(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 107508796 B
(45)授权公告日 2019.01.04

(21)申请号 201710632680.2

(22)申请日 2017.07.28

(65)同一申请的已公布的文献号
申请公布号 CN 107508796 A

(43)申请公布日 2017.12.22

(73)专利权人 北京明朝万达科技股份有限公司
地址 100097 北京市海淀区蓝靛厂南路25号嘉友国际大厦北区2层

(72)发明人 龚升俊 王志海 喻波 王志华 秦凯

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 莎日娜

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 106603485 A,2017.04.26,
CN 103812871 A,2014.05.21,
CN 101114450 A,2008.01.30,
CN 101242629 A,2008.08.13,
CN 104104672 A,2014.10.15,
CN 104618109 A,2015.05.13,
CN 105577768 A,2016.05.11,
CN 1764195 A,2006.04.26,
CN 1937489 A,2007.03.28,
CN 106131013 A,2016.11.16,
CN 1679271 A,2005.10.05,
CN 101322347 A,2008.12.10,
CN 101465732 A,2009.06.24,
CN 101496338 A,2009.07.29,
CN 101527629 A,2009.09.09,
CN 102412967 A,2012.04.11,
CN 103051459 A,2013.04.17,
CN 101895882 A,2010.11.24,
CN 106254327 A,2016.12.21,
CN 104468126 A,2015.03.25,
WO 2011114460 A1,2011.09.22,
US 2014136853 A1,2014.05.15,

审查员 舒思

权利要求书3页 说明书10页 附图5页

(54)发明名称

一种数据通信方法和装置

(57)摘要

本发明提供了一种数据通信方法和装置，该方法包括：发送身份认证请求至服务器，身份认证请求包括用户公钥信息；接收身份认证请求的认证响应信息，认证响应信息包括服务器公钥信息；保存服务器公钥信息；发送密钥协商请求至服务器，密钥协商请求包括用户加密信息；接收密钥协商请求的协商响应信息，协商响应信息包括：通信密钥的加密信息；根据协商响应信息确定通信密钥；按照预设加密策略，生成多种等级的加密方式；根据业务数据的安全级别选择目标等级的加密方式；采用目标等级的加密方式对业务数据进行加密并将目标等级和加密后的业务数据发送至服务器。本发明能够提升加密强度和加密灵活性。

CN 107508796 B

1.一种数据通信方法,应用于移动终端,所述移动终端安装有加密卡,其特征在于,包括:

发送身份认证请求至服务器,所述身份认证请求包括:用户公钥信息;

接收身份认证请求的认证响应信息,所述认证响应信息包括:服务器公钥信息;

保存所述服务器公钥信息;

发送密钥协商请求至所述服务器,所述密钥协商请求包括:用户加密信息,所述用户加密信息为采用所述服务器公钥信息加密后的用户信息;

接收所述密钥协商请求的协商响应信息,所述协商响应信息包括:通信密钥的加密信息,其中,通信密钥为所述服务器随机生成的密钥;

根据所述协商响应信息确定通信密钥;

按照预设加密策略,生成多种等级的加密方式,其中,所述预设加密策略中的加密原则选自以下多种加密原则中的一种或多种:采用所述服务器公钥加密的加密原则、采用所述通信密钥加密的加密原则、添加用户签名信息的加密原则、在加密卡中加密的加密原则;

根据业务数据的安全级别选择目标等级的加密方式;

采用所述目标等级的加密方式对所述业务数据进行加密并将所述目标等级和加密后的所述业务数据发送至所述服务器。

2.根据权利要求1所述的方法,其特征在于,所述认证响应信息还包括:服务器签名信息,所述服务器签名信息为预先采用服务器私钥信息对服务器信息的签名;

所述保存所述服务器公钥信息之前,所述方法还包括:

根据所述服务器公钥信息和预先保存的服务器信息,对所述服务器签名信息进行签名验证;

所述保存所述服务器公钥信息,包括:

若所述服务器的签名验证通过,则保存所述服务器公钥信息。

3.根据权利要求1所述的方法,其特征在于,所述协商响应信息还包括:服务器签名信息,所述通信密钥的加密信息为采用所述用户公钥信息加密后的通信密钥;

所述根据所述协商响应信息确定通信密钥,包括:

根据保存的所述服务器公钥信息和预先保存的服务器信息,对所述服务器签名信息进行签名验证;

若对所述服务器的签名验证通过,则将所述通信密钥的加密信息发送至所述加密卡进行解密,并将解密后的通信密钥保存至所述加密卡。

4.根据权利要求1所述的方法,其特征在于,所述将加密后的业务数据发送至所述服务器之后,所述方法还包括:

接收所述服务器的对所述业务数据的业务响应数据,所述业务响应数据包括:采用目标等级的响应加密方式加密后的响应数据;

按照预设响应加密策略,生成多种等级的响应加密方式,其中,所述预设响应加密策略中的加密原则选自以下多种加密原则中的一种或多种:采用所述用户公钥加密的加密原则、采用所述通信密钥加密的加密原则、添加服务器签名信息的加密原则、在加密卡中加密的加密原则。

5.根据权利要求1所述的方法,其特征在于,所述根据所述协商响应信息确定通信密钥

之后，所述方法还包括：

记录确定所述通信密钥的时间点；

若记录的所述时间点距离当前时间点的时间间隔超过预设时长，则中断当前流程，重新发送所述身份认证请求至所述服务器。

6.一种数据通信装置，应用于移动终端，所述数据通信装置包括加密卡，其特征在于，包括：

第一发送模块，用于发送身份认证请求至服务器，所述身份认证请求包括：用户公钥信息；

第一接收模块，用于接收身份认证请求的认证响应信息，所述认证响应信息包括：服务器公钥信息；

保存模块，用于保存所述服务器公钥信息；

第二发送模块，用于发送密钥协商请求至所述服务器，所述密钥协商请求包括：用户加密信息，所述用户加密信息为采用所述服务器公钥信息加密后的用户信息；

第二接收模块，用于接收所述密钥协商请求的协商响应信息，所述协商响应信息包括：通信密钥的加密信息，其中，通信密钥为所述服务器随机生成的密钥；

确定模块，用于根据所述协商响应信息确定通信密钥；

第一生成模块，用于按照预设加密策略，生成多种等级的加密方式，其中，所述预设加密策略中的加密原则选自以下多种加密原则中的一种或多种：采用所述服务器公钥加密的加密原则、采用所述通信密钥加密的加密原则、添加用户签名信息的加密原则、在加密卡中加密的加密原则；

