(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2016 年 12 月 22 日 (22.12.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/201732 A1

(51) 国际专利分类号:
H04W 12/02 (2009.01) *H04L 9/14* (2006.01)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2015/082921

(22) 国际申请日: 2015 年 6 月 30 日 (30.06.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510344953.4 2015 年 6 月 19 日 (19.06.2015) CN

(71) 申请人: **宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.)** [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(72) 发明人: **罗茂清 (LUO, Maoqing)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(74) 代理人: **广州三环专利代理有限公司 (GUANGZHOU SCIHEAD PATENT AGENT CO.. LTD)**; 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: VIRTUAL SIM CARD PARAMETER MANAGEMENT METHOD, MOBILE TERMINAL, AND SERVER

(54) **发明名称** : 一种虚拟 SIM 卡参数管理方法、移动终端及服务器

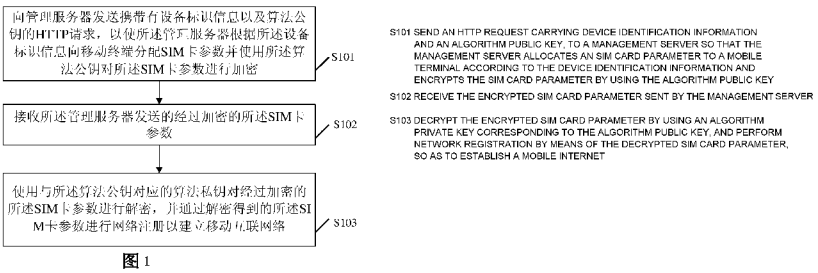

图 1

(57) **Abstract**: Disclosed are a virtual SIM card parameter management method, a mobile terminal, and a server. The method comprises: sending an HTTP request carrying device identification information and an algorithm public key, to a management server so that the management server allocates an SIM card parameter to a mobile terminal according to the device identification information and encrypts the SIM card parameter by using the algorithm public key; receiving the encrypted SIM card parameter sent by the management server; and decrypting the encrypted SIM card parameter by using an algorithm private key corresponding to the algorithm public key, and performing network registration by means of the decrypted SIM card parameter, so as to establish a mobile internet. By using embodiments of the present invention, the method in which an encrypted SIM card parameter is acquired from a server by means of an HTTP request is more efficient and securer.

(57) **摘要**: 本发明实施例公开了一种虚拟 SIM 卡参数管理方法、移动终端及服务器，包括：向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求，以使所述管理服务器根据所述设备标识信息向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密；接收所述管理服务器发送的经过加密的所述 SIM 卡参数；使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密，并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。采用本发明实施例，通过 HTTP 请求从服务器中获取经过加密的 SIM 卡参数的方法更为高效安全。

WO 2016/201732 A1

一种虚拟SIM卡参数管理方法、移动终端及服务器

本申请要求于2015年06月19日提交中国专利局，申请号为201510344953.4、发明名称为“一种虚拟SIM卡参数管理方法、移动终端及服务器”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及电子技术领域，尤其涉及一种虚拟SIM卡参数管理方法、移动终端及服务器。

背景技术

随着物联网技术的发展，对物联网网络安全也提出了新的要求，物联网连接和处理的对象主要是机器或物以及其相关的大量数据，这些处理对象的“所有权”特性导致物联网对数据安全的要求要比以处理“文本”信息为主的互联网要高，这些需要保护的信息包括网络中传输处理的业务数据，也包括网络中各个节点身份信息，即隐私信息。移动终端作为物联网的一类终端节点，一方面由于需要和整个物联网互联互通，因此具有物联网网络中的身份标签；另一方面由于需要接入传统的无线网络，因此具有无线接入网络的身份标签，这些身份标签信息的发放以及存储过程都应该受到安全保护，防止信息泄露。

虚拟SIM卡的文件参数可以直接存储在移动终端中，相较于传统的SIM卡，具有方便集中管理、工作温度范围广、成本低等优点，虚拟SIM卡的文件参数可以作为移动终端的身份标签进行网络注册进而加入物联网网络。在现有技术方案中，移动终端向服务器提出请求，请求服务器授权SIM卡参数，但是，在请求过程中安全性低。

发明内容

本发明实施例提供一种虚拟 SIM 卡参数管理方法、移动终端及服务器。通过 HTTP 请求从服务器中获取经过加密的 SIM 卡参数的方法更为高效安全。

本发明实施例提供了一种虚拟 SIM 卡参数管理方法，包括:

所述管理服务器根据所述设备标识信息向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密;

接收所述管理服务器发送的经过加密的所述 SIM 卡参数;

使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密，并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

其中，所述向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求之前还包括:

获取所述设备标识信息以及所述算法公钥;

根据所述设备标识信息以及所述算法公钥，生成得到所述 HTTP 请求。

其中，所述通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络之后，还包括:

当检测到所述 SIM 卡参数的使用时间超过有效期限时，向所述管理服务器发送 SIM 卡参数的更新请求，以使所述管理服务器对所述移动终端中的所述 SIM 卡参数进行更新。

相应地，本发明实施例提供了另一种虚拟 SIM 卡参数管理方法，包括:

接收移动终端发送的携带有设备标识信息以及算法公钥的 HTTP 请求;

根据所述 HTTP 请求中的所述设备标识信息，向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密;

将经过加密的所述 SIM 卡参数发送至所述移动终端，以使所述移动终端使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

其中，所述将经过加密的所述 SIM 卡参数发送至所述移动终端之后，还

包括:

接收所述移动终端发送的更新请求;

