

(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
2014 年 3 月 6 日 (06.03.2014)



(10) 国际公布号
WO 2014/032612 A1

- (51) 国际专利分类号:
H04W 4/14 (2009.01)
- (21) 国际申请号: PCT/CN2013/082678
- (22) 国际申请日: 2013 年 8 月 30 日 (30.08.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210320720.7 2012 年 8 月 31 日 (31.08.2012) CN
- (71) 申请人: 小米科技有限责任公司 (XIAOMI INC.)
[CN/CN]; 中国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, Beijing 100085 (CN)。
- (72) 发明人: 万钰臻 (WAN, Yuzhen); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。孙鹏 (SUN, Peng); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。金凡 (JIN, Fan); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。林俊琦 (LIN, Junqi); 中国北

京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。

(74) 代理人: 北京律智知识产权代理有限公司 (BEIJING INTELLEGAL INTELLECTUAL PROPERTY AGENT LTD.); 中国北京市朝阳区慧忠路 5 号 B 座 1802, 1803, 1805, Beijing 100101 (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, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH,

[见续页]

(54) Title: METHOD, DEVICE, SERVER, SYSTEM, AND APPARATUS FOR PREVENTING INFORMATION LEAKAGE

(54) 发明名称: 防止信息泄露的方法、装置、服务器、系统和设备

当移动终端接收到短信时, 判断该短信是否为与服务器
约定的第一短信 S101

当该短信为第一短信时, 清除移动终端中的用户信息 S102

图 1 / FIG. 1

S101 WHEN THE MOBILE TERMINAL RECEIVES THE SHORT MESSAGE, DETERMINATION OF WHETHER OR NOT THE SHORT MESSAGE IS THE FIRST SHORT MESSAGE AS AGREED WITH THE SERVER

S102 WHEN THE SHORT MESSAGE IS THE FIRST SHORT MESSAGE, REMOVAL OF THE USER INFORMATION IN THE MOBILE TERMINAL

(57) Abstract: The present invention relates to the field of communications. Disclosed are a method, device, server, system, and apparatus for preventing information leakage. The technical solution disclosed in the present invention allows, when a mobile terminal of a user is lost, a first short message to be transmitted to the mobile terminal via a short message network, and, when the mobile terminal determines that a short message received is the first short message, user information in the mobile terminal to be removed. This ensures the security of personal privacy information of the user, prevents malicious leakage of the personal privacy information saved in the mobile terminal when the mobile terminal of the user is lost.

(57) 摘要: 本发明公开了一种防止信息泄露的方法、装置、服务器、系统和设备, 属于通信领域。本发明所公开的技术方案使得在用户的移动终端丢失后, 可以通过短信网络向移动终端发送第一短信, 当移动终端判断得到接收的短信为第一短信时, 清除移动终端中的用户信息, 可保证用户的个人隐私信息的安全性, 防止用户的移动终端丢失后保存在移动终端中的个人隐私信息被恶意泄露。

WO 2014/032612 A1



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))。

防止信息泄露的方法、装置、服务器、系统和设备

技术领域

- 5 本发明涉及通信领域，尤其涉及一种防止信息泄露的方法、装置、服务器、系统和设备。

背景技术

- 10 随着移动终端技术的发展，移动终端（尤其是手机）能够给人们提供越来越便捷的功能，人们在生活中也越来越依赖移动终端。以手机为例进行说明，手机能够给人们提供短信、通话以及拍照等功能，并且在手机中存储有大量用户的个人隐私信息，当手机发生丢失或被盗时，很容易造成用户的个人隐私信息的泄露。

目前，大多数手机不具有防止移动终端丢失后避免用户的个人隐私信息泄露的保护机制，只有一小部分手机采用如下保护机制防止手机丢失后被拾到者非法使用：

- 15 在手机中设置 SIM（Subscriber Identity Module，客户识别模块）卡的保护密码，当欲更换 SIM 卡时，必须通过 SIM 卡保护密码的认证，当密码输错次数大于预设的次数时，则将手机锁定。

- 20 但是，这种保护机制只能保证用户的手机不被非法利用，在一定程度上保护用户的个人隐私信息的安全，但是在不更换 SIM 卡的情况下，用户存储在手机或手机的存储卡中的个人隐私信息仍是可见的，可能发生隐私泄露。

发明内容

本发明实施例提供了一种防止信息泄露的方法、装置、服务器、系统和设备，可以防止移动终端丢失后引起的用户信息的泄露。

- 25 一种防止信息泄露的方法，当移动终端连接有短信网络时，所述方法包括：
当移动终端接收到短信时，判断所述短信是否为与服务器约定的第一短信；
当所述短信为所述第一短信时，清除所述移动终端中的用户信息。
一种防止信息泄露的方法，所述方法包括：
接收用户发出的清除移动终端中的用户信息的指令；
30 获取所述移动终端连接的网络的网络类型；

当所述移动终端连接有短信网络时，通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信，以使所述移动终端在接收到所述第一短信后执行清除所述移动终端中的用户信息的操作。

一种用于防止信息泄露的装置，所述装置包括：

- 5 判断模块，用于当移动终端接收到短信时，判断所述短信是否为与服务器约定的第一短信；

清除模块，用于当所述判断模块判断得到所述短信为所述第一短信时，清除所述移动终端中的用户信息。

一种用于防止信息泄露的服务器，所述服务器包括：

- 10 第一接收模块，用于接收用户发出的清除移动终端中的用户信息的指令；
获取模块，用于获取所述移动终端连接的网络的网络类型；

第一发送模块，用于当所述获取模块获取得到所述移动终端连接有短信网络时，通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信，以使所述移动终端执行清除所述移动终端中的用户信息的操作。

- 15 一种用于防止信息泄露的系统，所述系统包括如上所述的任一用于防止信息泄露的装置和如上所述的任一用于防止信息泄露的服务器。

一种设备，所述设备包括：

显示屏幕；

一个或多个处理器；

- 20 存储器；和

一个或多个模块，所述一个或多个模块存储于所述存储器中并被配置成由所述一个或多个处理器执行，其中，所述一个或多个模块具有如下功能：

当所述设备接收到短信时，判断所述短信是否为与服务器约定的第一短信；

当所述短信为所述第一短信时，清除所述设备中的用户信息。

- 25 一种设备，所述设备包括：

一个或多个处理器；

存储器；和

一个或多个模块，所述一个或多个模块存储于所述存储器中并被配置成由所述一个或多个处理器执行，其中，所述一个或多个模块具有如下功能：

- 30 接收用户发出的清除移动终端中的用户信息的指令；

获取所述移动终端连接的网络的网络类型；

当获取得到所述移动终端连接有短信网络时，通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信，以使所述移动终端执行清除所述移动终端中的用户信息的操作。

5 本发明实施例的有益效果包括：

本发明实施例提供了一种防止信息泄露的方法、装置、服务器、系统和设备，使得在用户的移动终端丢失后，可以通过短信网络向移动终端发送第一短信，当移动终端判断得到接收的短信为第一短信时，清除移动终端中的用户信息，可保证用户的个人隐私信息的安全性，防止用户的移动终端丢失后保存在移动终端中的个人隐私信息被恶意泄露。

10

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对本发明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，下面描述中的附图仅仅是本发明实施例的一些举例，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。

15

图 1 为本发明实施例提供的一种防止信息泄露的方法的流程示意图；

图 2 为本发明实施例提供的另一种防止信息泄露的方法的流程示意图；

图 3 为本发明实施例提供的再一种防止信息泄露的方法的流程示意图；

图 4 为本发明实施例提供的一种用于防止信息泄露的装置的结构示意图；

20

图 5 为本发明实施例提供的一种用于防止信息泄露的装置中的清除模块的结构示意图；

图 6 为本发明实施例提供的一种用于防止信息泄露的装置的第二种结构示意图；

图 7 为本发明实施例提供的一种用于防止信息泄露的装置的第三种结构示意图；

图 8 为本发明实施例提供的一种用于防止信息泄露的装置的第四种结构示意图；

25

图 9 为本发明实施例提供的一种用于防止信息泄露的装置的第五种结构示意图；

图 10 是本发明实施例提供的一种用于防止信息泄露的服务器的结构示意图；

图 11 是本发明实施例提供的一种用于防止信息泄露的服务器的第二种结构示意图；

图 12 是本发明实施例提供的一种用于防止信息泄露的服务器的第三种结构示意图；

图 13 是本发明实施例提供的一种用于防止信息泄露的服务器的第四种结构示意图；

30

图 14 是本发明实施例提供的一种用于防止信息泄露的服务器的第五种结构示意图；

图 15 是本发明实施例提供的一种用于防止信息泄露的服务器的第六种结构示意图；
图 16 是本发明实施例提供的一种用于防止信息泄露的服务器的第七种结构示意图；
图 17 是本发明实施例提供的一种用于防止信息泄露的服务器的第八种结构示意图。