选择模块，用于根据业务数据的安全级别选择目标等级的加密方式；

加密发送模块，用于采用所述目标等级的加密方式对所述业务数据进行加密并将所述目标等级和加密后的所述业务数据发送至所述服务器。

7.根据权利要求6所述的装置，其特征在于，所述认证响应信息还包括：服务器签名信息，所述服务器签名信息为预先采用服务器私钥信息对服务器信息的签名，所述装置还包括：

签名模块，用于根据所述服务器公钥信息和预先保存的服务器信息，对所述服务器签名信息进行签名验证；

所述保存模块包括：

保存子模块，用于若所述服务器的签名验证通过，则保存所述服务器公钥信息。

8.根据权利要求6所述的装置，其特征在于，所述协商响应信息还包括：服务器签名信息，所述通信密钥的加密信息为采用所述用户公钥信息加密后的通信密钥，所述确定模块，包括：

签名子模块，用于根据保存的所述服务器公钥信息和预先保存的服务器信息，对所述服务器签名信息进行签名验证；

解密保存子模块，用于若对所述服务器的签名验证通过，则将所述通信密钥的加密信息发送至所述加密卡进行解密，并将解密后的通信密钥保存至所述加密卡。

9.根据权利要求6所述的装置，其特征在于，所述装置还包括：

第三接收模块，用于接收所述服务器的对所述业务数据的业务响应数据，所述业务响

应数据包括:采用目标等级的响应加密方式加密后的响应数据;

第二生成模块,用于按照预设响应加密策略,生成多种等级的响应加密方式,其中,所述预设响应加密策略中的加密原则选自以下多种加密原则中的一种或多种:采用所述用户公钥加密的加密原则、采用所述通信密钥加密的加密原则、添加服务器签名信息的加密原则、在加密卡中加密的加密原则。

10.根据权利要求6所述的装置,其特征在于,所述装置还包括:

记录模块,用于记录确定所述通信密钥的时间点;

中断模块,用于若记录的所述时间点距离当前时间点的时间间隔超过预设时长,则中断当前流程,重新发送所述身份认证请求至所述服务器。

一种数据通信方法和装置

技术领域

[0001] 本发明涉及数据通信技术领域,特别是涉及一种数据通信方法和装置。

背景技术

[0002] 移动互联网时代让人类与信息的关系越加密切,如今,人们的日常生活、工作、娱乐每时每刻都需要通过移动互联网传递信息。在移动互联网产业链下,移动智能终端的重要性越发凸显,已经不可或缺。移动智能终端不仅是社交、通讯、娱乐的工具,也参与到人们的工作中,各种办公软件、政务软件、执法软件等也越来越受欢迎。与此同时,使用移动智能终端在移动互联网下的信息传递也存在安全隐患,移动终端的信息安全已成为研发人员的关注点,所以如何保证移动互联网下信息的安全性,才是移动互联网下衡量软件产品质量的关键因素。

[0003] 为了保证通信数据的安全,有些应用程序(APP,application)也采用了加密技术,但是加密方法一般强度不高,且加密方式单一,对于一些重要数据仍存在安全隐患。例如,图1所示的某交互软件的注册流程:新用户输入用户名密码以及确认密码信息,以及其他注册需要的用户相关信息等,点击注册之后,软件对用户的密码进行加密,组建注册请求报文,并发送至相应服务器;服务器接收到注册请求之后,解析报文,得到新用户的注册信息(包括上述用户名、加密密码等);然后,对用户信息的合法性进行校验之后,就保存该新用户的基本信息,并返回注册结果。

[0004] 在这个过程中注册的用户信息在发送至服务器的过程中是明文传送,只针对一些敏感信息(例如密码、身份证号、真实姓名等)做加密,而该加密方式一般采用Base64加密方法,安全性很低,加密强度不高,且没有完整的密钥管理机制。

[0005] 因此,现有技术中在对通信数据进行加密时,普遍存在着加密强度低、加密灵活性差的问题。

发明内容

[0006] 本发明提供了一种数据通信方法和装置,以解决现有技术中在对通信数据进行加密时所存在的加密强度低、加密灵活性差的问题。

[0007] 为了解决上述问题,根据本发明的一个方面,本发明公开了一种数据通信方法,应用于移动终端,所述移动终端安装有加密卡,所述方法包括:

[0008] 发送身份认证请求至服务器,所述身份认证请求包括:用户公钥信息;

[0009] 接收身份认证请求的认证响应信息,所述认证响应信息包括:服务器公钥信息;

[0010] 保存所述服务器公钥信息;

[0011] 发送密钥协商请求至所述服务器,所述密钥协商请求包括:用户加密信息,所述用户加密信息为采用所述服务器公钥信息加密后的用户信息;

[0012] 接收所述密钥协商请求的协商响应信息,所述协商响应信息包括:通信密钥的加密信息,其中,通信密钥为所述服务器随机生成的密钥;

[0013] 根据所述协商响应信息确定通信密钥；

[0014] 按照预设加密策略，生成多种等级的加密方式，其中，所述预设加密策略中的加密原则选自以下多种加密原则中的一种或多种：采用所述服务器公钥加密的加密原则、采用所述通信密钥加密的加密原则、添加用户签名信息的加密原则、在加密卡中加密的加密原则；

[0015] 根据业务数据的安全级别选择目标等级的加密方式；

[0016] 采用所述目标等级的加密方式对所述业务数据进行加密并将所述目标等级和加密后的所述业务数据发送至所述服务器。

[0017] 根据本发明的另一方面，本发明还公开了一种数据通信装置，应用于移动终端，所述数据通信装置包括加密卡，所述数据通信装置包括：

[0018] 第一发送模块，用于发送身份认证请求至服务器，所述身份认证请求包括：用户公钥信息；

[0019] 第一接收模块，用于接收身份认证请求的认证响应信息，所述认证响应信息包括：服务器公钥信息；

[0020] 保存模块，用于保存所述服务器公钥信息；

[0021] 第二发送模块，用于发送密钥协商请求至所述服务器，所述密钥协商请求包括：用户加密信息，所述用户加密信息为采用所述服务器公钥信息加密后的用户信息；

[0022] 第二接收模块，用于接收所述密钥协商请求的协商响应信息，所述协商响应信息包括：通信密钥的加密信息，其中，通信密钥为所述服务器随机生成的密钥；

[0023] 确定模块，用于根据所述协商响应信息确定通信密钥；

[0024] 第一生成模块，用于按照预设加密策略，生成多种等级的加密方式，其中，所述预设加密策略中的加密原则选自以下多种加密原则中的一种或多种：采用所述服务器公钥加密的加密原则、采用所述通信密钥加密的加密原则、添加用户签名信息的加密原则、在加密卡中加密的加密原则；