根据所述更新请求，对所述移动终端中的所述 SIM 卡参数进行更新。

相应地，本发明实施例提供了一种移动终端，包括:

请求发送模块，用于向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求，以使所述管理服务器根据所述设备标识信息向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密;

信息接收模块，用于接收所述管理服务器发送的经过加密的所述 SIM 卡参数;

解密注册模块，用于使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密，并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

其中，所述移动终端还包括:

信息获取模块，用于获取所述设备标识信息以及所述算法公钥;

请求生成模块，用于根据所述设备标识信息以及所述算法公钥，生成得到所述 HTTP 请求。

其中，所述移动终端还包括:

参数更新模块，用于当检测到所述 SIM 卡参数的使用时间超过有效期限时，向所述管理服务器发送 SIM 卡参数的更新请求，以使所述管理服务器对所述移动终端中的所述 SIM 卡参数进行更新。

相应地，本发明实施例提供了一种管理服务器，包括:

请求接收模块，用于接收移动终端发送的携带有设备标识信息以及算法公钥的 HTTP 请求;

信息处理模块，用于根据所述 HTTP 请求中的所述设备标识信息，向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密;

信息发送模块，用于将经过加密的所述 SIM 卡参数发送至所述移动终端，以使所述移动终端使用与所述算法公钥对应的算法私钥对经过加密的所

述 SIM 卡参数进行解密并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

其中，所述请求接收模块，还用于接收所述移动终端发送的更新请求；

所述信息发送模块，还用于根据所述更新请求，对所述移动终端中的所述 SIM 卡参数进行更新。

实施本发明实施例，首先向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求，以使管理服务器根据设备标识信息向移动终端分配 SIM 卡参数并使用算法公钥对 SIM 卡参数进行加密；然后接收管理服务器发送的经过加密的 SIM 卡参数；最后使用与算法公钥对应的算法私钥对经过加密的 SIM 卡参数进行解密，并通过解密得到的 SIM 卡参数进行网络注册以建立移动互联网络，从而实现了通过 HTTP 请求从服务器中获取经过加密的 SIM 卡参数的方法更为高效安全。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明提出的一种虚拟 SIM 卡参数管理方法的第一实施例的流程图；

图 2 是本发明提出的一种虚拟 SIM 卡参数管理方法的第二实施例的流程图；

图 3 是本发明提出的一种虚拟 SIM 卡参数管理方法的第三实施例的流程图；

图 4 是本发明实施例提出的一种移动终端的结构示意图；

图 5 是本发明实施例提出的一种管理服务器的结构示意图；

图 6 是本发明实施例提出的一种虚拟 SIM 卡参数管理系统的结构示意

图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

请参考图 1，图 1 是本发明提出的一种虚拟 SIM 卡参数管理方法的第一实施例的流程图。如图所示，本发明实施例的执行主体为移动终端，本发明实施例中的方法包括:

S101，向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求，以使所述管理服务器根据所述设备标识信息向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密。

具体实现中，移动终端可以预先通过加密算法计算出加密密钥，所述加密密钥包括算法公钥和算法私钥。当移动终端需要向管理服务器申请 SIM 卡参数时，可以获取所述设备标识信息以及所述算法公钥；根据所述设备标识信息以及所述算法公钥，生成得到所述 HTTP 请求；然后向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求。其中，设备标识信息可以为移动终端标识号(MEID，Mobile Equipment Identifier)、国际移动设备身份码(IMEI，International Mobile Equipment Identity)等等。

管理服务器接收到所述 HTTP 请求之后，首先对所述 HTTP 请求进行解析进而从所述 HTTP 请求中获取设备标识信息以及算法公钥，然后确认设备标识信息是否符合终端设备标识要求，当所述设备标识信息不符合终端设备标识要求时，向所述移动终端返回所述设备标识信息错误的消息并提示用户重新提交所述设备标识信息，当所述设备标识信息符合终端设备标识要求时，向所述移动终端分配 SIM 卡参数，并使用算法公钥对 SIM 卡参数进行加密，并将经过加密的 SIM 卡参数发送至移动终端。其中，SIM 卡参数可以包括国

际移动用户识别码(IMSI， International Mobile Subscriber Identification Number)。

S102，接收所述管理服务器发送的经过加密的所述 SIM 卡参数。

S103，使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密，并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

具体实现中， 所述 SIM 卡参数还可以包括注册密码，在解密得到国际移动用户识别码和注册密码之后，可以使用国际移动用户识别码和注册密码进行网络注册，当确认网络注册成功时，提示用户可以进行移动互联网络操作。

可选的，当检测到所述 SIM 卡参数的使用时间超过有效期限时，向所述管理服务器发送 SIM 卡参数的更新请求，以使所述管理服务器对所述移动终端中的所述 SIM 卡参数进行更新。其中，有效期限可以是一个月或半个月，也可以由用户与移动网络运营商协商确定，更新请求也可以为携带有设备标识信息以及算法公钥的 HTTP 请求，可以重复执行上述操作对 SIM 卡参数进行更新。

需要说明的是，本发明实施例中的移动终端和管理服务器可以使用其他网络资源进行信息传输，当使用请求得到的 SIM 卡参数进行网络注册成功之后，可以使用该 SIM 卡参数注册的网络资源进行信息传输。

在本发明实施例中，首先向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求，以使管理服务器根据设备标识信息向移动终端分配 SIM 卡参数并使用算法公钥对 SIM 卡参数进行加密；然后接收管理服务器发送的经过加密的 SIM 卡参数；最后使用与算法公钥对应的算法私钥对经过加密的 SIM 卡参数进行解密，并通过解密得到的 SIM 卡参数进行网络注册以建立移动互联网络，从而实现了通过 HTTP 请求从服务器中获取经过加密的 SIM 卡参数的方法更为高效安全。