5 具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合附图对优选实施例作进一步地详细描述。

下面结合附图，对本发明实施例提供的一种防止信息泄露的方法、装置、服务器、系统和设备的具体实施方式进行详细地说明。

10 如图 1 所示，本发明实施例提供的一种防止信息泄露的方法，在进行具体实现时，可以通过程序实现在移动终端中，例如可通过在移动终端中安装软件或将程序集成在操作系统中的形式，本实施例以移动终端为执行主体为例进行说明。

当移动终端连接有短信网络时，该方法包括以下步骤：

S101、当移动终端接收到短信时，判断该短信是否为与服务器约定的第一短信；

15 需要说明的是，在现有情况下，移动终端可连接有互联网网络进行因特网的访问，也可连接有短信网络进行短信的发送与接收。现有的运营商网络部署情况是，用户可连接短信网络的区域更加广泛。因此，在手机丢失后，如若连接不到互联网网络，可连接短信网络完成用户信息的清除。

S102、当该短信为第一短信时，清除移动终端中的用户信息。

20 上述清除所述移动终端中的用户信息，具体包括：

删除移动终端本地保存的用户信息，并格式化与移动终端连接的存储卡。

进一步地，第一短信中携带有用户设定的锁定密码或用户设定的锁定密码对应的密文；

当上述短信为第一短信时，上述方法还包括：

25 锁定移动终端，以使移动终端在接收并成功验证用户输入的锁定密码之前处于不可使用状态。

进一步地，当移动终端连接有互联网网络时，上述方法还包括：

接收服务器通过互联网网络发送的第一指令；

清除移动终端中的用户信息；

30 其中，第一指令用于指示移动终端清除移动终端中的用户信息。

需要说明的是，在本实施例中，第一短信对于用户不可见。

更近一步地，当上述短信为第一短信时，本方法还包括：

使移动终端发声；

或，

5 向服务器上报移动终端的位置信息。

如图 2 所示，以服务器端为例进行说明，本发明实施例提供的一种防止信息泄露的方法，包括如下步骤：

S201、接收用户发出的清除移动终端中的用户信息的指令；

S202、获取移动终端连接的网络的网络类型；

10 需要说明的是，在本实施例中，移动终端连接的网络的网络类型包括：
短信网络和互联网网络。

S203、当移动终端连接有短信网络时，通过短信网络向移动终端发送与移动终端约定的第一短信，以使移动终端执行清除移动终端中的用户信息的操作。

15 需要说明的是，当接收用户发出的清除移动终端中的用户信息的指令时，本方法还包括：

接收用户输入的锁定密码；

其中，锁定密码用于锁定移动终端。

相应地，通过短信网络向移动终端发送与移动终端约定的第一短信之前，本方法还包括：

20 将锁定密码以与移动终端约定的格式添加到上述第一短信中。

或，

对锁定密码进行加密运算得到锁定密码对应的密文，将该锁定密码对应的密文以与移动终端约定的格式添加到第一短信中。

进一步地，当移动终端连接有互联网网络时，该方法还包括：

25 通过互联网网络发送向移动终端发送第一指令，以便于移动终端在接收到第一指令后清除移动终端中的用户信息。

进一步地，在通过短信网络向移动终端发送与移动终端约定的第一短信之前，本方法还包括：

根据用户预先输入的身份信息查找该身份信息对应的电话号码。

30 相应地，接收用户发出的清除移动终端中的用户信息的指令之前，本方法还包括：

接收用户输入的身份信息和电话号码，并通过该电话号码向移动终端发送验证短信，以对该电话号码进行验证；

当该电话号码被验证通过后，保存用户输入的身份信息与电话号码的对应关系。

进一步地，通过短信网络向移动终端发送与移动终端约定的第一短信之后，本方法还

5 包括：

接收移动终端发送的该移动终端的位置信息。

为了便于说明，本实施例提供了如图 3 所示的防止信息泄露的方法，该实施例中，移动终端为手机为例进行说明，当用户的手机丢失后，具体包括如下步骤：

S301、用户通过网站登录服务器；

10 具体地，用户通过网站登录服务器，包括有服务器对用户的身份信息的验证过程，具体可以采取如下方式：

用户输入自身的账户以及账户的密码，服务器对用户输入的账户和密码进行验证，如果用户输入的账户和密码匹配成功，则验证通过，用户可以登录服务器，如果用户输入的账户和密码匹配失败，则验证失败，结束操作。

15 需要说明的是，用户在使用服务器提供的防止手机丢失后信息泄露的功能前，还包括如下过程：

用户在服务器注册账户，并将自身的账户与手机号码进行绑定，使得服务器保存用户的账户与手机号码的对应关系。

其中，将自身的账户与手机号码进行绑定，具体可以采取如下两种方式：

20 用户通过网站输入自身的账户和手机号码，服务器向该手机号码发送一条验证短信，且在该短信中包括有一个验证密码，用户接收到短信后，通过网站输入该验证密码，如果验证通过，则绑定成功。

25 用户通过网站输入自身的账户后，网站提示用户使用手机发送约定信息（例如用户的账户名称+绑定指示）到服务器指定的号码，如果服务器接收到用户发送的约定信息，则绑定成功。

S302、用户输入锁定密码，并通过服务器发出清除手机中的用户信息的指令。

其中，锁定密码用于锁定手机，使得手机在接收到正确的锁定密码前不能执行除了验证锁定密码的任何其他操作。

S303、服务器对锁定密码进行加密运算，得到锁定密码对应的密文；

30 其中，上述加密运算优选地使用散列算法，例如 MD5（Message-Digest Algorithm 5，

消息摘要算法第五版) 算法, 所述锁定密码对应的密文具体为锁定密码的 MD5 值。

需要说明的是, 散列算法为不可逆加密算法, 将锁定密码加密后进行发送, 可以使得即使消息被截获, 也不可能得到用户设定的锁定密码。

5 S304、判断手机是否通过互联网网络与服务器建立有连接, 如果是, 执行步骤 S305, 如果不是, 执行步骤 S306;

其中, 手机通过互联网网络与服务器建立有连接, 包括:

手机通过运营商提供的 PS (Packet Switch, 分组交换) 域业务建立的网络连接或由 WiFi (Wireless-Fidelity, 无线保真) 等无线网络建立的网络连接。

需要说明的是, 在本实施例中, 优选地通过互联网网络指示手机清除用户信息。

10 其中, 判断手机是否通过互联网网络与服务器建立有连接, 具体的可以为:

查找用户的账户对应的手机, 并判断手机与服务器预先建立的网络通道是否开启, 如果是, 则认为手机通过互联网网络与服务器建立有连接。

需要说明的是, 在用户启用手机的防止信息泄露的功能后, 应与服务器保持有同感互联网网络建立连接。

15 具体地, 上述连接可以为 TCP (Transmission Control Protocol, 传输层控制协议) 连接。

S305、服务器通过互联网网络向手机发送第一指令, 执行步骤 S307。

其中, 第一指令用于指示手机清除用户信息。

具体地, 在向手机发送第一指令前, 本方法还包括:

20 将锁定密码按照服务器与手机约定的格式添加到第一指令中, 以使得手机在接收到第一指令后, 完成用户信息的清除, 并使用锁定密码将手机锁定。

S306、服务器通过短信网络向手机发送第一短信, 执行步骤 S307;

其中, 短信网络包括运营商提供的 CS (Circuit Switched, 电路交换) 域对应的网络或 LTE (Long Term Evolution, 长期演进) 网络中用于负责短信服务的网络。

25 其中, 第一短信用于指示手机清除用户信息, 且该第一短信的格式为服务器与手机预先约定。

相应地, 手机在每次接收到短信时, 需首先判断接收到的短信是否为第一短信, 如果是, 则执行步骤 S307, 如果不是, 则显示接收到的短信, 作为普通短信进行处理。

30 需要说明的是, 手机判断接收到的短信是否为第一短信, 具体的可以通过短信的格式或短信中的内容进行判断, 例如可以包括以下两种方式:

第一种，服务器和手机预先约定第一短信的格式，当手机解析接收到的短信，发现该短信符合第一短信的格式时，则将接收到的短信作为第一短信。

第二种，服务器和手机预先约定第一短信的标识（例如短信的发送号码），当手机解析接收到的短信时，发现该短信中包括有预先约定的标识时，则将接收到的短信作为第一短信。

具体地，在向手机发送与手机约定的第一短信之前，本方法还包括：

将锁定密码按照服务器与手机约定的格式添加到第一短信中，以使得手机在接收到第一短信后，完成用户信息的清除，并使用锁定密码对应的密文将手机锁定。

并且，第一短信对于用户是不可见的，以防止手机在丢失后，被手机的拾取者发现并阻止手机中的用户信息的清除操作。

S307、清除手机中的用户信息，并锁定手机。

其中，清除手机中的用户信息包括：

清除手机本地存储的用户信息，并格式化手机的存储卡。

上述用户信息包括：用户的短信、通讯录、照片等涉及个人隐私的信息，清除方式可选的为，将手机恢复到出厂状态。

在本实施例中，锁定手机具体的执行方式可为将手机置为锁屏状态，以使得手机不能进行除进行除锁屏密码的认证外的其他任何操作。

进一步地，手机对于锁屏密码的认证，具体包括：

接收用户输入的锁屏密码，并对该锁屏密码进行加密运算得到新的密文，将新的密文与第一短信或第一指令中携带的锁屏密码对应的密文进行比对，如果相同，则解除锁屏状态。

需要说明的是，当手机处于关机状态时，手机无法接受到第一短信，具体的可以采取如下方式：

当用户手机开机后接收到短信后，启动执行判断该短信是否为第一短信的操作，当该短信为第一短信时，执行清除用户信息的操作。

需要说明的是，在本实施例中，在手机接收到第一短信或第一指令之后，还可以包括：使手机发声；

或，

使手机上报自身的位置信息。

其中，第一短信或第一指令中可携带有使手机发声的指示，手机按照该发声的指示发

声，以使得手机的拥有者能够靠声音找到手机的位置。

第一短信或第一指令中也可携带有使手机上报位置信息的指示，上述手机的位置信息可通过手机的定位功能得到，例如基于基站的定位或基于 GPS（Global Positioning System，全球定位系统）的定位。

- 5 相应地，上述手机的位置信息具体的为由 GPS 定位得到的手机所处位置的经纬度或手机所处的基站的基站位置。

如图 4 所示，本实施例提供了一种用于防止信息泄露的装置，该装置包括：

判断模块 401，用于当移动终端接收到短信时，判断该短信是否为与服务器约定的第一短信；

- 10 清除模块 402，用于当判断模块 401 判断得到上述短信为第一短信时，清除该移动终端中的用户信息。

进一步地，如图 5 所示，上述清除模块 402，具体包括：

第一删除单元 4021，用于删除移动终端本地保存的用户信息；

第二删除单元 4022，用于格式化与移动终端连接的存储卡。

- 15 进一步地，上述第一短信中携带有用户设定的锁定密码或用户设定的锁定密码对应的密文；

相应地，如图 6 所示，当上述短信为第一短信时，上述装置还包括：

锁定模块 403，用于锁定移动终端，以使移动终端在接收并成功验证用户输入的锁定密码之前处于不可使用状态。

- 20 进一步地，如图 7 所示，当移动终端连接有互联网网络时，上述装置还包括：

接收模块 404，用于接收服务器通过互联网网络发送的第一指令；

相应地，清除模块 402，还用于在接收模块 403 接收服务器通过互联网网络发送的第一指令之后，清除移动终端中的用户信息；

其中，第一指令用于指示移动终端清除移动终端中的用户信息。

- 25 进一步地，如图 8 或图 9 所示，上述装置还包括：

发声模块 405，用于当判断模块 401 判断得到上述短信为第一短信时，使移动终端发声；

或，

上报模块 406，用于当判断模块 401 判断得到上述短信为第一短信时，向服务器上述

- 30 移动终端的位置信息。

进一步地，上述第一短信对于用户不可见。

如图 10 所示，本实施例还提供了一种用于防止信息泄露的服务器，该服务器包括：

第一接收模块 501，用于接收用户发出的清除移动终端中的用户信息的指令；

获取模块 502，用于获取移动终端连接的网络的网络类型；

- 5 第一发送模块 503，用于当获取模块 502 获取得到移动终端连接有短信网络时，通过短信网络向移动终端发送与移动终端约定的第一短信，以使移动终端执行清除该移动终端中的用户信息的操作。

进一步地，如图 11 所示，上述服务器还包括：

- 10 第二发送模块 504，用于当获取模块 502 获取得到移动终端连接有互联网网络时，通过互联网网络发送向移动终端发送第一指令，以使移动终端在接收到第一指令后执行清除移动终端中的用户信息的操作。

进一步地，如图 12 所示，上述服务器还包括：

第二接收模块 505，用于在第一接收模块 501 接收用户发出的清除移动终端中的用户信息的指令之前，接收用户输入的锁定密码；

- 15 其中，锁定密码用于锁定移动终端。

进一步地，如图 13 所示，上述服务器还包括：

第一添加模块 506，用于在第一发送模块 503 通过短信网络向移动终端发送与移动终端约定的第一短信之前，将锁定密码以与移动终端约定的格式添加到第一短信中。

进一步地，如图 14 所示，上述服务器还包括：

- 20 加密模块 507，用于在第一发送模块 503 通过短信网络向移动终端发送与移动终端约定的第一短信之前，对锁定密码进行加密运算得到锁定密码对应的密文；

第二添加模块 508，用于将上述锁定密码对应的密文以与移动终端约定的格式添加到第一短信中。

进一步地，如图 15 所示，上述服务器还包括：

- 25 查找模块 509，用于在第一发送模块 503 通过短信网络向移动终端发送第一短信之前，根据用户预先输入的身份信息查找该身份信息对应的电话号码。

进一步地，如图 16 所示，上述服务器还包括：

- 30 第三接收模块 510，用于在第一接收模块 501 接收用户发出的清除移动终端中的用户信息的指令之前，接收用户输入的身份信息和电话号码，并通过电话号码向移动终端发送验证短信，以对上述电话号码进行验证；

保存模块 511，用于当上述电话号码验证通过后，保存用户输入的身份信息与上述电话号码的对应关系。

进一步地，如图 17 所示，上述服务器还包括：

5 第四接收模块 512，用于在第一发送模块 503 通过短信网络向移动终端发送与移动终端约定的第一短信之后，接收移动终端发送的该移动终端的位置信息。

另外，本发明实施例还提供了一种用于防止信息泄露的系统，该系统包括如上所述的任一用于防止信息泄露的装置和如上所述的任一用于防止信息泄露的服务器。

本发明实施例还提供了一种设备，该设备包括：

显示屏幕；

10 一个或多个处理器；

存储器；和

一个或多个模块，所述一个或多个模块存储于所述存储器中并被配置成由所述一个或多个处理器执行，其中，所述一个或多个模块具有如下功能：

当设备接收到短信时，判断该短信是否为与服务器约定的第一短信；

15 当上述短信为第一短信时，清除设备中的用户信息。

进一步地，上述清除设备中的用户信息，具体包括：

删除设备本地保存的用户信息；

格式化与设备连接的存储卡。

20 进一步地，第一短信中携带有用户设定的锁定密码或所述用户设定的锁定密码对应的密文；

相应地，当所述短信为所述第一短信时，上述设备还具有如下功能：

锁定设备，以使设备在接收并成功验证用户输入的锁定密码之前处于不可使用状态。

进一步地，当设备连接有互联网网络时，上述设备还具有如下功能：

接收服务器通过互联网网络发送的第一指令；

25 在接收服务器通过互联网网络发送的第一指令之后，清除设备中的用户信息；

其中，第一指令用于指示设备清除设备中的用户信息。

进一步地，上述设备还具有如下功能：

当判断得到上述短信为第一短信时，使设备发声；

或，

30 当判断得到上述短信为第一短信时，向服务器上报设备的位置信息。

进一步地，上述第一短信对于用户不可见。

本实施例还提供了一种设备，该设备包括：

一个或多个处理器；

存储器；和

- 5 一个或多个模块，该一个或多个模块存储于上述存储器中并被配置成由上述一个或多个处理器执行，其中，上述一个或多个模块具有如下功能：

接收用户发出的清除移动终端中的用户信息的指令；

获取移动终端连接的网络的网络类型；

- 10 当获取得到移动终端连接有短信网络时，通过短信网络向移动终端发送与移动终端约定的第一短信，以使移动终端执行清除该移动终端中的用户信息的操作。

进一步地，上述设备还具有如下功能：

当获取得到移动终端连接有互联网网络时，通过互联网网络发送向移动终端发送第一指令，以使移动终端在接收到第一指令后执行清除该移动终端中的用户信息的操作。

进一步地，上述设备还具有如下功能：

- 15 在接收用户发出的清除移动终端中的用户信息的指令之前，接收用户输入的锁定密码；

其中，上述锁定密码用于锁定移动终端。

进一步地，上述设备还具有如下功能：

- 20 在通过短信网络向移动终端发送与移动终端约定的第一短信之前，将锁定密码以与移动终端约定的格式添加到第一短信中。

进一步地，上述设备还具有如下功能：

在通过短信网络向移动终端发送与移动终端约定的第一短信之前，对锁定密码进行加密运算得到该锁定密码对应的密文；

将锁定密码对应的密文以与移动终端约定的格式添加到第一短信中。

- 25 进一步地，上述设备还具有如下功能：

在通过短信网络向移动终端发送与移动终端约定的第一短信之前，根据用户预先输入的身份信息查找该身份信息对应的电话号码。

进一步地，上述设备还具有如下功能：

- 30 在接收用户发出的清除移动终端中的用户信息的指令之前，接收用户输入的身份信息和电话号码，并通过该电话号码向移动终端发送验证短信，以对该电话号码进行验证；

当上述电话号码验证通过后，保存用户输入的身份信息与该电话号码的对应关系。

进一步地，上述设备还具有如下功能：

在通过所述短信网络向移动终端发送与移动终端约定的第一短信之后，接收移动终端发送的该移动终端的位置信息。

- 5 另外，本实施例还提供了一种非易失性可读存储介质，该存储介质中存储有一个或多个模块，该一个或多个模块被应用在具有一个或多个处理器的设备时，可以使得该设备具有如下功能：

