(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 106559217 B
(45)授权公告日 2019.09.20

(21)申请号 201510631689.2

(22)申请日 2015.09.29

(65)同一申请的已公布的文献号
申请公布号 CN 106559217 A

(43)申请公布日 2017.04.05

(73)专利权人 腾讯科技(深圳)有限公司
地址 518044 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 郭懿心 于航 汪春 杜现华

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 蒋雅洁 任媛

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/18(2006.01)
H04L 29/06(2006.01)

(56)对比文件
US 2013031369 A1,2013.01.31,
US 2010211787 A1,2010.08.19,
CN 103220280 A,2013.07.24,
CN 103986583 A,2014.08.13,
US 2013031369 A1,2013.01.31,

审查员 黄苏一

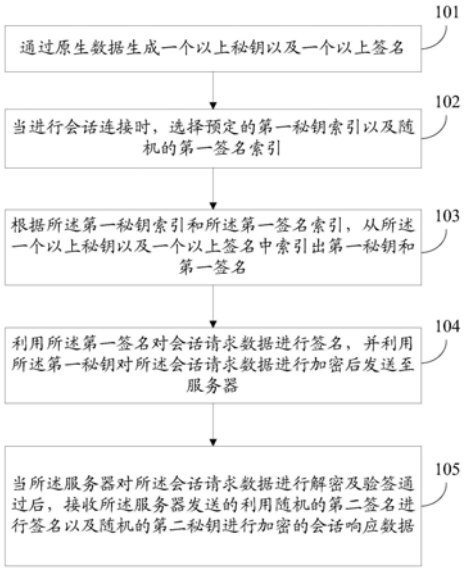
权利要求书4页 说明书12页 附图6页

(54)发明名称

一种动态加密方法、终端、服务器

(57)摘要

本发明公开了一种动态加密签名方法、终端、服务器，包括：通过原生数据生成一个以上密钥以及一个以上签名；当进行会话连接时，选择预定的第一密钥索引以及随机的第一签名索引；根据所述第一密钥索引和所述第一签名索引，从所述一个以上密钥以及一个以上签名中索引出第一密钥和第一签名；利用所述第一签名对会话请求数据进行签名，并利用所述第一密钥对所述会话请求数据进行加密后发送至服务器；当所述服务器对所述会话请求数据进行解密及验签通过后，接收所述服务器发送的利用随机的第二签名进行签名以及随机的第二密钥进行加密的会话响应数据。



CN 106559217 B

1.一种动态加密签名方法,其特征在于,所述方法包括:

通过原生数据生成一个以上密钥以及一个以上签名;所述原生数据以动态原生库的方式提供相关接口;

当进行会话连接时,选择预定的第一密钥索引以及随机的第一签名索引;

根据所述第一密钥索引和所述第一签名索引,从所述一个以上密钥以及一个以上签名中索引出第一密钥和第一签名;

利用所述第一签名对会话请求数据进行签名,并利用所述第一密钥对所述会话请求数据进行加密后发送至服务器;

当所述服务器对所述会话请求数据进行解密及验签通过后,接收所述服务器发送的利用随机的第二签名进行签名以及随机的第二密钥进行加密的会话响应数据;

选择的随机的第一签名索引,包括:

获取当前时间戳,对所述当前时间戳进行第一变换处理,得到所述第一签名索引;或者,

获取随机数,对所述随机数进行第二变换处理,得到所述第一签名索引。

2.根据权利要求1所述的动态加密签名方法,其特征在于,所述方法还包括:

利用所述第一密钥对所述会话请求数据进行加密的同时,对所述第一签名索引进行加密;

将加密后的所述会话请求数据以及第一签名索引发送至所述服务器。

3.根据权利要求1所述的动态加密签名方法,其特征在于,所述方法还包括:

获取第一操作,确定所述第一操作对应的第一数据;

根据第二密钥索引和第二签名索引,从所述一个以上密钥以及一个以上签名中索引出第二密钥和第二签名;

利用所述第二签名对所述第一数据进行签名,并利用所述第二密钥对所述第一数据进行加密后发送至服务器;

当所述服务器对所述第一数据进行解密及验签通过后,接收所述服务器发送的利用所述第二签名进行签名以及所述第二密钥进行加密的第二数据,其中,所述第二数据为所述第一数据的执行结果。

4.根据权利要求1所述的动态加密签名方法,其特征在于,所述方法还包括:

获取第二操作,确定所述第二操作对应的第三数据;

根据第二密钥索引和第二签名索引,从所述一个以上密钥以及一个以上签名中索引出第二密钥和第二签名;

利用所述第二签名对所述第三数据进行签名,并利用所述第二密钥对所述第三数据进行加密后发送至服务器;

当所述服务器对所述第三数据进行解密及验签通过后,接收所述服务器发送的利用第三签名进行签名以及所述第二密钥进行加密的第四数据,其中,所述第四数据为所述第三数据的执行结果。

5.一种动态加密签名方法,其特征在于,所述方法包括:

当进行会话连接时,接收终端发送的利用第一签名进行签名以及第一密钥进行加密的会话请求数据;

获取预定的第一密钥索引以及随机的第一签名索引；

根据所述第一密钥索引和所述第一签名索引，从预存的一个以上密钥以及一个以上签名中索引出第一密钥和第一签名；

利用所述第一密钥对所述会话请求数据进行解密，并利用所述第一签名对所述会话请求数据进行验签；

验签通过后，随机选择出第二密钥索引以及第二签名索引；

利用所述第二签名索引对应的第二签名对会话响应数据进行签名，并利用所述第二密钥索引对应的第二密钥对所述会话响应数据进行加密后发送至所述终端；

获取第一签名索引，包括：

接收终端发送的利用第一签名进行签名以及第一密钥进行加密的会话请求数据的同时，接收终端发送的利用第一密钥进行加密的第一签名索引；

利用预定的第一密钥索引对所述加密的第一签名索引进行解密，得到所述第一签名索引。

6.根据权利要求5所述的动态加密签名方法，其特征在于，所述方法还包括：

接收所述终端发送的利用第二签名进行签名以及第二密钥进行加密的第一数据；

根据所述第二密钥索引和所述第二签名索引，从预存的一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

利用所述第二密钥对所述第一数据进行解密，并利用所述第二签名对所述第一数据进行验签；

验签通过后，对所述第一数据进行处理，得到第二数据；

利用所述第二签名对所述第二数据进行签名，并利用所述第二密钥对所述第二数据进行加密后发送至所述终端。

7.根据权利要求5所述的动态加密签名方法，其特征在于，所述方法还包括：

接收所述终端发送的利用第二签名进行签名以及第二密钥进行加密的第三数据；

根据所述第二密钥索引和所述第二签名索引，从预存的一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

利用所述第二密钥对所述第三数据进行解密，并利用所述第二签名对所述第三数据进行验签；

验签通过后，对所述第三数据进行处理，得到第四数据；

随机选择第三签名索引，并将所述第二签名索引替换为所述第三签名索引；

利用所述第三签名索引对应的第三签名对所述第四数据进行签名，并利用所述第二密钥索引对应的第二密钥对所述第四数据进行加密后发送至所述终端。

8.一种终端，其特征在于，所述终端包括：

密钥签名库单元，用于通过原生数据生成一个以上密钥以及一个以上签名；所述原生数据以动态原生库的方式提供相关接口；

选择单元，用于当进行会话连接时，选择预定的第一密钥索引以及随机的第一签名索引；

索引单元，用于根据所述第一密钥索引和所述第一签名索引，从所述一个以上密钥以及一个以上签名中索引出第一密钥和第一签名；

签名加密单元，用于利用所述第一签名对会话请求数据进行签名，并利用所述第一密钥对所述会话请求数据进行加密；

发送单元，用于将加密后的所述会话请求数据发送至服务器；

接收单元，用于当所述服务器对所述会话请求数据进行解密及验签通过后，接收所述服务器发送的利用随机的第二签名进行签名以及随机的第二密钥进行加密的会话响应数据；

所述选择单元，还用于获取当前时间戳，对所述当前时间戳进行第一变换处理，得到所述第一签名索引；或者，获取随机数，对所述随机数进行第二变换处理，得到所述第一签名索引。

9.根据权利要求8所述的终端，其特征在于，所述签名加密单元，还用于利用所述第一密钥对所述会话请求数据进行加密的同时，对所述第一签名索引进行加密；

所述发送单元，还用于将加密后的所述会话请求数据以及第一签名索引发送至所述服务器。

10.根据权利要求8所述的终端，其特征在于，所述终端还包括：

第一获取单元，用于获取第一操作，确定所述第一操作对应的第一数据；

所述索引单元，还用于根据第二密钥索引和第二签名索引，从所述一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

所述签名加密单元，还用于利用所述第二签名对所述第一数据进行签名，并利用所述第二密钥对所述第一数据进行加密；

所述发送单元，还用于将加密后的所述第一数据发送至服务器；

所述接收单元，还用于当所述服务器对所述第一数据进行解密及验签通过后，接收所述服务器发送的利用所述第二签名进行签名以及所述第二密钥进行加密的第二数据，其中，所述第二数据为所述第一数据的执行结果。

