



(12)发明专利申请

(10)申请公布号 CN 106332053 A

(43)申请公布日 2017.01.11

(21)申请号 201610795801.0

(22)申请日 2016.08.31

(71)申请人 宇龙计算机通信科技(深圳)有限公司

地址 518057 广东省深圳市南山区高新技术工业园北区酷派信息港1栋6层

(72)发明人 赵龙凯

(74)专利代理机构 工业和信息化部电子专利中心 11010

代理人 吴永亮

(51)Int.Cl.

H04W 8/18(2009.01)

H04W 8/20(2009.01)

H04W 12/02(2009.01)

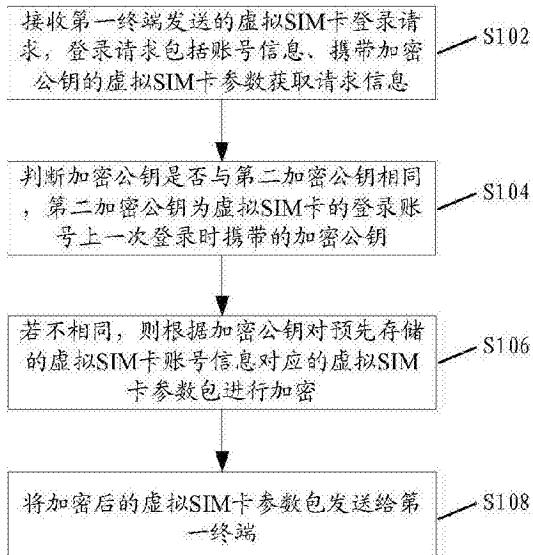
权利要求书2页 说明书6页 附图2页

(54)发明名称

虚拟SIM卡的数据传输方法、服务器及终端

(57)摘要

本发明公开了一种虚拟SIM卡的数据传输方法、服务器及终端，其中，该方法包括：接收第一终端发送的虚拟SIM卡登录请求，登录请求包括账号信息、携带加密公钥的虚拟SIM卡参数获取请求信息；判断加密公钥是否与第二加密公钥相同，第二加密公钥为虚拟SIM卡的登录账号上一次登录时携带的加密公钥；若不相同，则根据加密公钥对预先存储的虚拟SIM卡账号信息对应的虚拟SIM卡参数包进行加密；将加密后的虚拟SIM卡参数包发送给第一终端。本发明接收来自第一终端的加密公钥，并判断该加密公钥是否与上一次登陆时携带的加密公钥相同，如果不相同，就使用该加密公钥加密虚拟SIM卡参数包，并发给第一终端，解决了现有技术的问题。



1.一种虚拟用户身份模块SIM卡的数据传输方法,其特征在于,所述方法包括:

接收第一终端发送的虚拟SIM卡登录请求,所述登录请求包括账号信息、携带加密公钥的虚拟SIM卡参数获取请求信息;

判断所述加密公钥是否与第二加密公钥相同,所述第二加密公钥为所述虚拟SIM卡的登录账号上一次登录时携带的加密公钥;

在所述加密公钥与所述第二加密公钥不相同的情况下,根据所述加密公钥对预先存储的所述虚拟SIM卡账号信息对应的虚拟SIM卡参数包进行加密;

将加密后的虚拟SIM卡参数包发送给第一终端。

2.根据权利要求1所述的方法,其特征在于,在所述接收第一终端发送的虚拟SIM卡登录请求之后,所述判断所述加密公钥是否与第二加密公钥相同之前,所述方法还包括:

根据所述账号信息检测是否存在已经登录同一账号的第二终端;

在不存在已经登录同一账号的第二终端的情况下,执行所述判断所述加密公钥是否与第二加密公钥相同的步骤;

在存在已经登录同一账号的第二终端的情况下,发送提示信息给第一终端,并根据第一终端的反馈结果执行相应的操作。

3.根据权利要求1所述的方法,其特征在于,所述方法还包括:

在所述加密公钥与所述第二加密公钥相同的情况下,提示第一终端登录不成功。

4.一种虚拟用户身份模块SIM卡的数据传输方法,其特征在于,所述方法包括:

第一终端接收用户输入的虚拟SIM卡登录账号信息;

第一终端根据虚拟SIM卡登录账号信息生成一对公私钥对,所述公私钥对包括加密公钥和解密私钥;

第一终端发送虚拟SIM卡登录请求至服务器,所述虚拟SIM卡登录请求包括账号信息、携带所述加密公钥的虚拟SIM卡参数获取请求信息;

在服务器判断所述加密公钥与第二加密公钥不相同的情况下,第一终端接收服务器下发的虚拟SIM卡参数包,所述第二加密公钥为所述虚拟SIM卡的登录账号上一次登录时携带的加密公钥;