当设备接收到短信时，判断该短信是否为与服务器约定的第一短信；

当上述短信为第一短信时，清除设备中的用户信息。

- 10 进一步地，上述清除设备中的用户信息，具体包括：

删除设备本地保存的用户信息；

格式化与设备连接的存储卡。

进一步地，第一短信中携带有用户设定的锁定密码或所述用户设定的锁定密码对应的密文；

- 15 相应地，当所述短信为所述第一短信时，上述一个或多个模块还具有如下功能：

锁定设备，以使设备在接收并成功验证用户输入的锁定密码之前处于不可使用状态。

进一步地，当设备连接有互联网网络时，上述一个或多个模块还具有如下功能：

接收服务器通过互联网网络发送的第一指令；

在接收服务器通过互联网网络发送的第一指令之后，清除设备中的用户信息；

- 20 其中，第一指令用于指示设备清除设备中的用户信息。

进一步地，上述一个或多个模块还具有如下功能：

当判断得到上述短信为第一短信时，使设备发声；

或，

当判断得到上述短信为第一短信时，向服务器上报设备的位置信息。

- 25 进一步地，上述第一短信对于用户不可见。

本实施例还提供了一种非易失性可读存储介质，该存储介质中存储有一个或多个模块，该一个或多个模块被应用在具有一个或多个处理器的设备时，可以使得该设备具有如下功能：

接收用户发出的清除移动终端中的用户信息的指令；

- 30 获取移动终端连接的网络的网络类型；

当获取得到移动终端连接有短信网络时，通过短信网络向移动终端发送与移动终端约定的第一短信，以使移动终端执行清除该移动终端中的用户信息的操作。

进一步地，上述一个或多个模块还具有如下功能：

- 5 当获取得到移动终端连接有互联网网络时，通过互联网网络发送向移动终端发送第一指令，以使移动终端在接收到第一指令后执行清除该移动终端中的用户信息的操作。

进一步地，上述一个或多个模块还具有如下功能：

在接收用户发出的清除移动终端中的用户信息的指令之前，接收用户输入的锁定密码；

其中，上述锁定密码用于锁定移动终端。

- 10 进一步地，上述一个或多个模块还具有如下功能：

在通过短信网络向移动终端发送与移动终端约定的第一短信之前，将锁定密码以与移动终端约定的格式添加到第一短信中。

进一步地，上述一个或多个模块还具有如下功能：

- 15 在通过短信网络向移动终端发送与移动终端约定的第一短信之前，对锁定密码进行加密运算得到该锁定密码对应的密文；

将锁定密码对应的密文以与移动终端约定的格式添加到第一短信中。

进一步地，上述一个或多个模块还具有如下功能：

在通过短信网络向移动终端发送与移动终端约定的第一短信之前，根据用户预先输入的身份信息查找该身份信息对应的电话号码。

- 20 进一步地，上述一个或多个模块还具有如下功能：

在接收用户发出的清除移动终端中的用户信息的指令之前，接收用户输入的身份信息和电话号码，并通过该电话号码向移动终端发送验证短信，以对该电话号码进行验证；

当上述电话号码验证通过后，保存用户输入的身份信息与该电话号码的对应关系。

进一步地，上述一个或多个模块还具有如下功能：

- 25 在通过所述短信网络向移动终端发送与移动终端约定的第一短信之后，接收移动终端发送的该移动终端的位置信息。

本实施例提供了一种防止信息泄露的方法、装置、服务器、系统和设备，使得在用户的移动终端丢失后，可以通过短信网络向移动终端发送第一短信，当移动终端判断得到接收的短信为第一短信时，清除移动终端中的用户信息，可保证用户的个人隐私信息的安全性，防止用户的移动终端丢失后保存在移动终端中的个人隐私信息被恶意泄露。

30

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明实施例可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本发明实施例的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

本领域技术人员可以理解附图只是一个优选实施例的示意图，附图中的模块或流程并不一定是实施本发明所必须的。

本领域技术人员可以理解实施例中的装置中的模块可以按照实施例描述进行分布于实施例的装置中，也可以进行相应变化位于不同于本实施例的一个或多个装置中。上述实施例的模块可以合并为一个模块，也可以进一步拆分成多个子模块。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

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。

权利要求

1、一种防止信息泄露的方法，其特征在于，当移动终端连接有短信网络时，所述方法包括：

当移动终端接收到短信时，判断所述短信是否为与服务器约定的第一短信；

5 当所述短信为所述第一短信时，清除所述移动终端中的用户信息。

2、根据权利要求 1 所述的方法，其特征在于，所述清除所述移动终端中的用户信息，具体包括：

删除所述移动终端本地保存的用户信息，并格式化与所述移动终端连接的存储卡。

10

3、根据权利要求 1 所述的方法，其特征在于，所述第一短信中携带有用户设定的锁定密码或所述用户设定的锁定密码对应的密文；

当所述短信为所述第一短信时，所述方法还包括：

15 锁定所述移动终端，以使所述移动终端在接收并成功验证所述用户输入的所述锁定密码之前处于不可使用状态。

4、根据权利要求 1 所述的方法，其特征在于，当所述移动终端连接有互联网网络时，所述方法还包括：

接收所述服务器通过互联网网络发送的第一指令；

20 清除所述移动终端中的用户信息；

其中，所述第一指令用于指示所述移动终端清除所述移动终端中的用户信息。

5、根据权利要求 1 所述的方法，其特征在于，当所述短信为所述第一短信时，所述方法还包括：

25 使所述移动终端发声；

或，

向所述服务器上报所述移动终端的位置信息。

6、根据权利要求 1-5 中任一权利要求所述的方法，其特征在于，所述第一短信对于
30 用户不可见。

7、一种防止信息泄露的方法，其特征在于，所述方法包括：

接收用户发出的清除移动终端中的用户信息的指令；

获取所述移动终端连接的网络的网络类型；

5 当所述移动终端连接有短信网络时，通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信，以使所述移动终端在接收到所述第一短信后执行清除所述移动终端中的用户信息的操作。

8、根据权利要求 7 所述的方法，其特征在于，当所述移动终端连接有互联网网络时，

10 所述方法还包括：

通过互联网网络发送向所述移动终端发送第一指令，以使所述移动终端在接收到所述第一指令后执行清除所述移动终端中的用户信息的操作。

9、根据权利要求 7 所述的方法，其特征在于，所述接收用户发出的清除移动终端中

15 的用户信息的指令之前，所述方法还包括：

接收所述用户输入的锁定密码；

其中，所述锁定密码用于锁定所述移动终端。

10、根据权利要求 9 所述的方法，其特征在于，所述通过所述短信网络向所述移动终

20 端发送与所述移动终端约定的第一短信之前，所述方法还包括：

将所述锁定密码以与所述移动终端约定的格式添加到所述第一短信中。

11、根据权利要求 9 所述的方法，其特征在于，所述通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信之前，所述方法还包括：

25 对所述锁定密码进行加密运算得到所述锁定密码对应的密文；

将所述锁定密码对应的密文以与所述移动终端约定的格式添加到所述第一短信中。

12、根据权利要求 7 所述的方法，其特征在于，所述通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信之前，所述方法还包括：

30 根据所述用户预先输入的身份信息查找所述身份信息对应的电话号码。

13、根据权利要求 12 所述的方法，其特征在于，所述接收用户发出的清除移动终端中的用户信息的指令之前，所述方法还包括：

接收所述用户输入的身份信息和电话号码，并通过所述电话号码向所述移动终端发送
5 验证短信，以对所述电话号码进行验证；

当所述电话号码验证通过后，保存所述用户输入的身份信息与所述电话号码的对应关系。

14、根据权利要求 7 所述的方法，其特征在于，所述通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信之后，所述方法还包括：

