

[0305] 图 9 是根据一示例性实施例示出的一种数据传输方法的流程图，如图 9 所示，该数据传输方法用于存储有服务器公钥的手机中，包括以下步骤：

[0306] 在步骤 S91 中，获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0307] 在步骤 S92 中，使用数据接收端的公钥对所要传输的第一数据进行加密，得到加

密后的第二数据；

[0308] 在步骤 S93 中，使用数据发送端的私钥对第二数据进行签名，得到第一签名值；

[0309] 在步骤 S94 中，使用数据发送端的唯一标识对第二数据和第一签名值进行签名，得到第二签名值；

[0310] 在步骤 S95 中，将第二数据，第一签名值和第二签名值发送到数据接收端。

[0311] 例如，数据发送端为手机，数据接收端为手机安装的某个应用的后台服务器，手机要发送加密数据给服务器，先根据预先保存的服务器的公钥对要传输的数据 P 进行加密，得到加密后的数据 C，再利用手机的私钥对加密后的数据进行签名，得到签名值 DS。根据手机的唯一标识对 C、DS 进行签名，得到第三签名值 S。然后将 C、DS 和 S 发送给服务器。本方法适用于对无时效性要求的数据的发送。

[0312] 本公开的实施例提供的技术方案可以包括以下有益效果：在对数据进行加密之后又对加密数据进行签名，增加了数据传输过程中数据的安全性。

[0313] 图 10 是根据一示例性实施例示出的一种数据传输方法的流程图，如图 10 所示，该数据传输方法用于接收数据的服务器中，包括以下步骤：

[0314] 在步骤 S101 中，接收数据发送端发送的数据；

[0315] 在步骤 S102 中，获取数据接收端的私钥，数据发送端的唯一标识和公钥；

[0316] 在步骤 S103 中，从数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值，第二数据为使用数据接收端的公钥对所要传输的第一数据进行加密后得到的，第一签名值为使用数据发送端的私钥对第二数据进行签名得到的，第二签名值为使用数据发送端的唯一标识对第二数据和第一签名值进行签名得到的；

[0317] 在步骤 S104 中，根据数据发送端的唯一标识对第二签名值进行验证；

[0318] 在步骤 S105 中，当对第二签名值验证通过时，使用数据发送端的公钥对第一签名值进行验证；

[0319] 在步骤 S106 中，当对第一签名值验证通过时，使用数据接收端的私钥对第二数据进行解密，得到第一数据。

[0320] 例如，数据发送端为手机，数据接收端为手机安装的某个应用的后台服务器。在服务器与手机进行数据交互之前，首先需要在本身的数据库中存储该手机的公钥信息和唯一标识符信息。根据服务器中预先存储的服务器的唯一标识对第二签名值进行验证，验证通过后，使用预先存储在服务器中的手机的公钥对第一签名值进行验证；验证通过后再使用自身的私钥对该加密后的数据 C 进行解密，得到原始数据。

[0321] 本公开的实施例提供的技术方案可以包括以下有益效果：通过数据发送端的唯一标识，可以验证发送端的合法性，该唯一标识和数据发送端的公钥是预先存储在数据接收端的，并不携带在上下行的数据中，因此即使数据发送端发送的数据被第三方截获，第三方也无法得到未加密的第一数据。

[0322] 图 11 是根据一示例性实施例示出的一种数据传输装置的框图，应用于数据发送端。如图 11 所示，该装置包括第一获取模块 111，第一加密模块 112，第一签名模块 113，第一生成模块 114，第二签名模块 115，第一发送模块 116。

[0323] 该第一获取模块 111 被配置为获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0324] 该第一加密模块 112 被配置为使用数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0325] 第一签名模块 113 被配置为使用数据发送端的私钥对第二数据进行签名，得到第一签名值；

[0326] 第一生成模块 114 被配置为生成包括当前时间的随机字符串；

[0327] 第二签名模块 115 被配置为使用数据发送端的唯一标识对第二数据、第一签名值和随机字符串进行签名，得到第三签名值；

[0328] 第一发送模块 116 被配置为将第二数据，第一签名值、随机字符串和第三签名值发送到数据接收端。

[0329] 本公开的实施例提供的技术方案可以包括以下有益效果：通过数据接收端的公钥对第一数据进行加密，得到第二数据，再通过数据发送端的私钥对第二数据进行签名得到第一签名值，在对数据进行加密之后又对加密数据进行签名，增加了数据传输过程中数据的安全性，根据设备的唯一标识对第二数据，第一签名值进行签名，进一步增加了数据传输过程中数据的安全性。

[0330] 图 12 是根据另一示例性实施例示出的第二签名模块 115 的框图。如图 12 所示，第二签名模块 115 包括：运算子模块 121。

[0331] 该运算子模块 121 被配置为以数据发送端的唯一标识为密钥，对第二数据、第一签名值和随机字符串进行哈希运算消息认证码 (HMAC) 运算。

[0332] 本公开的实施例提供的技术方案可以包括以下有益效果：通过将数据发送端的唯一标识作为密钥，具备了采用哈希运算消息认证码运算的条件，而采用该运算方法，有第三方非法截获消息时，只能获取到 HMAC 结果，仅仅根据该结果并不能推出密钥，即无法获知数据发送端的唯一标识。保证了设备唯一标识在发送过程中的安全性，保证了验证设备合法性的正确无误。

[0333] 图 13 是根据另一示例性实施例示出的第一获取模块 111 的框图。如图 13 所示，第一获取模块 111 包括：提取子模块 131。

[0334] 该提取子模块 131 被配置为当数据发送端为移动终端时，从移动终端的信任区域 (TrustZone) 的回访保护存储块 (RPMB) 区域或安全文件系统 (SFS) 区域提取移动终端的私钥。

[0335] 本公开的实施例提供的技术方案可以包括以下有益效果：将私钥存储在移动终端的信任区域 (TrustZone) 的回访保护存储块 (RPMB) 区域或安全文件系统 (SFS) 区域，保证了私钥在本地的安全性。

[0336] 图 14 是根据一示例性实施例示出的一种数据传输装置的框图，应用于数据接收端。如图 14 所示，该装置包括第一接收模块 141，第二获取模块 142，第一提取模块 143，第一验证模块 144，第二提取模块 145，第一判断模块 146，第二验证模块 147 和第一解密模块 148。

[0337] 第一接收模块 141 被配置为接收数据发送端发送的数据；

[0338] 第二获取模块 142 被配置为获取数据接收端的私钥，数据发送端的唯一标识和公钥；

[0339] 第一提取模块 143 被配置为从数据发送端发送的数据中提取出第二数据，第一签

名值，随机字符串和第三签名值，第二数据为使用数据接收端的公钥对所要传输的第一数据进行加密后得到的，第一签名值为使用数据发送端的私钥对第二数据进行签名得到的，随机字符串包括数据发送端生成随机字符串的时间，第三签名值为使用数据发送端的唯一标识对第二数据、随机字符串和第一签名值进行签名得到的；

[0340] 第一验证模块 144 被配置为根据数据发送端的唯一标识对第三签名值进行验证；

[0341] 第二提取模块 145 被配置为当对第三签名值验证通过时，从随机字符串中提取数据发送端生成随机字符串的时间；

[0342] 第一判断模块 146 被配置为判断数据发送端生成随机字符串的时间是否在预设时间范围内；

[0343] 第二验证模块 147 被配置为当数据发送端生成随机字符串的时间在预设时间范围内时，使用数据发送端的公钥对第一签名值进行验证；

[0344] 第一解密模块 148 被配置为当对第一签名值验证通过时，使用数据接收端的私钥对第二数据进行解密，得到第一数据。

[0345] 本公开的实施例提供的技术方案可以包括以下有益效果：通过数据发送端的唯一标识对第三签名进行验证，提取随机字符串中携带的时间信息，当生成随机字符串的时间在预设时间范围内时使用数据发送端的公钥对第一签名值进行验证，从而保证了数据的时效性。

[0346] 其次，由于随机数的非唯一性，以及使用随机数对签名信息加解密算法的不可确定性，不仅使签名信息的解密复杂度提高，利用随机字符串携带时间信息，还保证了时间信息的安全性，从而进一步提高了数据发送过程中数据的安全性。

[0347] 图 15 是根据一示例性实施例示出的一种数据传输装置的框图，应用于被识别设备。如图 15 所示，该装置包括第三获取模块 151，第二生成模块 152，第三签名模块 153 和第二发送模块 154。

[0348] 第三获取模块 151 被配置为获取被识别设备的唯一标识；

[0349] 第二生成模块 152 被配置为生成包括当前时间的随机字符串；

[0350] 第三签名模块 153 被配置为根据发送端唯一标识对随机字符串进行签名，得到第三签名值；

[0351] 第二发送模块 154 被配置为将随机字符串和第三签名值发送到识别设备。

[0352] 本公开的实施例提供的技术方案可以包括以下有益效果：利用发送端的唯一标识对携带时间信息的随机字符串进行签名，使数据接收端能够通过该唯一标识验证发送端的合法性，并且根据该唯一标识对携带时间信息的随机字符串进行签名，保证了时间值的安全性，避免了时间值在传输过程中被篡改。

[0353] 图 16 是根据一示例性实施例示出的一种数据传输装置的框图，应用于识别设备。如图 16 所示，该装置包括第二接收模块 161，第四获取模块 162，第三提取模块 163，第四提取模块 164，第二判断模块 165，第三验证模块 166 和确定模块 167。

[0354] 第二接收模块 161，用于接收被识别设备发送的数据；

[0355] 第四获取模块 162，用于获取被识别设备的唯一标识；

[0356] 第三提取模块 163，用于从被识别设备发送的数据中提取出随机字符串和第三签名值，随机字符串包括被识别设备生成随机字符串的时间，第三签名值为使用数据发送端

的唯一标识对随机字符串进行签名得到的；

[0357] 第四提取模块 164，用于从随机字符串中提取被识别设备生成随机字符串的时间；

[0358] 第二判断模块 165，用于判断被识别设备生成随机字符串的时间是否在预设时间范围内；

[0359] 第三验证模块 166，用于当被识别设备生成随机字符串的时间在预设时间范围内时，使用被识别设备的唯一标识对第三签名值进行验证；

[0360] 确定模块 167，用于当对第三签名值的验证通过时，确定被识别设备为可信的。

[0361] 本公开的实施例提供的技术方案可以包括以下有益效果：利用发送端的唯一标识对携带时间信息的随机字符串进行签名，通过该唯一标识，可以验证发送端的合法性，并且，根据该唯一标识对携带时间信息的随机字符串进行签名，保证了时间值的安全性，避免了时间值在传输过程中被篡改。

[0362] 图 17 是根据一示例性实施例示出的一种数据传输装置的框图，应用于数据发送端。如图 17 所示，该装置包括第五获取模块 171，第三生成模块 172，第四签名模块 173 和第三发送模块 174。

[0363] 第五获取模块 171 被配置为获取数据发送端的私钥；

[0364] 第三生成模块 172 被配置为生成包括当前时间的随机字符串；

[0365] 第四签名模块 173 被配置为使用数据发送端的私钥对所要传输的第一数据和随机字符串进行签名，得到第四签名值；

[0366] 第三发送模块 174 被配置为将第一数据，随机字符串和第四签名值发送到数据接收端。

[0367] 本公开的实施例提供的技术方案可以包括以下有益效果：利用数据发送端自身的私钥对要传送的数据和包含时间信息的随机字符串进行签名，这样的签名方式，无需获知数据接收端的公钥，在保证数据发送过程安全的基础上，可实现对多个存储有该数据发送端私钥的数据接收端发送数据。

[0368] 图 18 是根据一示例性实施例示出的一种数据传输装置的框图，应用于数据接收端。如图 18 所示，该装置包括第三接收模块 181，第六获取模块 182，第五提取模块 183，第四验证模块 184，第六提取模块 185，第三判断模块 186 和使用模块 187。

[0369] 第三接收模块 181 被配置为接收数据发送端发送的数据；

[0370] 第六获取模块 182 被配置为获取数据发送端的公钥；

[0371] 第五提取模块 183 被配置为从数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值，随机字符串包括数据发送端生成随机字符串的时间，第四签名值为使用数据发送端的私钥对第一数据和随机字符串进行签名得到的；

[0372] 第四验证模块 184 被配置为根据数据发送端的公钥对第四签名值进行验证；

[0373] 第六提取模块 185 被配置为当对第四签名值验证通过时，从随机字符串中提取数据发送端生成随机字符串的时间；

[0374] 第三判断模块 186 被配置为判断数据发送端生成随机字符串的时间是否在预设时间范围内；

[0375] 使用模块 187 被配置为当数据发送端生成随机字符串的时间在预设时间范围内

时，使用第一数据。

[0376] 本公开的实施例提供的技术方案可以包括以下有益效果：由于第四签名值为使用数据发送端的私钥对第一数据和随机字符串进行签名得到的，因此，仅需存储有数据发送端的公钥，就可以通过验证第四签名值得到生成该随机字符串的时间信息，简化了数据验证操作。

[0377] 图 19 是根据一示例性实施例示出的一种数据传输装置的框图，应用于数据发送端。如图 19 所示，该装置包括第七获取模块 191，第二加密模块 192，第五签名模块 193，第六签名模块 194 和第四发送模块 195。

[0378] 第七获取模块 191 被配置为获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0379] 第二加密模块 192 被配置为使用数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0380] 第五签名模块 193 被配置为使用数据发送端的私钥对第二数据进行签名，得到第一签名值；

[0381] 第六签名模块 194 被配置为使用数据发送端的唯一标识对第二数据和第一签名值进行签名，得到第二签名值；

[0382] 第四发送模块 195 被配置为将第二数据，第一签名值和第二签名值发送到数据接收端。

[0383] 本公开的实施例提供的技术方案可以包括以下有益效果：在对数据进行加密之后又对加密数据进行签名，增加了数据传输过程中数据的安全性。

[0384] 图 20 是根据一示例性实施例示出的一种数据传输装置的框图，应用于数据接收端。如图 20 所示，该装置包括第四接收模块 201，第八获取模块 202，第七提取模块 203，第五验证模块 204，第六验证模块 205 和第二解密模块 206。