第一终端根据所述解密私钥对所述虚拟SIM卡参数包进行解密,以获取虚拟SIM卡参数信息。

5.根据权利要求4所述的方法,其特征在于,第一终端发送虚拟SIM卡登录请求至服务器之后,还包括:

在服务器判断所述加密公钥与第二加密公钥相同的情况下,第一终端接收服务器发送的已经登录同一账号的第二终端的提示信息;

在第一终端接收到所述提示信息的情况下,第一终端判断是否接收到用户输入的注销信息,其中,所述注销信息用于注销第二终端的登录信息;

第一终端在接收到所述注销信息时,将所述注销信息反馈至服务器。

6.一种服务器,其特征在于,包括:

第一接收模块,用于接收第一终端发送的虚拟SIM卡登录请求,所述登录请求包括账号信息、携带加密公钥的虚拟SIM卡参数获取请求信息;

密钥判断模块,用于判断所述加密公钥是否与第二加密公钥相同,所述第二加密公钥

为所述虚拟SIM卡的登录账号上一次登录时携带的加密公钥；

加密模块，用于在所述加密公钥与所述第二加密公钥不相同的情况下，根据所述加密公钥对预先存储的所述虚拟SIM卡账号信息对应的虚拟SIM卡参数包进行加密；

第一发送模块，用于将加密后的虚拟SIM卡参数包发送给第一终端。

7. 根据权利要求6所述的服务器，其特征在于，所述装置还包括：

检测模块，用于在所述接收第一终端发送的虚拟SIM卡登录请求之后，根据所述账号信息检测是否存在已经登录同一账号的第二终端，并在不存在所述第二终端的情况下，触发所述密钥判断模块工作；

所述第一发送模块，还用于在存在已经登录同一账号的第二终端的情况下，发送提示信息给第一终端，并根据第一终端的反馈结果执行相应的操作。

8. 根据权利要求6所述的服务器，其特征在于，

所述第一发送模块，还用于在确定所述加密公钥与所述第二加密公钥相同的情况下，提示所述第一终端登录不成功。

9. 一种终端，其特征在于，包括：

第二接收模块，用于接收用户输入的虚拟SIM卡登录账号信息；

生成模块，用于根据虚拟SIM卡登录账号信息生成一对公私钥对，所述公私钥对包括加密公钥和解密私钥；

第二发送模块，用于发送虚拟SIM卡登录请求至服务器，所述虚拟SIM卡登录请求包括账号信息、携带所述加密公钥的虚拟SIM卡参数获取请求信息；

第三接收模块，用于在服务器判断所述加密公钥与第二加密公钥不相同的情况下，接收服务器下发的虚拟SIM卡参数包，所述第二加密公钥为所述虚拟SIM卡的登录账号上一次登录时携带的加密公钥；

解密模块，用于根据所述解密私钥对所述虚拟SIM卡参数包进行解密，以获取虚拟SIM卡参数信息。

10. 根据权利要求9所述的终端，其特征在于，还包括：

所述第三接收模块，还用于在服务器判断所述加密公钥与第二加密公钥相同的情况下，接收服务器发送的存在已经登录同一账号的第二终端的提示信息；

消息判断模块，用于在接收到所述提示信息的情况下，判断是否接收到用户输入的注销信息，其中，所述注销信息用于注销第二终端的登录信息；

所述第二发送模块，还用于在接收到所述注销信息时，将所述注销信息反馈至服务器。

虚拟SIM卡的数据传输方法、服务器及终端

技术领域

[0001] 本发明涉及移动通讯领域,特别是涉及一种虚拟SIM(客户识别模块或用户身份模块,Subscriber Identification Module)卡的数据传输方法、服务器及终端。

背景技术

[0002] 实体SIM卡在使用时,在需要切换移动终端的情况下,可以将SIM卡拨出后在新的移动终端中插入,然后走完正常的检卡流程,SIM卡就可以在新的移动终端上使用。

[0003] 为了解决现有需要查卡切换的问题,提出了一种Softsim(虚拟SIM)技术,然而,Softsim作为一种基于纯软件的SIM卡技术,移动终端产生的私钥只保留在自己当前所用的移动终端的modem(调制解调器)模块中。这样如果当用户因某种原因(比如使用过程中电量耗尽、移动终端突然损坏)想更换移动终端时,那此时更换的新移动终端上没有对应Softsim相关的参数,所以在新的移动终端上将无法利用这些SIM卡参数接入网络享受服务。