接收所述移动终端发送的所述移动终端的位置信息。

15、一种用于防止信息泄露的装置，其特征在于，所述装置包括：

判断模块，用于当移动终端接收到短信时，判断所述短信是否为与服务器约定的第一
15 短信；

清除模块，用于当所述判断模块判断得到所述短信为所述第一短信时，清除所述移动终端中的用户信息。

16、根据权利要求 15 所述的装置，其特征在于，所述清除模块，具体包括：

20 第一删除单元，用于删除所述移动终端本地保存的用户信息；

第二删除单元，用于格式化与所述移动终端连接的存储卡。

17、根据权利要求 15 所述的装置，其特征在于，所述第一短信中携带有用户设定的锁定密码或所述用户设定的锁定密码对应的密文；

25 当所述短信为所述第一短信时，所述装置还包括：

锁定模块，用于锁定所述移动终端，以使所述移动终端在接收并成功验证所述用户输入的所述锁定密码之前处于不可使用状态。

18、根据权利要求 15 所述的装置，其特征在于，当所述移动终端连接有互联网网络
30 时，所述装置还包括：

接收模块，用于接收所述服务器通过互联网网络发送的第一指令；

相应地，所述清除模块，还用于在所述接收模块接收所述服务器通过互联网网络发送的第一指令之后，清除所述移动终端中的用户信息；

其中，所述第一指令用于指示所述移动终端清除所述移动终端中的用户信息。

5

19、根据权利要求 15 所述的装置，其特征在于，所述装置还包括：

发声模块，用于当所述判断模块判断得到所述短信为所述第一短信时，使所述移动终端发声；

或，

10 上报模块，用于当所述判断模块判断得到所述短信为所述第一短信时，向所述服务器上报告所述移动终端的位置信息。

20、根据权利要求 15-19 中任一权利要求所述的装置，其特征在于，所述第一短信对于用户不可见。

15

21、一种用于防止信息泄露的服务器，其特征在于，所述服务器包括：

第一接收模块，用于接收用户发出的清除移动终端中的用户信息的指令；

获取模块，用于获取所述移动终端连接的网络的网络类型；

20 第一发送模块，用于当所述获取模块获取得到所述移动终端连接有短信网络时，通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信，以使所述移动终端执行清除所述移动终端中的用户信息的操作。

22、根据权利要求 21 所述的服务器，其特征在于，所述服务器还包括：

25 第二发送模块，用于当所述获取模块获取得到所述移动终端连接有互联网网络时，通过互联网网络发送向所述移动终端发送第一指令，以使所述移动终端在接收到所述第一指令后执行清除所述移动终端中的用户信息的操作。

23、根据权利要求 21 所述的服务器，其特征在于，所述服务器还包括：

30 第二接收模块，用于在所述第一接收模块接收用户发出的清除移动终端中的用户信息的指令之前，接收所述用户输入的锁定密码；

其中，所述锁定密码用于锁定所述移动终端。

24、根据权利要求 23 所述的服务器，其特征在于，所述服务器还包括：

5 第一添加模块，用于在所述第一发送模块通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信之前，将所述锁定密码以与所述移动终端约定的格式添加到所述第一短信中。

25、根据权利要求 23 所述的服务器，其特征在于，所述服务器还包括：

10 加密模块，用于在所述第一发送模块通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信之前，对所述锁定密码进行加密运算得到所述锁定密码对应的密文；

第二添加模块，用于将所述锁定密码对应的密文以与所述移动终端约定的格式添加到所述第一短信中。

15 26、根据权利要求 21 所述的服务器，其特征在于，所述服务器还包括：

查找模块，用于在所述第一发送模块通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信之前，根据所述用户预先输入的身份信息查找所述身份信息对应的电话号码。

20 27、根据权利要求 26 所述的服务器，其特征在于，所述服务器还包括：

第三接收模块，用于在所述第一接收模块接收用户发出的清除移动终端中的用户信息的指令之前，接收所述用户输入的身份信息和电话号码，并通过所述电话号码向所述移动终端发送验证短信，以对所述电话号码进行验证；

25 保存模块，用于当所述电话号码验证通过后，保存所述用户输入的身份信息与所述电话号码的对应关系。

28、根据权利要求 21 所述的服务器，其特征在于，所述服务器还包括：

第四接收模块，用于在所述第一发送模块通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信之后，接收所述移动终端发送的所述移动终端的位置信息。

30

29、一种用于防止信息泄露的系统，其特征在于，所述系统包括如权利要求 15-20 任一权利要求所述的装置和如权利要求 21-28 任一权利要求所述的服务器。

30、一种设备，其特征在于，所述设备包括：

5 显示屏幕；

一个或多个处理器；

存储器；和

一个或多个模块，所述一个或多个模块存储于所述存储器中并被配置成由所述一个或多个处理器执行，其中，所述一个或多个模块具有如下功能：

10 当所述设备接收到短信时，判断所述短信是否为与服务器约定的第一短信；

当所述短信为所述第一短信时，清除所述设备中的用户信息。

31、一种设备，其特征在于，所述设备包括：

一个或多个处理器；

15 存储器；和

一个或多个模块，所述一个或多个模块存储于所述存储器中并被配置成由所述一个或多个处理器执行，其中，所述一个或多个模块具有如下功能：

接收用户发出的清除移动终端中的用户信息的指令；

获取所述移动终端连接的网络的网络类型；

20 当获取得到所述移动终端连接有短信网络时，通过所述短信网络向所述移动终端发送与所述移动终端约定的第一短信，以使所述移动终端执行清除所述移动终端中的用户信息的操作。