[0025] 选择模块，用于根据业务数据的安全级别选择目标等级的加密方式；

[0026] 加密发送模块，用于采用所述目标等级的加密方式对所述业务数据进行加密并将所述目标等级和加密后的所述业务数据发送至所述服务器。

[0027] 与现有技术相比，本发明包括以下优点：

[0028] 本发明通过交换移动终端侧和服务器侧的公钥信息，并依据双方公钥信息协商出通信密钥，进而可以依据服务器公钥加密、通信密钥加密、加密卡中加密和添加用户签名信息的多种加密原则来形成多种等级的加密方式，丰富了加密方式，提高了通信数据的加密强度；并根据业务数据的安全级别灵活选择对应等级的加密方式进行数据的加密传输，增强了数据的加密灵活性，能够根据业务数据的不同层次需求选择不同强度的加密方式进行加密。

附图说明

[0029] 图1是现有技术的一种数据通信方法实施例的流程图；

[0030] 图2是本发明的一种数据通信方法实施例的步骤流程图；

[0031] 图3是本发明的另一种数据通信方法实施例的步骤流程图；

[0032] 图4是本发明的一种数据通信系统实施例的框架图；

[0033] 图5是本发明的一种数据通信装置实施例的结构框图。

具体实施方式

[0034] 为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0035] 参照图2，示出了本发明的一种数据通信方法实施例的步骤流程图，应用于移动终端，所述移动终端安装有加密卡，那么在使用移动终端上安装的应用程序来与服务器进行数据通信时，所述方法具体可以包括如下三个流程：交换公钥流程，密钥协商流程和层次化加密通信流程。

[0036] 其中，交换公钥流程由以下步骤101～步骤103来实现：

[0037] 步骤101，发送身份认证请求至服务器；

[0038] 其中，所述身份认证请求包括：用户公钥信息；

[0039] 步骤102，接收身份认证请求的认证响应信息；

[0040] 所述认证响应信息包括：服务器公钥信息；

[0041] 步骤103，保存所述服务器公钥信息；

[0042] 密钥协商流程由以下步骤104～步骤106来实现：

[0043] 步骤104，发送密钥协商请求至所述服务器；

[0044] 所述密钥协商请求包括：用户加密信息，所述用户加密信息为采用所述服务器公钥信息加密后的用户信息；

[0045] 其中，该用户信息可以是应用程序的用户ID、用户的身份证号等标识性信息。

[0046] 步骤105，接收所述密钥协商请求的协商响应信息；

[0047] 所述协商响应信息包括：通信密钥的加密信息，其中，通信密钥为所述服务器随机生成的密钥；

[0048] 步骤106，根据所述协商响应信息确定通信密钥；

[0049] 层次化加密通信流程由以下步骤107～步骤109来实现：

[0050] 步骤107，按照预设加密策略，生成多种等级的加密方式；

[0051] 其中，所述预设加密策略中的加密原则选自以下多种加密原则中的一种或多种：采用所述服务器公钥加密的加密原则、采用所述通信密钥加密的加密原则、添加用户签名信息的加密原则、在加密卡中加密的加密原则。

[0052] 也就是说，可以从上述多种加密原则中选择一种或多种加密原则来形成不同加密原则的组合，这些组合都是预设加密策略，然后，按照这些预设加密策略中所包含的加密原则的数量多少、加密级别高低，将这些预设加密方式定义为不同等级的加密方式，等级越高的加密方式加密级别越高。

[0053] 步骤108，根据业务数据的安全级别选择目标等级的加密方式；

[0054] 其中，可以根据业务数据的安全级别，按照用户的指令来选择目标等级的加密方式；也可以预先设置的安全级别和加密方式级别之间的对应关系，按照该对应关系来确定业务数据的安全级别所对应的目标等级的加密方式。

[0055] 步骤109，采用所述目标等级的加密方式对所述业务数据进行加密并将所述目标

等级和加密后的所述业务数据发送至所述服务器。

[0056] 借助于本发明上述实施例的技术方案，本发明通过交换移动终端侧和服务器侧的公钥信息，并依据双方公钥信息协商出通信密钥，进而可以依据服务器公钥加密、通信密钥加密、加密卡中加密和添加用户签名信息的多种加密原则来形成多种等级的加密方式，丰富了加密方式，提高了通信数据的加密强度；并根据业务数据的安全级别灵活选择对应等级的加密方式进行数据的加密传输，增强了数据的加密灵活性，能够根据业务数据的不同层次需求选择不同强度的加密方式进行加密。

[0057] 可选地，上述公钥交互流程也是移动终端和服务器之间的身份认证过程，在本实施例中，在该过程中，为了保证公钥信息的交换安全，双方不仅要彼此交换公钥信息，双方在发送自身的公钥信息的同时还会发送各自的签名信息，这样移动终端或服务器就可以使用对方的公钥信息来验证对方发送的签名，称为验签过程，以此来避免接收到被篡改的公钥信息。其中，对方在验签时只能使用签名方的公钥信息才能解密，进而验证签名的完整性与正确性，以此可以确定接收到的公钥信息是否为签名方的公钥信息，避免信息篡改。

[0058] 可选地，所述身份认证请求还包括：用户签名信息，所述用户签名信息为所述加密卡预先采用用户私钥信息对用户信息的签名；

[0059] 这样，可以便于服务器侧对移动终端发送的身份认证请求进行身份认证，避免用户公钥是篡改的，这里服务器需要根据用户公钥信息和预先保存的用户信息来对用户签名信息进行验签，在验签通过后，才会发送认证响应信息。

[0060] 可选地，所述认证响应信息还包括：服务器签名信息，所述服务器签名信息为预先采用服务器私钥信息对服务器信息的签名；

[0061] 这里为了便于移动终端对服务器侧发送的认证响应信息进行身份认证，避免服务器公钥是篡改的，在执行步骤103之前，根据本发明实施例的方法还可以包括：根据所述服务器公钥信息和预先保存的服务器信息，对所述服务器签名信息进行签名验证；