11.根据权利要求8所述的终端，其特征在于，所述终端还包括：

第二获取单元，用于获取第二操作，确定所述第二操作对应的第三数据；

所述索引单元，还用于根据第二密钥索引和第二签名索引，从所述一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

所述签名加密单元，还用于利用所述第二签名对所述第三数据进行签名，并利用所述第二密钥对所述第三数据进行加密；

所述发送单元，还用于将加密后的所述第三数据发送至服务器；

所述接收单元，还用于当所述服务器对所述第三数据进行解密及验签通过后，接收所述服务器发送的利用第三签名进行签名以及所述第二密钥进行加密的第四数据，其中，所述第四数据为所述第三数据的执行结果。

12.一种服务器，其特征在于，所述服务器包括：

接收单元，用于当进行会话连接时，接收终端发送的利用第一签名进行签名以及第一密钥进行加密的会话请求数据；

获取单元，用于获取预定的第一密钥索引以及随机的第一签名索引；

索引单元，用于根据所述第一密钥索引和所述第一签名索引，从预存的一个以上密钥以及一个以上签名中索引出第一密钥和第一签名；

解密验签单元，用于利用所述第一密钥对所述会话请求数据进行解密，并利用所述第一签名对所述会话请求数据进行验签；

第一选择单元，用于验签通过后，随机选择出第二密钥索引以及第二签名索引；

签名加密单元，用于利用所述第二签名索引对应的第二签名对会话响应数据进行签名，并利用所述第二密钥索引对应的第二密钥对所述会话响应数据进行加密；

发送单元，用于将加密后的所述会话响应数据发送至所述终端；

所述接收单元，还用于接收终端发送的利用第一签名进行签名以及第一密钥进行加密的会话请求数据的同时，接收终端发送的利用第一密钥进行加密的第一签名索引；

所述解密验签单元，还用于利用预定的第一密钥索引对所述加密的第一签名索引进行解密，得到所述第一签名索引。

13.根据权利要求12所述的服务器，其特征在于，

所述接收单元，还用于接收所述终端发送的利用第二签名进行签名以及第二密钥进行加密的第一数据；

所述索引单元，还用于根据所述第二密钥索引和所述第二签名索引，从预存的一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

解密验签单元，还用于利用所述第二密钥对所述第一数据进行解密，并利用所述第二签名对所述第一数据进行验签；

所述服务器还包括：执行处理单元，用于验签通过后，对所述第一数据进行处理，得到第二数据；

所述签名加密单元，还用于利用所述第二签名对所述第二数据进行签名，并利用所述第二密钥对所述第二数据进行加密；

所述发送单元，还用于将加密后的所述第二数据发送至所述终端。

14.根据权利要求12所述的服务器，其特征在于，

所述接收单元，还用于接收所述终端发送的利用第二签名进行签名以及第二密钥进行加密的第三数据；

所述索引单元，还用于根据所述第二密钥索引和所述第二签名索引，从预存的一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

所述解密验签单元，还用于利用所述第二密钥对所述第三数据进行解密，并利用所述第二签名对所述第三数据进行验签；

所述服务器还包括：执行处理单元，用于验签通过后，对所述第三数据进行处理，得到第四数据；

第二选择单元，用于随机选择第三签名索引；

保存单元，还用于将所述第二签名索引替换为所述第三签名索引；

所述签名加密单元，还用于利用所述第三签名索引对应的第三签名对所述第四数据进行签名，并利用所述第二密钥索引对应的第二密钥对所述第四数据进行加密；

所述发送单元，还用于将加密后的所述第四数据发送至所述终端。

一种动态加密方法、终端、服务器

技术领域

[0001] 本发明涉及加密技术，尤其涉及一种动态加密方法、终端、服务器。

背景技术

[0002] 终端与服务器之间的通信一般使用以安全为目标的超文本传输协议通道(HTTPS，Hyper Text Transfer Protocol over Secure Socket Layer)进行服务器的身份认证和建立可信的通道，具体通过浏览器的CA证书认证服务器证书，从而获取服务器的公钥，并利用服务器的公钥和存储在服务器的私钥进行非对称密钥的协商，一旦协商好，则保持到会话对象中。终端与服务器双方在后续会话中使用非对称密钥加密。

[0003] 终端与服务器之间的通信还可以通过业务自己开发对称加密体系，把对称密钥硬编码到终端，对称加密效率较高。

[0004] 现有的HTTPS的技术由于使用非对称加密算法，对计算资源要求高，并且需要进行安全套接层/安全传输层(SSL/TLS，Secure Socket Layer/Transport Layer Security)的会话握手机制，浪费网络资源；在配置方面需要准备认证证书，并且需要后续维护，操作繁琐。

[0005] 单纯的高级加密标准(AES，Advanced Encryption Standard)等对称加密体系无法满足动态密钥和防篡改的要求。

发明内容

[0006] 为解决上述技术问题，本发明实施例提供了一种动态加密签名方法、终端、服务器。

[0007] 本发明实施例提供的动态加密签名方法包括：

[0008] 通过原生数据生成一个以上密钥以及一个以上签名；

[0009] 当进行会话连接时，选择预定的第一密钥索引以及随机的第一签名索引；

[0010] 根据所述第一密钥索引和所述第一签名索引，从所述一个以上密钥以及一个以上签名中索引出第一密钥和第一签名；

[0011] 利用所述第一签名对会话请求数据进行签名，并利用所述第一密钥对所述会话请求数据进行加密后发送至服务器；

[0012] 当所述服务器对所述会话请求数据进行解密及验签通过后，接收所述服务器发送的利用随机的第二签名进行签名以及随机的第二密钥进行加密的会话响应数据。

[0013] 本发明另一实施例提供的动态加密签名方法包括：

[0014] 当进行会话连接时，接收终端发送的利用第一签名进行签名以及第一密钥进行加密的会话请求数据；

[0015] 获取预定的第一密钥索引以及随机的第一签名索引；

[0016] 根据所述第一密钥索引和所述第一签名索引，从预存的一个以上密钥以及一个以上签名中索引出第一密钥和第一签名；

[0017] 利用所述第一密钥对所述会话请求数据进行解密，并利用所述第一签名对所述会话请求数据进行验签；

[0018] 验签通过后，随机选择出第二密钥索引以及第二签名索引；

[0019] 利用所述第二签名索引对应的第二签名对会话响应数据进行签名，并利用所述第二密钥索引对应的第二密钥对所述会话响应数据进行加密后发送至所述终端。

[0020] 本发明实施例提供的终端包括：

[0021] 密钥签名库单元，用于通过原生数据生成一个以上密钥以及一个以上签名；

[0022] 选择单元，用于当进行会话连接时，选择预定的第一密钥索引以及随机的第一签名索引；

[0023] 索引单元，用于根据所述第一密钥索引和所述第一签名索引，从所述一个以上密钥以及一个以上签名中索引出第一密钥和第一签名；

[0024] 签名加密单元，用于利用所述第一签名对会话请求数据进行签名，并利用所述第一密钥对所述会话请求数据进行加密；

[0025] 发送单元，用于将加密后的所述会话请求数据发送至服务器；

[0026] 接收单元，用于当所述服务器对所述会话请求数据进行解密及验签通过后，接收所述服务器发送的利用随机的第二签名进行签名以及随机的第二密钥进行加密的会话响应数据。

[0027] 本发明实施例提供的服务器包括：

[0028] 接收单元，用于当进行会话连接时，接收终端发送的利用第一签名进行签名以及第一密钥进行加密的会话请求数据；

[0029] 获取单元，用于获取预定的第一密钥索引以及随机的第一签名索引；

[0030] 索引单元，用于根据所述第一密钥索引和所述第一签名索引，从预存的一个以上密钥以及一个以上签名中索引出第一密钥和第一签名；

[0031] 解密验签单元，用于利用所述第一密钥对所述会话请求数据进行解密，并利用所述第一签名对所述会话请求数据进行验签；

[0032] 第一选择单元，用于验签通过后，随机选择出第二密钥索引以及第二签名索引；

[0033] 签名加密单元，用于利用所述第二签名索引对应的第二签名对会话响应数据进行签名，并利用所述第二密钥索引对应的第二密钥对所述会话响应数据进行加密；

[0034] 发送单元，用于将加密后的所述会话响应数据发送至所述终端。

[0035] 本发明另一实施例提供的动态加密签名方法包括：

[0036] 向服务器发送请求配置消息，所述请求配置消息经第一签名进行签名，以及第一密钥进行加密；

[0037] 接收服务器发送的配置信息，所述配置信息由服务器经第二签名进行签名，以及第二密钥进行加密；

[0038] 对所述配置信息进行解密及验签通过后，利用所述配置信息查找到第一指令集；

[0039] 利用所述第一指令集进行读卡操作，得到卡信息。

[0040] 本发明另一实施例提供的终端包括：

[0041] 发送单元，用于向服务器发送请求配置消息，所述请求配置消息经第一签名进行签名，以及第一密钥进行加密；

[0042] 接收单元，用于接收服务器发送的配置信息，所述配置信息由服务器经第二签名进行签名，以及第二密钥进行加密；

[0043] 查找单元，用于对所述配置信息进行解密及验签通过后，利用所述配置信息查找到第一指令集；

[0044] 读卡单元，用于利用所述第一指令集进行读卡操作，得到卡信息。

[0045] 本发明实施例的技术方案中，终端原生埋入了一系列对称的密钥和签名，同时在服务器也埋入了和终端一一对应的密钥和签名，这些密钥和签名通过原生数据生成，提高了密钥和签名的安全性，避免了密钥和签名被破解的风险。终端与服务器建立会话的过程中，服务器随机选取了密钥索引和签名索引，建立了对称加密体系。该协商的签名密钥生命周期是登录态会话，利用该对称加密通道协商一个会话生命周期的签名密钥和一次性有效的签名密钥，从而实现了加密通信和动态签名的三层体系，解决了通信过程中固定签名容易被劫持后破解伪造数据的问题。