25

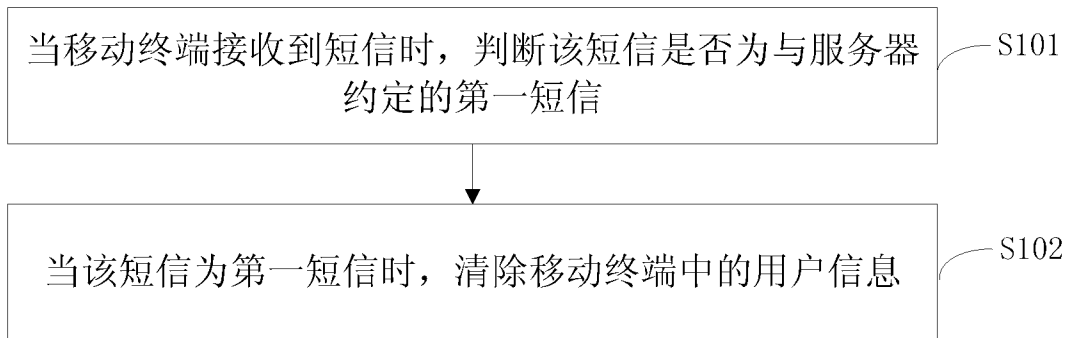


图 1

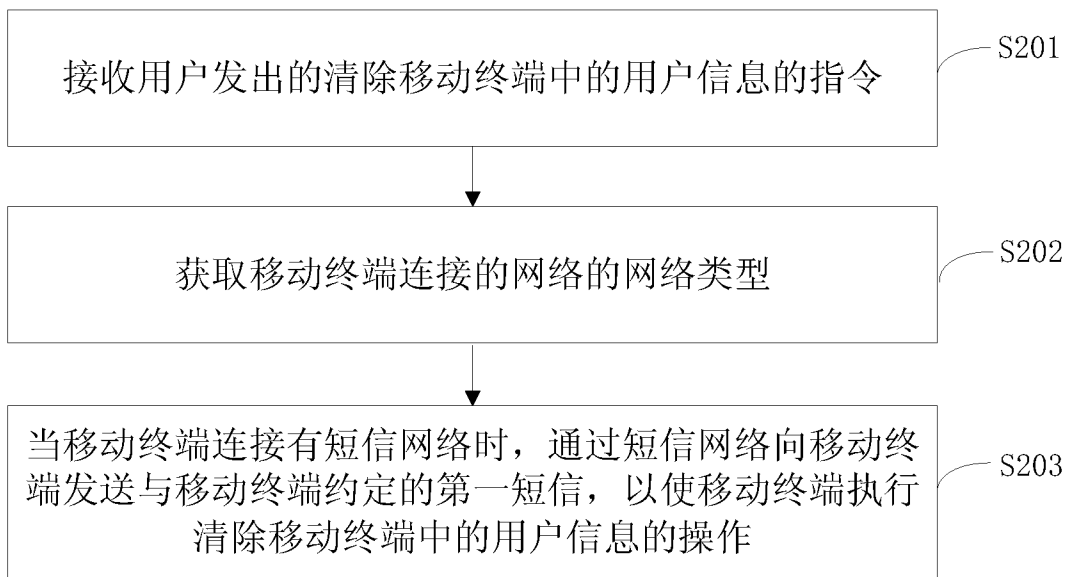


图 2

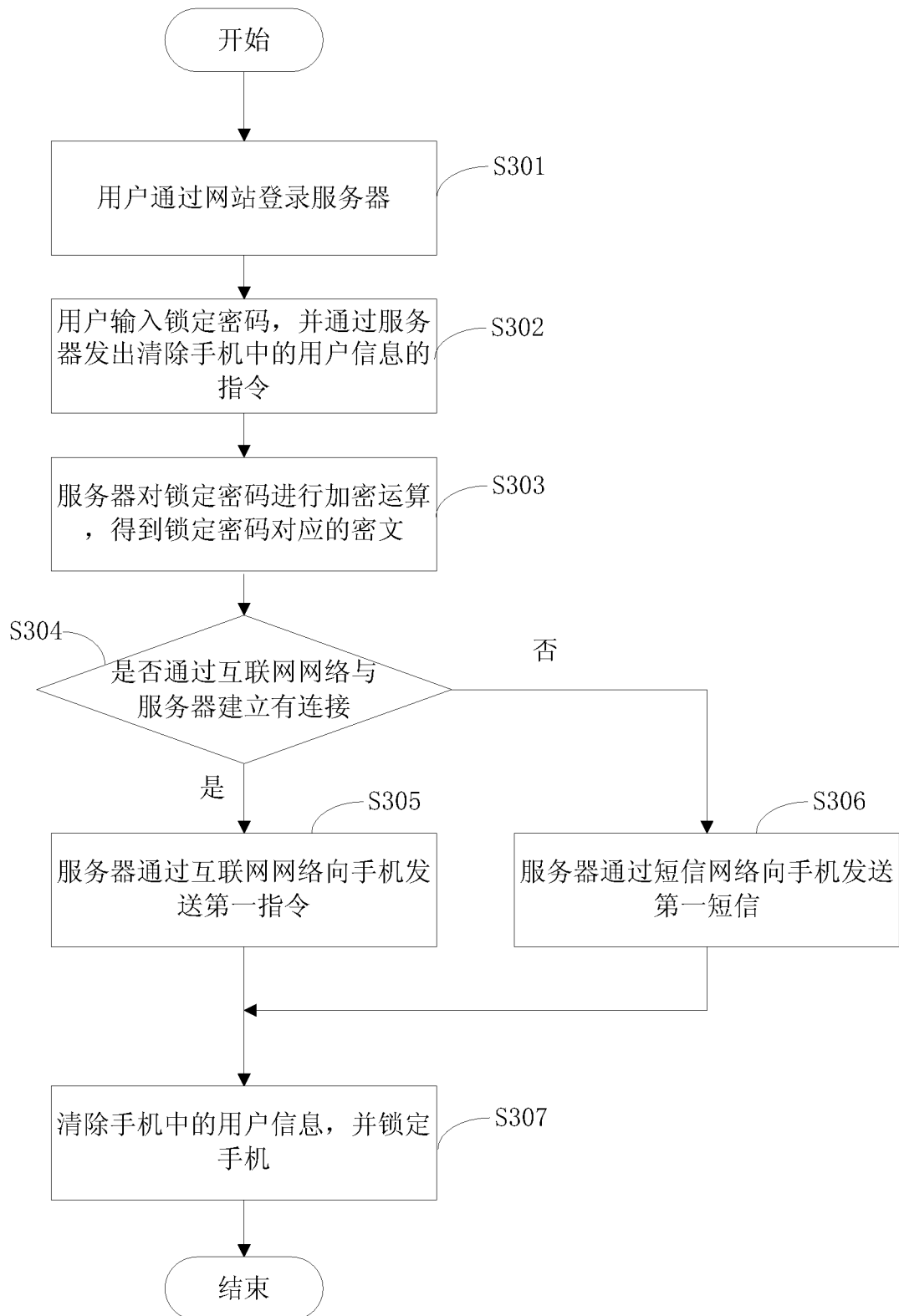


图 3

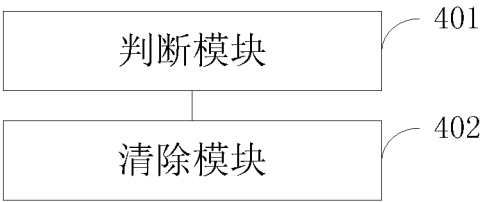


图 4

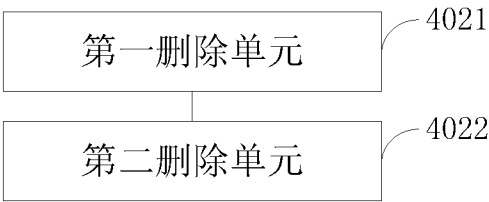


图 5



图 6

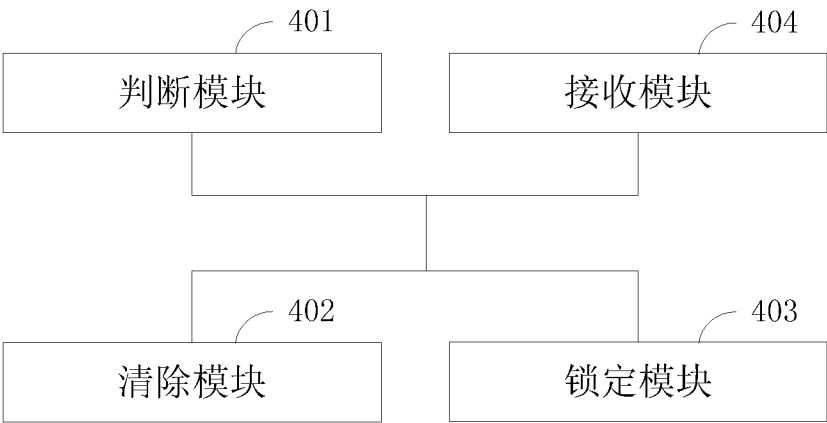


图 7

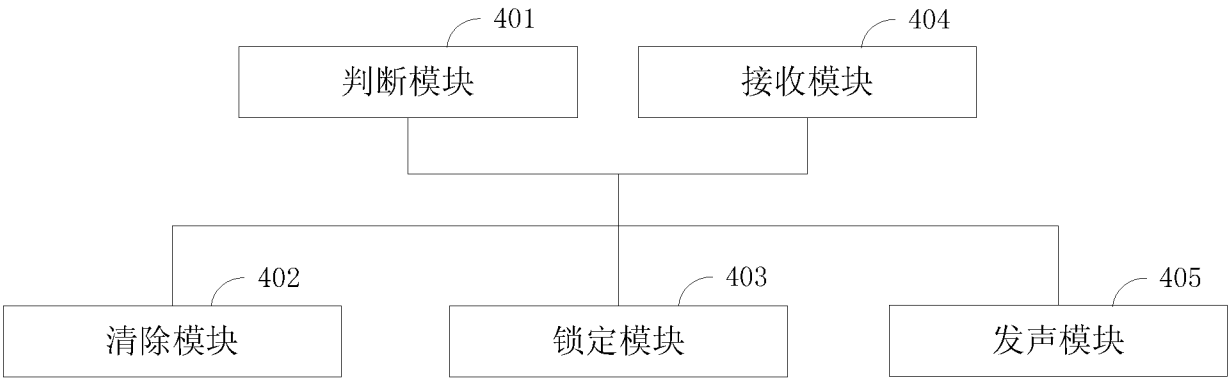


图 8

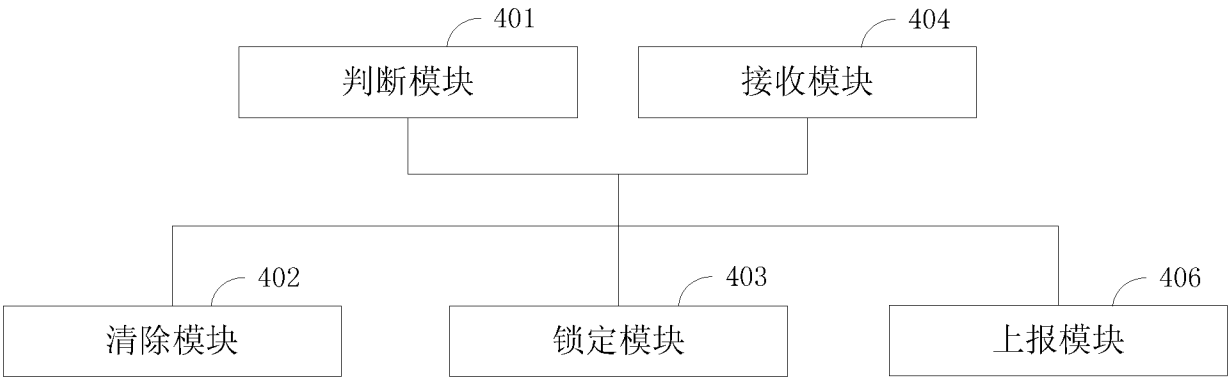


图 9

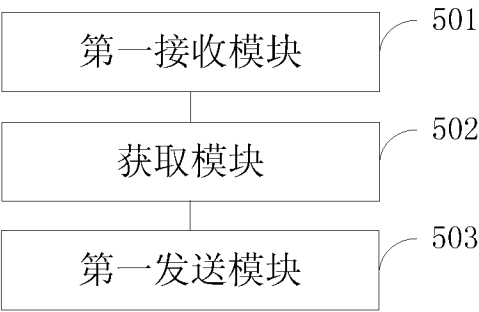


图 10

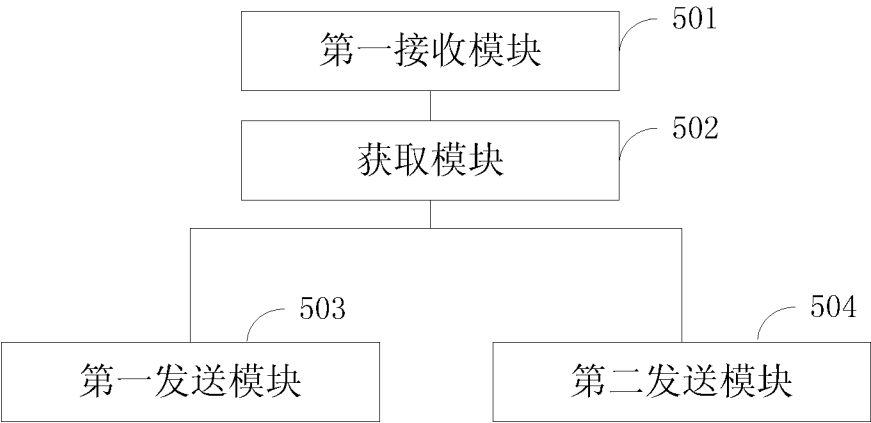


图 11

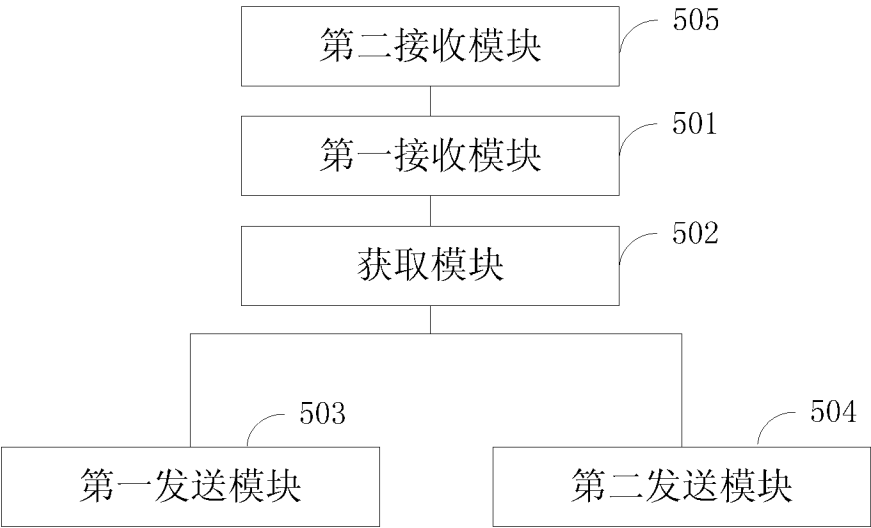


图 12

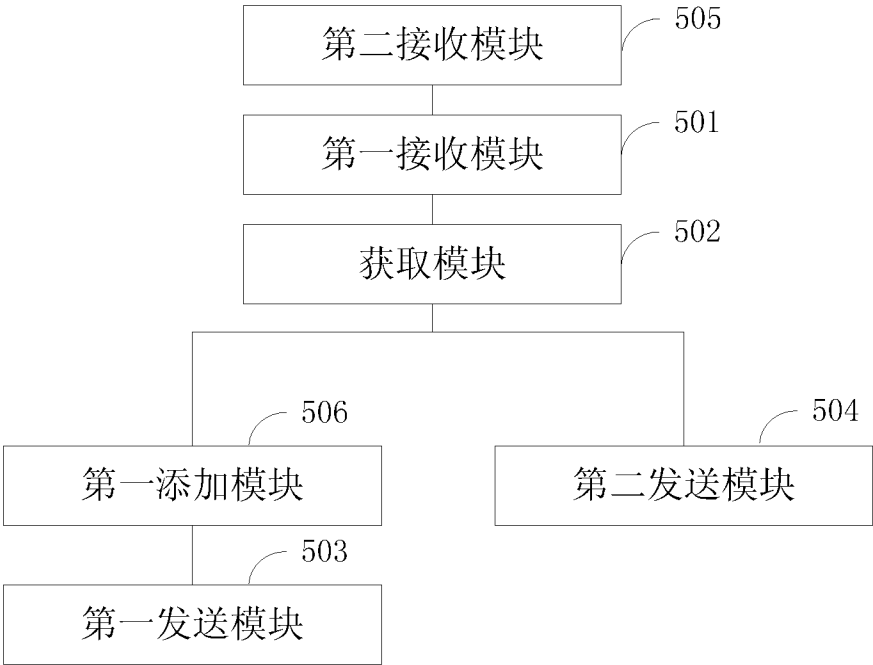


图 13

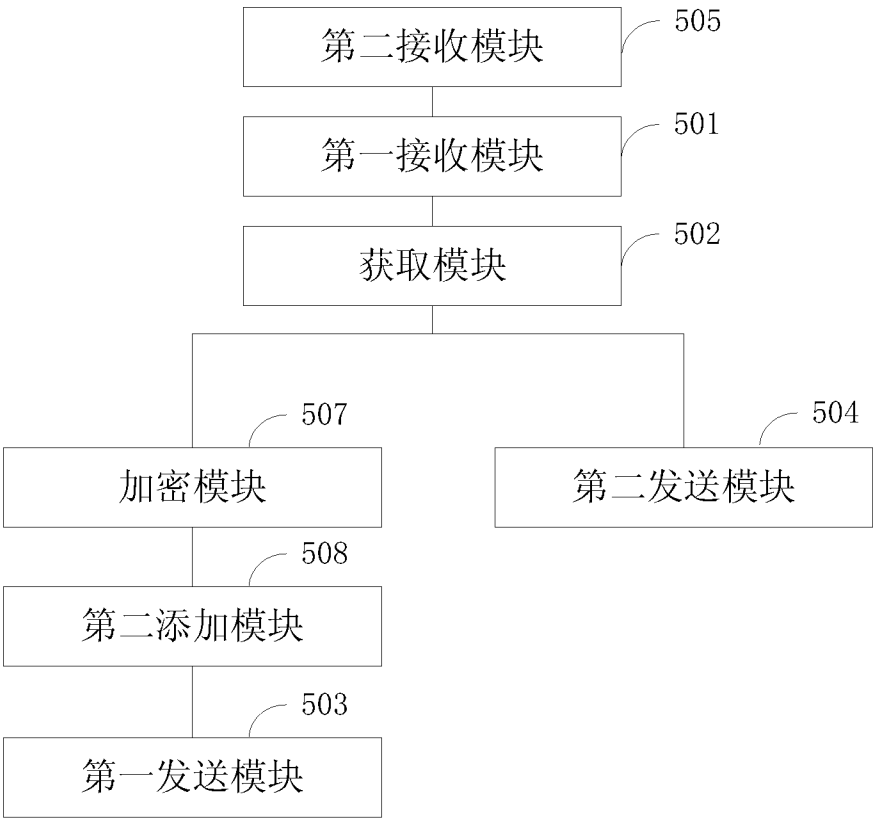


图 14

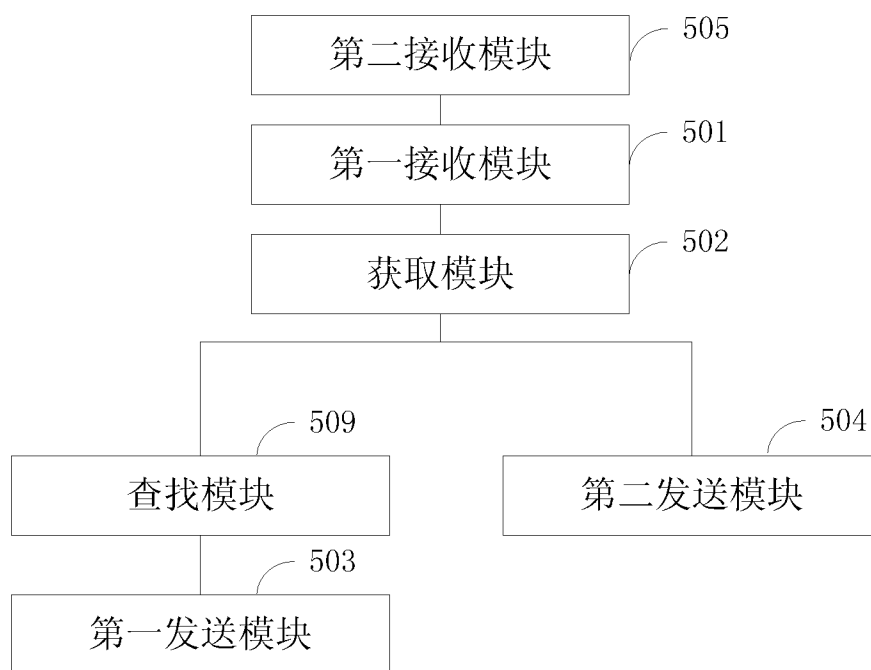


图 15

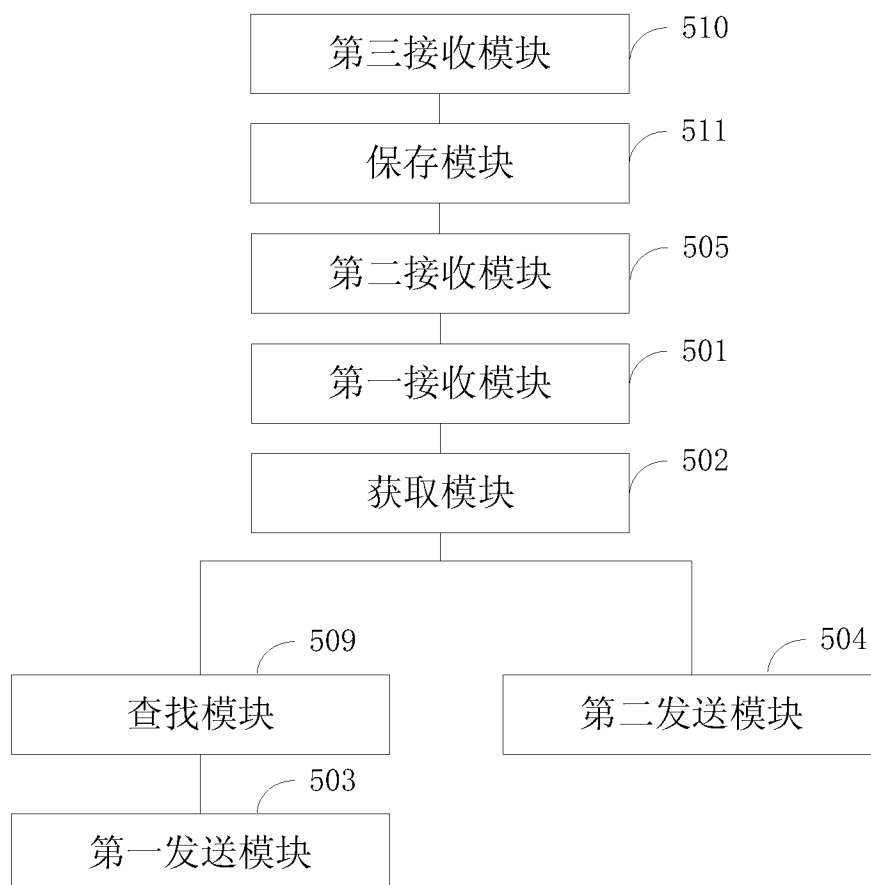


图 16

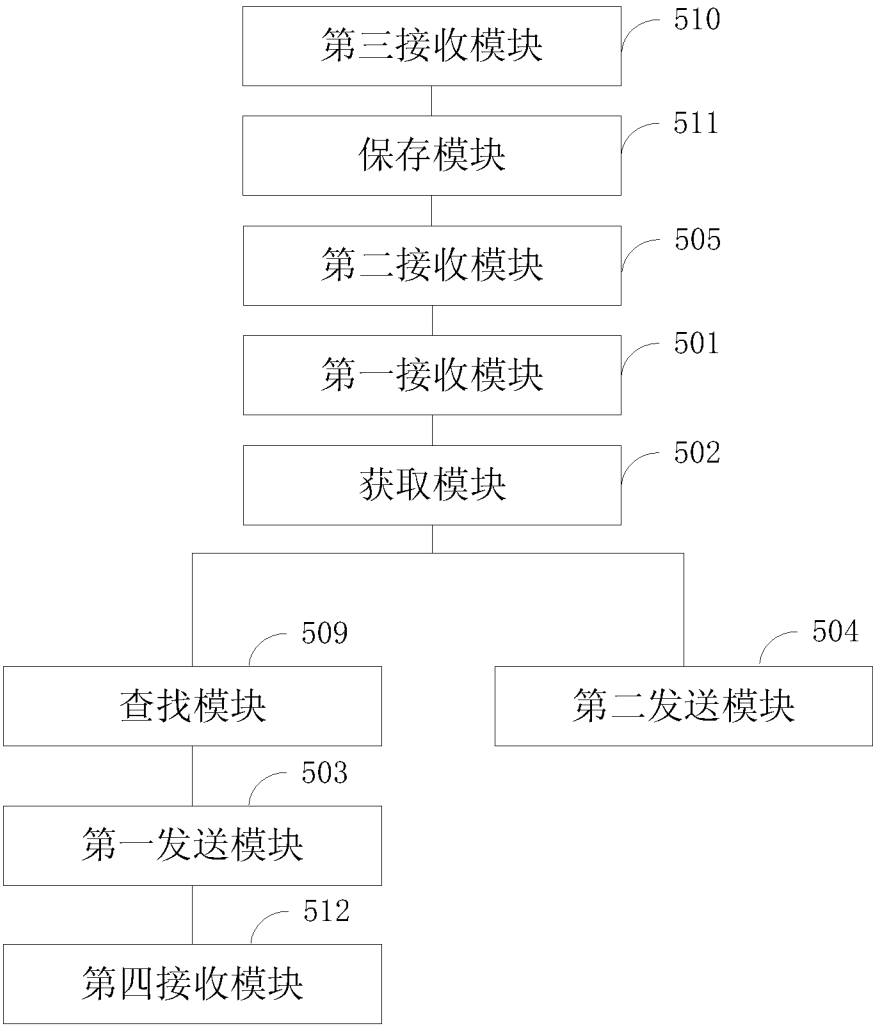


图 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/082678

A. CLASSIFICATION OF SUBJECT MATTER

H04W 4/14 (2009.01) 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)

IPC: H04L; H04Q; H04W; H04B; G02B; G01J; G06F

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)

WPI, EPODOC, CNPAT, CNKI, GOOGLE, 3GPP:
leak+, private, privacy, message, SMS, delet+, phone, format, terminal, instruction