[0062] 那么在执行步骤103所述保存所述服务器公钥信息的步骤时，则是在所述服务器的签名验证通过的情况下，才会保存所述服务器公钥信息。

[0063] 在另一个实施例中，在密钥协商流程中，为了确定协商过程中所接收到的信息都是来自双发(即移动终端和服务器)的，在密钥协商过程中也需要发送各自的签名信息。具体而言：

[0064] 可选地，所述密钥协商请求还包括：用户签名信息；

[0065] 这样，可以使服务器通过对用户签名信息验签，在验签通过的情况下可以确定该密钥协商请求来自与该移动终端。

[0066] 可选地，所述协商响应信息还包括：所述服务器签名信息，其中，所述通信密钥的加密信息为采用所述用户公钥信息加密后的通信密钥；

[0067] 在执行上述步骤106根据所述协商响应信息确定通信密钥时，可以通过以下方式来实现：

[0068] 根据保存的所述服务器公钥信息和预先保存的服务器信息，对所述服务器签名信息进行签名验证；

[0069] 若对所述服务器的签名验证通过，则将所述通信密钥的加密信息发送至所述加密卡进行解密，并将解密后的通信密钥保存至所述加密卡。

[0070] 其中，对通信密钥为用户公钥加密的，因此，可以直接使用加密卡中的用户私钥来对加密后的通信密钥进行解密，并将解密后的通信密钥直接保存在加密卡中。

[0071] 这样，通信密钥的解密过程和保存过程都是直接在加密卡中完成的，而未在移动终端侧完成，保证了通信密钥的安全。

[0072] 可选地，在上述步骤107之后，根据本发明实施例的方法还可以包括：

[0073] 接收所述服务器的对所述业务数据的业务响应数据，所述业务响应数据包括：采用目标等级的响应加密方式加密后的响应数据；

[0074] 按照预设响应加密策略，生成多种等级的响应加密方式，其中，所述预设响应加密策略中的响应加密原则选自以下多种加密原则中的一种或多种：采用所述用户公钥加密的响应加密原则、采用所述通信密钥加密的响应加密原则、添加服务器签名信息的响应加密原则、在加密卡中加密的响应加密原则。

[0075] 也就是说，当移动终端发送至服务器的业务数据为采用目标等级的加密方式加密过的情况下，为了保证数据的双向安全传输，服务器侧也需要采用对应于该目标等级的加密方式的目标等级响应加密方式来对响应数据进行加密，再进行传输。

[0076] 而至于加密方式和响应加密方式之间的等级对应关系来说，以下进行如下说明：

[0077] 服务器公钥加密的加密原则与用户公钥加密的响应加密原则是一对对应的原则；

[0078] 添加用户签名信息的加密原则和添加服务器签名信息的响应加密原则是一对对应的原则；

[0079] 而通信密钥加密的加密原则和通信密钥加密的响应加密原则是一对对应的原则；

[0080] 在加密卡中加密的加密原则和在加密卡中加密的响应加密原则也是一对对应的原则。

[0081] 因此，在形成多种等级的加密方式和多种等级的响应加密方式时，相同等级的加密方式和响应加密方式中所分别构成的原则都是符合上述对应关系的。

[0082] 举例来说，如果移动终端在对业务数据进行加密传输时，采用的目标等级的加密方式包括的加密原则为服务器公钥加密、通信密钥加密，那么服务器在返回该业务数据的响应数据时，则会采用相应的目标等级的响应加密方式，具体包括的响应加密原则为用户公钥加密、通信密钥加密。其他原则的组合类似，在此不再赘述。

[0083] 其中，在上述实施例中，所述加密卡预先保存有用户公钥信息、用户私钥信息。

[0084] 其中，对于上述多种等级的加密方式，这里以几个具体级别的加密方式实例来进行简要说明：

[0085] 级别1：添加用户签名；

[0086] 级别2；采用通信密钥加密；

[0087] 级别3；添加用户签名并且采用通信密钥加密；

[0088] 级别4：采用服务器公钥加密；

[0089] 级别5：添加用户签名并且采用服务器公钥加密；

[0090] 级别6：添加用户签名并且采用服务器公钥加密以及采用通信密钥加密(即签名+双重加密)；

[0091] 级别7：采用通信密钥加密并且在加密卡中加密；

[0092] 级别8：采用服务器公钥加密并且在加密卡中加密；

[0093] 级别9:添加用户签名并且在加密卡中采用服务器公钥、通信密钥加密(即签名+加密卡中双重加密)……..。

[0094] 而各个级别的响应加密方式的构成同理,在此不再赘述。

[0095] 其中,级别9的上述列举的级别中最高的,因为在加密卡中的安全度最高,并且又采用了双重加密以及签名。

[0096] 而针对业务数据的安全需求可以灵活选择不同级别的加密方式。例如采用级别4的加密方式,这种方式由于是非对称加密方式,因此,数据加解密步骤多,速度慢,更适合哪些对数据传输效率要求比较低的数据;例如采用级别2的加密方式,这种方式由于是对称加密方式,因此,数据加解密步骤少,速度快,更适合哪些对数据传输效率要求比较高的数据;例如采用级别7的加密方式,这种方式由于是在加密卡中完成的,因此,数据的安全度相比于在移动终端中完成更高,但是,加密卡存储容量有限,如果是大量的数据进行加密则速度比较么,因此,在加密卡中加密更适合哪些对数据传输安全要求比较高且数据量小的数据;相反,对于数据安全要求一般且数据量较大的数据则可以不在加密卡中完成,而是直接在移动终端中完成。

[0097] 这样,本发明实施例通过形成不同层次等级的加密方式,能够在应用程序的数据与服务器交互时,灵活的选择不同等级的加密方式对待传输的数据进行加密,既保证了数据的安全传输,又能够提升传输效率。

[0098] 可选地,在另一个实施例中,为了进一步的保证数据的安全传输,通信密钥具有时效性,所述根据所述协商响应信息确定通信密钥之后,根据本发明实施例的方法还包括:

[0099] 记录确定所述通信密钥的时间点;

[0100] 若记录的所述时间点距离当前时间点的时间间隔超过预设时长,则中断当前流程,重新发送所述身份认证请求至所述服务器。

[0101] 也就是说,从移动终端侧确定该通信密钥的时间点开始,则开始计时,若从所述时间点到当前时间之间的时间间隔例如超过5分钟,则不论当前流程是哪些步骤,都需要中断该步骤,而是重新回到上述步骤101中,重新发送身份认证请求。