[0046] 再者，对于具有依赖关系的操作流程，服务器每次会动态生成一次性有效的签名并随同服务器响应数据一起发送给终端，终端在处理完业务逻辑后，在下次交互中，利用上次下发的签名进行签名后发送至服务器，可以保证终端请求结果的防篡改。

附图说明

[0047] 图1为本发明实施例一的动态加密签名方法的流程示意图；

[0048] 图2为本发明实施例二的动态加密签名方法的流程示意图；

[0049] 图3为本发明实施例三的动态加密签名方法的流程示意图；

[0050] 图4为本发明实施例四的动态加密签名方法的流程示意图；

[0051] 图5为本发明实施例的终端的结构组成示意图；

[0052] 图6为本发明实施例的服务器的结构组成示意图；

[0053] 图7为本发明另一实施例的动态加密签名方法的流程示意图；

[0054] 图8为本发明另一实施例的终端的结构组成示意图。

具体实施方式

[0055] 为了能够更加详尽地了解本发明实施例的特点与技术内容，下面结合附图对本发明实施例的实现进行详细阐述，所附附图仅供参考说明之用，并非用来限定本发明实施例。

[0056] 图1为本发明实施例一的动态加密签名方法的流程示意图，本示例中的动态加密签名方法应用于终端侧，如图1所示，所述动态加密签名方法包括以下步骤：

[0057] 步骤101：通过原生数据生成一个以上密钥以及一个以上签名。

[0058] 这里，所述终端可以为个人计算机(PC，Personal Computer)这种固定的电子设备，还可以为如个人数字助理(PAD)、平板电脑、手提电脑这种便携式的电子设备，当然还可以为如智能手机这种智能移动终端。

[0059] 本发明实施例中，为了实现终端和服务器建立高效可靠的加密通道，且为了防止密钥硬编码到终端导致被暴力破解的问题，终端的密钥以及签名通过原生数据实现，例如C语言，并以动态原生库的方式提供相关接口。同时，为了防止只有一个密钥或签名被破解，在原生库中埋入一系列对称密钥和签名，并且提供了基于密钥索引和签名索引的访问方

式，避免了埋入的对称密钥和签名被读出。服务器同样配置了和终端一一对应的对称密钥和签名。

[0060] 参见表1，表1共配置了5组密钥索引以及对应的密钥，5组签名索引及其对应的签名。利用密钥索引可索引出与其对应的密钥，利用签名索引可以索引出与其对应的签名。例如，利用密钥索引2可以索引出对应的密钥为C1，利用签名索引0可以索引出对应的签名为A2。

[0061]

密钥索引	密钥	签名索引	签名
0	A1	0	A2

[0062]

1	B1	1	B2
2	C1	2	C2
3	D1	3	D2
4	E1	4	E2

[0063] 表1

[0064] 步骤102：当进行会话连接时，选择预定的第一密钥索引以及随机的第一签名索引。

[0065] 本发明实施例中，在每次会话初始化过程中，终端首先选择预定的第一密钥索引以及随机的第一签名索引。

[0066] 这里，预定的第一密钥索引为终端和服务器提前约定好的密钥索引，一般可设置为默认的密钥索引，密钥索引号为0。

[0067] 这里，随机的第一签名索引可通过获取当前时间戳或者随机数的方式进行确定。

[0068] 具体地，获取当前时间戳，对所述当前时间戳进行第一变换处理，得到所述第一签名索引；或者，获取随机数，对所述随机数进行第二变换处理，得到所述第一签名索引。

[0069] 例如，当前时间戳为2015.05.05.08.34，表明的是2015年5月5号8时34分，则对该时间戳进行变换处理，例如，取秒数除以5后取余数，得到的结果即为签名索引。

[0070] 再例如，利用终端的随机函数取随机数，对该随机数除以5后取余数，得到的结果即为签名索引。

[0071] 本发明实施例中，会话是管理一系列相互有状态依赖的对象，通过会话可以把一个业务流程的上下文进行串联起来。

[0072] 步骤103：根据所述第一密钥索引和所述第一签名索引，从所述一个以上密钥以及一个以上签名中索引出第一密钥和第一签名。

[0073] 终端确定出第一密钥索引和第一签名索引后，即可根据第一密钥索引和第一签名索引从所述一个以上密钥以及一个以上签名中索引出第一密钥和第一签名。例如表1，利用密钥索引2可以索引出对应的密钥为C1，利用签名索引0可以索引出对应的签名为A2。

[0074] 步骤104：利用所述第一签名对会话请求数据进行签名，并利用所述第一密钥对所述会话请求数据进行加密后发送至服务器。

[0075] 这里，会话请求数据根据终端的具体实现方式而不同，例如，终端为近场通信(NFC，Near Field Communication)类型的电子设备时，且终端利用NFC实现了圈存功能，则

会话请求数据中包括了用户标识、交易信息等。

[0076] 这里,NFC是一种短距高频的无线电技术,在13.56MHz频率运行于20厘米距离内。其传输速度有106Kbit/秒、212Kbit/秒或者424Kbit/秒三种。目前近场通信已通过成为ISO/IEC IS 18092国际标准、ECMA-340标准与ETSI TS102190标准。NFC技术能够用作机场登机验证、大厦的门禁钥匙、交通一卡通、信用卡、支付卡等等。

[0077] 圈存是指将消费者银行户头中的钱直接圈存(存入)IC晶片上,亦即有了电子钱包的过程,这样一来,消费者就免除携带现金找零、遗失、伪钞、被抢之风险。

[0078] 此外,终端为NFC类型的电子设备时,且利用NFC实现了信息验证功能,则会话请求数据中包括了用户标识。

[0079] 再例如,终端具有蓝牙(Bluetooth)功能时,终端通过蓝牙向服务器发送查询账单的请求,则会话请求数据包括了用户标识、查询对象信息等。

[0080] 步骤105:当所述服务器对所述会话请求数据进行解密及验签通过后,接收所述服务器发送的利用随机的第二签名进行签名以及随机的第二密钥进行加密的会话响应数据。

[0081] 其中,登录会话对象中存储有第二密钥索引以及第二签名索引。

[0082] 这里,终端与服务器之间一旦建立会话,该会话则一直存在,会话处于登录状态,直到终端空闲(未进行会话请求)时间超过了某一个时限,服务器才释放该会话资源。在会话的登录期间,终端可能给服务器发送了很多会话请求,这些会话请求都存储在同一会话中。而会话对象则是用于存储某一特定终端会话所需的信息,如会话标识(ID,IDentification),会话密钥等等;在会话建立时,由服务器为终端建立一个会话对象,由于该会话对象适用于登录状态,因此,称为登录会话对象。

[0083] 本发明实施例中,将第二密钥索引以及第二签名索引存储至登录会话对象中,这样,终端与服务器都能够通过登录会话对象获得第二密钥索引以及第二签名索引,从而进一步获得对应的第二密钥和第二签名实现双方的数据加密解密,提高了数据的安全性。

[0084] 服务器对终端的会话请求数据,按照约定的密钥索引和签名索引进行解密和验签,验签通过后,服务器随机选择一个新的密钥索引和签名索引,并且把这个新的密钥索引和签名索引跟随登录态一起保存到登录会话对象中,因此,该密钥索引和签名索引会存在于整个登录会话中,同时,利用新的签名索引对应的签名(First Key)对响应数据进行签名,并利用新的密钥索引对应的密钥加密响应数据后发送到终端。从而,终端接收服务器发送的利用新的签名(First Key)进行签名以及新的密钥进行加密的会话响应数据。

[0085] 通过上述步骤建立了一个从终端到服务器之间的登录态生命周期的加密通道。

[0086] 本发明实施例中,利用所述第一密钥对所述会话请求数据进行加密的同时,对所述第一签名索引进行加密;将加密后的所述会话请求数据以及第一签名索引发送至所述服务器。