[0385] 第四接收模块 201 被配置为接收数据发送端发送的数据；

[0386] 第八获取模块 202 被配置为获取数据接收端的私钥，数据发送端的唯一标识和公钥；

[0387] 第七提取模块 203 被配置为从数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值，第二数据为使用数据接收端的公钥对所要传输的第一数据进行加密后得到的，第一签名值为使用数据发送端的私钥对第二数据进行签名得到的，第二签名值为使用数据发送端的唯一标识对第二数据和第一签名值进行签名得到的；

[0388] 第五验证模块 204 被配置为根据数据发送端的唯一标识对第二签名值进行验证；

[0389] 第六验证模块 205 被配置为当对第二签名值验证通过时，使用数据发送端的公钥对第一签名值进行验证；

[0390] 第二解密模块 206 被配置为当对第一签名值验证通过时，使用数据接收端的私钥对第二数据进行解密，得到第一数据。

[0391] 本公开的实施例提供的技术方案可以包括以下有益效果：通过数据发送端的唯一标识，可以验证发送端的合法性，该唯一标识和数据发送端的公钥是预先存储在数据接收端的，并不携带在上下行的数据中，因此即使数据发送端发送的数据被第三方截获，第三方也无法得到未加密的第一数据。

[0392] 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。

[0393] 图 21 是根据一示例性实施例示出的一种用于数据传输的装置 2100 的框图。例如，装置 2100 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。

[0394] 如图 21 所示，装置 2100 可以包括以下一个或多个组件：处理组件 2102，存储器 2104，电源组件 2106，多媒体组件 2108，音频组件 2110，输入 / 输出 (I/O) 的接口 2112，传感器组件 2114，以及通信组件 2116。

[0395] 处理组件 2102 通常控制装置 2100 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 2102 可以包括一个或多个处理器 2120 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 2102 可以包括一个或多个模块，便于处理组件 2102 和其他组件之间的交互。例如，处理组件 2102 可以包括多媒体模块，以方便多媒体组件 2108 和处理组件 2102 之间的交互。

[0396] 存储器 2104 被配置为存储各种类型的数据以支持在设备 2100 的操作。这些数据的示例包括用于在装置 2100 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 2104 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。

[0397] 电源组件 2106 为装置 2100 的各种组件提供电力。电源组件 2106 可以包括电源管理系统，一个或多个电源，及其他与为装置 2100 生成、管理和分配电力相关联的组件。

[0398] 多媒体组件 2108 包括在所述装置 2100 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 2108 包括一个前置摄像头和 / 或后置摄像头。当设备 2100 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。

[0399] 音频组件 2110 被配置为输出和 / 或输入音频信号。例如，音频组件 2110 包括一个麦克风 (MIC)，当装置 2100 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 2104 或经由通信组件 2116 发送。在一些实施例中，音频组件 2110 还包括一个扬声器，用于输出音频信号。

[0400] I/O 接口 2112 为处理组件 2102 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。

[0401] 传感器组件 2114 包括一个或多个传感器，用于为装置 2100 提供各个方面的状态评估。例如，传感器组件 2114 可以检测到设备 2100 的打开 / 关闭状态，组件的相对定位，

例如所述组件为装置2100的显示器和小键盘，传感器组件2114还可以检测装置2100或装置2100一个组件的位置改变，用户与装置2100接触的存在或不存在，装置2100方位或加速/减速和装置2100的温度变化。传感器组件2114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2114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2114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。

[0402] 通信组件2116被配置为便于装置2100和其他设备之间有线或无线方式的通信。装置2100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2116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2116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。

[0403] 在示例性实施例中，装置2100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。

[0404] 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2104，上述指令可由装置2100的处理器2120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。

[0405] 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数据传输方法，所述方法包括：

[0406] 获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0407] 使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0408] 使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

[0409] 生成包括当前时间的随机字符串；

[0410] 使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，得到第三签名值；

[0411] 将所述第二数据，第一签名值、所述随机字符串和第三签名值发送到所述数据接收端。

[0412] 在一个实施例中，使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，包括：

[0413] 以所述数据发送端的唯一标识为密钥，对所述第二数据、第一签名值和所述随机字符串进行哈希运算消息认证码(HMAC)运算。

[0414] 在一个实施例中，当所述数据发送端为移动终端时，所述获取数据发送端的私钥，包括：

[0415] 从所述移动终端的信任区域(TrustZone)的回访保护存储块(RPMB)区域或安全文件系统(SFS)区域提取所述移动终端的私钥。

[0416] 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数据传输方法，所述方法包括：

[0417] 接收数据发送端发送的数据；

[0418] 获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

[0419] 从所述数据发送端发送的数据中提取出第二数据，第一签名值，随机字符串和第三签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述第二数据、所述随机字符串和第一签名值进行签名得到的；

[0420] 根据所述数据发送端的唯一标识对所述第三签名值进行验证；

[0421] 当对所述第三签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

[0422] 判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

[0423] 当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述数据发送端的公钥对所述第一签名值进行验证；当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

[0424] 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数据传输方法，所述方法包括：

[0425] 获取被识别设备的唯一标识；

[0426] 生成包括当前时间的随机字符串；

[0427] 根据所述发送端唯一标识对所述随机字符串进行签名，得到第三签名值；

[0428] 将所述随机字符串和所述第三签名值发送到识别设备。

[0429] 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数据传输方法，所述方法包括：

[0430] 接收被识别设备发送的数据；

[0431] 获取所述被识别设备的唯一标识；

[0432] 从所述被识别设备发送的数据中提取出随机字符串和第三签名值，所述随机字符串包括所述被识别设备生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述随机字符串进行签名得到的；

[0433] 从所述随机字符串中提取所述被识别设备生成所述随机字符串的时间；

[0434] 判断所述被识别设备生成所述随机字符串的时间是否在预设时间范围内；

[0435] 当所述被识别设备生成所述随机字符串的时间在所述预设时间范围内时，使用所述被识别设备的唯一标识对所述第三签名值进行验证；

[0436] 当对所述第三签名值的验证通过时，确定所述被识别设备为可信的。

[0437] 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数据传输方法，所述方法包括：

[0438] 获取数据发送端的私钥；

[0439] 生成包括当前时间的随机字符串；

[0440] 使用所述数据发送端的私钥对所要传输的第一数据和所述随机字符串进行签名，

得到第四签名值；

[0441] 将所述第一数据，所述随机字符串和所述第四签名值发送到所述数据接收端。

[0442] 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数据传输方法，所述方法包括：

[0443] 接收数据发送端发送的数据；

[0444] 获取所述数据发送端的公钥；

[0445] 从所述数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第四签名值为使用所述数据发送端的私钥对所述第一数据和随机字符串进行签名得到的；

[0446] 根据所述数据发送端的公钥对所述第四签名值进行验证；

[0447] 当对所述第四签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

[0448] 判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

[0449] 当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述第一数据。

[0450] 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数据传输方法，所述方法包括：

[0451] 获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0452] 使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0453] 使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

[0454] 使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名，得到第二签名值；

[0455] 将所述第二数据，第一签名值和第二签名值发送到所述数据接收端。

[0456] 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数据传输方法，所述方法包括：

[0457] 接收数据发送端发送的数据；

[0458] 获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

[0459] 从所述数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述第二签名值为使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名得到的；

[0460] 根据所述数据发送端的唯一标识对所述第二签名值进行验证；

[0461] 当对所述第二签名值验证通过时，使用所述数据发送端的公钥对所述第一签名值进行验证；

[0462] 当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

[0463] 图22是根据一示例性实施例示出的一种用于数据传输的装置2200的框图。例如，装置2200可以被提供为一服务器。参照图22，装置2200包括处理组件2222，其进一步包括

一个或多个处理器，以及由存储器 2232 所代表的存储器资源，用于存储可由处理组件 2222 的执行的指令，例如应用程序。存储器 2232 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 2222 被配置为执行指令，以执行上述方法。

[0464] 装置 2200 还可以包括一个电源组件 2226 被配置为执行装置 2200 的电源管理，一个有线或无线网络接口 2250 被配置为将装置 2200 连接到网络，和一个输入输出 (I/O) 接口 2258。装置 2200 可以操作基于存储在存储器 2232 的操作系统，例如 Windows ServerTM，Mac OS XTM，UnixTM，LinuxTM，FreeBSDTM 或类似。

[0465] 本公开还提供一种数据传输装置，包括：

[0466] 处理器；

[0467] 用于存储处理器可执行指令的存储器；

[0468] 其中，所述处理器被配置为：

[0469] 获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0470] 使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0471] 使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

[0472] 生成包括当前时间的随机字符串；

[0473] 使用所述数据发送端的唯一标识对所述第二数据、第一签名值和所述随机字符串进行签名，得到第三签名值；

[0474] 将所述第二数据，第一签名值、所述随机字符串和第三签名值发送到所述数据接收端。

[0475] 本公开还提供一种数据传输装置，包括：

[0476] 处理器；

[0477] 用于存储处理器可执行指令的存储器；

[0478] 其中，所述处理器被配置为：

[0479] 接收数据发送端发送的数据；

[0480] 获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

[0481] 从所述数据发送端发送的数据中提取出第二数据，第一签名值，随机字符串和第三签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述第二数据、所述随机字符串和第一签名值进行签名得到的；

[0482] 根据所述数据发送端的唯一标识对所述第三签名值进行验证；

[0483] 当对所述第三签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

[0484] 判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

[0485] 当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述数据发送端的公钥对所述第一签名值进行验证；

[0486] 当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进

行解密，得到所述第一数据。

[0487] 本公开还提供一种数据传输装置，包括：

[0488] 处理器；

[0489] 用于存储处理器可执行指令的存储器；

[0490] 其中，所述处理器被配置为：

[0491] 获取被识别设备的唯一标识；

[0492] 生成包括当前时间的随机字符串；

[0493] 根据所述发送端唯一标识对所述随机字符串进行签名，得到第三签名值；

[0494] 将所述随机字符串和所述第三签名值发送到识别设备。

[0495] 本公开还提供一种数据传输装置，包括：

[0496] 处理器；

[0497] 用于存储处理器可执行指令的存储器；

[0498] 其中，所述处理器被配置为：

[0499] 接收被识别设备发送的数据；

[0500] 获取所述被识别设备的唯一标识；

[0501] 从所述被识别设备发送的数据中提取出随机字符串和第三签名值，所述随机字符串包括所述被识别设备生成所述随机字符串的时间，所述第三签名值为使用所述数据发送端的唯一标识对所述随机字符串进行签名得到的；

[0502] 从所述随机字符串中提取所述被识别设备生成所述随机字符串的时间；

[0503] 判断所述被识别设备生成所述随机字符串的时间是否在预设时间范围内；

[0504] 当所述被识别设备生成所述随机字符串的时间在所述预设时间范围内时，使用所述被识别设备的唯一标识对所述第三签名值进行验证；

[0505] 当对所述第三签名值的验证通过时，确定所述被识别设备为可信的。

[0506] 本公开还提供一种数据传输装置，包括：

[0507] 处理器；

[0508] 用于存储处理器可执行指令的存储器；

[0509] 其中，所述处理器被配置为：

[0510] 获取数据发送端的私钥；

[0511] 生成包括当前时间的随机字符串；

[0512] 使用所述数据发送端的私钥对所要传输的第一数据和所述随机字符串进行签名，得到第四签名值；

[0513] 将所述第一数据，所述随机字符串和所述第四签名值发送到所述数据接收端。

[0514] 本公开还提供一种数据传输装置，包括：

[0515] 处理器；

[0516] 用于存储处理器可执行指令的存储器；

[0517] 其中，所述处理器被配置为：

[0518] 接收数据发送端发送的数据；

[0519] 获取所述数据发送端的公钥；

[0520] 从所述数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值，所

述随机字符串包括所述数据发送端生成所述随机字符串的时间，所述第四签名值为使用所述数据发送端的私钥对所述第一数据和随机字符串进行签名得到的；

[0521] 根据所述数据发送端的公钥对所述第四签名值进行验证；

[0522] 当对所述第四签名值验证通过时，从所述随机字符串中提取所述数据发送端生成所述随机字符串的时间；

[0523] 判断所述数据发送端生成所述随机字符串的时间是否在预设时间范围内；

[0524] 当所述数据发送端生成所述随机字符串的时间在所述预设时间范围内时，使用所述第一数据。

[0525] 本公开还提供一种数据传输装置，包括：

[0526] 处理器；

[0527] 用于存储处理器可执行指令的存储器；

[0528] 其中，所述处理器被配置为：

[0529] 获取数据发送端的唯一标识和私钥，以及数据接收端的公钥；

[0530] 使用所述数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据；

[0531] 使用所述数据发送端的私钥对所述第二数据进行签名，得到第一签名值；

[0532] 使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名，得到第二签名值；

[0533] 将所述第二数据，第一签名值和第二签名值发送到所述数据接收端。

[0534] 本公开还提供一种数据传输装置，包括：

[0535] 处理器；

[0536] 用于存储处理器可执行指令的存储器；

[0537] 其中，所述处理器被配置为：

[0538] 接收数据发送端发送的数据；

[0539] 获取所述数据接收端的私钥，所述数据发送端的唯一标识和公钥；

[0540] 从所述数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值，所述第二数据为使用所述数据接收端的公钥对所要传输的第一数据进行加密后得到的，所述第一签名值为使用所述数据发送端的私钥对所述第二数据进行签名得到的，所述第二签名值为使用所述数据发送端的唯一标识对所述第二数据和第一签名值进行签名得到的；