[0102] 下面结合图3所示的安卓(Android)移动终端的APP与该APP的服务器之间的通信流程以及图4所示的通信系统架构图来对本发明实施例的上述方法进行说明。

[0103] 如图4所示,本发明实施例的通信系统包括移动终端的Android APP、服务器和安装在移动终端的TF加密卡驱动接口,其中,服务器的功能包括:身份认证、密钥协商、证书管理和密钥管理;Android APP的功能包括:身份认证、密钥协商、层次化加密管理;TF加密卡驱动接口的功能包括:初始化/反初始化、加密/解密、签名/验签、证书读写。

[0104] TF加密卡相关技术:Android移动的移动终端的身份认证、密钥协商、层次化加密通信的流程都依赖于TF加密卡。TF加密卡以及卡操作相关的驱动库由TF卡厂商提供,此处不做过多说明。本发明实施例的TF加密卡相关技术是指,根据TF卡厂商提供的驱动库进行初始化、安全口令验证、以及公钥证书信息读取、私钥证书的使用(解密、签名等)。

[0105] 如图3所示,基于加密卡的智能手机层次化网络通信方法实现的分为四个部分:TF卡口令验证(图3未示出)、身份认证、密钥协商、与层次化加密通信。

[0106] 1)TF卡口令验证:例如该APP为警务APP,警务人员在登录APP之前,需要先进行TF卡安全口令验证:输入验证口令,如果开卡失败,则登录失败;如果开卡成功,则进行2)身份

认证流程；

[0107] 2)身份认证流程：读取自身的公钥信息，并用自身的私钥信息签名用户ID(用户唯一标识，例如身份证号等)，然后将用户ID、用户公钥信息、用户签名信息组建身份认证请求报文并发送；服务器接收并解析身份认证请求报文，使用得到的用户公钥信息验证用户签名，如果验签失败，则身份认证失败，流程结束；若验签通过则服务器将该移动终端视为合法用户、保存其公钥信息；服务器将用户ID、服务器自身公钥信息、服务器签名信息组建身份认证响应报文并返回；移动终端接收响应信息后，使用得到的服务器公钥信息验证服务器签名，如果验签失败，则服务器的身份认证失败，流程结束；若验签通过则保存服务器公钥信息，整个身份认证过程完成，进入步骤密钥协商流程。

[0108] 3)密钥协商过程是建立在身份认证完成基础之上的。移动终端发送协商请求报文，请求报文具体内容包括：用户ID、使用服务器公钥信息加密的用户敏感信息(即图3中的加密用户信息)、用户签名信息；服务器接收并解析密钥协商请求报文，使用服务器私钥信息解密用户信息，并使用移动终端公钥信息和解密后的用户信息验证用户签名，如果验签失败，则密钥协商失败，流程结束；若验签通过，则将解密后的用户信息更新至数据库，然后使用加密卡(这里服务器侧也安装有加密卡)生成随机的通信密钥；服务器返回协商响应报文，响应报文的具体信息包括：用户ID、使用移动终端公钥信息加密的通信密钥(即通信密钥加密信息)、服务器签名信息；移动终端接收响应报文后，使用服务器的公钥信息验证服务器签名，如果验签失败，则密钥协商失败；如果验签通过，则使用移动终端的私钥信息解密通信密钥，并保存该通信密钥(其中可以对该通信密钥进行加密保存，可以保存在手机上或TF卡上)，密钥协商成功，到此整个登录过程完成。

[0109] 其中，密钥协商的目的是生成本次会话的通信密钥，该通信密钥由服务器生成，使用移动终端公钥证书加密之后再传输给移动终端，移动终端必须使用自身的私钥信息才能解密和使用该密钥，并且，通信密钥具有时效性，一旦超时必须重新进行身份认证和密钥协商流程。

[0110] 4)层次化加密通信过程是建立在密钥协商完成基础之上的。警务人员在成功登录APP之后，可以录入案件信息(案件名称、类型、时间、地点、参与人员、状态、详细描述等信息)，录入完成之后根据业务需要选择适合该案件信息的加密等级。移动终端对这些案件信息使用对应的加密级别加密之后，将用户ID、所用的加密级别(例如加密级别A)、加密后的案件信息、用户签名信息组建案件信息上报请求报文并发送；服务器接收并解析案件信息请求报文，从中获取本次加密使用的加密级别以及加密的案件信息，验证用户签名，如果验签失败，则案件信息上报失败；如果验签通过，则使用加密级别A对应的解密方式解密案件信息，并存储至数据库；对该业务数据(这里的案件信息)进行业务处理，得到结果数据；然后，采用对应等级的响应加密方式来对结果数据进行加密，得到结果数据加密信息；最后，将结果数据加密信息连同服务器签名信息组建为案件信息上报的响应报文，一起发送至移动终端。移动终端对服务器签名验签，具体验签步骤同上，不在赘述，验签通过后，解密该结果数据。

[0111] 本发明实施例的数据通信方法适配Android手机，并使TF加密卡作为底层加解密手段，将Android应用产生的网络流量根据业务需要或定义进行层次化划分(如定义为机密、秘密等)，根据不同层次进行不同强度的加密，依靠服务器进行密钥协商与交换等，从而

保证不同安全需要或级别的网络数据流量获得相应的通信保密强度，能够对不同安全需要或级别的业务数据，灵活选择不同加密强度的加密方式进行加密传输。

[0112] 并且，Android移动终端基于TF加密卡与服务器进行身份认证，既确认了认证双方的身份，有保证了认证登录流程的安全性；非对称密钥的加密与签名、以及配合具有时效性的协商密钥组合使用，使得加密方式更加多样化、能够保障更多场景下的数据安全性与完整性；对企业、公安、政府等办公类软件尤为重要，更加注重用户与数据的信息保护。

[0113] 需要说明的是，对于方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明实施例并不受所描述的动作顺序的限制，因为依据本发明实施例，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作并不一定是本发明实施例所必须的。

[0114] 与上述本发明实施例所提供的方法相对应，参照图5，示出了本发明一种数据通信装置实施例的结构框图，应用于移动终端，所述数据通信装置包括加密卡，所述装置具体可以包括如下模块：