[0004] 此时,如果要想在新移动终端上使用Softsim服务,终端只能重新登录到Softsim管理中心,获取Softsim的相关参数数据包。网络服务器仍然是以之前的公钥进行加密,但是此时新的移动终端上并未存储之前的私钥信息,从而导致无法解密获取到Softsim卡参数,从而无法在新移动终端上使用之前自己所订阅的Softsim服务,给用户的使用带来了很大的不便。

[0005] 为了解决上述问题,现有技术将原有移动终端上产生的私钥进行加密并在云端备份,当用户更换移动终端时首先需要在云端下载并解密获取到私钥,之后当移动终端再次从运营商的云端下载用之前的公钥加密的Softsim卡参数包时,就可以用此私钥进行解密,从而获取到Softsim卡参数,实现了不同移动终端的Softsim的切换。但是,私钥作为用户非常重要的信息,上传云端可能存在被别人窃取的风险,一旦被别人盗取,那么自己的Softsim就很容易被别人复制窃取。因此,现有技术中没有一种方法能够让用户在更换移动终端时,安全的获取到Softsim卡参数来完成移动终端的切换。

发明内容

[0006] 本发明提供了一种虚拟SIM卡的数据传输方法、服务器及终端,以至少解决现有技术切换移动终端时,获取Softsim卡参数的过程中存在较大安全隐患,用户体验较低的问题。

[0007] 一方面,本发明提供一种虚拟用户身份模块SIM卡的数据传输方法,所述方法包括:接收第一终端发送的虚拟SIM卡登录请求,所述登录请求包括账号信息、携带加密公钥的虚拟SIM卡参数获取请求信息;判断所述加密公钥是否与第二加密公钥相同,所述第二加密公钥为所述虚拟SIM卡的登录账号上一次登录时携带的加密公钥;在所述加密公钥与所述第二加密公钥不相同的情况下,根据所述加密公钥对预先存储的所述虚拟SIM卡账号信息对应的虚拟SIM卡参数包进行加密;将加密后的虚拟SIM卡参数包发送给第一终端。

[0008] 可选的，在所述接收第一终端发送的虚拟SIM卡登录请求之后，所述判断所述加密公钥是否与第二加密公钥相同之前，所述方法还包括：根据所述账号信息检测是否存在已经登录同一账号的第二终端；在不存在已经登录同一账号的第二终端的情况下，执行所述判断所述加密公钥是否与第二加密公钥相同的步骤；在存在已经登录同一账号的第二终端的情况下，发送提示信息给第一终端，并根据第一终端的反馈结果执行相应的操作。

[0009] 可选的，所述方法还包括：在所述加密公钥与所述第二加密公钥相同的情况下，提示第一终端登录不成功。

[0010] 另一方面，本发明还提供了一种虚拟用户身份模块SIM卡的数据传输方法，所述方法包括：第一终端接收用户输入的虚拟SIM卡登录账号信息；第一终端根据虚拟SIM卡登录账号信息生成一对公私钥对，所述公私钥对包括加密公钥和解密私钥；第一终端发送虚拟SIM卡登录请求至服务器，所述虚拟SIM卡登录请求包括账号信息、携带加密公钥的虚拟SIM卡参数获取请求信息；在服务器判断所述加密公钥与第二加密公钥不相同的情况下，第一终端接收服务器下发的虚拟SIM卡参数包，所述第二加密公钥为所述虚拟SIM卡的登录账号上一次登录时携带的加密公钥；第一终端根据解密私钥对所述虚拟SIM卡参数包进行解密进而获取虚拟SIM卡参数信息。

[0011] 可选的，第一终端发送虚拟SIM卡登录请求至服务器之后，还包括：在服务器判断所述加密公钥与第二加密公钥相同的情况下，第一终端接收服务器发送的存在已经登录同一账号的第二终端的提示信息；在第一终端接收到所述提示信息的情况下，第一终端判断是否接收到用户输入的注销信息，其中，所述注销信息用于注销第二终端的登录信息；第一终端在接收到所述注销信息时，将所述注销信息反馈至服务器。

[0012] 可选的，所述方法还包括：第一终端接收服务器判断所述加密公钥与所述第二加密公钥相同后发送的登录不成功的提示信息。

[0013] 另一方面，本发明还提供了一种服务器，包括：第一接收模块，用于接收第一终端发送的虚拟SIM卡登录请求，所述登录请求包括账号信息、携带加密公钥的虚拟SIM卡参数获取请求信息；密钥判断模块，用于判断所述加密公钥是否与第二加密公钥相同，所述第二加密公钥为所述虚拟SIM卡的登录账号上一次登录时携带的加密公钥；加密模块，用于在所述加密公钥与所述第二加密公钥不相同的情况下，根据所述加密公钥对预先存储的所述虚拟SIM卡账号信息对应的虚拟SIM卡参数包进行加密；第一发送模块，用于将加密后的虚拟SIM卡参数包发送给第一终端。