[0541] 根据所述数据发送端的唯一标识对所述第二签名值进行验证；

[0542] 当对所述第二签名值验证通过时，使用所述数据发送端的公钥对所述第一签名值进行验证；

[0543] 当对所述第一签名值验证通过时，使用所述数据接收端的私钥对所述第二数据进行解密，得到所述第一数据。

[0544] 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。

[0545] 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。

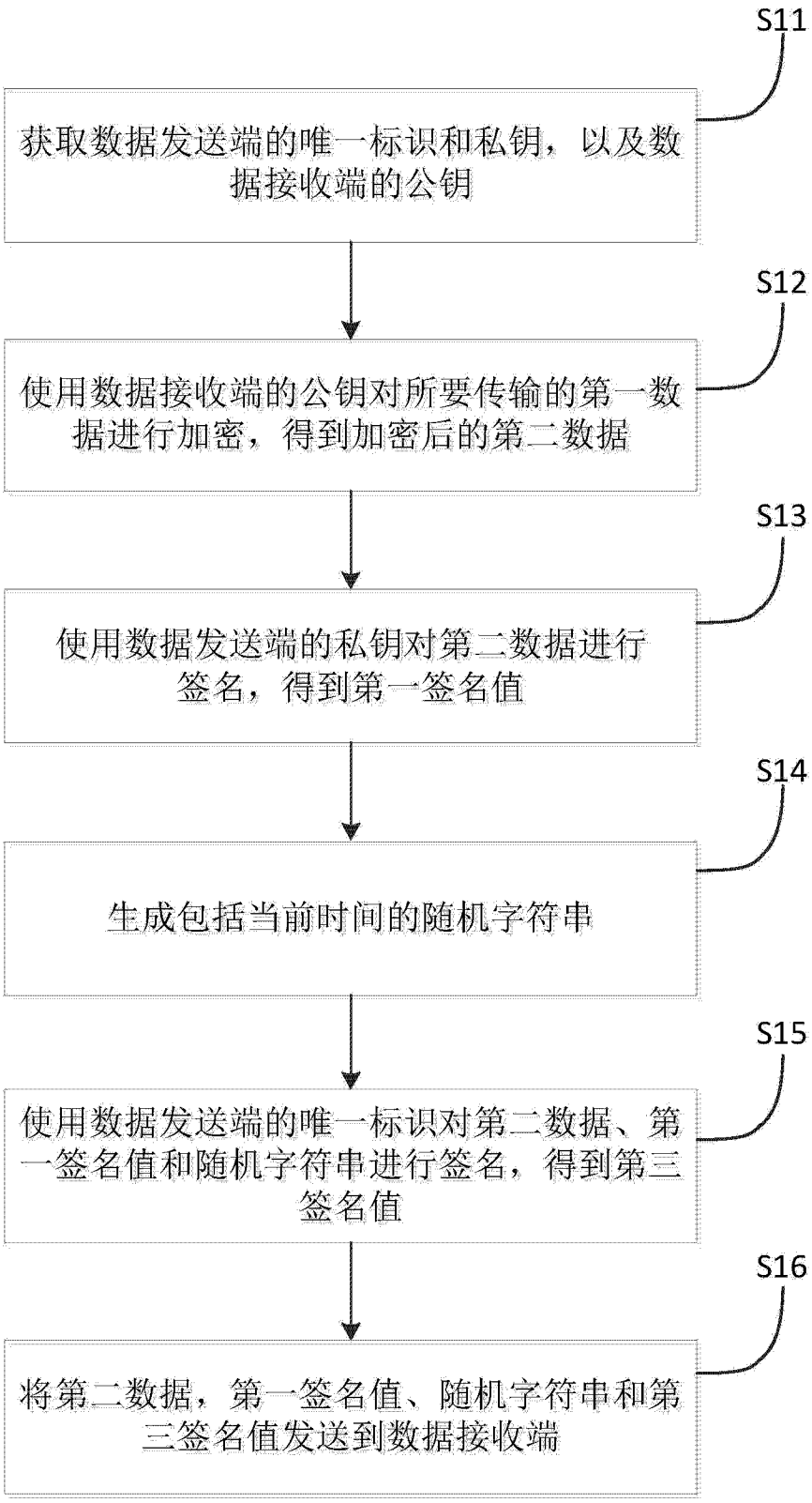

S11
获取数据发送端的唯一标识和私钥，以及数据接收端的公钥
S12
使用数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据
S13
使用数据发送端的私钥对第二数据进行签名，得到第一签名值
S14
生成包括当前时间的随机字符串
S15
使用数据发送端的唯一标识对第二数据、第一签名值和随机字符串进行签名，得到第三签名值
S16
将第二数据，第一签名值、随机字符串和第三签名值发送到数据接收端

图 1

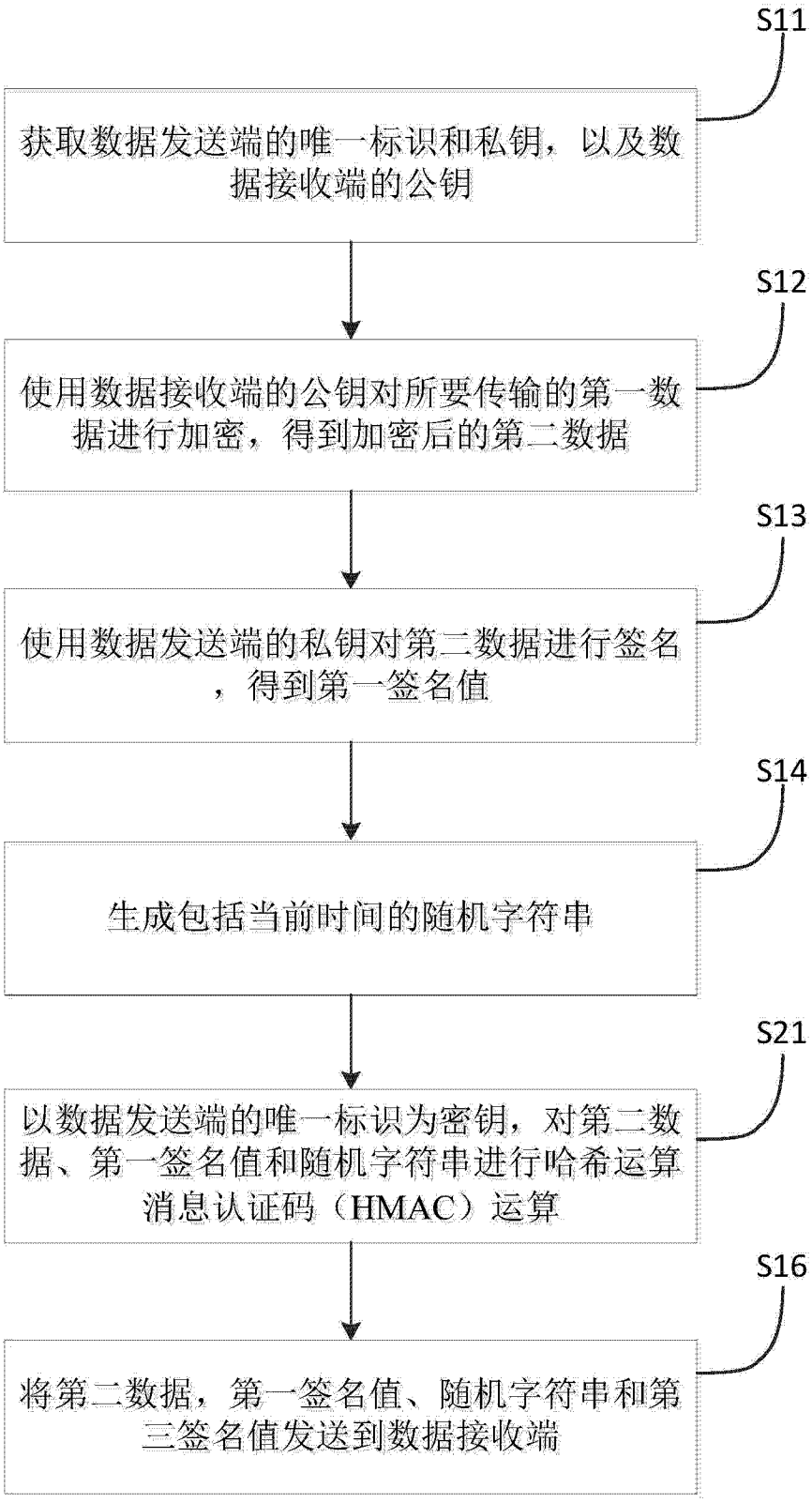

S11
获取数据发送端的唯一标识和私钥，以及数据接收端的公钥
S12
使用数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据
S13
使用数据发送端的私钥对第二数据进行签名，得到第一签名值
S14
生成包括当前时间的随机字符串
S21
以数据发送端的唯一标识为密钥，对第二数据、第一签名值和随机字符串进行哈希运算消息认证码（HMAC）运算
S16
将第二数据，第一签名值、随机字符串和第三签名值发送到数据接收端

图 2

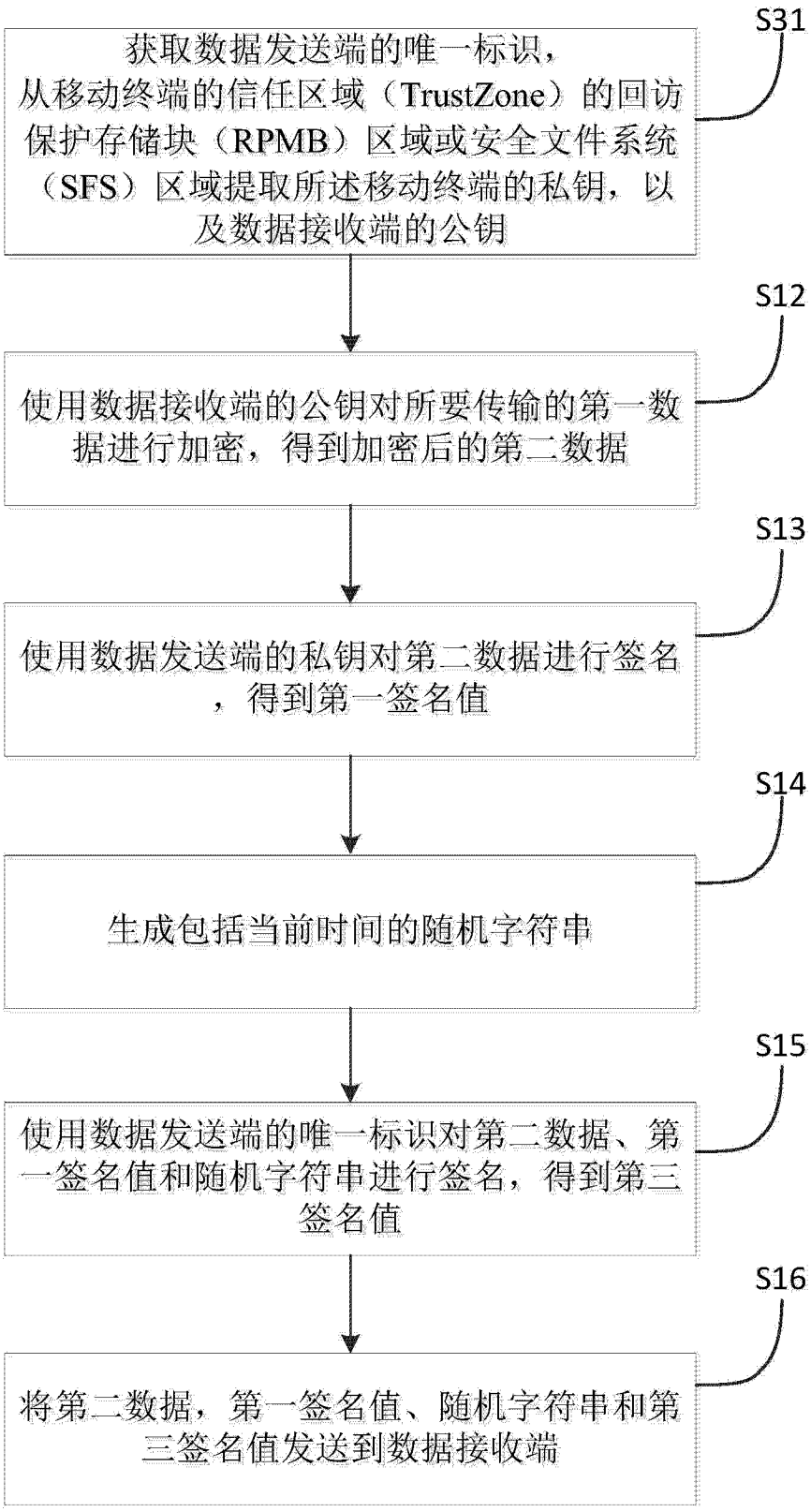

S31
获取数据发送端的唯一标识，从移动终端的信任区域（TrustZone）的回访保护存储块（RPMB）区域或安全文件系统（SFS）区域提取所述移动终端的私钥，以及数据接收端的公钥
S12
使用数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据
S13
使用数据发送端的私钥对第二数据进行签名，得到第一签名值
S14
生成包括当前时间的随机字符串
S15
使用数据发送端的唯一标识对第二数据、第一签名值和随机字符串进行签名，得到第三签名值
S16
将第二数据，第一签名值、随机字符串和第三签名值发送到数据接收端