[0115] 第一发送模块51，用于发送身份认证请求至服务器，所述身份认证请求包括：用户公钥信息；

[0116] 第一接收模块52，用于接收身份认证请求的认证响应信息，所述认证响应信息包括：服务器公钥信息；

[0117] 保存模块53，用于保存所述服务器公钥信息；

[0118] 第二发送模块54，用于发送密钥协商请求至所述服务器，所述密钥协商请求包括：用户加密信息，所述用户加密信息为采用所述服务器公钥信息加密后的用户信息；

[0119] 第二接收模块55，用于接收所述密钥协商请求的协商响应信息，所述协商响应信息包括：通信密钥的加密信息，其中，通信密钥为所述服务器随机生成的密钥；

[0120] 确定模块56，用于根据所述协商响应信息确定通信密钥；

[0121] 第一生成模块57，用于按照预设加密策略，生成多种等级的加密方式，其中，所述预设加密策略中的加密原则选自以下多种加密原则中的一种或多种：采用所述服务器公钥加密的加密原则、采用所述通信密钥加密的加密原则、添加用户签名信息的加密原则、在加密卡中加密的加密原则；

[0122] 选择模块58，用于根据业务数据的安全级别选择目标等级的加密方式；

[0123] 加密发送模块59，用于采用所述目标等级的加密方式对所述业务数据进行加密并将所述目标等级和加密后的所述业务数据发送至所述服务器。

[0124] 可选地，所述认证响应信息还包括：服务器签名信息，所述服务器签名信息为预先采用服务器私钥信息对服务器信息的签名，所述装置还包括：

[0125] 签名模块，用于根据所述服务器公钥信息和预先保存的服务器信息，对所述服务器签名信息进行签名验证；

[0126] 所述保存模块53包括：

[0127] 保存子模块，用于若所述服务器的签名验证通过，则保存所述服务器公钥信息。

[0128] 可选地，所述协商响应信息还包括：所述服务器签名信息，所述通信密钥的加密信息为采用所述用户公钥信息加密后的通信密钥，所述确定模块56，包括：

[0129] 签名子模块，用于根据保存的所述服务器公钥信息和预先保存的服务器信息，对所述服务器签名信息进行签名验证；

[0130] 解密保存子模块，用于若对所述服务器的签名验证通过，则将所述通信密钥的加密信息发送至所述加密卡进行解密，并将解密后的通信密钥保存至所述加密卡。

[0131] 可选地，所述装置还包括：

[0132] 第三接收模块，用于接收所述服务器的对所述业务数据的业务响应数据，所述业务响应数据包括：采用目标等级的响应加密方式加密后的响应数据；

[0133] 第二生成模块，用于按照预设响应加密策略，生成多种等级的响应加密方式，其中，所述预设响应加密策略中的加密原则选自以下多种加密原则中的一种或多种：采用所述用户公钥加密的加密原则、采用所述通信密钥加密的加密原则、添加服务器签名信息的加密原则、在加密卡中加密的加密原则。

[0134] 可选地，所述装置还包括：

[0135] 记录模块，用于记录确定所述通信密钥的时间点；

[0136] 中断模块，用于若记录的所述时间点距离当前时间点的时间间隔超过预设时长，则中断当前流程，重新发送所述身份认证请求至所述服务器。

[0137] 对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0138] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0139] 本领域内的技术人员应明白，本发明实施例的实施例可提供为方法、装置、或计算机程序产品。因此，本发明实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0140] 本发明实施例是参照根据本发明实施例的方法、终端设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理终端设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0141] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理终端设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0142] 这些计算机程序指令也可装载到计算机或其他可编程数据处理终端设备上，使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0143] 尽管已描述了本发明实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明实施例范围的所有变更和修改。

[0144] 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

[0145] 以上对本发明所提供的一种数据通信方法和一种数据通信装置，进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

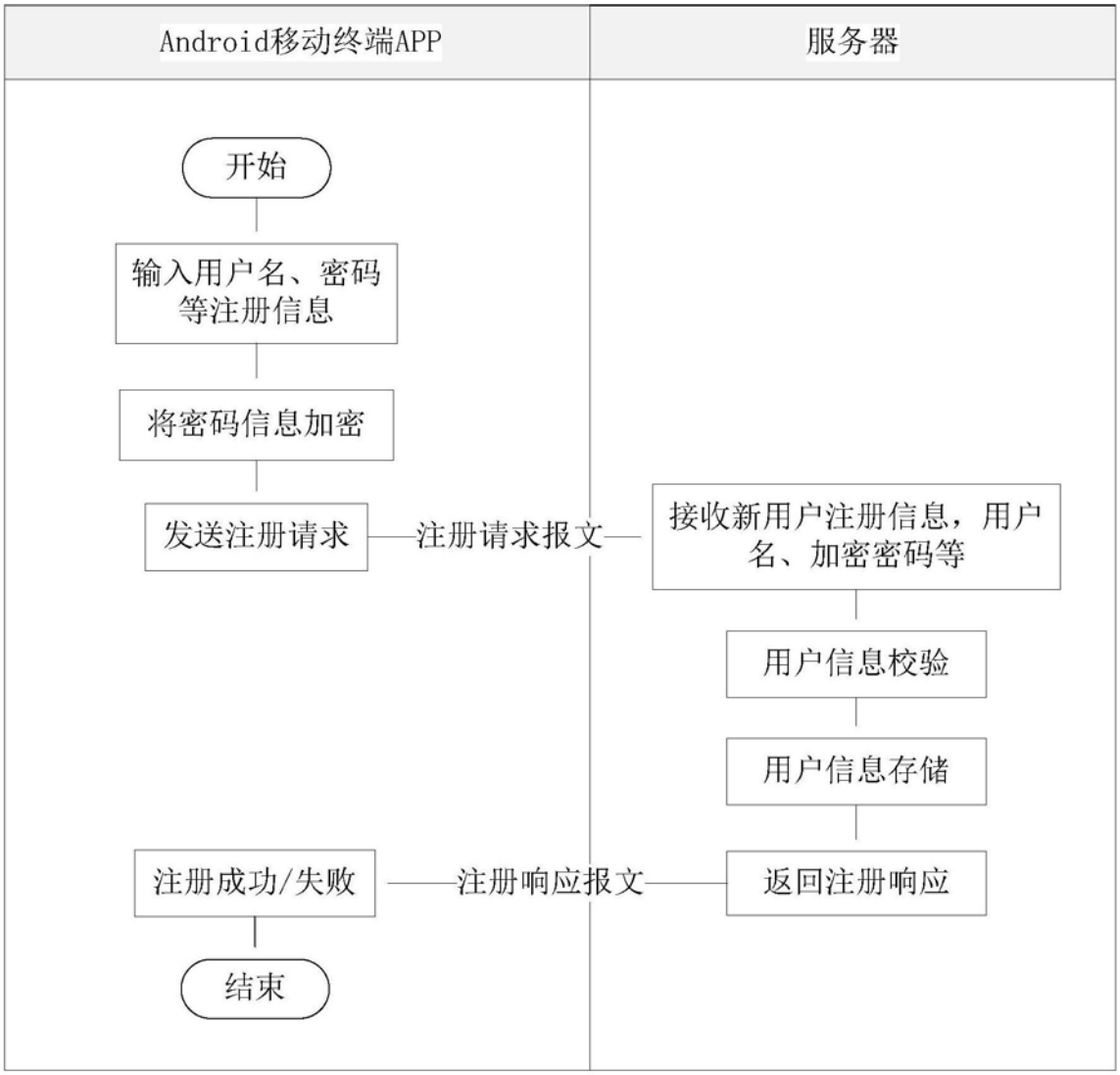
Android移动终端APP
服务器
开始
输入用户名、密码等注册信息
将密码信息加密
发送注册请求
注册请求报文
接收新用户注册信息，用户名、加密密码等
用户信息校验
用户信息存储
返回注册响应
注册响应报文
注册成功/失败
结束