请参考图 2，图 2 是本发明提出的一种虚拟 SIM 卡参数管理方法的第二实施例的流程图。如图所示，本发明实施例的执行主体为管理服务器，本发明实施例中的方法包括:

S201，接收移动终端发送的携带有设备标识信息以及算法公钥的 HTTP 请求。

具体实现中，移动终端可以预先通过加密算法计算出加密密钥，所述加密密钥包括算法公钥和算法私钥。当移动终端需要向管理服务器申请 SIM 卡参数时，可以获取所述设备标识信息以及所述算法公钥；根据所述设备标识信息以及所述算法公钥，生成得到所述 HTTP 请求；然后向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求。其中，设备标识信息可以为移动终端标识号(MEID，Mobile Equipment Identifier)、国际移动设备身份码(IMEI，International Mobile Equipment Identity)等等。

S202,根据所述 HTTP 请求中的所述设备标识信息,向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密。

具体实现中,管理服务器接收到所述 TTTP 请求之后,首先对所述 HTTP 请求进行解析进而从所述 HTTP 请求中获取设备标识信息以及算法公钥，然后确认设备标识信息是否符合终端设备标识要求，当所述设备标识信息不符合终端设备标识要求时，向所述移动终端返回所述设备标识信息错误的消息并提示用户重新提交所述设备标识信息，当所述设备标识信息符合终端设备标识要求时，向所述移动终端分配 SIM 卡参数，并使用算法公钥对 SIM 卡参数进行加密，并将经过加密的 SIM 卡参数发送至移动终端。其中，SIM 卡参数可以包括国际移动用户识别码(IMSI，International Mobile Subscriber Identification Number)。

S203，将经过加密的所述 SIM 卡参数发送至所述移动终端，以使所述移动终端使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

可选的，可以接收所述移动终端发送的更新请求；根据所述更新请求，对所述移动终端中的所述 SIM 卡参数进行更新。其中，更新请求也可以为携带有设备标识信息以及算法公钥的 HTTP 请求，可以重复执行上述操作对移动终端中的 SIM 卡参数进行更新。

在本发明实施例中，管理服务器首先接收移动终端发送的携带有设备标识信息以及算法公钥的 HTTP 请求；然后根据 HTTP 请求中的设备标识信息，最后向移动终端分配 SIM 卡参数并使用算法公钥对 SIM 卡参数进行加密。将经过加密的 SIM 卡参数发送至移动终端，以使移动终端使用与算法公钥对应的算法私钥对经过加密的 SIM 卡参数进行解密并通过解密得到的 SIM 卡参数进行网络注册以建立移动互联网络，从而实现了移动终端通过 HTTP 请求从服务器中获取经过加密的 SIM 卡参数的方法更为高效安全。

请参考图 3，图 3 是本发明提出的一种虚拟 SIM 卡参数管理方法的第三实施例的流程图。如图所示，本发明实施例中的方法包括：

S301，移动终端获取所述设备标识信息以及所述算法公钥。

具体实现中，移动终端可以首先确定加密密钥的宽度以及随机选择的两个素数，通过 RSA 加密算法计算得到加密密钥，所述加密密钥包括算法公钥和算法私钥；当移动终端检测到需要向管理服务器申请 SIM 卡参数时，获取所述加密密钥中的算法公钥以及识别出移动终端上的设备标识信息。

S302，移动终端根据所述设备标识信息以及所述算法公钥，生成得到所述 HTTP 请求。

S303，移动终端向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求。

S304，管理服务器根据所述设备标识信息向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密。

S305，管理服务器将经过加密的所述 SIM 卡参数发送至所述移动终端。

S306，移动终端使用与所述算法公钥对应的算法私钥对经过加密的所述

SIM卡参数进行解密并通过解密得到的所述SIM卡参数进行网络注册以建立移动互联网络。

S307，移动终端当检测到所述SIM卡参数的使用时间超过有效期限时，向所述管理服务器发送SIM卡参数的更新请求。

S308，管理服务器根据所述更新请求，对所述移动终端中的所述SIM卡参数进行更新。

在本发明实施例中，首先向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求，以使管理服务器根据设备标识信息向移动终端分配SIM卡参数并使用算法公钥对SIM卡参数进行加密；然后接收管理服务器发送的经过加密的SIM卡参数；最后使用与算法公钥对应的算法私钥对经过加密的 SIM 卡参数进行解密，并通过解密得到的 SIM 卡参数进行网络注册以建立移动互联网络，从而实现了通过HTTP请求从服务器中获取经过加密的SIM卡参数的方法更为高效安全。

请参考图 4，图 4 是本发明实施例提出的一种移动终端的结构示意图。如图所示，本发明实施例中的移动终端 40 包括:

请求发送模块 401，用于向管理服务器发送携带有设备标识信息以及算法公钥的HTTP请求，以使所述管理服务器根据所述设备标识信息向移动终端分配SIM卡参数并使用所述算法公钥对所述SIM卡参数进行加密。其中，设备标识信息可以为移动终端标识号(MEID，Mobile Equipment Identifier)、国际移动设备身份码(IMEI，International Mobile Equipment Identity)等等。