图 3

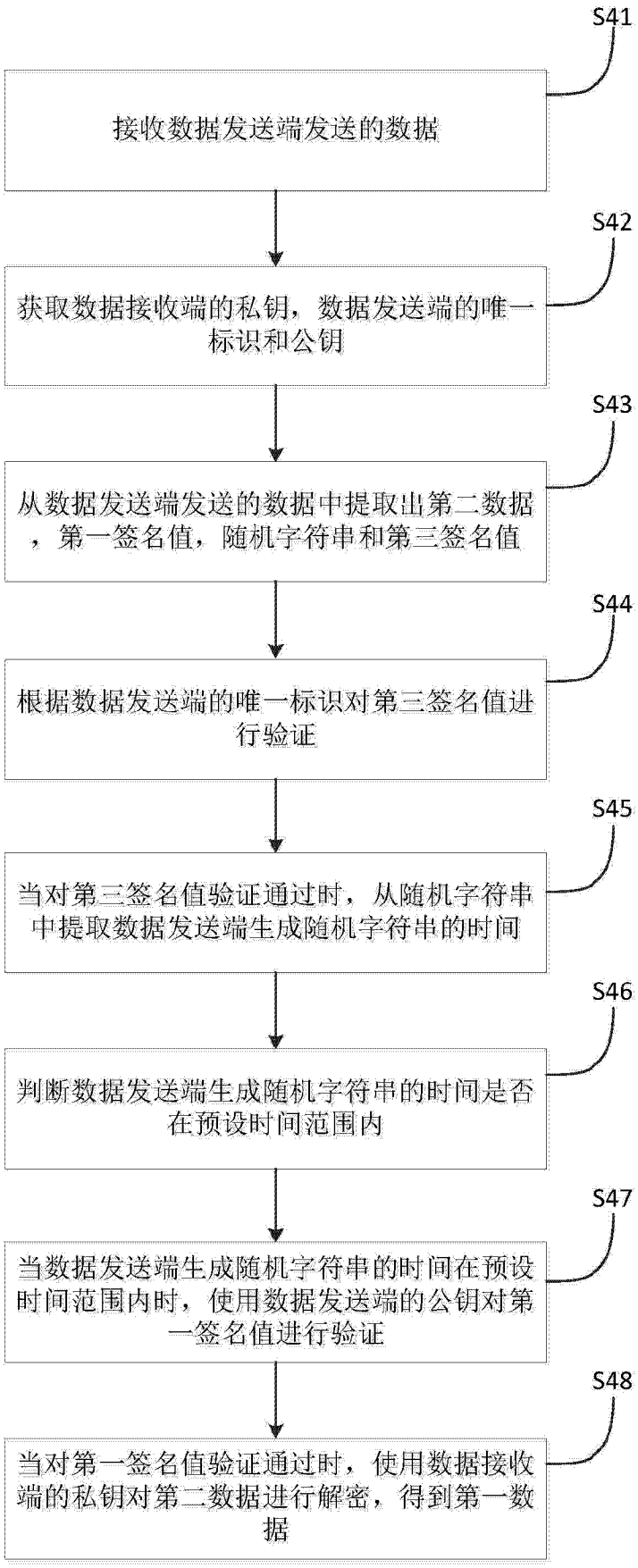

S41
接收数据发送端发送的数据
S42
获取数据接收端的私钥，数据发送端的唯一标识和公钥
S43
从数据发送端发送的数据中提取出第二数据，第一签名值，随机字符串和第三签名值
S44
根据数据发送端的唯一标识对第三签名值进行验证
S45
当对第三签名值验证通过时，从随机字符串中提取数据发送端生成随机字符串的时间
S46
判断数据发送端生成随机字符串的时间是否在预设时间范围内
S47
当数据发送端生成随机字符串的时间在预设时间范围内时，使用数据发送端的公钥对第一签名值进行验证
S48
当对第一签名值验证通过时，使用数据接收端的私钥对第二数据进行解密，得到第一数据

图 4

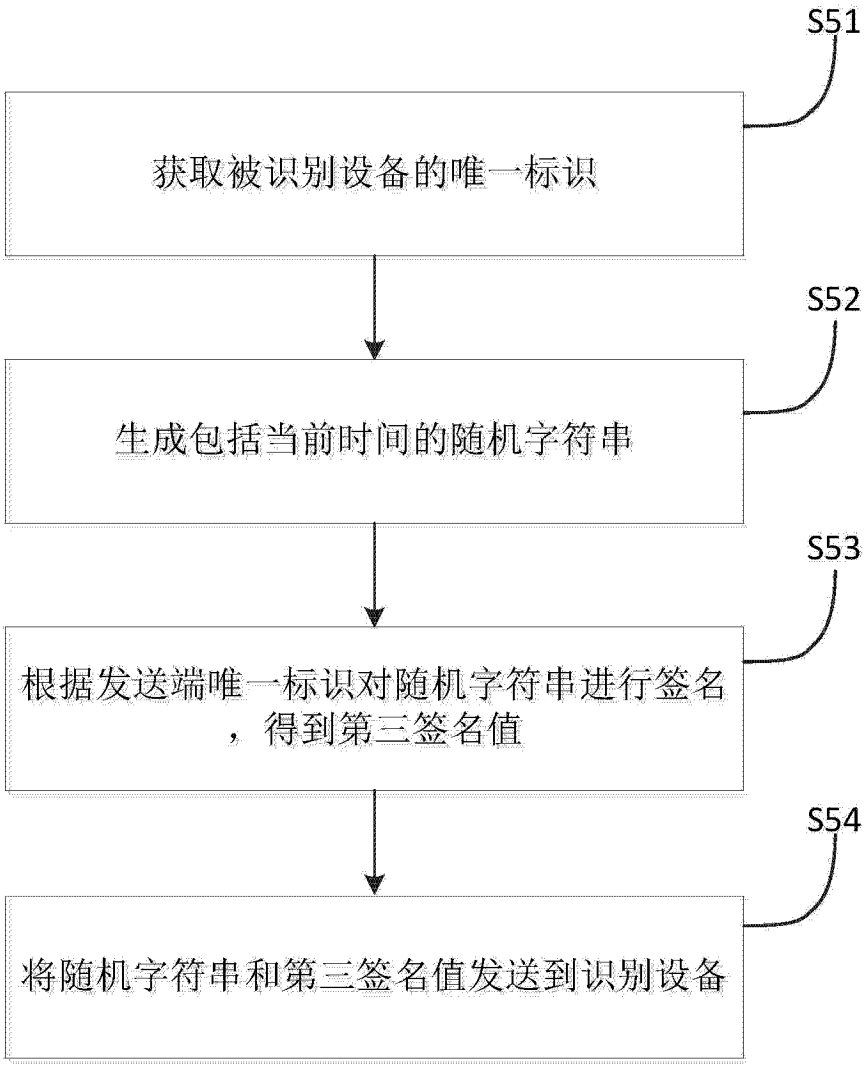

S51
获取被识别设备的唯一标识
S52
生成包括当前时间的随机字符串
S53
根据发送端唯一标识对随机字符串进行签名，得到第三签名值
S54
将随机字符串和第三签名值发送到识别设备

图 5

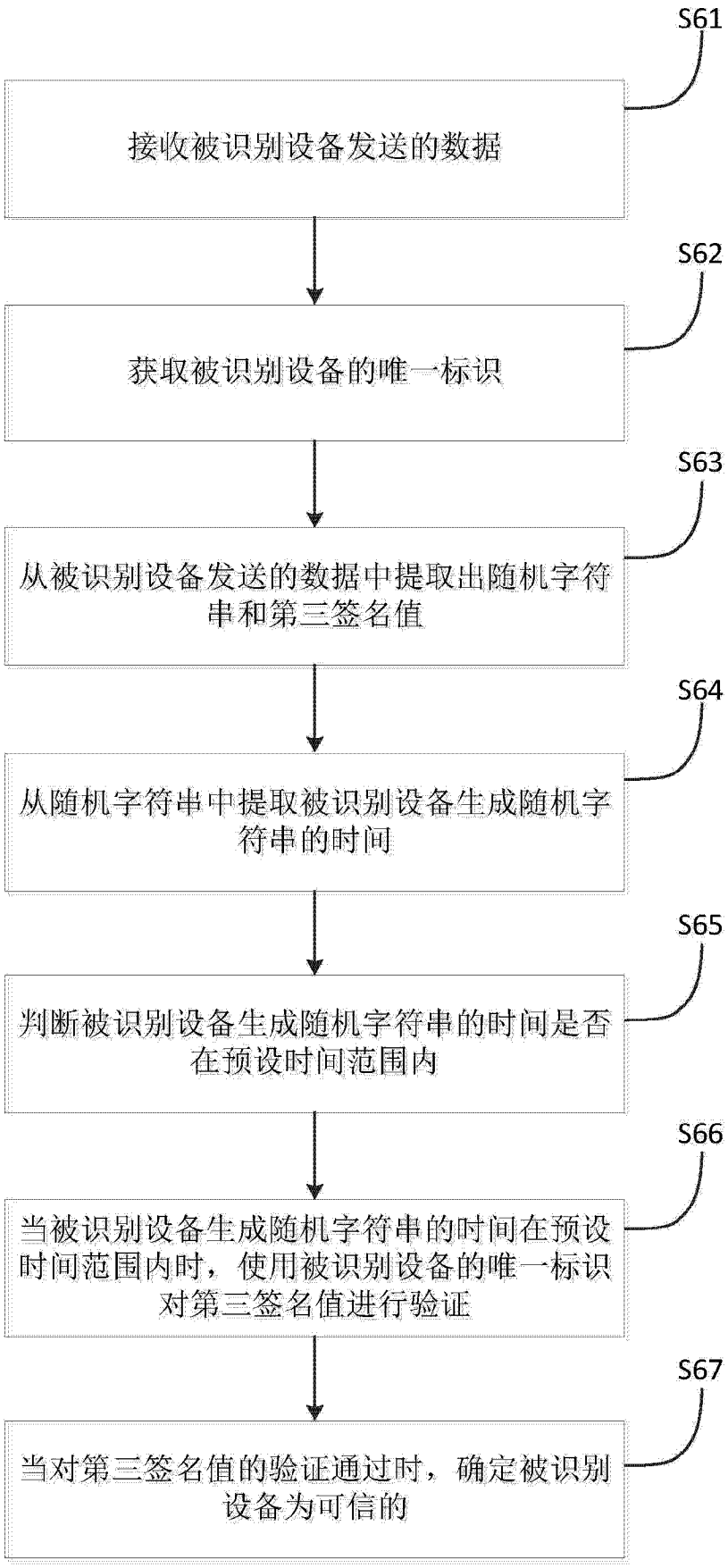

S61
接收被识别设备发送的数据
S62
获取被识别设备的唯一标识
S63
从被识别设备发送的数据中提取出随机字符串和第三签名值
S64
从随机字符串中提取被识别设备生成随机字符串的时间
S65
判断被识别设备生成随机字符串的时间是否在预设时间范围内
S66
当被识别设备生成随机字符串的时间在预设时间范围内时，使用被识别设备的唯一标识对第三签名值进行验证
S67
当对第三签名值的验证通过时，确定被识别设备为可信的

图 6

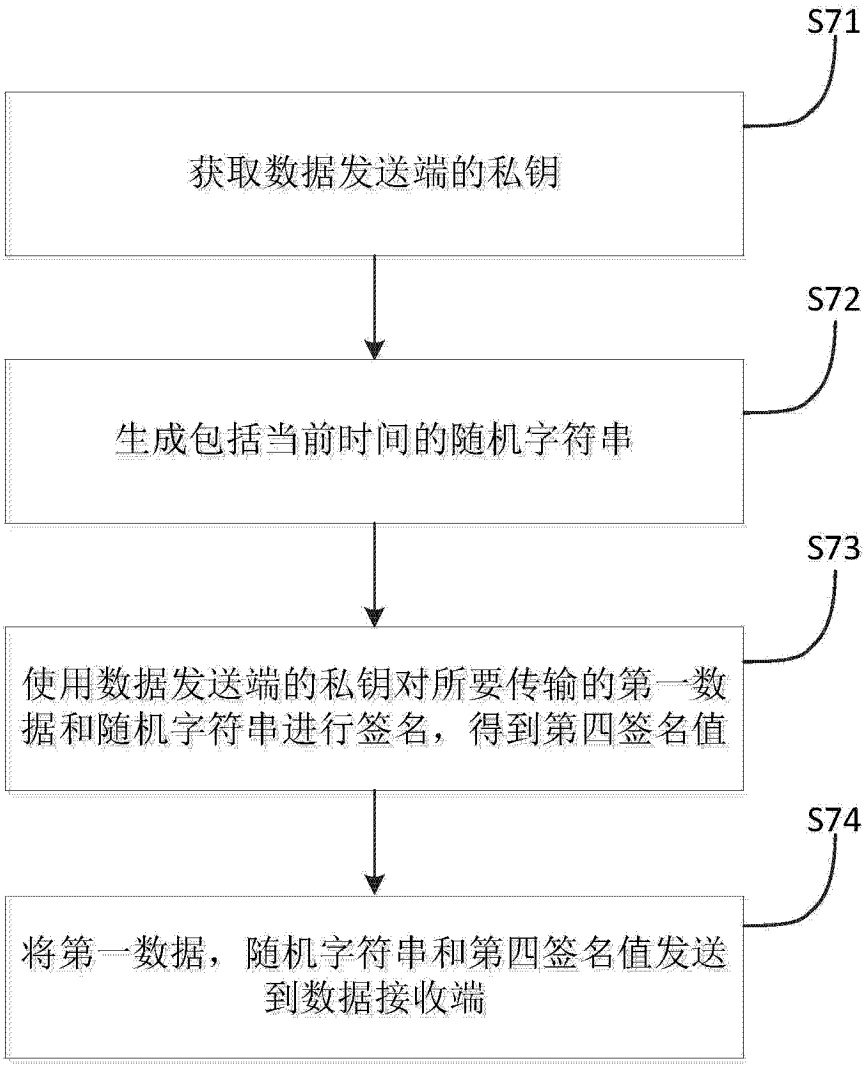

S71
获取数据发送端的私钥
S72
生成包括当前时间的随机字符串
S73
使用数据发送端的私钥对所要传输的第一数据和随机字符串进行签名，得到第四签名值
S74
将第一数据，随机字符串和第四签名值发送到数据接收端