[0087] 这里,将第一签名索引加密后发送至服务器后,服务器可获取到第一签名索引,然后再索引出第一签名进行验签。

[0088] 在一实施方式中,当建立了加密通道后,终端与服务器之间可进行后续的会话,具体地:

[0089] 获取第一操作,确定所述第一操作对应的第一数据;

[0090] 根据所述第二密钥索引和所述第二签名索引,从所述一个以上密钥以及一个以上

签名中索引出第二密钥和第二签名；

[0091] 利用所述第二签名对所述第一数据进行签名，并利用所述第二密钥对所述第一数据进行加密后发送至服务器；

[0092] 当所述服务器对所述第一数据进行解密及验签通过后，接收所述服务器发送的利用所述第二签名进行签名以及所述第二密钥进行加密的第二数据，其中，所述第二数据为所述第一数据的执行结果。

[0093] 上述方案适用于一次性操作流程，如终端请求订单列表，由于该流程没有相互流程的依赖关系，终端进行如下处理：用户在终端上触发第一操作(请求订单列表)，终端获取到第一操作对应的第一数据(账户数据，订单列表标识等信息)，使用新的签名(第二签名)对第一数据进行签名后，使用新的密钥(第二密钥)进行加密，然后发送至服务器。服务器首先进行登录态的判断，从登录态会话对象中读取密钥索引和签名索引，利用密钥索引对应的密钥进行解密，利用签名索引对应的签名进行验签，若通过则执行业务逻辑，获得第二数据，再利用新的密钥和签名对第二数据签名加密后发送至终端。

[0094] 在另一实施方式中，当建立了加密通道后，终端与服务器之间可进行后续的会话，具体地：

[0095] 获取第二操作，确定所述第二操作对应的第三数据；

[0096] 根据所述第二密钥索引和所述第二签名索引，从所述一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

[0097] 利用所述第二签名对所述第三数据进行签名，并利用所述第二密钥对所述第三数据进行加密后发送至服务器；

[0098] 当所述服务器对所述第三数据进行解密及验签通过后，接收所述服务器发送的利用第三签名进行签名以及所述第二密钥进行加密的第四数据，其中，所述第四数据为所述第三数据的执行结果，所述登录会话对象中存储有第二密钥索引以及第三签名索引。

[0099] 上述方案适用于多次具有依赖关系的操作流程，如NFC圈存需要多次交互，且各个交互流程之前存在依赖关系的流程中，每次请求响应过程中，服务器指定一个全新的签名索引，并把该签名索引一起存入登录会话对象后随同响应一起发送给终端。在接下来的终端请求中，整个通信过程使用密钥索引对应的密钥(第二密钥)进行加密，使用不断更新的签名索引对应的签名(Next Key)进行签名。对接下来的终端请求处理中，服务器除了继续使用登录会话对象中的密钥索引对应的密钥进行解密外，会用一次性有效的签名索引对应的签名(Next Key)进行验签，从而极大的提升了安全性。

[0100] 下面参照图2对上述动态加密签名方法再做描述，本示例中的密钥和签名都是根据上述方案中的密钥索引和签名索引所获得，此时不再赘述，直接描述加密签名的过程，本领域技术人员应当理解，此处还包括有利用密钥索引得到密钥，以及利用签名索引得到签名的过程，图2为本发明实施例二的动态加密签名方法的流程示意图，包括以下步骤：

[0101] 步骤201：终端使用默认的密钥和随机的签名对会话请求数据签名加密，发送至服务器。

[0102] 步骤202：服务器收到会话请求数据，解密验签通过后，随机选择新的密钥和签名并发送至终端。

[0103] 步骤203：终端利用新的密钥和签名对后续会话数据进行签名加密，发送至服务

器。

[0104] 下面参照图3对上述动态加密签名方法再做描述，本示例中的密钥和签名都是根据上述方案中的密钥索引和签名索引所获得，此时不再赘述，直接描述加密签名的过程，本领域技术人员应当理解，此处还包括有利用密钥索引得到密钥，以及利用签名索引得到签名的过程，图3为本发明实施例三的动态加密签名方法的流程示意图，包括以下步骤：

[0105] 步骤301：终端使用当前登录会话对象中的密钥和签名对请求数据签名加密，发送至服务器。

[0106] 步骤302：服务器收到请求数据，解密验签通过后，随机选择新签名并发送至终端。

[0107] 新的签名保存至登录会话对象中。

[0108] 步骤303：终端利用当前登录会话对象中的密钥和新的签名对后续会话数据进行签名加密，发送至服务器。

[0109] 对于具有依赖关系的操作流程，服务器每次会动态生成一次性有效的签名并随同服务器响应数据一起发送给终端，终端在处理完业务逻辑后，在下次交互中，利用上次下发的签名进行签名后发送至服务器，可以保证终端请求结果的防篡改。

[0110] 图4为本发明实施例四的动态加密签名方法的流程示意图，本示例中的动态加密签名方法应用于服务器侧，如图4所示，所述动态加密签名方法包括以下步骤：

[0111] 步骤401：当进行会话连接时，接收终端发送的利用第一签名进行签名以及第一密钥进行加密的会话请求数据。

[0112] 步骤402：获取预定的第一密钥索引以及随机的第一签名索引。

[0113] 这里，终端与服务器预先约定了第一密钥索引，因此，服务器可直接获取第一密钥索引。

[0114] 本发明实施例中，第一签名索引通过以下步骤获得：

[0115] 接收终端发送的利用第一签名进行签名以及第一密钥进行加密的会话请求数据的同时，接收终端发送的利用第一密钥进行加密的第一签名索引；

[0116] 利用预定的第一密钥索引对所述加密的第一签名索引进行解密，得到所述第一签名索引。

[0117] 步骤403：根据所述第一密钥索引和所述第一签名索引，从预存的一个以上密钥以及一个以上签名中索引出第一密钥和第一签名。

[0118] 步骤404：利用所述第一密钥对所述会话请求数据进行解密，并利用所述第一签名对所述会话请求数据进行验签。

[0119] 步骤405：验签通过后，随机选择出第二密钥索引以及第二签名索引。

[0120] 步骤406：将所述第二密钥索引以及第二签名索引存储至登录会话对象中，利用所述第二签名索引对应的第二签名对会话响应数据进行签名，并利用所述第二密钥索引对应的第二密钥对所述会话响应数据进行加密后发送至所述终端。

[0121] 通过上述步骤建立了一个从终端到服务器之间的登录态生命周期的加密通道。

[0122] 在一实施方式中，建立了加密通道后，接收所述终端发送的利用第二签名进行签名以及第二密钥进行加密的第一数据；

[0123] 根据所述第二密钥索引和所述第二签名索引，从预存的一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

[0124] 利用所述第二密钥对所述第一数据进行解密，并利用所述第二签名对所述第一数据进行验签；

[0125] 验签通过后，对所述第一数据进行处理，得到第二数据；

[0126] 利用所述第二签名对所述第二数据进行签名，并利用所述第二密钥对所述第二数据进行加密后发送至所述终端。

[0127] 上述方案适用于一次性操作流程，如终端请求订单列表，由于该流程没有相互流程的依赖关系，终端进行如下处理：用户在终端上触发第一操作(请求订单列表)，终端获取到第一操作对应的第一数据(账户数据，订单列表标识等信息)，使用新的签名(第二签名)对第一数据进行签名后，使用新的密钥(第二密钥)进行加密，然后发送至服务器。服务器首先进行登录态的判断，从登录态会话对象中读取密钥索引和签名索引，利用密钥索引对应的密钥进行解密，利用签名索引对应的签名进行验签，若通过则执行业务逻辑，获得第二数据，再利用新的密钥和签名对第二数据签名加密后发送至终端。

[0128] 在另一实施方式中，建立了加密通道后，接收所述终端发送的利用第二签名进行签名以及第二密钥进行加密的第三数据；

[0129] 根据所述第二密钥索引和所述第二签名索引，从预存的一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

[0130] 利用所述第二密钥对所述第三数据进行解密，并利用所述第二签名对所述第三数据进行验签；

[0131] 验签通过后，对所述第三数据进行处理，得到第四数据；

[0132] 随机选择第三签名索引，并将所述登录会话对象中的第二签名索引替换为所述第三签名索引；

[0133] 利用所述第三签名索引对应的第三签名对所述第四数据进行签名，并利用所述第二密钥索引对应的第二密钥对所述第四数据进行加密后发送至所述终端。

[0134] 上述方案适用于多次具有依赖关系的操作流程，如NFC圈存需要多次交互，且各个交互流程之前存在依赖关系的流程中，每次请求响应过程中，服务器指定一个全新的签名索引，并把该签名索引一起存入登录会话对象后随同响应一起发送给终端。

[0135] 在接下来的终端请求中，整个通信过程使用密钥索引对应的密钥(第二密钥)进行加密，使用不断更新的签名索引对应的签名(Next Key)进行签名。对接下来的终端请求处理中，服务器除了继续使用登录会话对象中的密钥索引对应的密钥进行解密外，会用一次性有效的签名索引对应的签名(Next Key)进行验签，从而极大的提升了安全性。