管理服务器接收到所述HTTP请求之后，首先对所述HTTP请求进行解析进而从所述HTTP请求中获取设备标识信息以及算法公钥，然后确认设备标识信息是否符合终端设备标识要求，当所述设备标识信息不符合终端设备标识要求时，向所述移动终端返回所述设备标识信息错误的消息并提示用户重新提交所述设备标识信息，当所述设备标识信息符合终端设备标识要求时，向所述移动终端分配SIM卡参数，并使用算法公钥对SIM卡参数进行加密，

并将经过加密的 SIM 卡参数发送至移动终端。其中，SIM 卡参数可以包括国际移动用户识别码(IMSI， International Mobile Subscriber Identification Number)。

信息接收模块 402，用于接收所述管理服务器发送的经过加密的所述 SIM 卡参数。

解密注册模块 403，用于使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密，并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

具体实现中， 所述 SIM 卡参数还可以包括注册密码，在解密得到国际移动用户识别码和注册密码之后，可以使用国际移动用户识别码和注册密码进行网络注册，当确认网络注册成功时，提示用户可以进行移动互联网络操作。

可选的，如图 4 所示，本发明实施例中的移动终端 40 还可以包括:

信息获取模块 405，用于获取所述设备标识信息以及所述算法公钥。

具体实现中，移动终端可以预先通过加密算法计算出加密密钥，所述加密密钥包括算法公钥和算法私钥。当移动终端需要向管理服务器申请 SIM 卡参数时，可以获取所述设备标识信息以及所述算法公钥。

请求生成模块 406，用于根据所述设备标识信息以及所述算法公钥，生成得到所述 HTTP 请求。

可选的，如图 4 所示，本发明实施例中的移动终端 40 还可以包括:

参数更新模块 404，用于当检测到所述 SIM 卡参数的使用时间超过有效期限时，向所述管理服务器发送 SIM 卡参数的更新请求，以使所述管理服务器对所述移动终端中的所述 SIM 卡参数进行更新。其中，有效期限可以是一个月或半个月，也可以由用户与移动网络运营商协商确定，更新请求也可以为携带有设备标识信息以及算法公钥的 HTTP 请求，可以重复执行上述操作对 SIM 卡参数进行更新。

需要说明的是，本发明实施例中的移动终端和管理服务器可以使用其他

网络资源进行信息传输，当使用请求得到的 SIM 卡参数进行网络注册成功之后，可以使用该 SIM 卡参数注册的网络资源进行信息传输。

在本发明实施例中，首先向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求，以使管理服务器根据设备标识信息向移动终端分配 SIM 卡参数并使用算法公钥对 SIM 卡参数进行加密；然后接收管理服务器发送的经过加密的 SIM 卡参数；最后使用与算法公钥对应的算法私钥对经过加密的 SIM 卡参数进行解密，并通过解密得到的 SIM 卡参数进行网络注册以建立移动互联网络，从而实现了通过 HTTP 请求从服务器中获取经过加密的 SIM 卡参数的方法更为高效安全。

请参考图 5，图 5 是本发明实施例提出的一种管理服务器的结构示意图。如图所示，本发明实施例中的管理服务器 50 包括：

请求接收模块 501，用于接收移动终端发送的携带有设备标识信息以及算法公钥的 HTTP 请求。

具体实现中，移动终端可以预先通过加密算法计算出加密密钥，所述加密密钥包括算法公钥和算法私钥。当移动终端需要向管理服务器申请 SIM 卡参数时，可以获取所述设备标识信息以及所述算法公钥；根据所述设备标识信息以及所述算法公钥，生成得到所述 HTTP 请求；然后向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求。其中，设备标识信息可以为移动终端标识号(MEID，Mobile Equipment Identifier)、国际移动设备身份码(IMEI，International Mobile Equipment Identity)等等。

信息处理模块 502，用于根据所述 HTTP 请求中的所述设备标识信息，向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密。

具体实现中，管理服务器接收到所述 TTTP 请求之后，首先对所述 HTTP 请求进行解析进而从所述 HTTP 请求中获取设备标识信息以及算法公钥，然后确认设备标识信息是否符合终端设备标识要求，当所述设备标识信息不符

合终端设备标识要求时，向所述移动终端返回所述设备标识信息错误的消息并提示用户重新提交所述设备标识信息，当所述设备标识信息符合终端设备标识要求时，向所述移动终端分配 SIM 卡参数，并使用算法公钥对 SIM 卡参数进行加密，并将经过加密的 SIM 卡参数发送至移动终端。其中，SIM 卡参数可以为国际移动用户识别码(IMSI，International Mobile Subscriber Identification Number)。

信息发送模块 503，用于将经过加密的所述 SIM 卡参数发送至所述移动终端，以使所述移动终端使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

可选的，可以接收所述移动终端发送的更新请求；根据所述更新请求，对所述移动终端中的所述 SIM 卡参数进行更新。其中，更新请求也可以为携带有设备标识信息以及算法公钥的 HTTP 请求，可以重复执行上述操作对移动终端中的 SIM 卡参数进行更新。

在本发明实施例中，管理服务器首先接收移动终端发送的携带有设备标识信息以及算法公钥的 HTTP 请求；然后根据 HTTP 请求中的设备标识信息，最后向移动终端分配 SIM 卡参数并使用算法公钥对 SIM 卡参数进行加密。将经过加密的 SIM 卡参数发送至移动终端，以使移动终端使用与算法公钥对应的算法私钥对经过加密的 SIM 卡参数进行解密并通过解密得到的 SIM 卡参数进行网络注册以建立移动互联网络，从而实现了移动终端通过 HTTP 请求从服务器中获取经过加密的 SIM 卡参数的方法更为高效安全。

请参考图 6，图 6 是本发明实施例提出的一种 SIM 卡参数管理系统的结构示意图。如图所示，本发明实施例中的系统包括:

移动终端 40，用于向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求，以使所述管理服务器根据所述设备标识信息向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密；接收所述管理

服务器发送的经过加密的所述 SIM 卡参数；使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密，并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

管理服务器 50，用于接收移动终端发送的携带有设备标识信息以及算法公钥的 HTTP 请求；根据所述 HTTP 请求中的所述设备标识信息，向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密；将经过加密的所述 SIM 卡参数发送至所述移动终端，以使所述移动终端使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

需要说明的是，对于前述的各个方法实施例，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，本发明并不受所描述的动作顺序的限制，因为依据本发明，某一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，所涉及的动作和模块并不一定是本发明所必须的。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详细描述的部分，可以参见其他实施例的相关描述。

本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器（英文：Read-Only Memory，简称：ROM）、随机存取器（英文：Random Access Memory，简称：RAM）、磁盘或光盘等。

以上对本发明实施例所提供的内容下载方法及相关设备、系统进行了详细介绍，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。

权 利 要 求

1、一种虚拟 SIM 卡参数管理方法，其特征在于，所述方法包括:

向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求，以使所述管理服务器根据所述设备标识信息向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密;

接收所述管理服务器发送的经过加密的所述 SIM 卡参数;

使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密，并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

2、如权利要求 1 所述的方法，其特征在于，所述向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求之前还包括:

获取所述设备标识信息以及所述算法公钥;

根据所述设备标识信息以及所述算法公钥，生成得到所述 HTTP 请求。

3、如权利要求 1 所述的方法，其特征在于，所述通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络之后，还包括:

当检测到所述 SIM 卡参数的使用时间超过有效期限时，向所述管理服务器发送 SIM 卡参数的更新请求，以使所述管理服务器对所述移动终端中的所述 SIM 卡参数进行更新。

4、一种虚拟 SIM 卡参数管理方法，其特征在于，所述方法包括:

接收移动终端发送的携带有设备标识信息以及算法公钥的 HTTP 请求;

根据所述 HTTP 请求中的所述设备标识信息，向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密;

将经过加密的所述 SIM 卡参数发送至所述移动终端，以使所述移动终端使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解

密并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

5、如权利要求 4 所述的方法，其特征在于，所述将经过加密的所述 SIM 卡参数发送至所述移动终端之后，还包括:

接收所述移动终端发送的更新请求;

根据所述更新请求，对所述移动终端中的所述 SIM 卡参数进行更新。

6、一种移动终端，其特征在于，所述移动终端包括:

请求发送模块，用于向管理服务器发送携带有设备标识信息以及算法公钥的 HTTP 请求，以使所述管理服务器根据所述设备标识信息向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密;

信息接收模块，用于接收所述管理服务器发送的经过加密的所述 SIM 卡参数;

解密注册模块，用于使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密，并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

7、如权利要求 6 所述的移动终端，其特征在于，所述移动终端还包括:

信息获取模块，用于获取所述设备标识信息以及所述算法公钥;

请求生成模块，用于根据所述设备标识信息以及所述算法公钥，生成得到所述 HTTP 请求。

8、如权利要求 6 所述的移动终端，其特征在于，所述移动终端还包括:

参数更新模块，用于当检测到所述 SIM 卡参数的使用时间超过有效期限时，向所述管理服务器发送 SIM 卡参数的更新请求，以使所述管理服务器对所述移动终端中的所述 SIM 卡参数进行更新。

9、一种管理服务器，其特征在于，所述管理服务器包括:

请求接收模块，用于接收移动终端发送的携带有设备标识信息以及算法

公钥的 HTTP 请求;

信息处理模块，用于根据所述 HTTP 请求中的所述设备标识信息，向移动终端分配 SIM 卡参数并使用所述算法公钥对所述 SIM 卡参数进行加密;

信息发送模块，用于将经过加密的所述 SIM 卡参数发送至所述移动终端，以使所述移动终端使用与所述算法公钥对应的算法私钥对经过加密的所述 SIM 卡参数进行解密并通过解密得到的所述 SIM 卡参数进行网络注册以建立移动互联网络。

10、如权利要求 9 所述的管理服务器，其特征在于，

所述请求接收模块，还用于接收所述移动终端发送的更新请求;