图 7

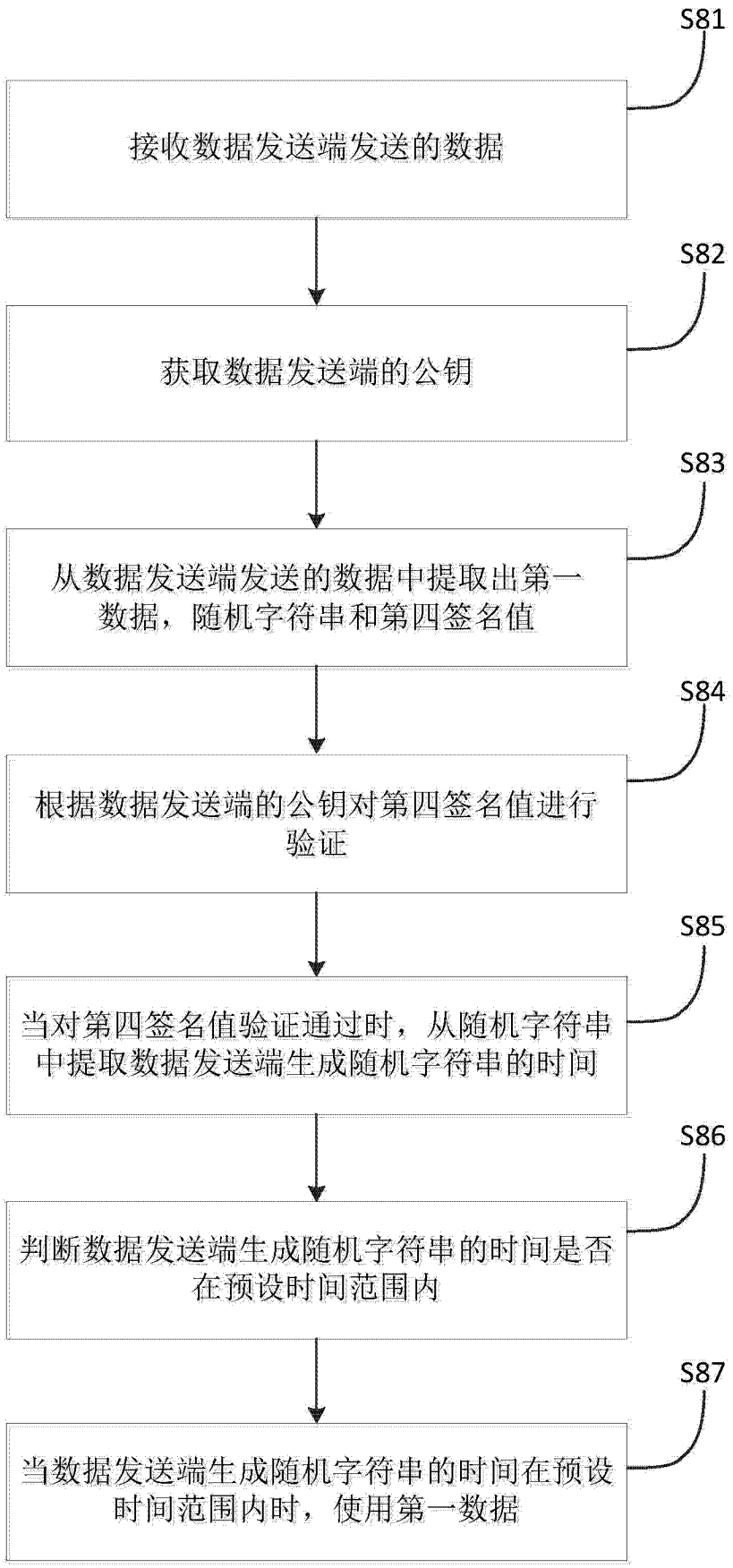

S81
接收数据发送端发送的数据
S82
获取数据发送端的公钥
S83
从数据发送端发送的数据中提取出第一数据，随机字符串和第四签名值
S84
根据数据发送端的公钥对第四签名值进行验证
S85
当对第四签名值验证通过时，从随机字符串中提取数据发送端生成随机字符串的时间
S86
判断数据发送端生成随机字符串的时间是否在预设时间范围内
S87
当数据发送端生成随机字符串的时间在预设时间范围内时，使用第一数据

图 8

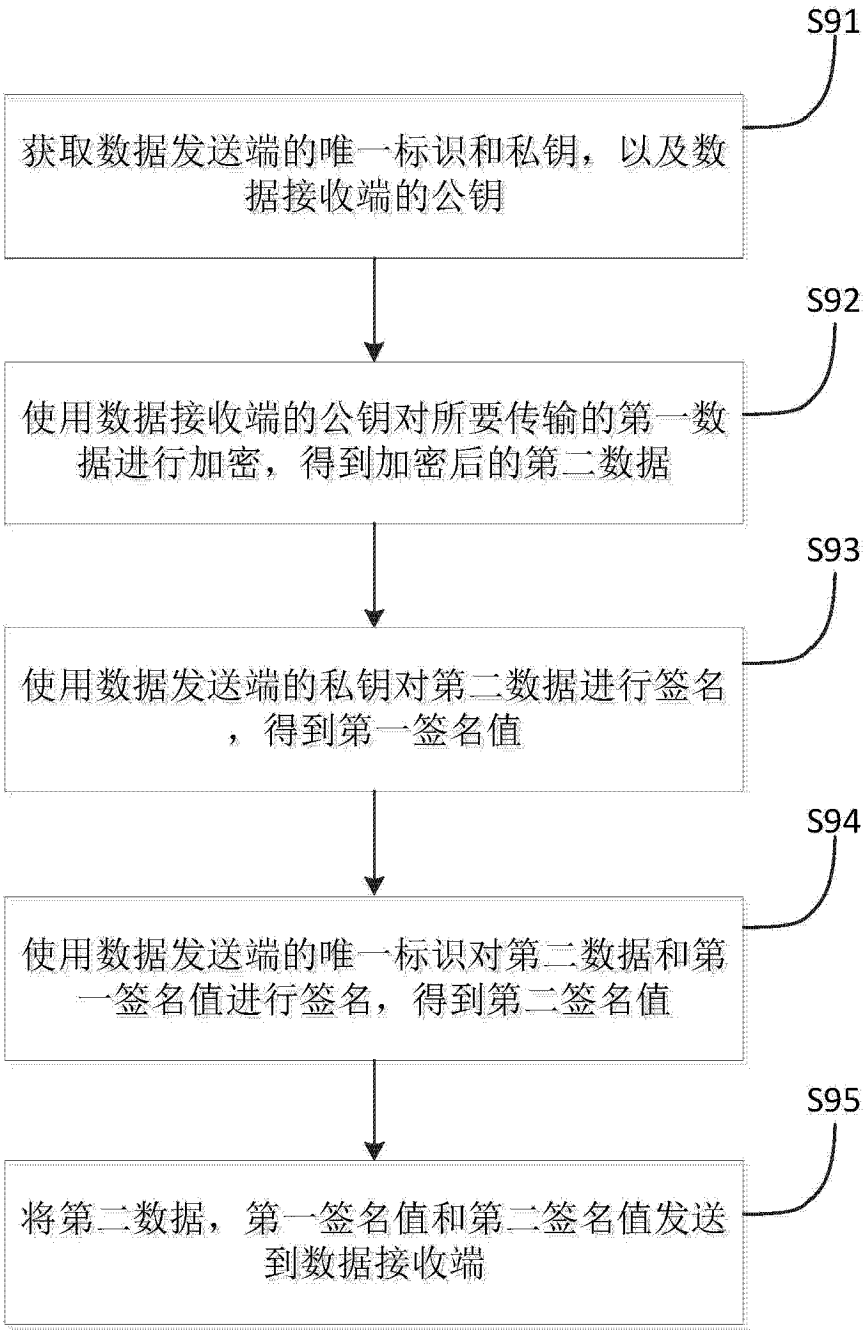

S91
获取数据发送端的唯一标识和私钥，以及数据接收端的公钥
S92
使用数据接收端的公钥对所要传输的第一数据进行加密，得到加密后的第二数据
S93
使用数据发送端的私钥对第二数据进行签名，得到第一签名值
S94
使用数据发送端的唯一标识对第二数据和第一签名值进行签名，得到第二签名值
S95
将第二数据，第一签名值和第二签名值发送到数据接收端

图 9

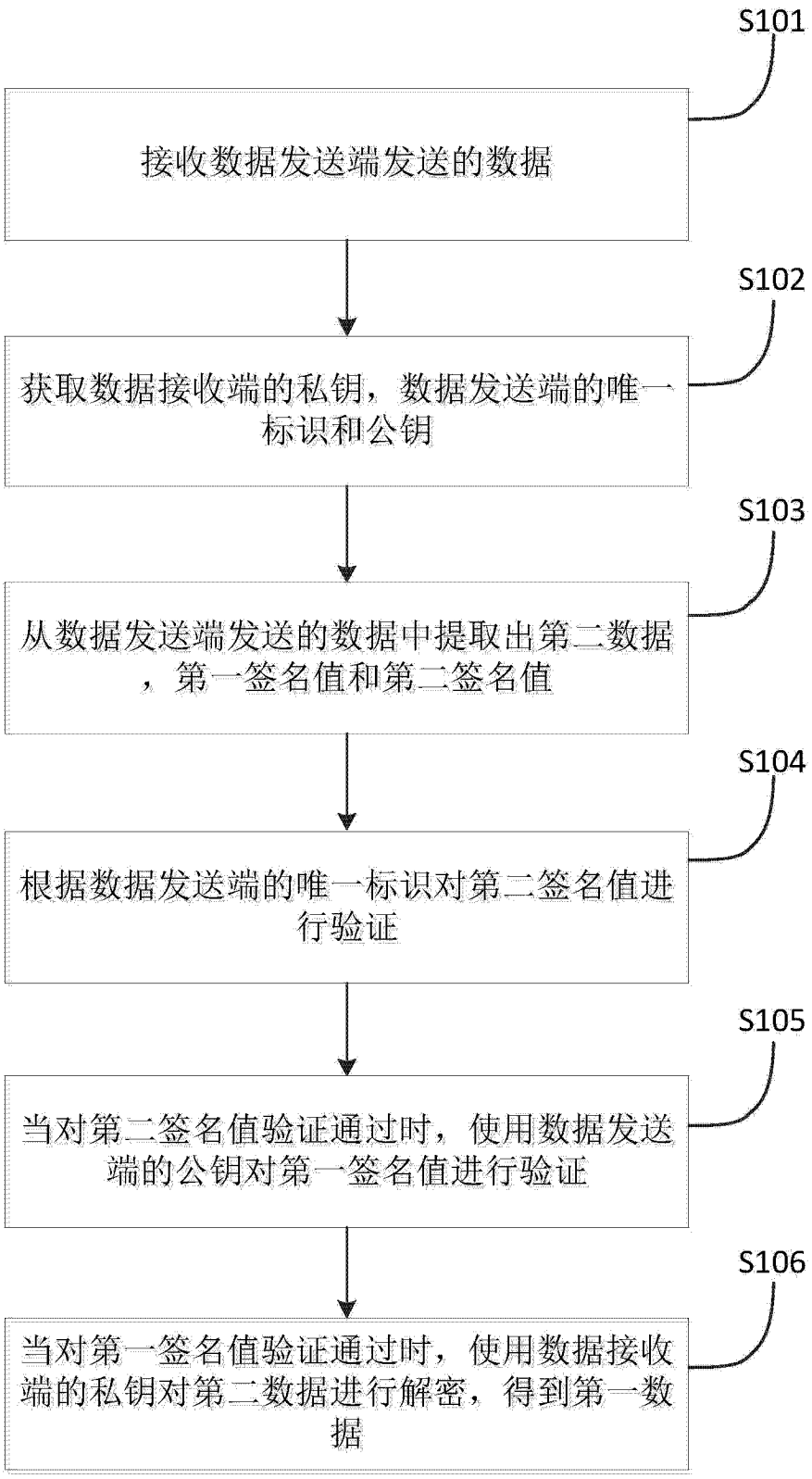

S101
接收数据发送端发送的数据
S102
获取数据接收端的私钥，数据发送端的唯一标识和公钥
S103
从数据发送端发送的数据中提取出第二数据，第一签名值和第二签名值
S104
根据数据发送端的唯一标识对第二签名值进行验证
S105
当对第二签名值验证通过时，使用数据发送端的公钥对第一签名值进行验证
S106
当对第一签名值验证通过时，使用数据接收端的私钥对第二数据进行解密，得到第一数据