[0014] 可选的，所述装置还包括：检测模块，用于在所述接收第一终端发送的虚拟SIM卡登录请求之后，根据所述账号信息检测是否存在已经登录同一账号的第二终端，并在不存在所述第二终端的情况下，触发所述密钥判断模块工作；所述第一发送模块，还用于在存在已经登录同一账号的第二终端的情况下，发送提示信息给第一终端，并根据第一终端的反馈结果执行相应的后续操作。

[0015] 可选的，所述第一发送模块，还用于在确定所述加密公钥与所述第二加密公钥相同的情况下，提示所述第一终端登录不成功。

[0016] 另一方面，本发明还提供了一种终端，包括：第二接收模块，用于接收用户输入的虚拟SIM卡登录账号信息；生成模块，用于根据虚拟SIM卡登录账号信息生成一对公私钥对，所述公私钥对包括加密公钥和解密私钥；第二发送模块，用于发送虚拟SIM卡登录请求至服

务器,所述虚拟SIM卡登录请求包括账号信息、携带加密公钥的虚拟SIM卡参数获取请求信息;第三接收模块,用于在服务器判断所述加密公钥与第二加密公钥不相同的情况下,接收服务器下发的虚拟SIM卡参数包,所述第二加密公钥为所述虚拟SIM卡的登录账号上一次登录时携带的加密公钥;解密模块,用于根据解密私钥对所述虚拟SIM卡参数包进行解密进而获取虚拟SIM卡参数信息。

[0017] 可选的,终端还包括:所述第三接收模块,还用于在服务器判断所述加密公钥与第二加密公钥相同的情况下,接收服务器发送的存在已经登录同一账号的第二终端的提示信息;消息判断模块,用于在接收到所述提示信息的情况下,判断是否接收到用户输入的注销信息,其中,所述注销信息用于注销第二终端的登录信息;所述第二发送模块,还用于在接收到所述注销信息时,将所述注销信息反馈至服务器。

[0018] 本发明接收来自第一终端的加密公钥,并判断该加密公钥是否与上一次登陆时携带的加密公钥相同,如果不相同,就使用该加密公钥加密虚拟SIM卡参数包,并发给第一终端,每次切换终端后,终端都会发送新生成的加密公钥给服务器侧,服务器侧都使用新的加密公钥来加密虚拟SIM卡参数包,获取虚拟SIM卡参数包的过程较为安全,解决了现有技术切换移动终端时,获取Softsim卡参数的过程中存在较大安全隐患,用户体验较低的问题。

附图说明

[0019] 通过阅读下文优选实施方式的详细描述,各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的,而并不认为是对本发明的限制。而且在整个附图中,用相同的参考符号表示相同的部件。在附图中:

- [0020] 图1是本发明第一实施例中虚拟SIM卡的数据传输方法的流程图;
- [0021] 图2是本发明第二实施例中虚拟SIM卡的数据传输方法的流程图;
- [0022] 图3是本发明第三实施例中服务器的结构示意图;
- [0023] 图4是本发明第三实施例中服务器的优选结构示意图;
- [0024] 图5是本发明第四实施例中终端的结构示意图;
- [0025] 图6是本发明第五实施例中Softsim在不同终端切换的方法流程图。

具体实施方式

[0026] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例,然而应当理解,可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反,提供这些实施例是为了能够更透彻地理解本公开,并且能够将本公开的范围完整的传达给本领域的技术人员。

[0027] 为了解决现有技术切换移动终端时,获取Softsim卡参数的过程中存在较大安全隐患,用户体验较低的问题,本发明提供了一种虚拟SIM卡的数据传输方法、服务器及终端,以下结合附图以及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不限定本发明。

[0028] 本发明第一实施例提供一种虚拟SIM卡的数据传输方法,该方法的流程如图1所示,方法包括步骤S102至S108:

[0029] S102,接收第一终端发送的虚拟SIM卡登录请求,登录请求包括账号信息、携带加

密公钥的虚拟SIM卡参数获取请求信息；

[0030] S104，判断加密公钥是否与第二加密公钥相同，第二加密公钥为虚拟SIM卡的登录账号上一次登录时携带的加密公钥；

[0031] S106，在加密公钥与第二加密公钥不相同的情况下，根据加密公钥对预先存储的虚拟SIM卡账号信息对应的虚拟SIM卡参数包进行加密；

[0032] S108，将加密后的虚拟SIM卡参数包发送给第一终端。

[0033] 本发明实施例接收来自第一终端的加密公钥，并判断该加密公钥是否与上一次登陆时携带的加密公钥相同，如果不相同，就使用该加密公钥加密虚拟SIM卡参数包，并发给第一终端，每次切换终端后，终端都会发送新生成的加密公钥给服务器侧，服务器侧都使用新的加密公钥来加密虚拟SIM卡参数包，获取虚拟SIM卡参数包的过程较为安全，解决了现有技术切换移动终端时，获取Softsim卡参数的过程中存在较大安全隐患，用户体验较低的问题。