所述信息发送模块，还用于根据所述更新请求，对所述移动终端中的所述 SIM 卡参数进行更新。

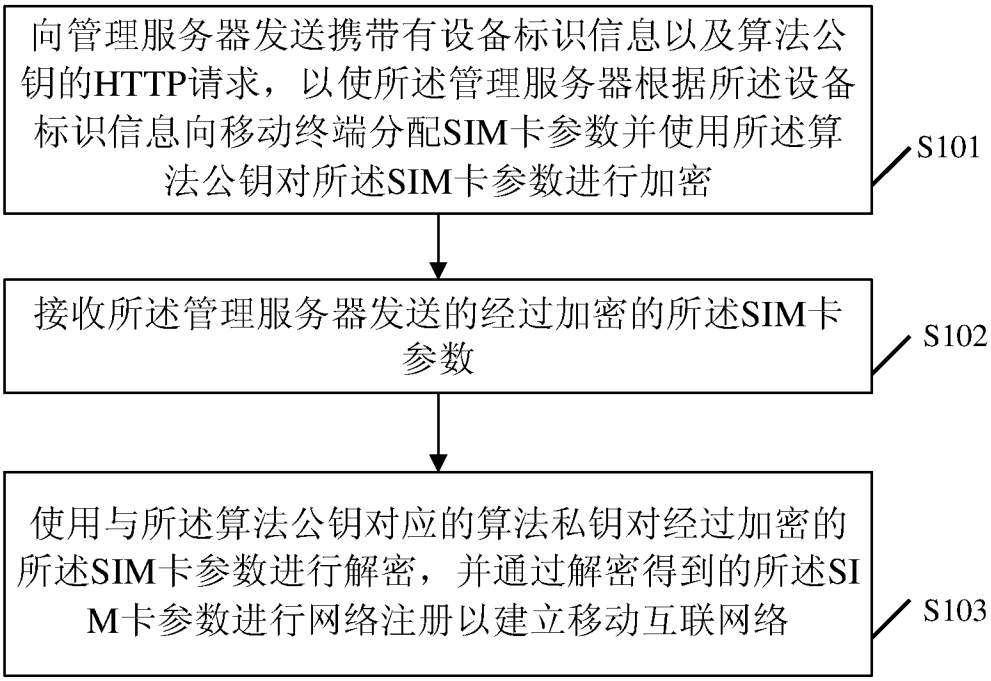
向管理服务器发送携带有设备标识信息以及算法公钥的HTTP请求，以使所述管理服务器根据所述设备标识信息向移动终端分配SIM卡参数并使用所述算法公钥对所述SIM卡参数进行加密
S101
接收所述管理服务器发送的经过加密的所述SIM卡参数
S102
使用与所述算法公钥对应的算法私钥对经过加密的所述SIM卡参数进行解密，并通过解密得到的所述SIM卡参数进行网络注册以建立移动互联网络
S103

图 1

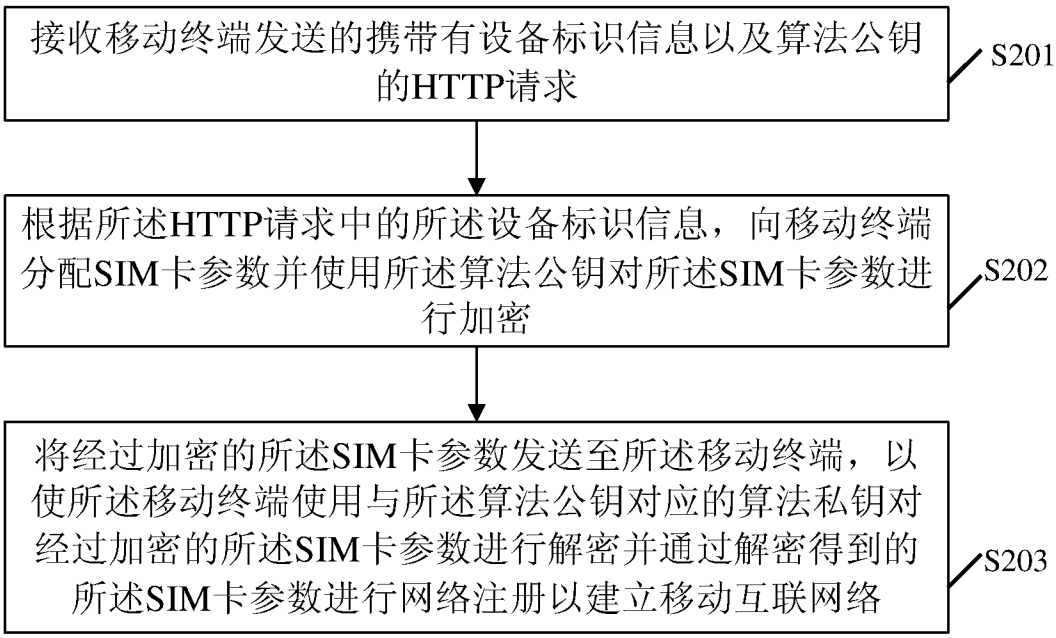
接收移动终端发送的携带有设备标识信息以及算法公钥的HTTP请求
S201
根据所述HTTP请求中的所述设备标识信息，向移动终端分配SIM卡参数并使用所述算法公钥对所述SIM卡参数进行加密
S202
将经过加密的所述SIM卡参数发送至所述移动终端，以使所述移动终端使用与所述算法公钥对应的算法私钥对经过加密的所述SIM卡参数进行解密并通过解密得到的所述SIM卡参数进行网络注册以建立移动互联网络
S203