图 10

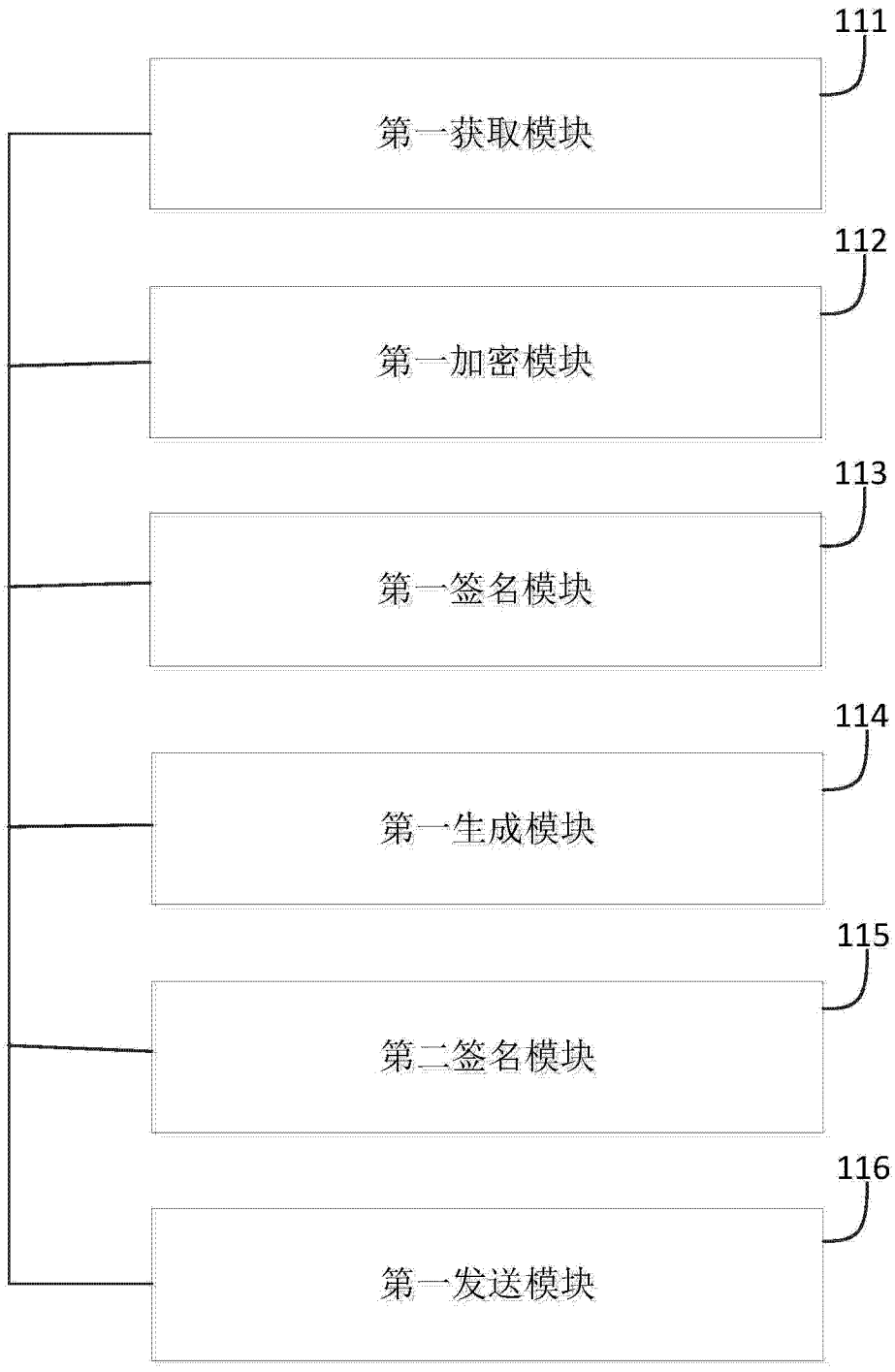

111
第一获取模块
112
第一加密模块
113
第一签名模块
114
第一生成模块
115
第二签名模块
116
第一发送模块

图 11

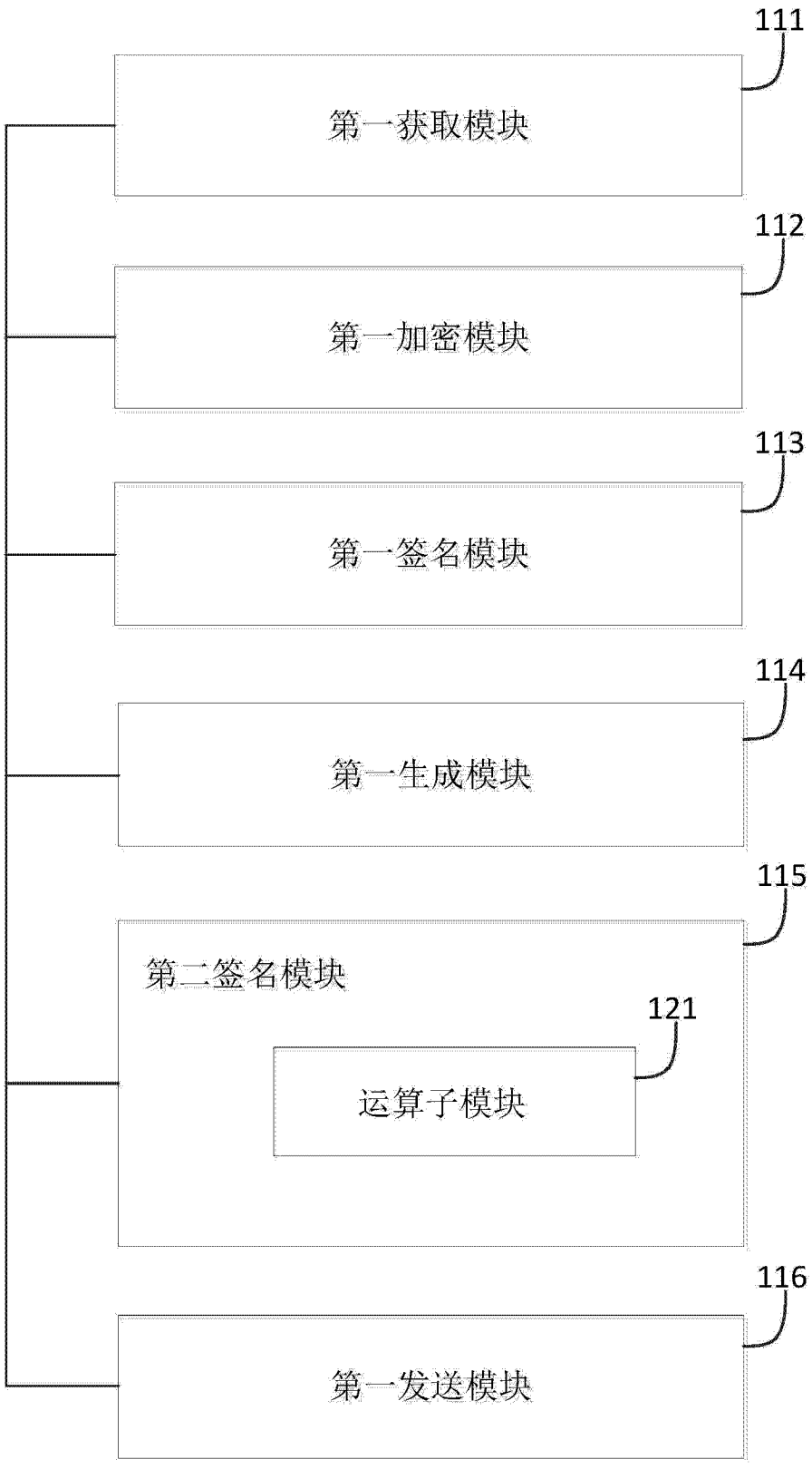

111
第一获取模块
112
第一加密模块
113
第一签名模块
114
第一生成模块
115
第二签名模块
121
运算子模块
116
第一发送模块

图 12

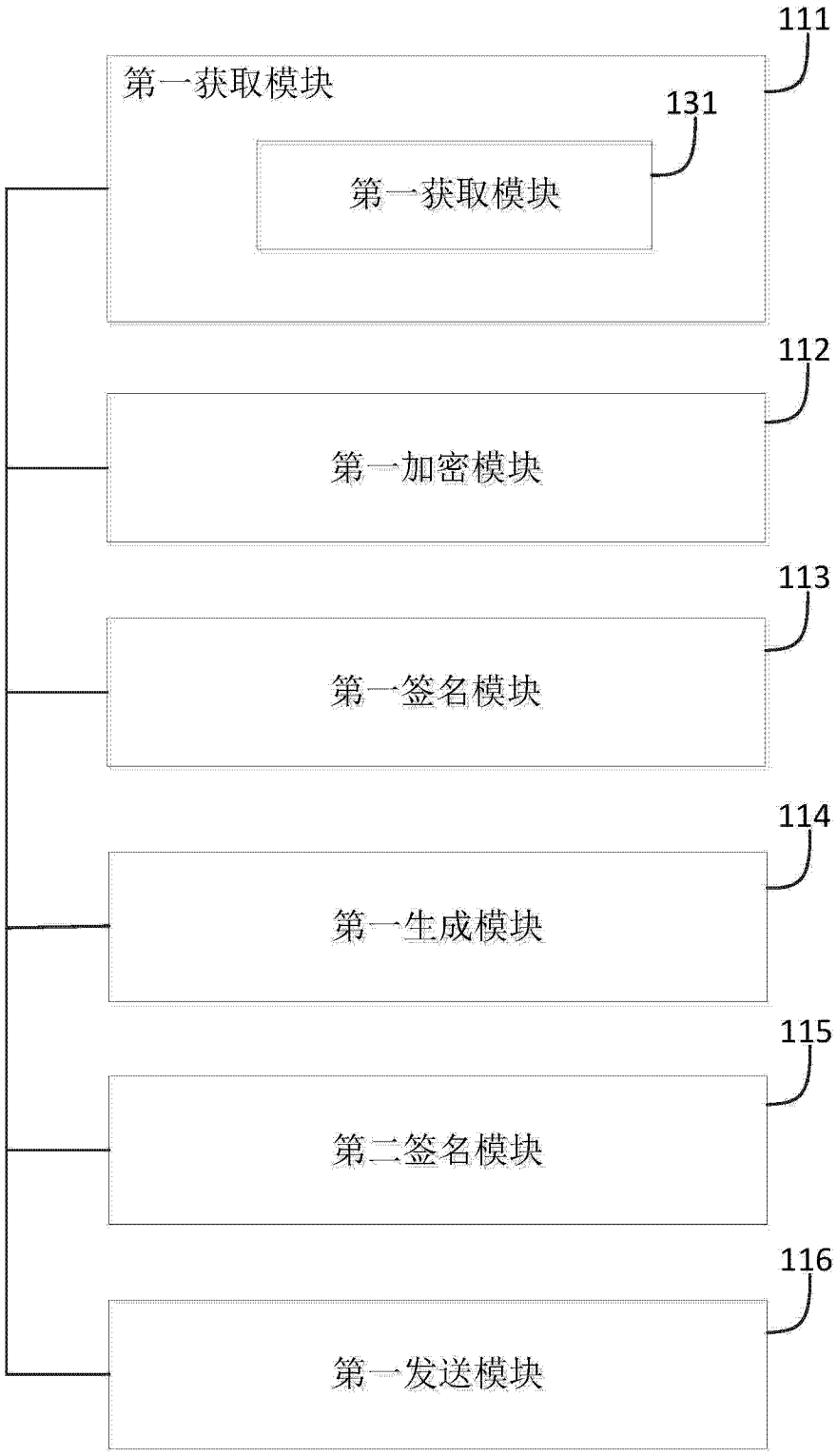

111
第一获取模块
131
第一获取模块
112
第一加密模块
113
第一签名模块
114
第一生成模块
115
第二签名模块
116
第一发送模块

图 13

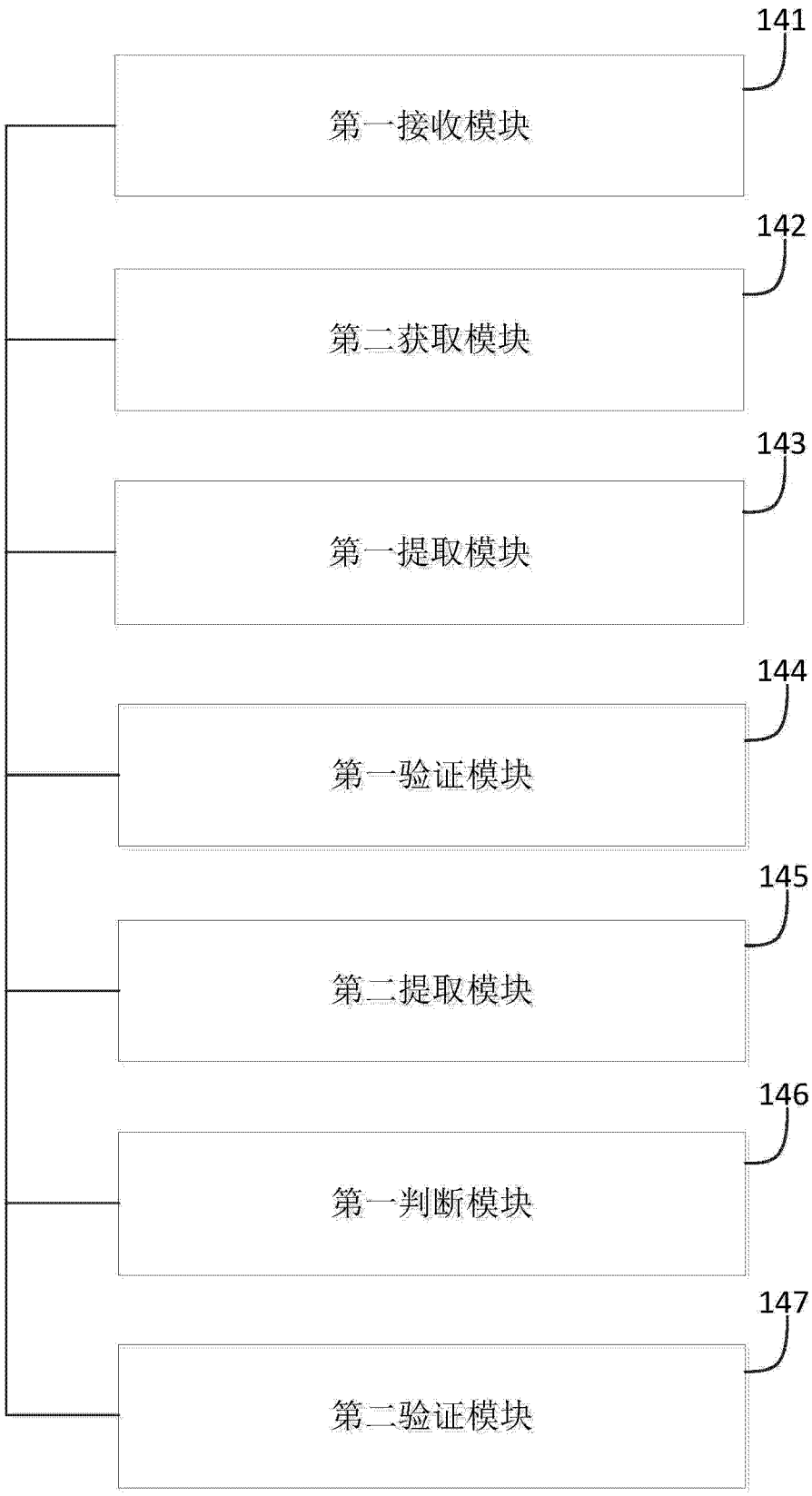