图1

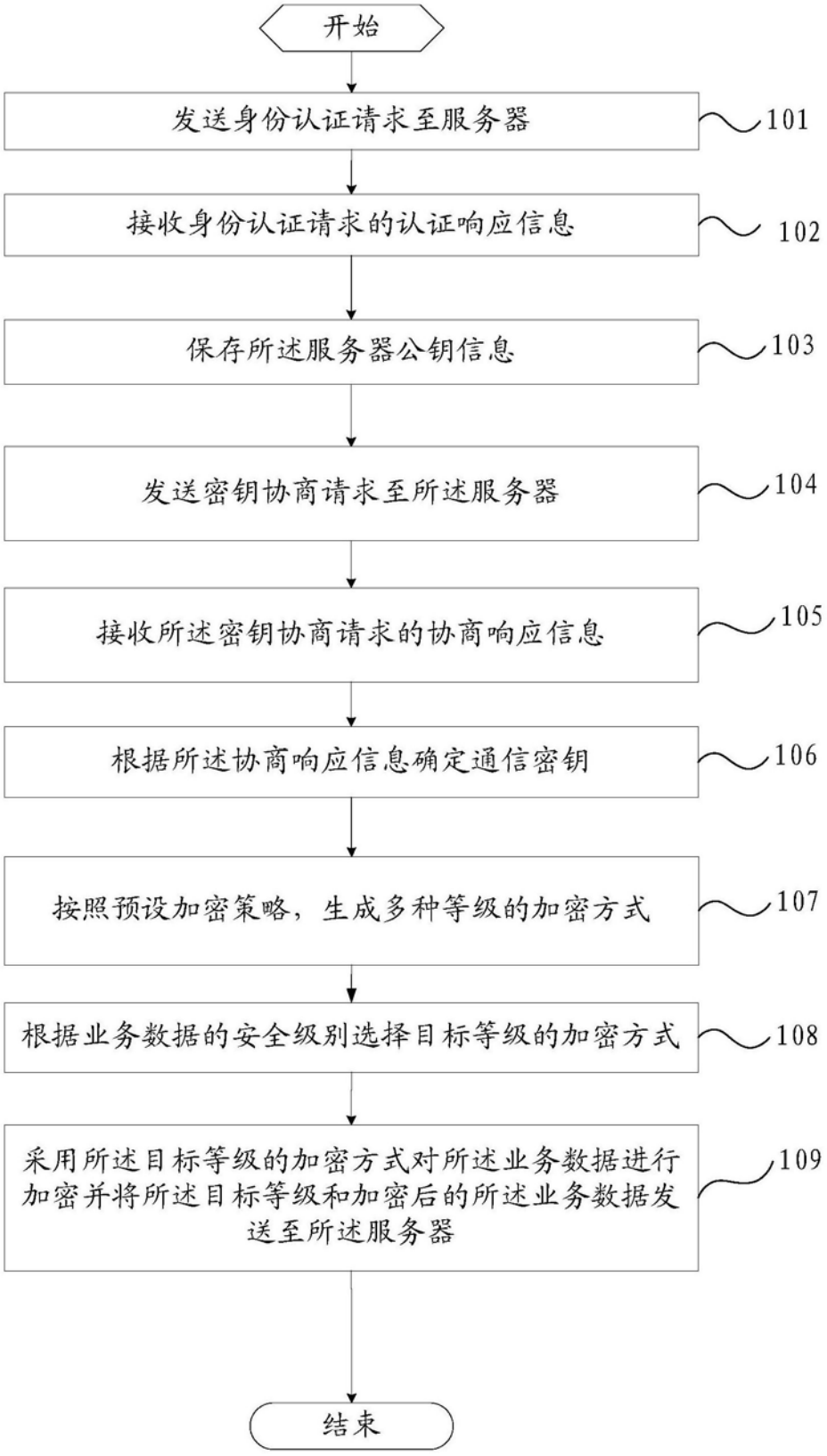
开始
发送身份认证请求至服务器
101
接收身份认证请求的认证响应信息
102
保存所述服务器公钥信息
103
发送密钥协商请求至所述服务器
104
接收所述密钥协商请求的协商响应信息
105
根据所述协商响应信息确定通信密钥
106
按照预设加密策略，生成多种等级的加密方式
107
根据业务数据的安全级别选择目标等级的加密方式
108
采用所述目标等级的加密方式对所述业务数据进行加密并将所述目标等级和加密后的所述业务数据发送至所述服务器
109
结束