[0136] 图5为本发明实施例的终端的结构组成示意图，如图5所示，所述终端包括：

[0137] 密钥签名库单元51，用于通过原生数据生成一个以上密钥以及一个以上签名；

[0138] 选择单元52，用于当进行会话连接时，选择预定的第一密钥索引以及随机的第一签名索引；

[0139] 索引单元53，用于根据所述第一密钥索引和所述第一签名索引，从所述一个以上密钥以及一个以上签名中索引出第一密钥和第一签名；

[0140] 签名加密单元54，用于利用所述第一签名对会话请求数据进行签名，并利用所述第一密钥对所述会话请求数据进行加密；

[0141] 发送单元55，用于将加密后的所述会话请求数据发送至服务器；

[0142] 接收单元56，用于当所述服务器对所述会话请求数据进行解密及验签通过后，接收所述服务器发送的利用随机的第二签名进行签名以及随机的第二密钥进行加密的会话响应数据，其中，登录会话对象中存储有第二密钥索引以及第二签名索引。

[0143] 本发明实施例中，所述选择单元52，还用于获取当前时间戳，对所述当前时间戳进行第一变换处理，得到所述第一签名索引；或者，获取随机数，对所述随机数进行第二变换处理，得到所述第一签名索引。

[0144] 本发明实施例中，所述签名加密单元54，还用于利用所述第一密钥对所述会话请求数据进行加密的同时，对所述第一签名索引进行加密；

[0145] 所述发送单元55，还用于将加密后的所述会话请求数据以及第一签名索引发送至所述服务器。

[0146] 本发明实施例中，所述终端还包括：

[0147] 第一获取单元57，用于获取第一操作，确定所述第一操作对应的第一数据；

[0148] 所述索引单元53，还用于根据所述第二密钥索引和所述第二签名索引，从所述一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

[0149] 所述签名加密单元54，还用于利用所述第二签名对所述第一数据进行签名，并利用所述第二密钥对所述第一数据进行加密；

[0150] 所述发送单元55，还用于将加密后的所述第一数据发送至服务器；

[0151] 所述接收单元56，还用于当所述服务器对所述第一数据进行解密及验签通过后，接收所述服务器发送的利用所述第二签名进行签名以及所述第二密钥进行加密的第二数据，其中，所述第二数据为所述第一数据的执行结果。

[0152] 本发明实施例中，所述终端还包括：

[0153] 第二获取单元58，用于获取第二操作，确定所述第二操作对应的第三数据；

[0154] 所述索引单元53，还用于根据所述第二密钥索引和所述第二签名索引，从所述一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

[0155] 所述签名加密单元54，还用于利用所述第二签名对所述第三数据进行签名，并利用所述第二密钥对所述第三数据进行加密；

[0156] 所述发送单元55，还用于将加密后的所述第三数据发送至服务器；

[0157] 所述接收单元56，还用于当所述服务器对所述第三数据进行解密及验签通过后，接收所述服务器发送的利用第三签名进行签名以及所述第二密钥进行加密的第四数据，其中，所述第四数据为所述第三数据的执行结果，所述登录会话对象中存储有第二密钥索引以及第三签名索引。

[0158] 本领域技术人员应当理解，图5所示的终端中的各单元的实现功能可参照前述动态加密签名方法的相关描述而理解。图5所示的终端中的各单元的功能可通过运行于处理器上的程序而实现，也可通过具体的逻辑电路而实现。、

[0159] 图6为本发明实施例的服务器的结构组成示意图，如图6所示，所述服务器包括：

[0160] 接收单元61，用于当进行会话连接时，接收终端发送的利用第一签名进行签名以及第一密钥进行加密的会话请求数据；

[0161] 获取单元62，用于获取预定的第一密钥索引以及随机的第一签名索引；

[0162] 索引单元63，用于根据所述第一密钥索引和所述第一签名索引，从预存的一个以

上密钥以及一个以上签名中索引出第一密钥和第一签名；

[0163] 解密验签单元64，用于利用所述第一密钥对所述会话请求数据进行解密，并利用所述第一签名对所述会话请求数据进行验签；

[0164] 第一选择单元65，用于验签通过后，随机选择出第二密钥索引以及第二签名索引；

[0165] 保存单元66，用于将所述第二密钥索引以及第二签名索引存储至登录会话对象中；

[0166] 签名加密单元67，用于利用所述第二签名索引对应的第二签名对会话响应数据进行签名，并利用所述第二密钥索引对应的第二密钥对所述会话响应数据进行加密；

[0167] 发送单元68，用于将加密后的所述会话响应数据发送至所述终端。

[0168] 本发明实施例中，所述接收单元61，还用于接收终端发送的利用第一签名进行签名以及第一密钥进行加密的会话请求数据的同时，接收终端发送的利用第一密钥进行加密的第一签名索引；

[0169] 所述解密验签单元64，还用于利用预定的第一密钥索引对所述加密的第一签名索引进行解密，得到所述第一签名索引。

[0170] 本发明实施例中，所述接收单元61，还用于接收所述终端发送的利用第二签名进行签名以及第二密钥进行加密的第一数据；

[0171] 所述索引单元63，还用于根据所述第二密钥索引和所述第二签名索引，从预存的一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

[0172] 解密验签单元64，还用于利用所述第二密钥对所述第一数据进行解密，并利用所述第二签名对所述第一数据进行验签；

[0173] 所述服务器还包括：执行处理单元69，用于验签通过后，对所述第一数据进行处理，得到第二数据；

[0174] 所述签名加密单元67，还用于利用所述第二签名对所述第二数据进行签名，并利用所述第二密钥对所述第二数据进行加密；

[0175] 所述发送单元68，还用于将加密后的所述第二数据发送至所述终端。

[0176] 本发明实施例中，所述接收单元61，还用于接收所述终端发送的利用第二签名进行签名以及第二密钥进行加密的第三数据；

[0177] 所述索引单元63，还用于根据所述第二密钥索引和所述第二签名索引，从预存的一个以上密钥以及一个以上签名中索引出第二密钥和第二签名；

[0178] 所述解密验签单元64，还用于利用所述第二密钥对所述第三数据进行解密，并利用所述第二签名对所述第三数据进行验签；

[0179] 所述服务器还包括：执行处理单元69，用于验签通过后，对所述第三数据进行处理，得到第四数据；

[0180] 第二选择单元610，用于随机选择第三签名索引；

[0181] 所述保存单元66，还用于将所述登录会话对象中的第二签名索引替换为所述第三签名索引；

[0182] 所述签名加密单元67，还用于利用所述第三签名索引对应的第三签名对所述第四数据进行签名，并利用所述第二密钥索引对应的第二密钥对所述第四数据进行加密；

[0183] 所述发送单元68，还用于将加密后的所述第四数据发送至所述终端。

[0184] 本领域技术人员应当理解，图6所示的服务器中的各单元的实现功能可参照前述动态加密签名方法的相关描述而理解。图6所示的服务器中的各单元的功能可通过运行于处理器上的程序而实现，也可通过具体的逻辑电路而实现。

[0185] 图7为本发明另一实施例的动态加密签名方法的流程示意图，应用于终端，如图7所示，所述方法包括以下步骤：

[0186] 步骤701：向服务器发送请求配置消息，所述请求配置消息经第一签名进行签名，以及第一密钥进行加密。

[0187] 本发明实施例中，终端具有NFC功能，可作为公交卡使用。公交卡中的信息具体有该公交卡归属哪个城市，该公交卡的余额信息等等。本发明实施例中的公交卡可适用于多个城市，为此，需要多种不同的配置信息来支持NFC具有这些功能。

[0188] 基于此，终端上安装有与公交卡相关的应用，用户打开该应用后，向服务器发送初始化的请求，该初始化请求中包括所述请求配置信息。

[0189] 步骤702：接收服务器发送的配置信息，所述配置信息由服务器经第二签名进行签名，以及第二密钥进行加密。

[0190] 这里，服务器不是每次都向终端发送配置信息，因为这样将消耗大量的流量，为此，终端发送请求配置信息时，还将终端当前的版本号发送给服务器，服务器对比终端的版本号与需要更新的版本号是否一致，只有当不一致的情况下，才向终端发送更新的配置信息。

[0191] 步骤703：对所述配置信息进行解密及验签通过后，利用所述配置信息查找到第一指令集。

[0192] 这里，第一指令集也即是配置信息，第一指令集包括但不限于：应用协议数据单元(APDU，Application Protocol Data Unit)指令集、UI动态文案、业务流程开关等。

[0193] 步骤704：利用所述第一指令集进行读卡操作，得到卡信息。

[0194] 这里，卡信息可以是该卡所述的城市以及对应的余额信息等等。

[0195] 本示例中的密钥和签名都是根据上述方案中的密钥索引和签名索引所获得，此时不再赘述，直接描述加密签名的过程，本领域技术人员应当理解，此处还包括有利用密钥索引得到密钥，以及利用签名索引得到签名的过程。