[0034] 实现过程中，第一终端可能并非第一个登陆该账号的终端，因此，在接收第一终端发送的虚拟SIM卡登录请求之后，根据账号信息检测是否存在已经登录同一账号的第二终端。

[0035] 若不存在第二终端，说明第一终端为第一个登陆该账号信息的终端，此时没有其他终端同时登陆该账号，则再执行S104的步骤。

[0036] 由于之前登录过虚拟SIM卡账号，再次登录该账号会造成重复登录的问题，进而可能会存在一SIM卡信息多终端使用的状态，所以，若存在已经登录同一账号的第二终端，则发送提示信息给第一终端，并根据第一终端的反馈结果执行相应的后续操作。一般而言，第一终端根据提示信息有两种处理方式，一是不再登录该账号信息，则服务器不做处理，另一个是注销已登录的账号信息并重新登录，此时服务器按照登录流程重新执行一遍，即再次执行S102至S108的过程。

[0037] 在判断加密公钥是否与第二加密公钥相同之后，如果判断加密公钥与第二加密公钥相同，则提示第一终端登录不成功。

[0038] 本发明第二实施例提供一种虚拟SIM卡的数据传输方法，该方法是实现第一实施例方法设备的对端设备，即终端设备，上述方法包括步骤S202至S210：

[0039] S202，第一终端接收用户输入的虚拟SIM卡登录账号信息；

[0040] S204，第一终端根据虚拟SIM卡登录账号信息生成一对公私钥对，公私钥对包括加密公钥和解密私钥；

[0041] S206，第一终端发送虚拟SIM卡登录请求至服务器，虚拟SIM卡登录请求包括账号信息、携带加密公钥的虚拟SIM卡参数获取请求信息；

[0042] S208，在服务器判断加密公钥与第二加密公钥不相同的情况下，第一终端接收服务器下发的虚拟SIM卡参数包，第二加密公钥为虚拟SIM卡的登录账号上一次登录时携带的加密公钥；

[0043] S210，第一终端根据解密私钥对虚拟SIM卡参数包进行解密，以获取虚拟SIM卡参数信息。

[0044] 本实施例第一终端在登录账号信息时，就会新生成一对公私钥对，然后发送新的公钥给服务器，服务器根据新的加密公钥来对虚拟SIM卡参数包进行加密，并将加密后的虚

拟SIM卡参数包返回给第一终端,第一终端就可以使用解密私钥对其进行解密,进而获得虚拟SIM卡参数包。

[0045] 虚拟SIM卡技术在使用时,需要终端登录一个虚拟SIM卡登录账号,利用该账号的信息与服务器交互,进而获取虚拟SIM参数包,以便根据参数完成虚拟SIM卡的注册,进而正常的使用终端。使用时,如果用户想更换使用的终端时,就需要在另一终端上登录虚拟SIM卡账号信息。

[0046] 实现过程中,如果服务器判断加密公钥与第二加密公钥相同,则确定服务器检测到存在已经登录同一账号的第二终端,此时,第一终端会接收到服务器返回的检测到存在已经登录同一账号的第二终端的提示信息。此时,用户可以注销第二终端,则第一终端判断是否接收到用户输入的注销信息,如果第一终端接收到用户输入的注销第二终端登录的注销信息,则反馈至服务器,以注销第二终端。

[0047] 实现过程中,如果服务器判断加密公钥与第二加密公钥相同,则第一终端会接收到服务器判断加密公钥与第二加密公钥相同后发送的登录不成功的提示信息。

[0048] 本发明第三实施例提供一种服务器,该服务器的结构示意如图3所示,包括:

[0049] 第一接收模块10,用于接收第一终端发送的虚拟SIM卡登录请求,登录请求包括账号信息、携带加密公钥的虚拟SIM卡参数获取请求信息;密钥判断模块11,与第一接收模块10耦合,用于判断加密公钥是否与第二加密公钥相同,第二加密公钥为虚拟SIM卡的登录账号上一次登录时携带的加密公钥;加密模块12,与密钥判断模块11耦合,用于在加密公钥与第二加密公钥不相同的情况下,根据加密公钥对预先存储的虚拟SIM卡账号信息对应的虚拟SIM卡参数包进行加密;第一发送模块13,与加密模块12耦合,用于将加密后的虚拟SIM卡参数包发送给第一终端。