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	CN 102833712 A (BEIJING XIAOMI TECHNOLOGY CO., LTD.) 19 December 2012 (19.12.2012) claims 1-31	1-31
X	CN 101389100 A (TCL TIANYI MOBILE COMMUNICATION (SHENZHEN) CO., LTD.) 18 March 2009 (18.03.2009) description, page 2, the last paragraph to page 3, paragraph [0004]	1-31
X	CN 102368841 A (HUIZHOU TCL MOBILE COMMUNICATION CO., LTD.) 07 March 2012 (07.03.2012) description, paragraphs [0045]-[0080]	1-31
X	CN 101772017 A (SAMSUNG ELECTRONICS (CHINA) R&D CENTER et al.) 07 July 2010 (07.07.2010) description, paragraphs [0015]-[0020]	1-31

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 14 November 2013 (14.11.2013)	Date of mailing of the international search report 12 December 2013 (12.12.2013)
Name and mailing address of the ISA 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 HAO, Zhengyu Telephone No. (86-10) 62413279

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/082678

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102833712 A	19.12.2012	None	
CN 101389100 A	18.03.2009	None	
CN 102368841 A	07.03.2012	None	
CN 101772017 A	07.07.2010	None	

国际检索报告

国际申请号

PCT/CN2013/082678

A. 主题的分类