[0196] 图8为本发明另一实施例的终端的结构组成示意图，如图8所示，所述终端包括：

[0197] 发送单元81，用于向服务器发送请求配置消息，所述请求配置消息经第一签名进行签名，以及第一密钥进行加密；

[0198] 接收单元82，用于接收服务器发送的配置信息，所述配置信息由服务器经第二签名进行签名，以及第二密钥进行加密；

[0199] 查找单元83，用于对所述配置信息进行解密及验签通过后，利用所述配置信息查找到第一指令集；

[0200] 读卡单元84，用于利用所述第一指令集进行读卡操作，得到卡信息。

[0201] 本发明实施例所记载的技术方案之间，在不冲突的情况下，可以任意组合。

[0202] 在本发明所提供的几个实施例中，应该理解到，所揭露的方法和智能设备，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，如：多个单元或组件可以结

合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

[0203] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元，即可以位于一个地方，也可以分布到多个网络单元上；可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0204] 另外，在本发明各实施例中的各功能单元可以全部集成在一个第二处理单元中，也可以是各单元分别单独作为一个单元，也可以两个或两个以上单元集成在一个单元中；上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0205] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。

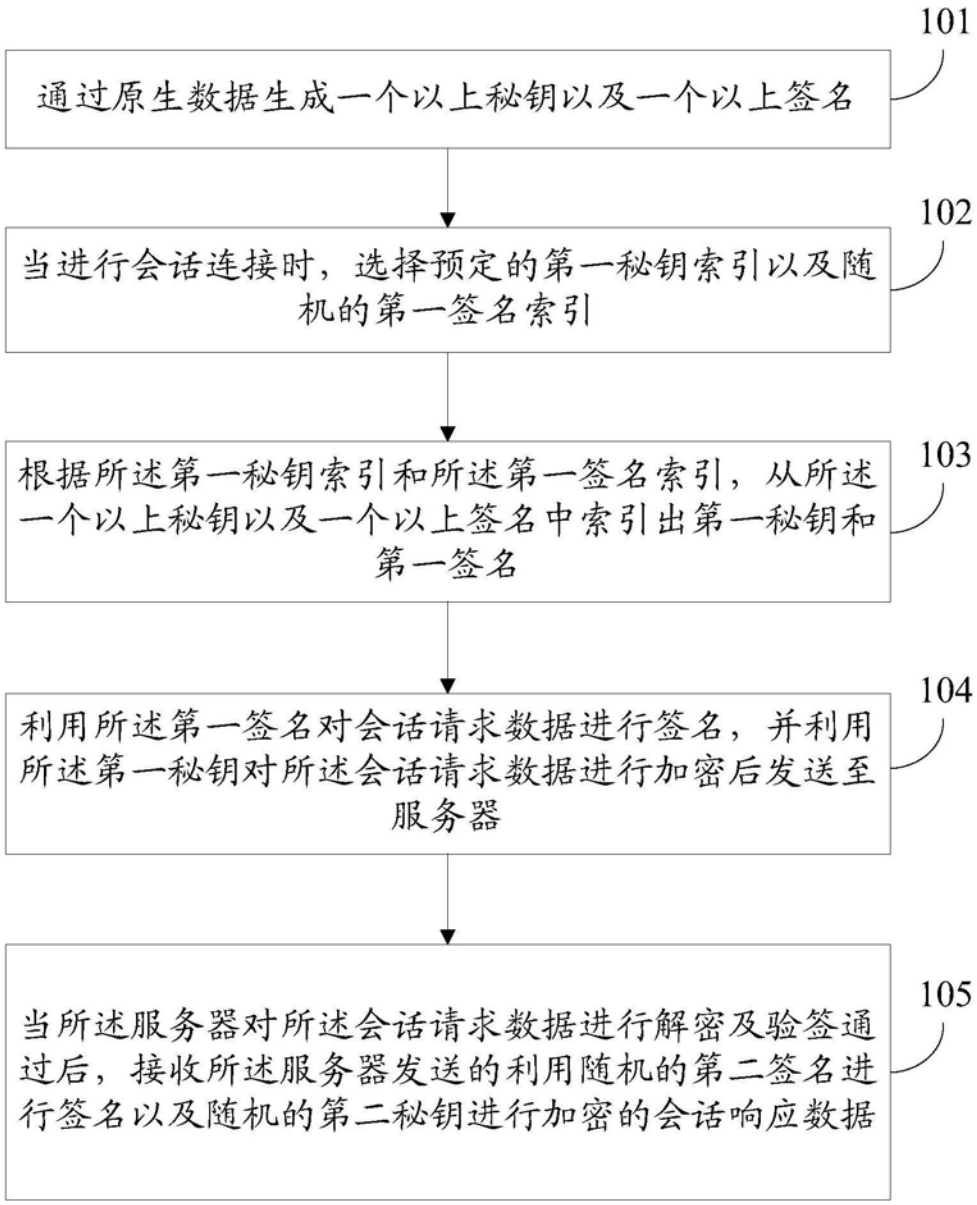

101
通过原生数据生成一个以上秘钥以及一个以上签名
102
当进行会话连接时，选择预定的第一秘钥索引以及随机的第一签名索引
103
根据所述第一秘钥索引和所述第一签名索引，从所述一个以上秘钥以及一个以上签名中索引出第一秘钥和第一签名
104
利用所述第一签名对会话请求数据进行签名，并利用所述第一秘钥对所述会话请求数据进行加密后发送至服务器
105
当所述服务器对所述会话请求数据进行解密及验签通过后，接收所述服务器发送的利用随机的第二签名进行签名以及随机的第二秘钥进行加密的会话响应数据

图1

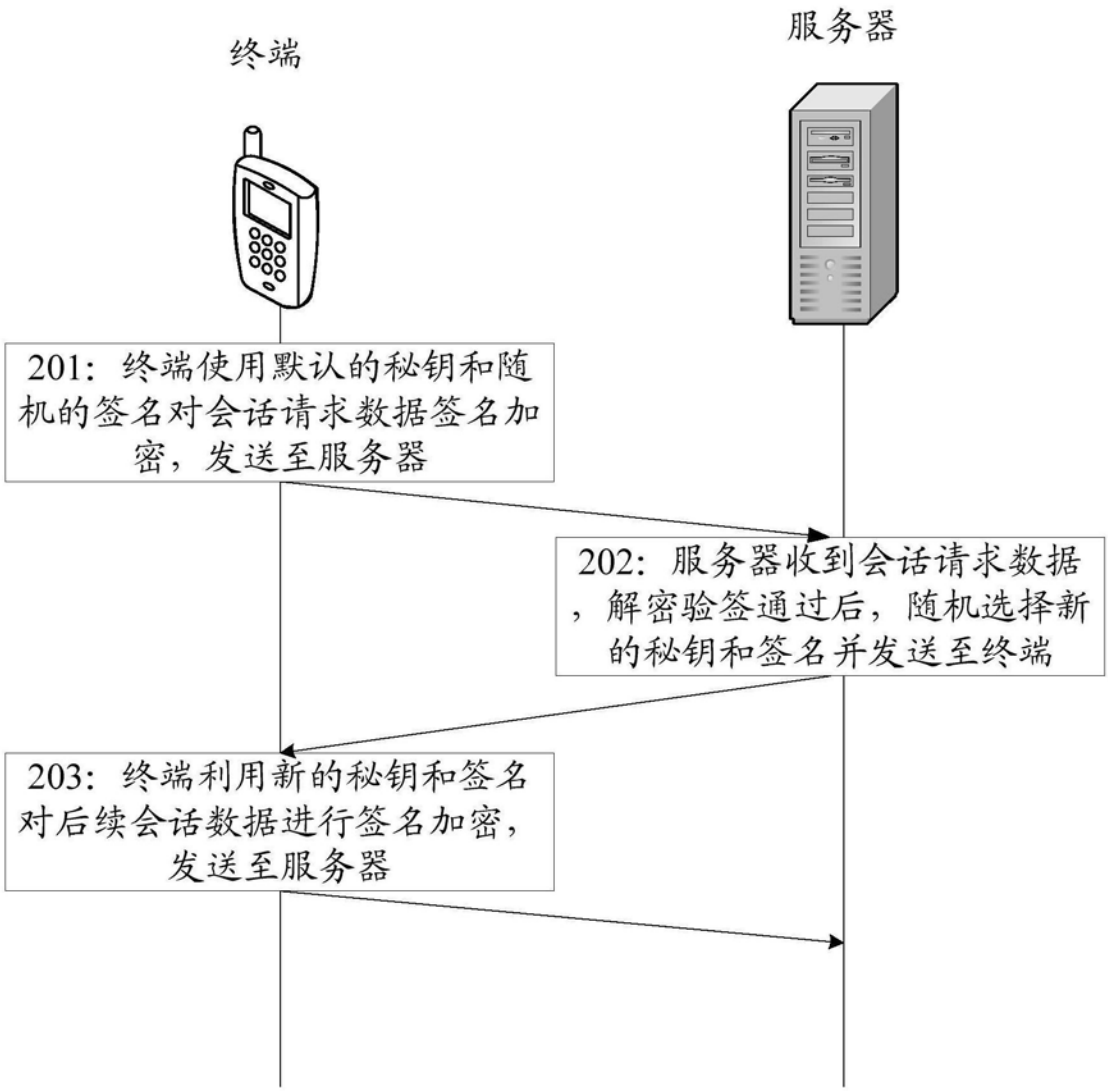

终端
服务器
201：终端使用默认的秘钥和随机的签名对会话请求数据签名加密，发送至服务器
202：服务器收到会话请求数据，解密验签通过后，随机选择新的秘钥和签名并发送至终端
203：终端利用新的秘钥和签名对后续会话数据进行签名加密，发送至服务器