[0050] 实现过程中,上述服务器还可以如图4所示,还包括:检测模块14,与第一接收模块10和密钥判断模块11耦合,用于在接收第一终端发送的虚拟SIM卡登录请求之后,根据账号信息检测是否存在已经登录同一账号的第二终端,并在不存在第二终端的情况下,触发密钥判断模块11工作。

[0051] 第一发送模块13,还用于在存在已经登录同一账号的第二终端的情况下,发送提示信息给第一终端,并根据第一终端的反馈结果执行相应的后续操作。第一发送模块13,还用于在确定加密公钥与第二加密公钥相同的情况下,提示第一终端登录不成功。

[0052] 本发明第四实施例还提供一种终端,该终端可以与第三实施例中的服务器进行交互,该终端的结构示意如图5所示,包括:

[0053] 第二接收模块20,用于接收用户输入的虚拟SIM卡登录账号信息;生成模块21,与第二接收模块20耦合,用于根据虚拟SIM卡登录账号信息生成一对公私钥对,公私钥对包括加密公钥和解密私钥;第二发送模块22,与生成模块21耦合,用于发送虚拟SIM卡登录请求至服务器,虚拟SIM卡登录请求包括账号信息、携带加密公钥的虚拟SIM卡参数获取请求信息;第三接收模块23,与第二发送模块22耦合,用于在服务器判断加密公钥与第二加密公钥不相同的情况下,接收服务器下发的虚拟SIM卡参数包,第二加密公钥为虚拟SIM卡的登录账号上一次登录时携带的加密公钥;解密模块24,与第三接收模块23耦合,用于根据解密私钥对虚拟SIM卡参数包进行解密,以获取虚拟SIM卡参数信息。

[0054] 具体实现时,上述终端还可以包括其他模块,例如,在服务器判断加密公钥与第二

加密公钥相同的情况下,还可以包括与第三接收模块和第二发送模块耦合的消息判断模块,各模块还可以存在其他功能,例如,第三接收模块,还用于接收服务器发送的存在已经登录同一账号的第二终端的提示信息;消息判断模块,用于在接收到提示信息的情况下,判断是否接收到用户输入的注销信息,其中,注销信息用于注销第二终端的登录信息;第二发送模块,还用于在接收到注销信息时,将注销信息反馈至服务器。

[0055] 本发明第五实施例提供一种Softsim在不同终端切换的方法,实现时,每次申请softsim卡参数包时,需重新实时的在用户终端的modem中生成新的公钥和私钥对,公钥发送给运营商服务器用于对softsim卡参数包加密,私钥留在用户终端解密公钥加密的softsim卡参数包。下面结合图6对上述过程进行说明,包括步骤S601至S606。

[0056] S601,用户切换到新的移动终端,在modem生成新的公钥和私钥对。

[0057] S602,为了完成切换,需要重新获取Softsim卡参数,则新的移动终端登录Softsim账户,并向网络侧服务器发送Softsim卡参数包申请请求,其中,Softsim卡参数包申请请求中包含新生成的公钥。

[0058] S603,网络侧服务器收到用户的Softsim卡参数包申请请求后,检查请求中是否携带用于加密的公钥。如果是,则执行S604,否则,执行S605。

[0059] S604,网络侧服务器用新的公钥对Softsim卡参数包进行加密,并下发给用户终端。随后,执行S606。

[0060] S605,不给用户终端下发Softsim卡参数包。

[0061] S606,用户终端在收到网络侧服务器下发的加密的Softsim卡参数包之后,利用新的私钥进行解密,以成功获得Softsim卡参数,这样就可以在新的终端上重新使用Softsim功能,实现了从之前移动终端到新移动终端的随机切换。

[0062] 本实施例实现了不同终端间softsim的实时切换,且私钥和公钥的生成和使用都是一次性能,安全级别非常高,解决了之前利用私钥备份的方案实现的softsim的切换的安全隐患。

[0063] 本发明实施例采用单交互单密钥,每当用户登录Softsim账户,终端向运营商服务器发起申请Softsim卡参数包时,用户终端首先实时生成公钥和私钥对。生成之后公钥会伴随Softsim卡参数包申请请求一起发送给运营商服务器,运营商服务器利用本次获得的公钥为Softsim卡参数包加密发送给用户终端,当下次用户终端申请softsim卡参数包时本次公钥失效,运营商服务器需重新拿到新的公钥才会下发Softsim卡参数包。这样当用户更换终端时,新的终端的modem会重新生成新的公私钥对,可以重新从运营商服务器端获取原本就分配给自己的softsim卡参数包,实现了不同终端间的softsim卡的实时有效的切换。