H04W 4/14 (2009.01) 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)

IPC: H04L; H04Q; H04W; H04B; G02B; G01J; G06F

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))

WPI, EPODOC, CNPAT, CNKI, GOOGLE, 3GPP:

泄露, 隐私, 保密, 短信, 短消息, 删除, 清除, 格式化, 手机, 终端, 指令, 命令, leak+, private, privacy, message, SMS, delet+, phone

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
P,X	CN 102833712 A (北京小米科技有限责任公司) 19.12 月 2012 (19.12.2012) 权利要求 1-31	1-31
X	CN 101389100 A (TCL 天一移动通信(深圳)有限公司) 18.3 月 2009 (18.03.2009) 说明书第 2 页倒数第 1 段至第 3 页第 4 段	1-31
X	CN 102368841 A (惠州 TCL 移动通信有限公司) 07.3 月 2012 (07.03.2012) 说明书第[0045]-[0080]段	1-31
X	CN 101772017 A (三星电子(中国)研发中心等) 07.7 月 2010 (07.07.2010) 说明书第[0015]-[0020]段	1-31

☐ 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

14.11 月 2013 (14.11.2013)

国际检索报告邮寄日期

12.12 月 2013 (12.12.2013)

ISA/CN 的名称和邮寄地址:

中华人民共和国国家知识产权局

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

受权官员

郝政宇

电话号码: (86-10) 62413279

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/082678

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN 102833712 A	19.12.2012	无	
CN 101389100 A	18.03.2009	无	
CN 102368841 A	07.03.2012	无	
CN 101772017 A	07.07.2010	无	