图2

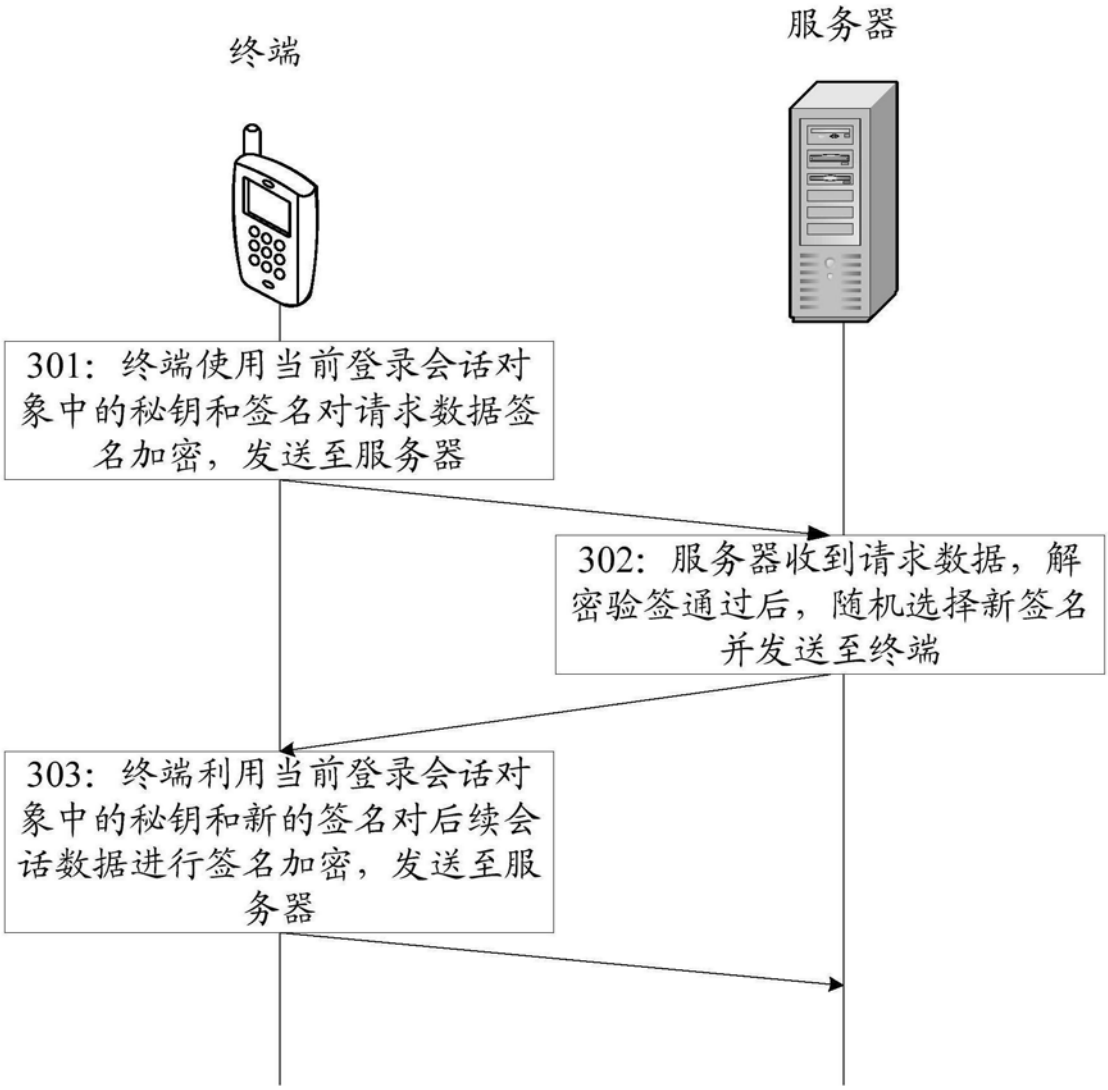

终端
服务器
301：终端使用当前登录会话对象中的秘钥和签名对请求数据签名加密，发送至服务器
302：服务器收到请求数据，解密验签通过后，随机选择新签名并发送至终端
303：终端利用当前登录会话对象中的秘钥和新的签名对后续会话数据进行签名加密，发送至服务器

图3

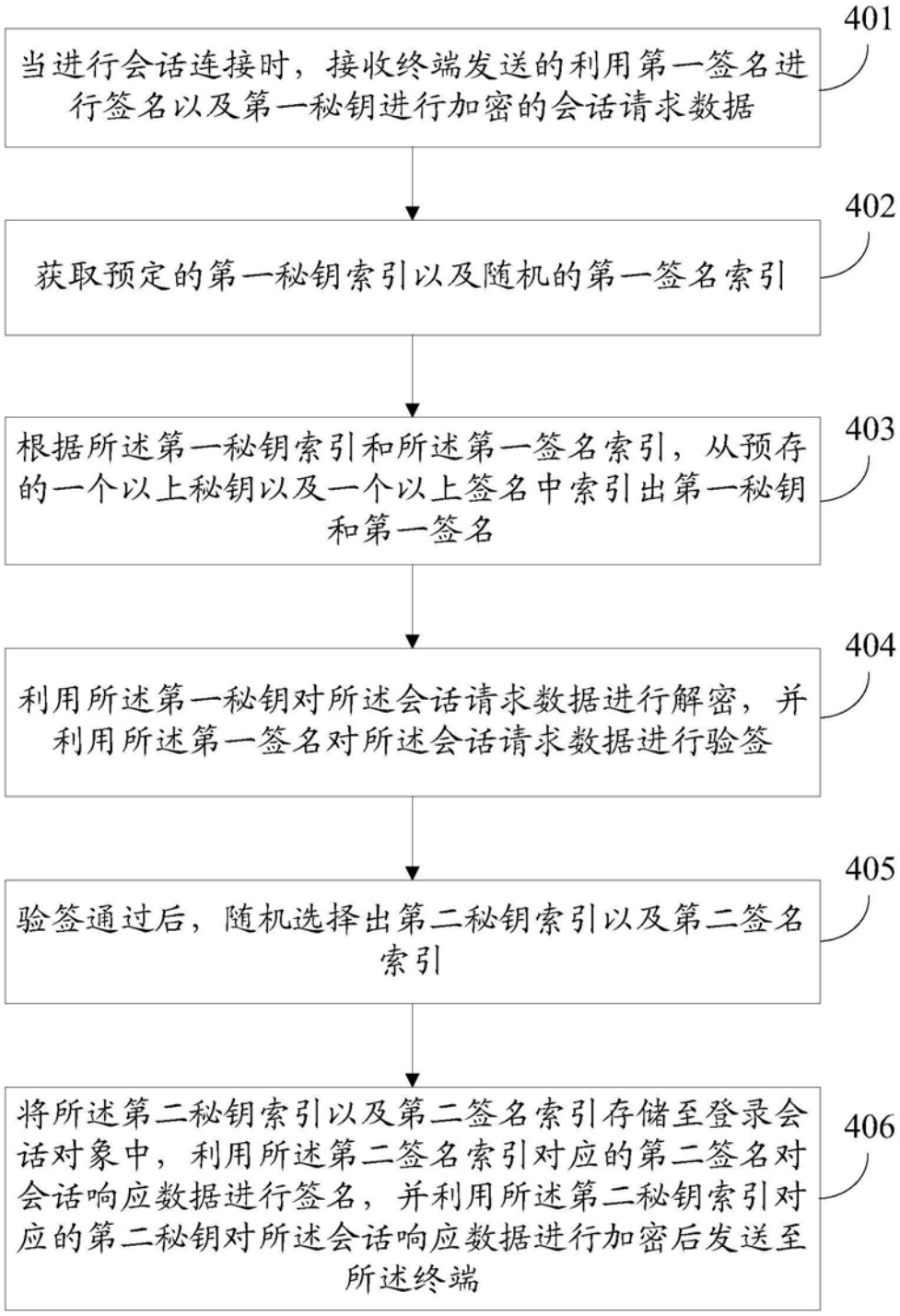

401
当进行会话连接时，接收终端发送的利用第一签名进行签名以及第一秘钥进行加密的会话请求数据
402
获取预定的第一秘钥索引以及随机的第一签名索引
403
根据所述第一秘钥索引和所述第一签名索引，从预存的一个以上秘钥以及一个以上签名中索引出第一秘钥和第一签名
404
利用所述第一秘钥对所述会话请求数据进行解密，并利用所述第一签名对所述会话请求数据进行验签
405
验签通过后，随机选择出第二秘钥索引以及第二签名索引
406
将所述第二秘钥索引以及第二签名索引存储至登录会话对象中，利用所述第二签名索引对应的第二签名对会话响应数据进行签名，并利用所述第二秘钥索引对应的第二秘钥对所述会话响应数据进行加密后发送至所述终端