图2

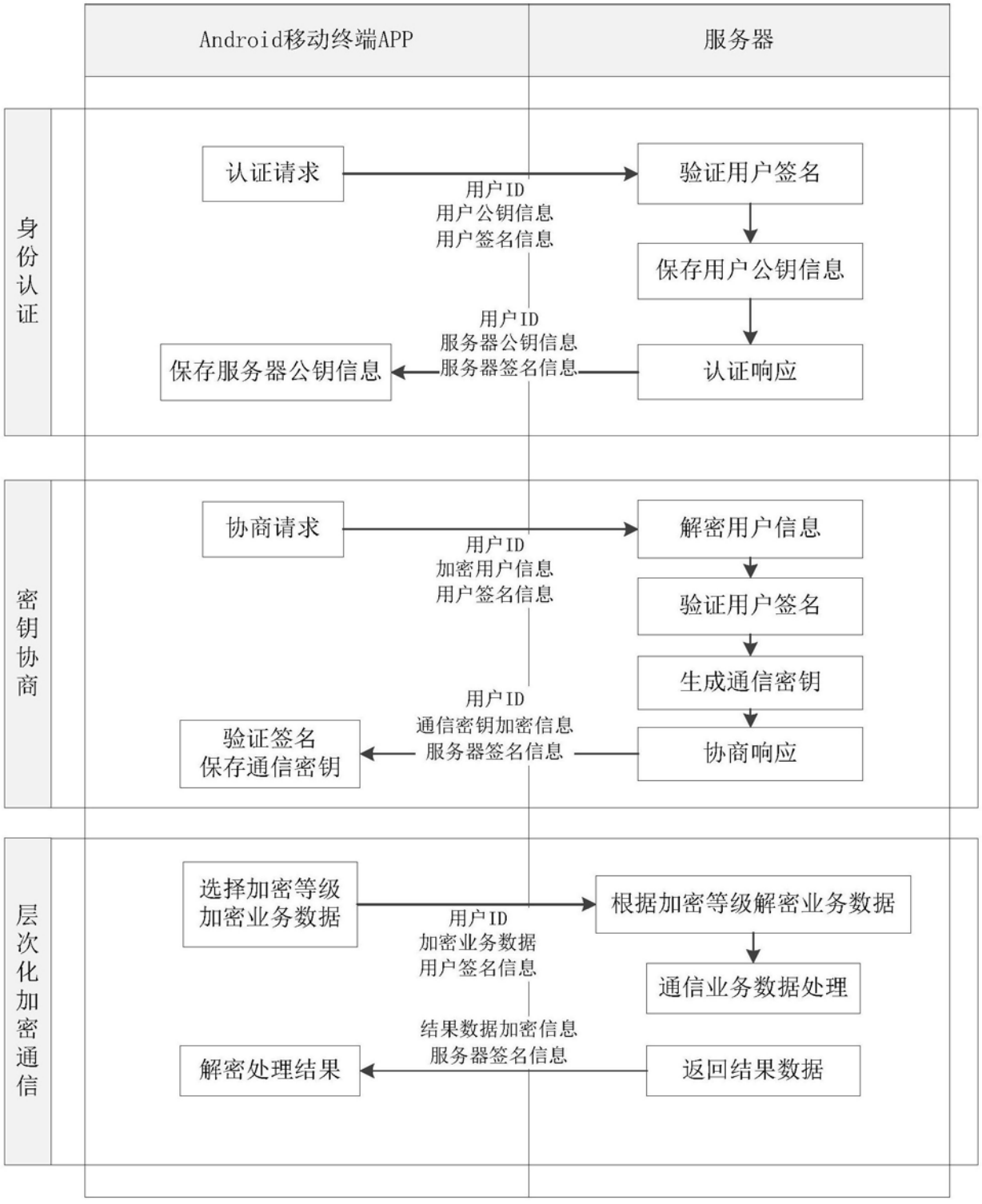
Android移动终端APP
服务器
身份认证
认证请求
用户ID
用户公钥信息
用户签名信息
验证用户签名
保存用户公钥信息
用户ID
服务器公钥信息
服务器签名信息
保存服务器公钥信息
认证响应
密钥协商
协商请求
用户ID
加密用户信息
用户签名信息
解密用户信息
验证用户签名
生成通信密钥
用户ID
通信密钥加密信息
服务器签名信息
验证签名
保存通信密钥
协商响应
层次化加密通信
选择加密等级
加密业务数据
用户ID
加密业务数据
用户签名信息
根据加密等级解密业务数据
通信业务数据处理
结果数据加密信息
服务器签名信息
解密处理结果
返回结果数据

图3


服务器
身份认证
密钥协商
证书管理
密钥管理
Android APP
身份认证
密钥协商
层次化加密管理
TF加密卡驱动接口
初始化/反初始化
加密/解密
签名/验签
证书读写

图4

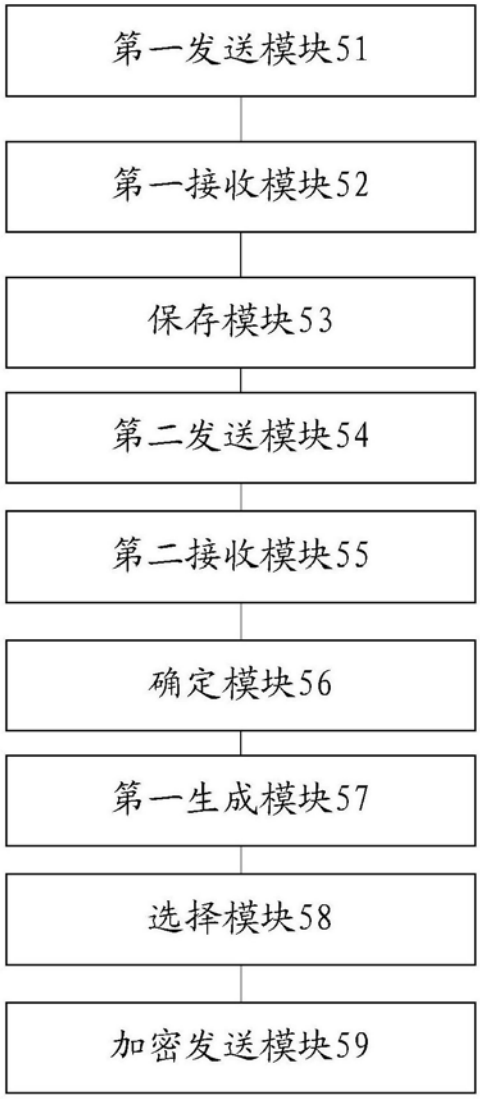
第一发送模块51
第一接收模块52
保存模块53
第二发送模块54
第二接收模块55
确定模块56
第一生成模块57
选择模块58
加密发送模块59

图5