[0064] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

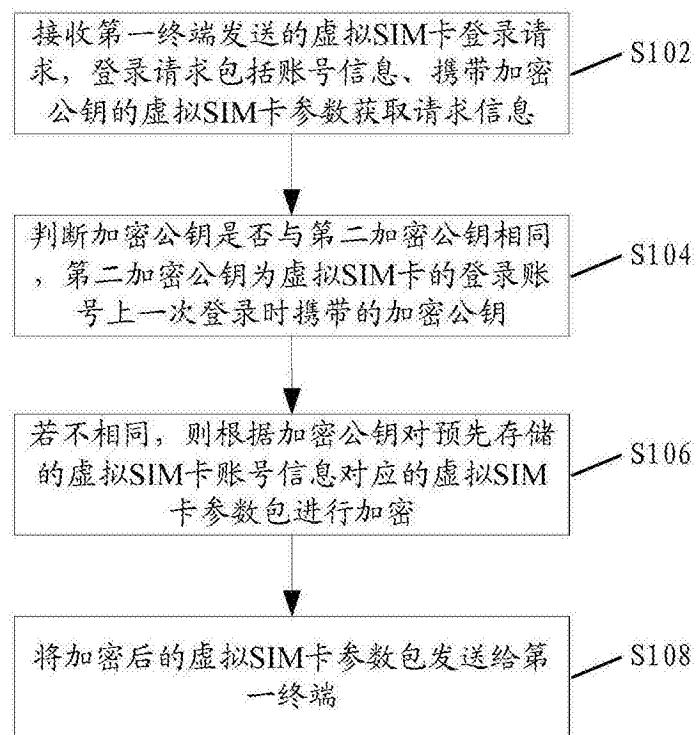


图1