图 2

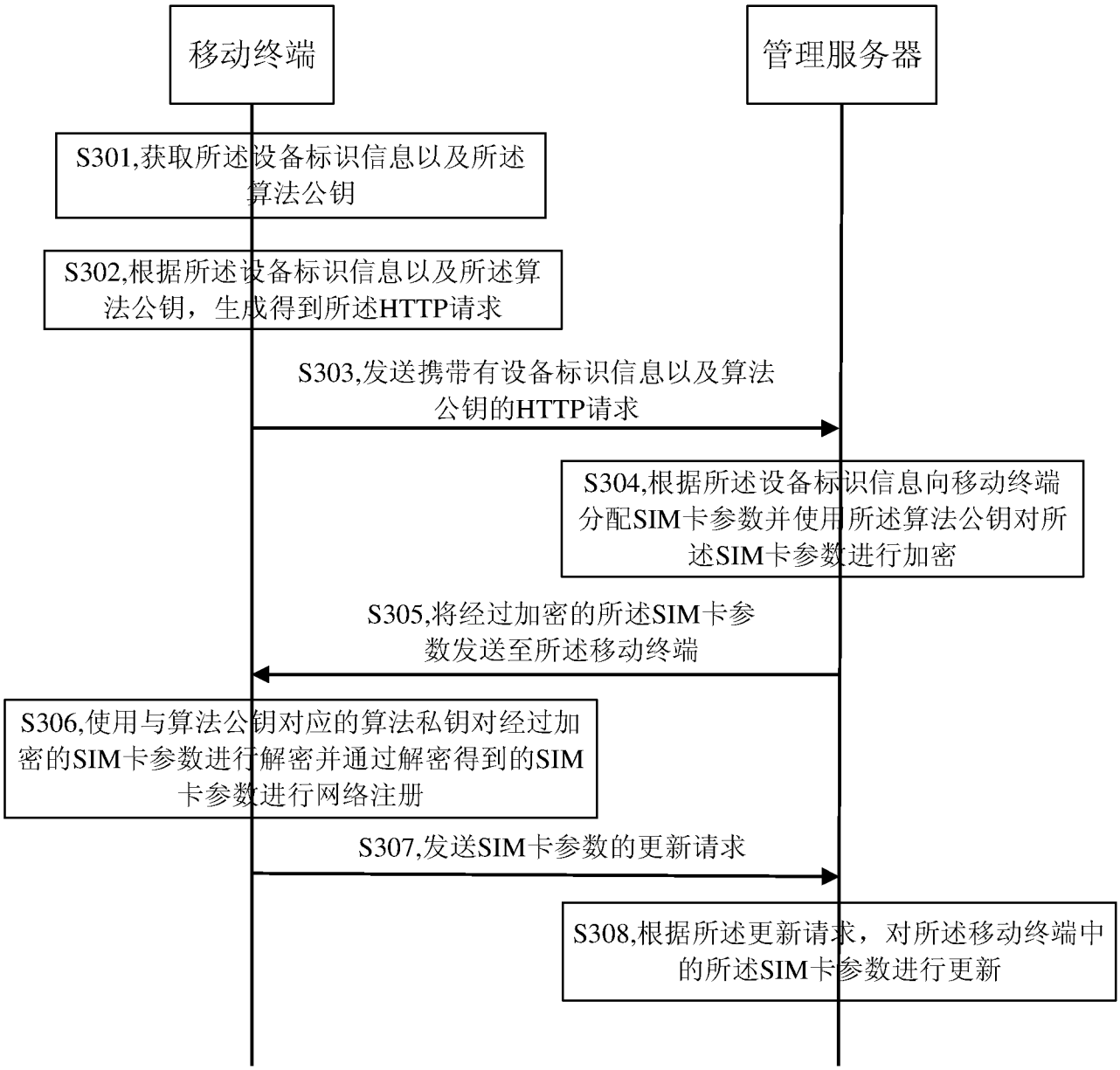
移动终端
管理服务器
S301,获取所述设备标识信息以及所述算法公钥
S302,根据所述设备标识信息以及所述算法公钥，生成得到所述HTTP请求
S303,发送携带有设备标识信息以及算法公钥的HTTP请求
S304,根据所述设备标识信息向移动终端分配SIM卡参数并使用所述算法公钥对所述SIM卡参数进行加密
S305,将经过加密的所述SIM卡参数发送至所述移动终端
S306,使用与算法公钥对应的算法私钥对经过加密的SIM卡参数进行解密并通过解密得到的SIM卡参数进行网络注册
S307,发送SIM卡参数的更新请求
S308,根据所述更新请求，对所述移动终端中的所述SIM卡参数进行更新

图 3

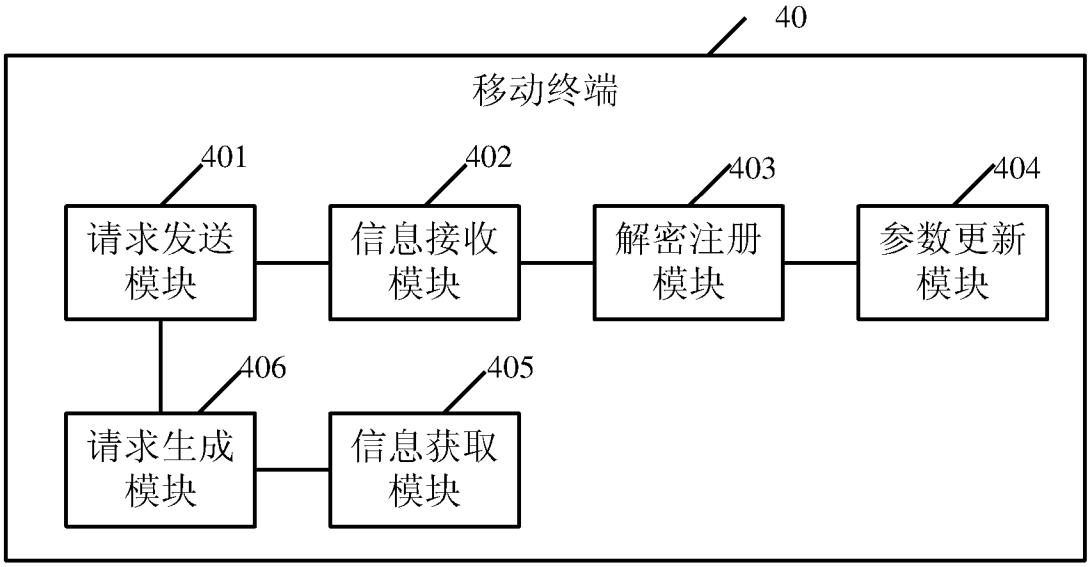
40
移动终端
401
请求发送模块
402
信息接收模块
403
解密注册模块
404
参数更新模块
406
请求生成模块
405
信息获取模块