141
第一接收模块
142
第二获取模块
143
第一提取模块
144
第一验证模块
145
第二提取模块
146
第一判断模块
147
第二验证模块

图 14

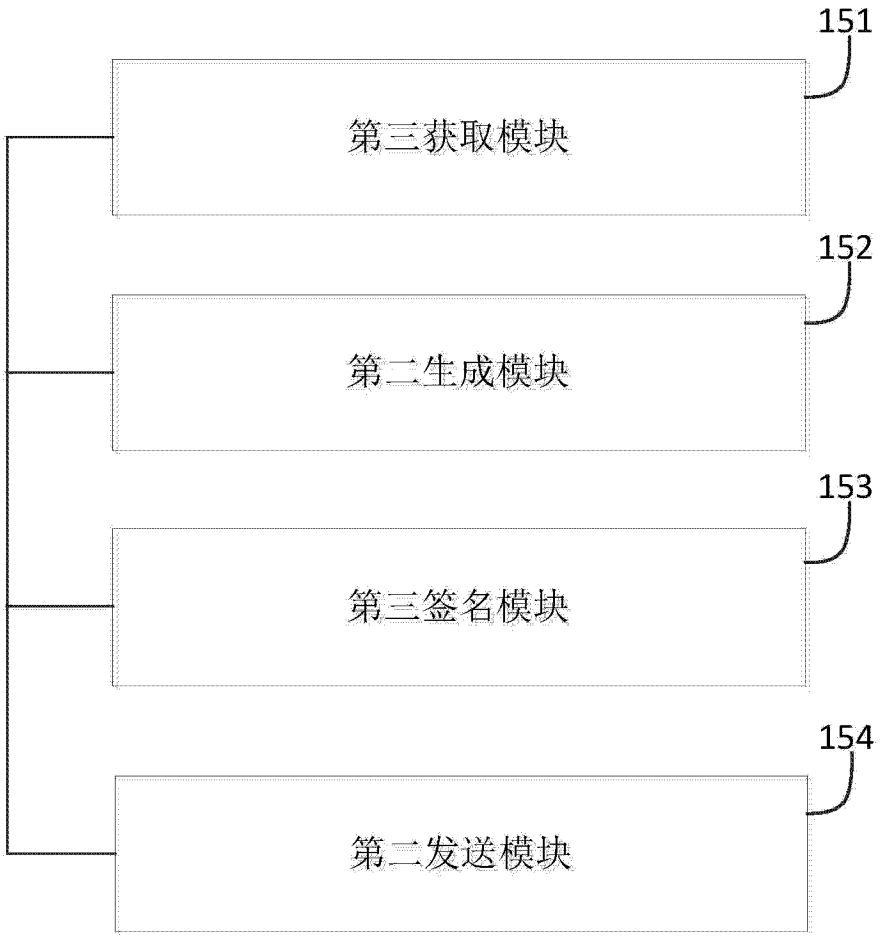


图 15

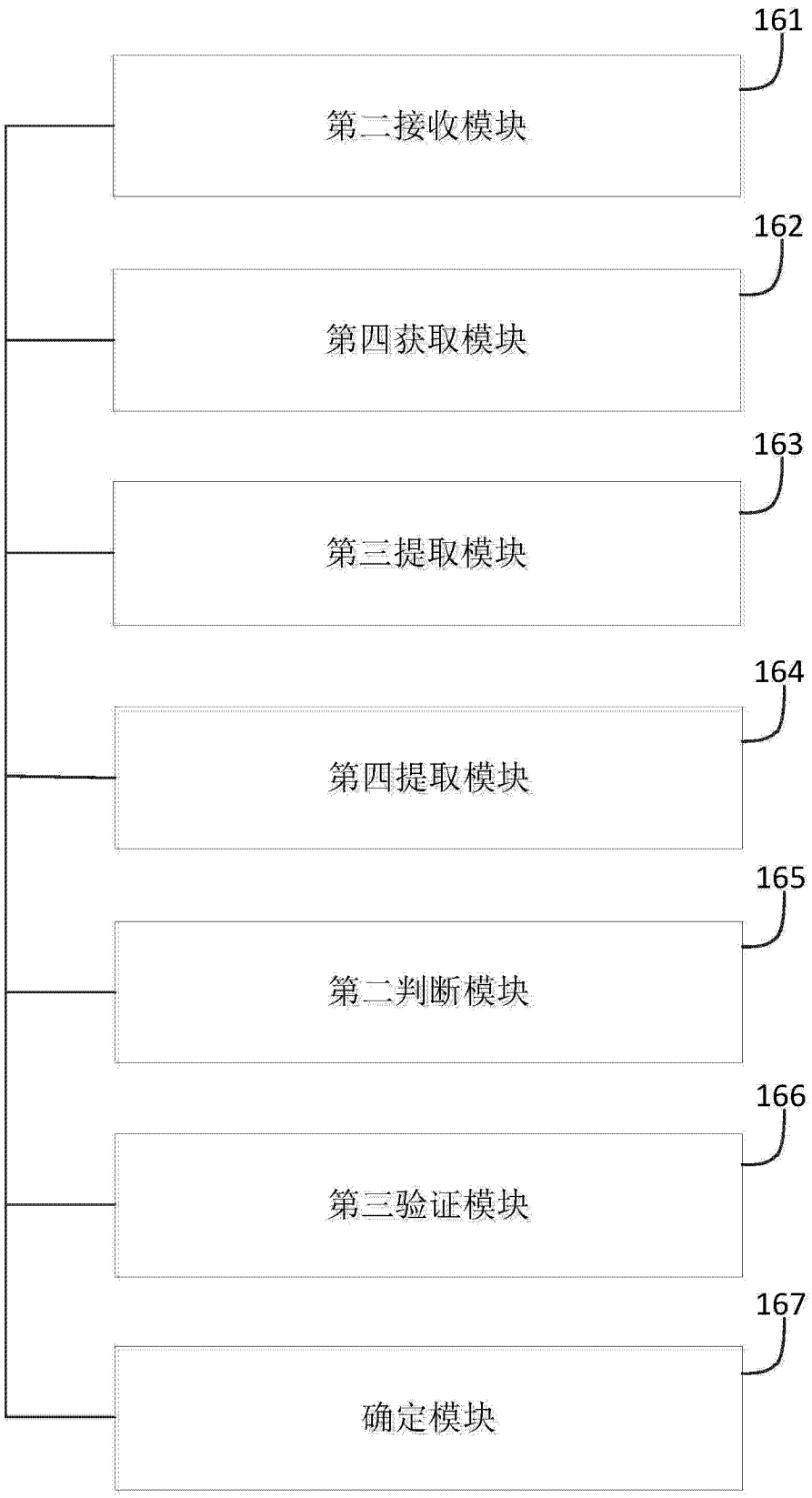

161
第二接收模块
162
第四获取模块
163
第三提取模块
164
第四提取模块
165
第二判断模块
166
第三验证模块
167
确定模块

图 16

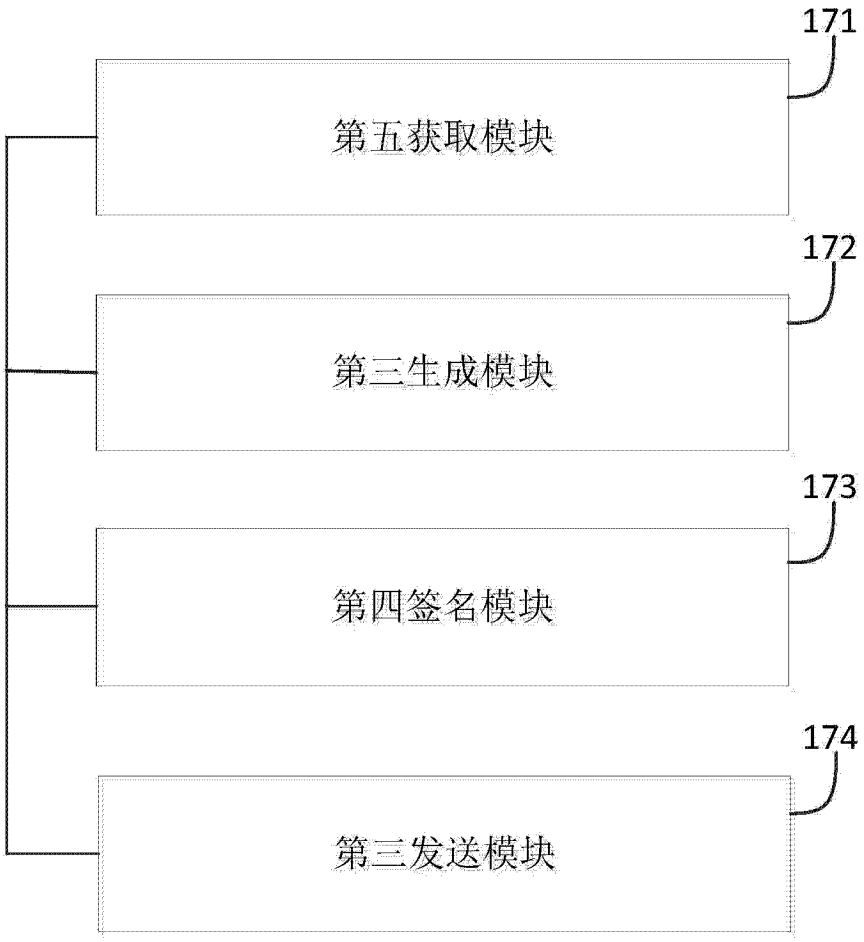


图 17

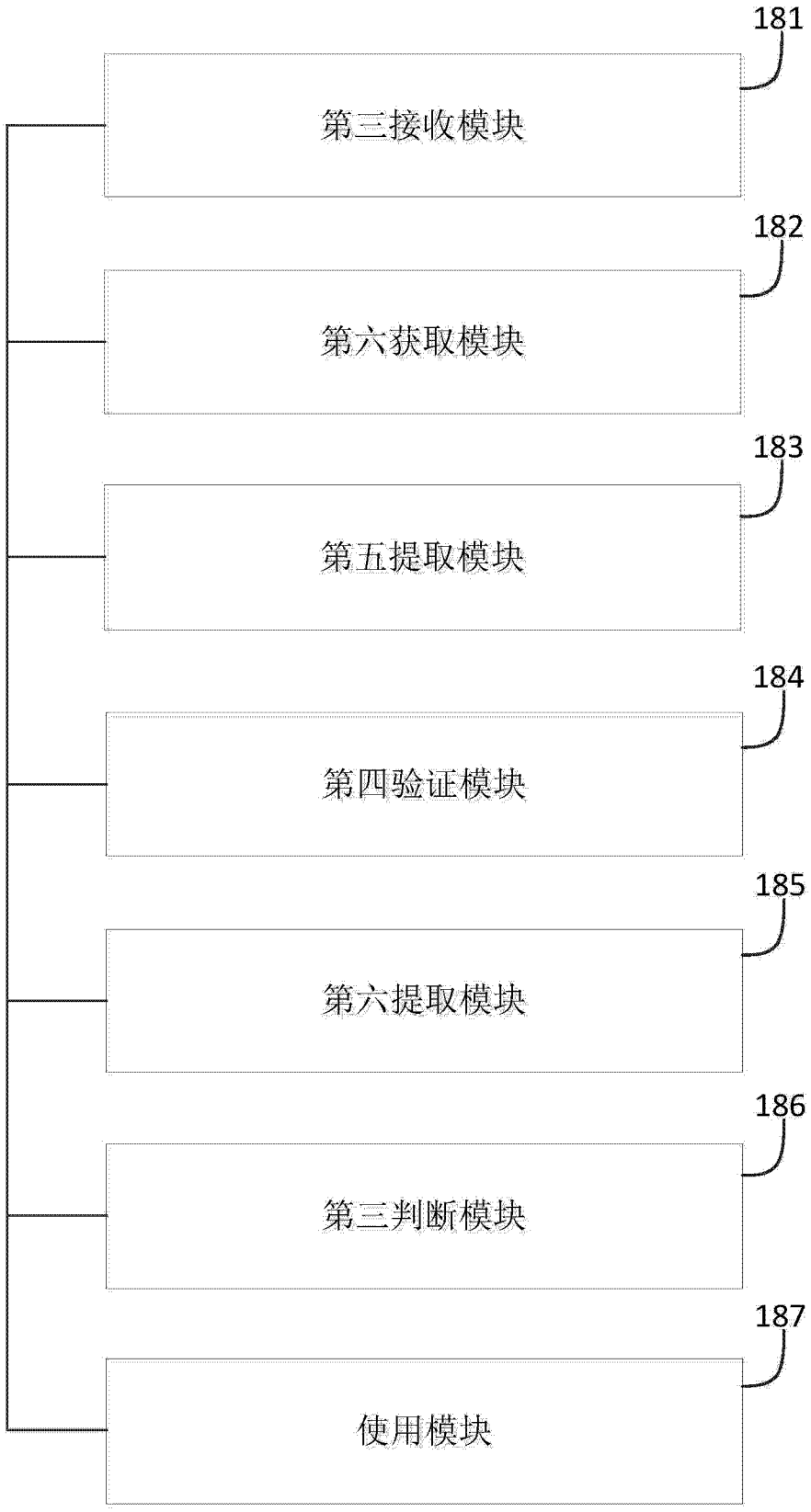

181
第三接收模块
182
第六获取模块
183
第五提取模块
184