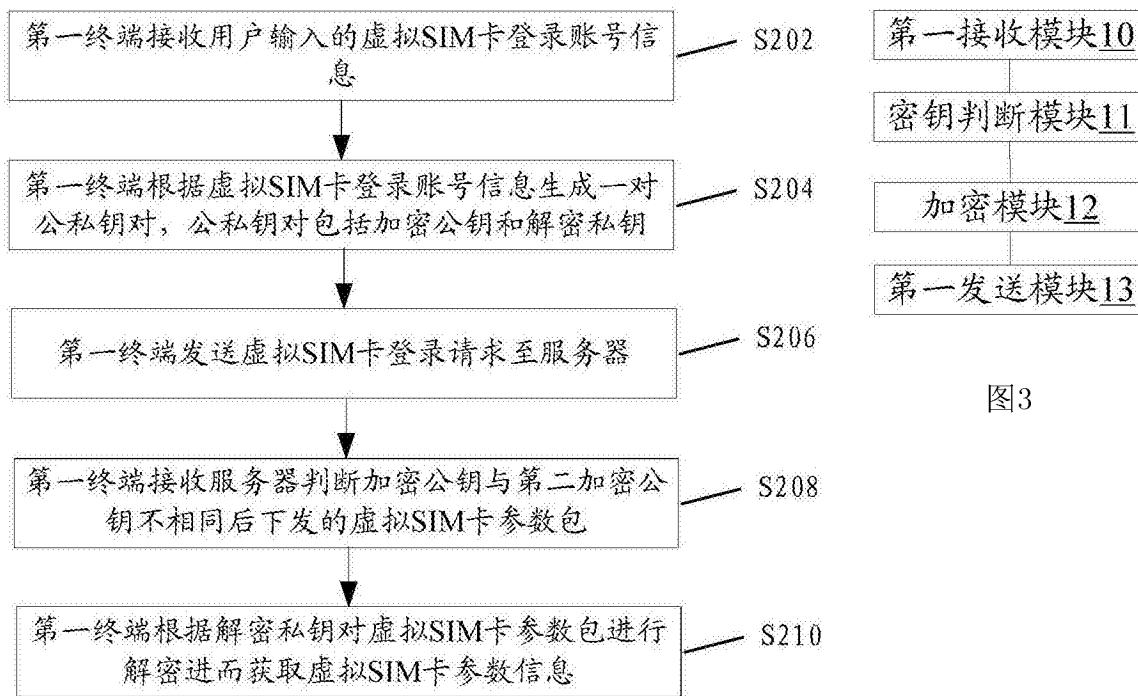


图3

图2

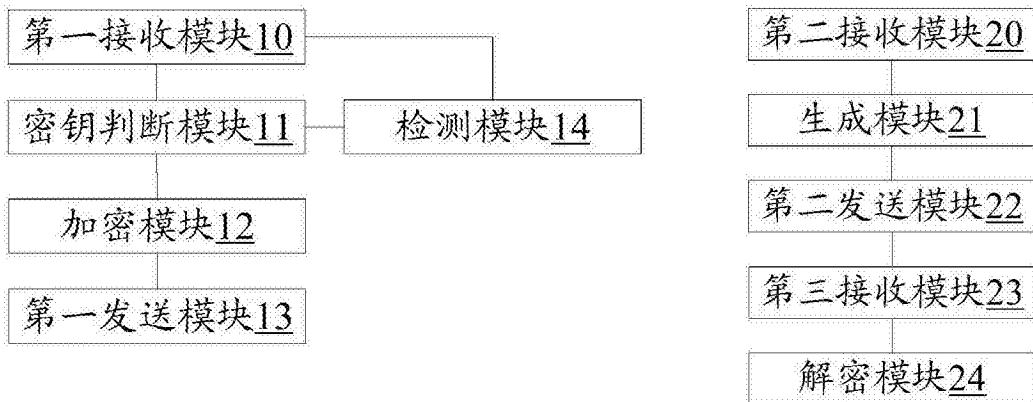


图4

图5

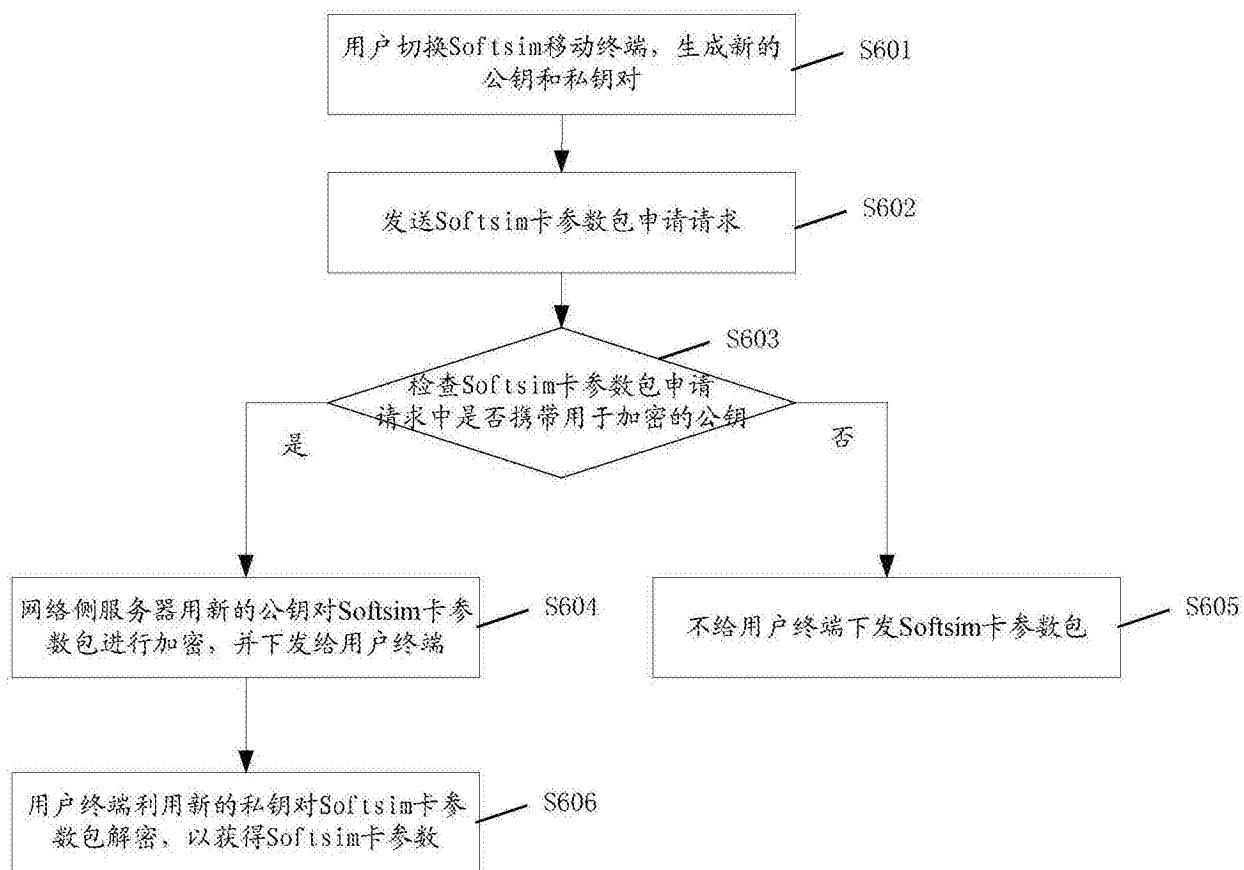


图6