图 4

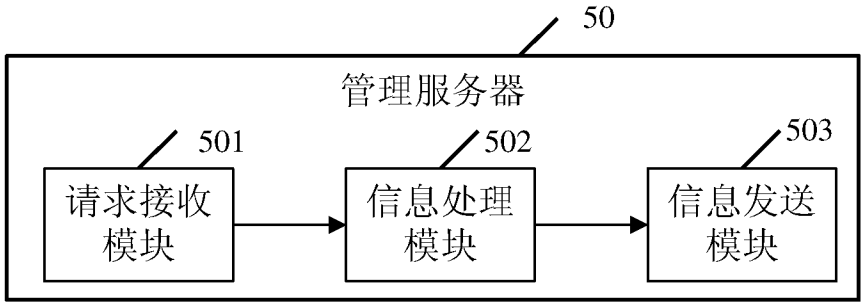
50
管理服务器
501
请求接收模块
502
信息处理模块
503
信息发送模块

图 5

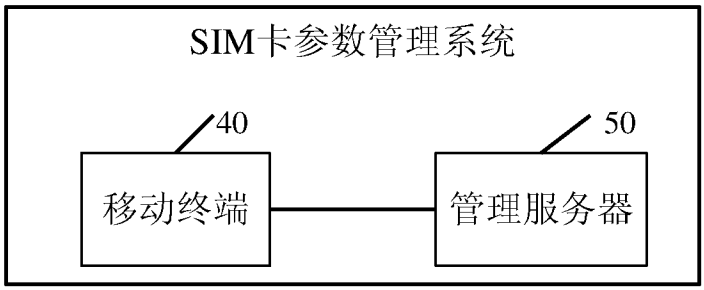
SIM卡参数管理系统
40
移动终端
50
管理服务器

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/082921

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/02 (2009.01) i; H04L 9/08 (2006.01) i; H04L 9/14 (2006.01) i; H04L 9/32 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNTXT, CNKI, VEN: SIM, secret key, public key, private key, machine to machine, M2M, virtual, SIM, encrypt+, security, key, Things

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103533539 A (ZTEWELINK CORPORATION), 22 January 2014 (22.01.2014), description, paragraphs 0037-0061, and figures 1 and 2	1-10
Y	US 2015121066 A1 (NIX, J.A. et al.), 30 April 2015 (30.04.2015), description, paragraphs 0020, 0021, 0116-0121, 0197 and 0209-0233, and figures 1a and 5b	1-10
A	CN 104185176 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 03 December 2014 (03.12.2014), the whole document	1-10
A	EP 2749003 A1 (DEUTSCHE TELEKOM AG), 02 July 2014 (02.07.2014), the whole document	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 February 2016 (20.02.2016)	**07 March 2016 (07.03.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **HU, Shaoqin** Telephone No.: (86-10) **62089559**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/082921

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103533539 A	22 January 2014	None	
US 2015121066 A1	30 April 2015	US 2015071139 A1	12 March 2015
		US 2015180653 A1	25 June 2015
		US 2015304113 A1	22 October 2015
		US 2015106616 A1	16 April 2015
		US 2015143125 A1	21 May 2015
		US 9118464 B2	25 August 2015
		WO 2015065913 A1	07 May 2015
		US 2015095648 A1	02 April 2015
CN 104185176 A	03 December 2014	None	
EP 2749003 A1	02 July 2014	US 9184913 B2	10 November 2015
		DE 102011118367 A1	28 February 2013
		WO 2013026875 A1	28 February 2013
		US 2014219448 A1	07 August 2014

国际检索报告

国际申请号
PCT/CN2015/082921

A. 主题的分类

H04W 12/02(2009.01)i; H04L 9/08(2006.01)i; H04L 9/14(2006.01)i; H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS, CNTXT, CNKI, VEN: 虚拟, SIM, 加密, 安全, 密钥, 公钥, 私钥, 公共密钥, 私有密钥, 物联, 机器到机器, M2M, virtual, SIM, encrypt+, security, key, Things

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 103533539 A (深圳市中兴物联科技有限公司) 2014年 1月 22日 (2014-01-22) 说明书第0037-0061段，图1、2	1-10
Y	US 2015121066 A1 (JOHN A. NIX等) 2015年 4月 30日 (2015-04-30) 说明书第0020、0021、0116-0121、0197、0209 -0233段，图1a、5b	1-10
A	CN 104185176 A (中国联合网络通信集团有限公司) 2014年 12月 3日 (2014-12-03) 全文	1-10
A	EP 2749003 A1 (德国电信股份有限公司) 2014年 7月 2日 (2014-07-02) 全文	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 2月 20日	2016年 3月 7日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	胡绍芹
传真号 (86-10)62019451	电话号码 (86-10)62089559

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/082921

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103533539	A	2014年 1月 22日	无			
US	2015121066	A1	2015年 4月 30日	US	2015071139	A1	2015年 3月 12日
				US	2015180653	A1	2015年 6月 25日
				US	2015304113	A1	2015年 10月 22日
				US	2015106616	A1	2015年 4月 16日
				US	2015143125	A1	2015年 5月 21日
				US	9118464	B2	2015年 8月 25日
				WO	2015065913	A1	2015年 5月 7日
				US	2015095648	A1	2015年 4月 2日
CN	104185176	A	2014年 12月 3日	无			
EP	2749003	A1	2014年 7月 2日	US	9184913	B2	2015年 11月 10日
				DE	102011118367	A1	2013年 2月 28日
				WO	2013026875	A1	2013年 2月 28日
				US	2014219448	A1	2014年 8月 7日