第四验证模块
185
第六提取模块
186
第三判断模块
187
使用模块

图 18

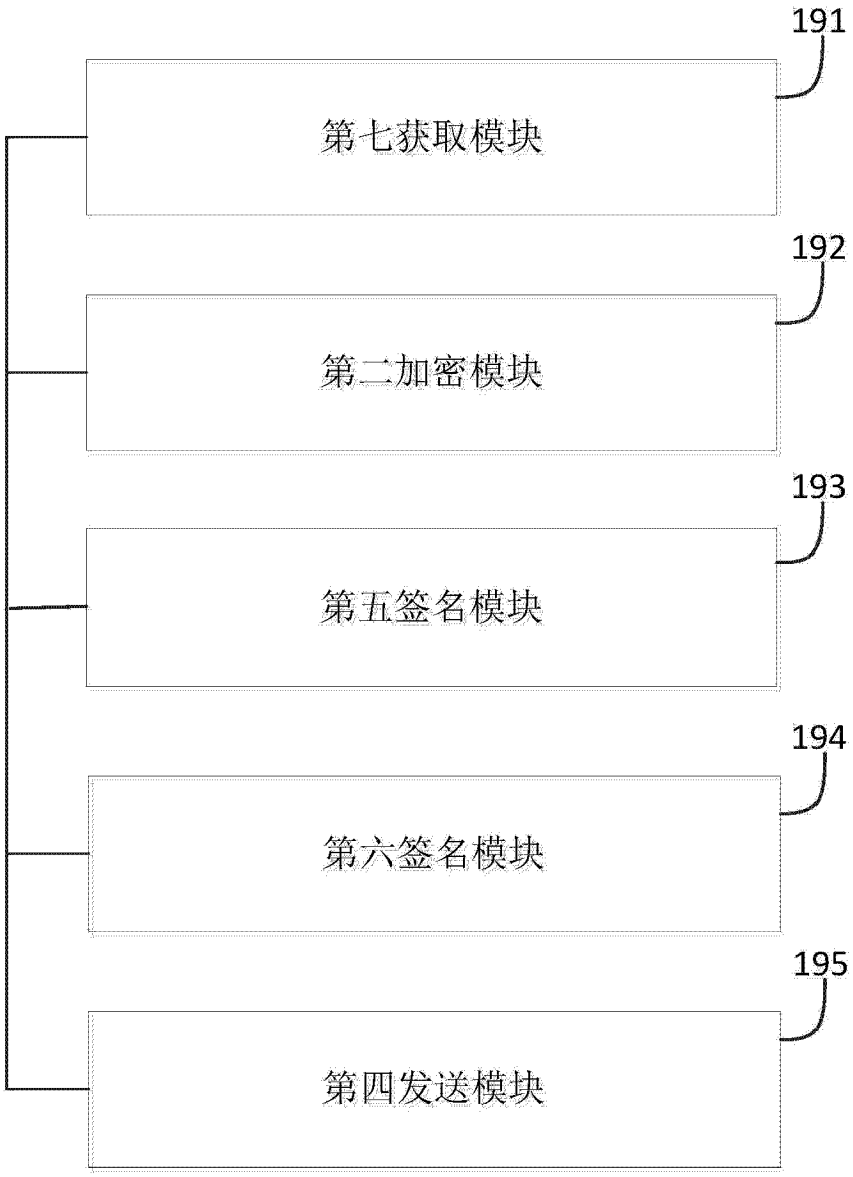


图 19

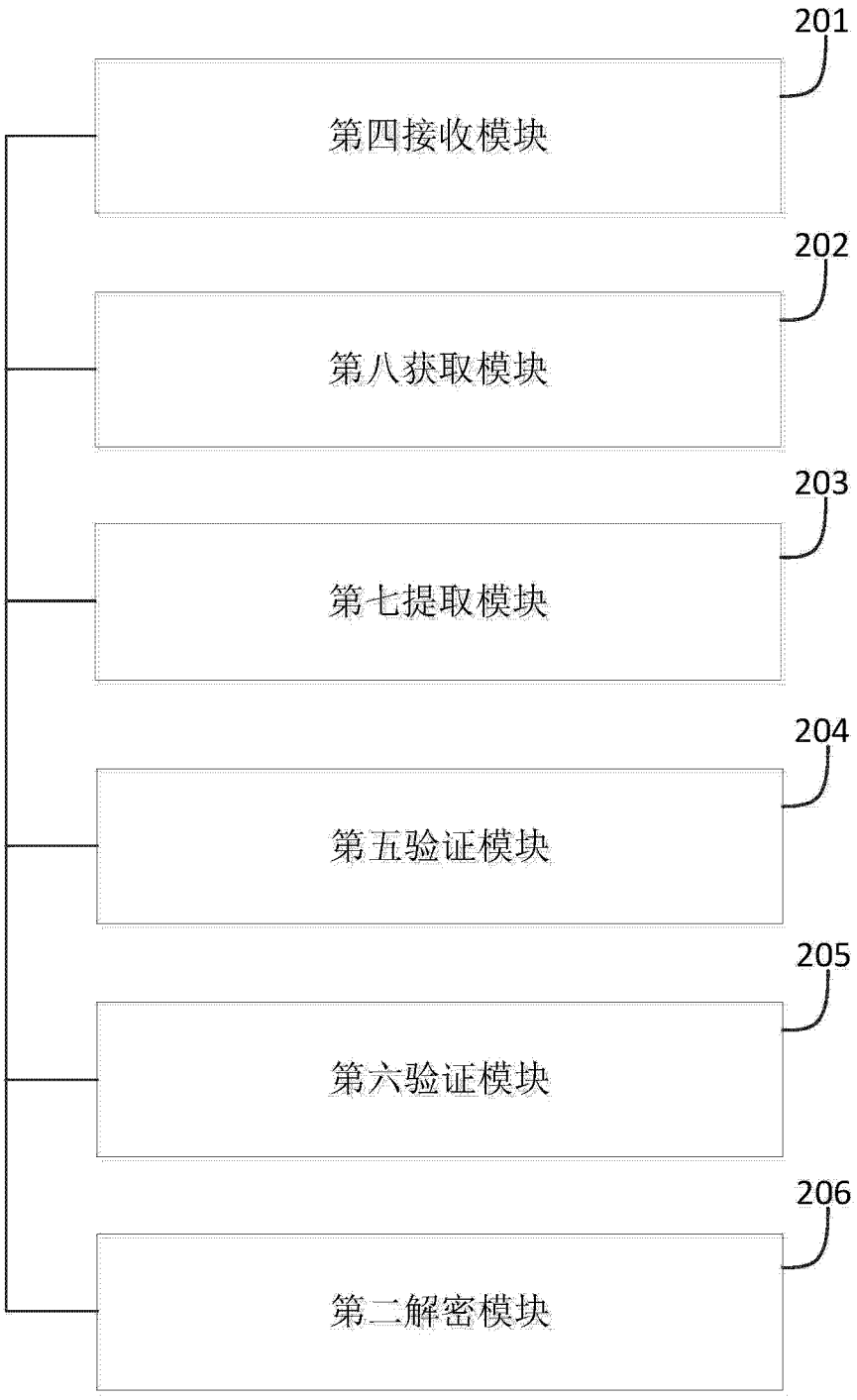

201
第四接收模块
202
第八获取模块
203
第七提取模块
204
第五验证模块
205
第六验证模块
206
第二解密模块

图 20

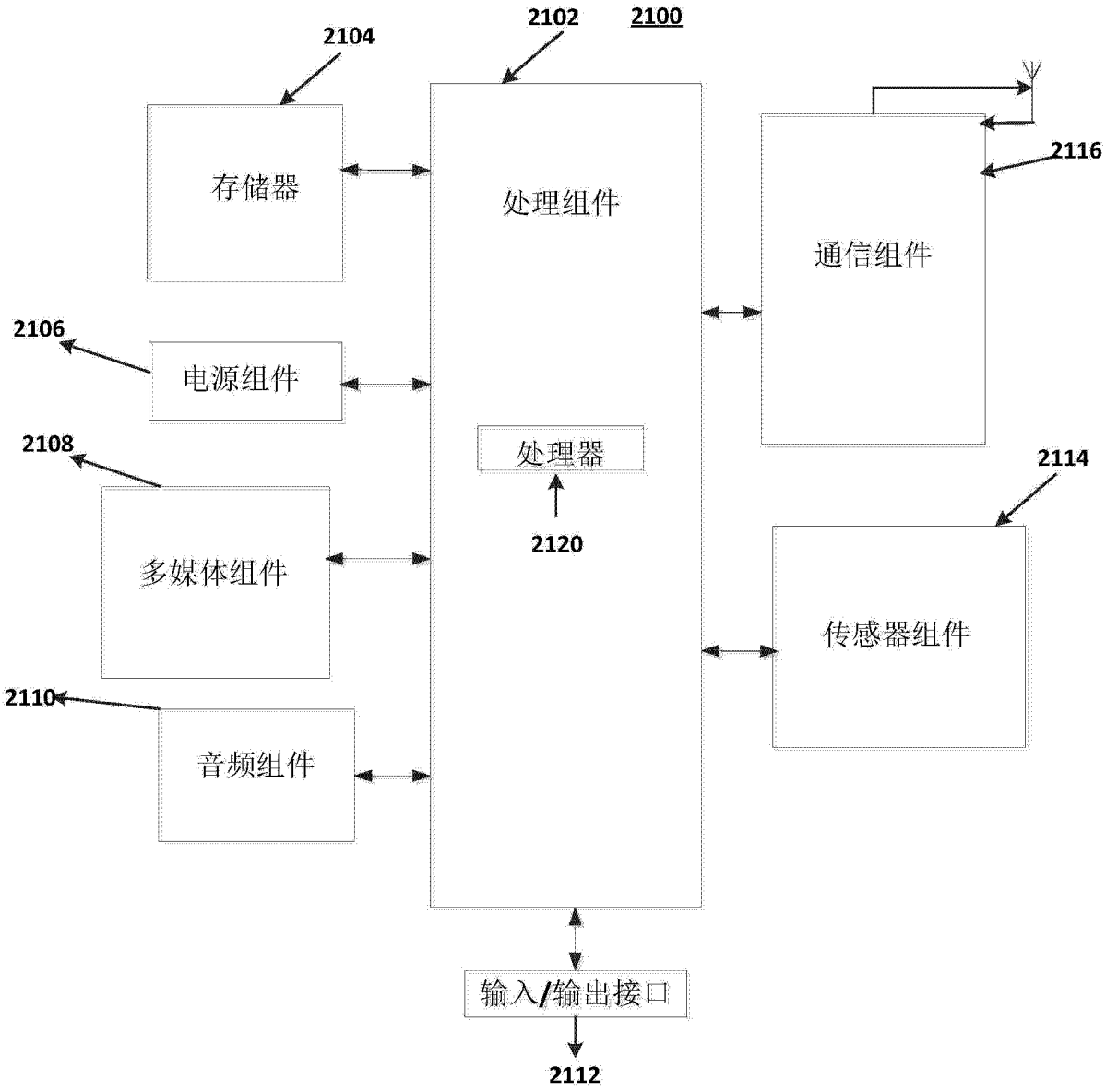

2102
2100
2104
存储器
处理组件
2116
通信组件
2106
电源组件
处理器
2120
2108
多媒体组件
2114
传感器组件
2110
音频组件
输入/输出接口
2112

图 21

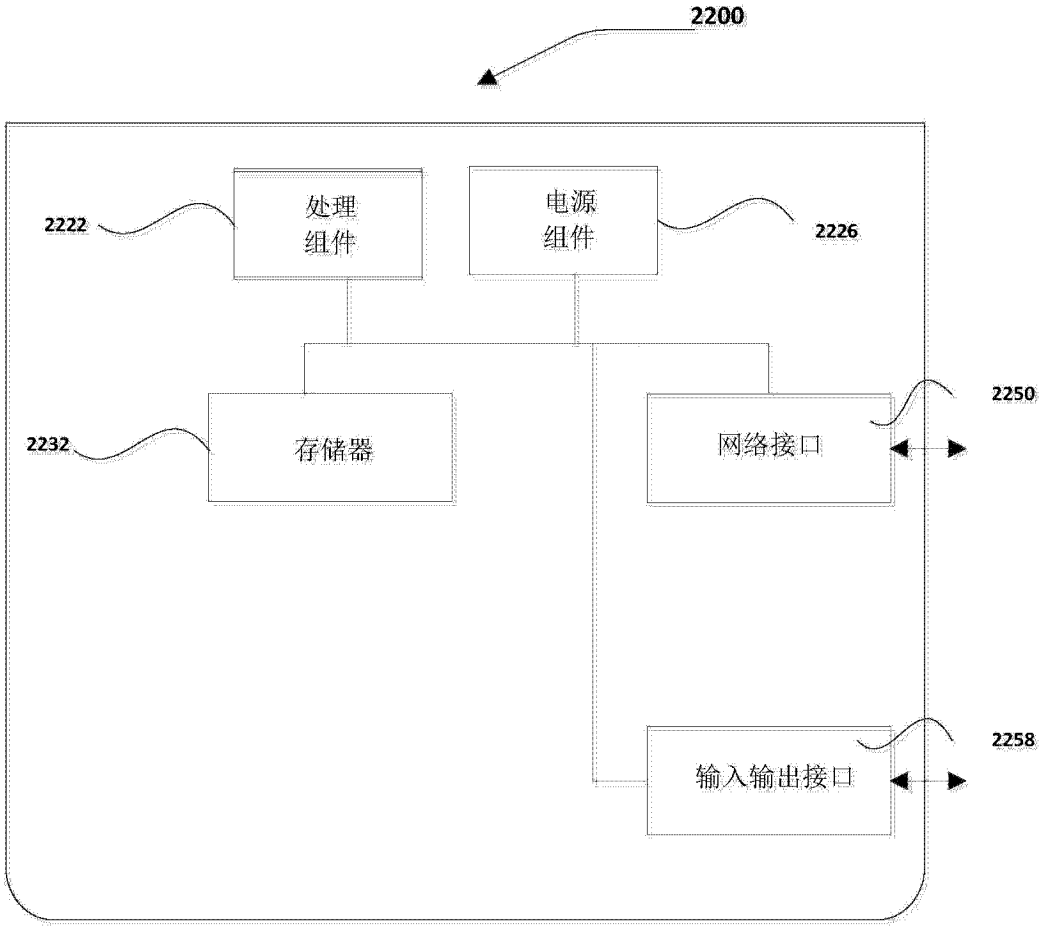


图 22