图4

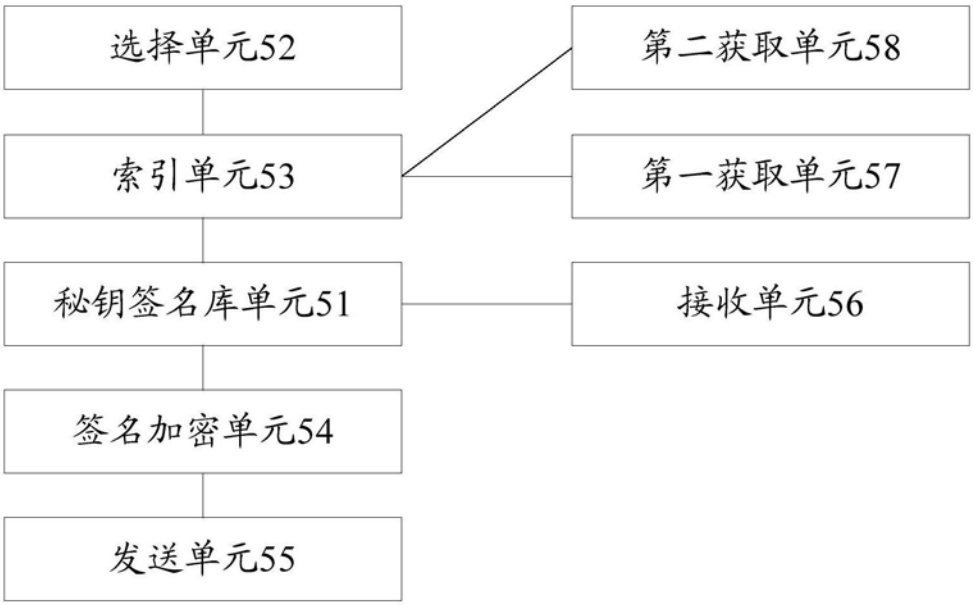

选择单元52
第二获取单元58
索引单元53
第一获取单元57
秘钥签名库单元51
接收单元56
签名加密单元54
发送单元55

图5

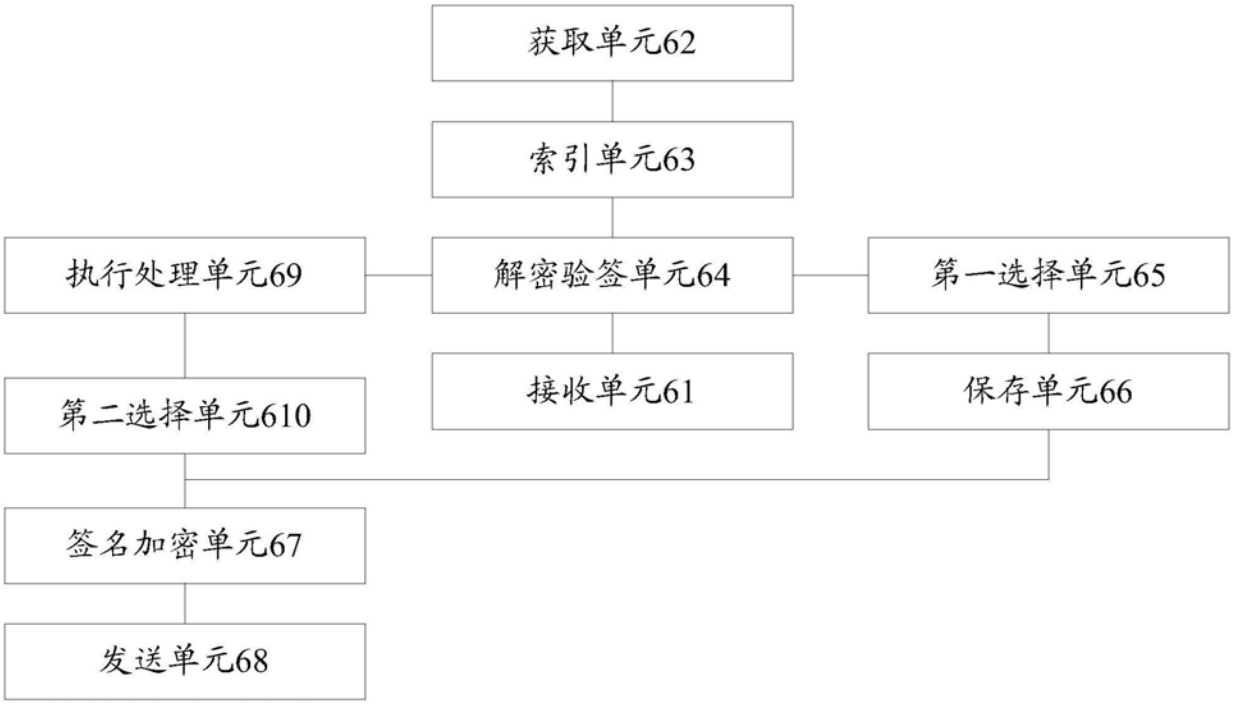

获取单元62
索引单元63
执行处理单元69
解密验签单元64
第一选择单元65
接收单元61
第二选择单元610
保存单元66
签名加密单元67
发送单元68

图6

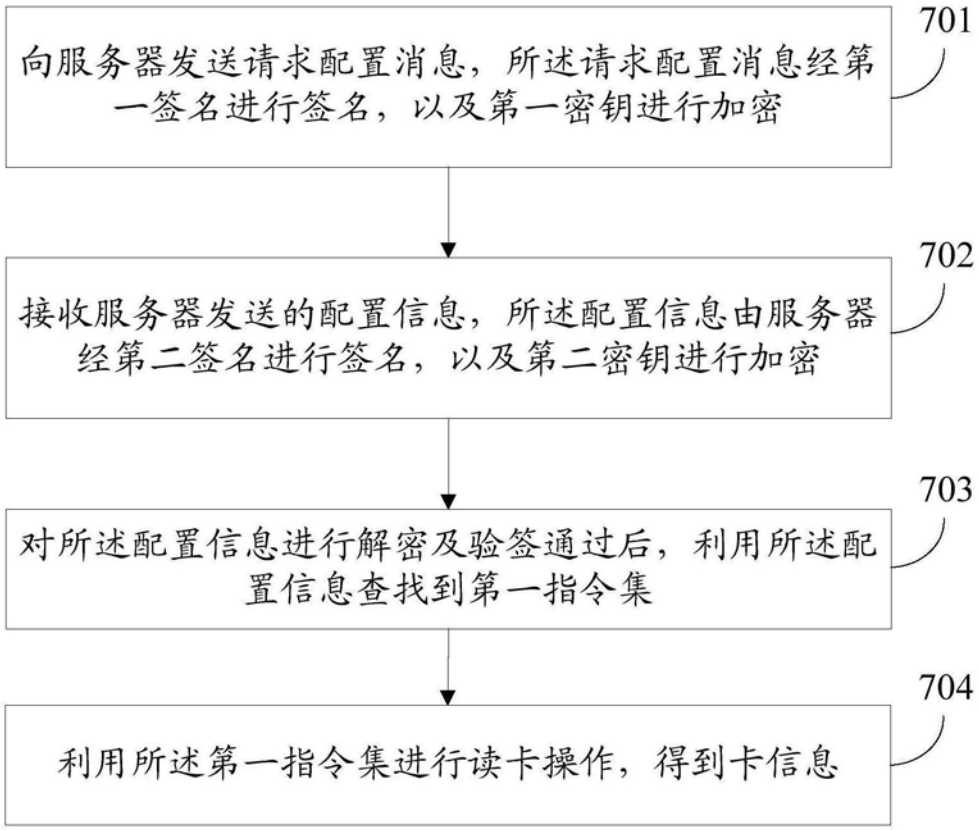

向服务器发送请求配置消息，所述请求配置消息经第一签名进行签名，以及第一密钥进行加密
701
接收服务器发送的配置信息，所述配置信息由服务器经第二签名进行签名，以及第二密钥进行加密
702
对所述配置信息进行解密及验签通过后，利用所述配置信息查找到第一指令集
703
利用所述第一指令集进行读卡操作，得到卡信息
704

图7


发送单元81
接收单元82
查找单元83
读卡单元84

图8