(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
2017 年 11 月 30 日 (30.11.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/202025 A1

(51) 国际专利分类号:
H04W 12/02 (2009.01)

(21) 国际申请号: PCT/CN2017/000057

(22) 国际申请日: 2017 年 1 月 3 日 (03.01.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610348798.8 2016年5月24日 (24.05.2016) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 张乐 (ZHANG, Le); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京康信知识产权代理有限责任公司 (KANGXIN PARTNERS, P.C.); 中国北京市海淀区知春路甲48号盈都大厦A座16层, Beijing 100098 (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, DJ, 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, KH, KN, KP, KR, KW, 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,

(54) **Title:** TERMINAL FILE ENCRYPTION METHOD, TERMINAL FILE DECRYPTION METHOD, AND TERMINAL

(54) **发明名称**: 终端文件加密方法、终端文件解密方法和终端

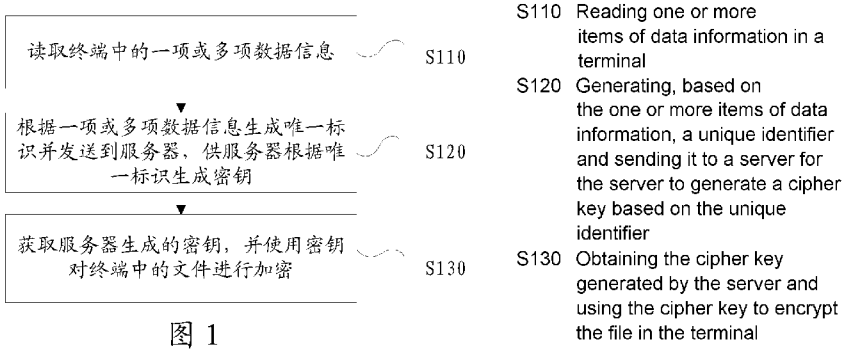

图 1

(57) **Abstract:** The embodiment of the present invention discloses a terminal file encryption method, a terminal file decryption method and a terminal, the terminal file encryption method comprising: reading one or more items of data information in a terminal; generating, based on the one or more items of data information, a unique identifier and sending it to a server for the server to generate a cipher key based on the unique identifier; obtaining the cipher key generated by the server and using the cipher key to encrypt the file in the terminal. The embodiment of the present invention differs from a solution of the related art in which a user him/herself sets a password for encryption and decryption. In the embodiment of the present invention, a cipher key is generated by a server according to the unique identifier of the terminal and is transmitted to the terminal for encryption and decryption without depending on the user to set a password; thus, the cipher key is located in the server and is difficult to be illegally obtained, thereby being useful for ensuring the security of the terminal file.

(57) **摘要**: 本发明实施例公开了一种终端文件加密方法、终端文件解密方法和终端，该终端文件加密方法包括：读取终端中的一项或多项数据信息；根据一项或多项数据信息生成唯一标识并发送到服务器，供服务器根据唯一标识生成密钥；获取服务器生成的密钥，并使用密钥对终端中的文件进行加密。本发明实施例不同于相关技术的用户自行设置密码进行加解密的方案，本发明实施例在不依赖用户设置密码的情况下，通过服务器按终端的唯一标识生成密钥发送给终端进行加解密，则密钥位于服务器中难以被非法获取，有利于保证终端文件的安全性。

WO 2017/202025 A1

[见续页]

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))。

说 明 书

终端文件加密方法、终端文件解密方法和终端

技术领域

本发明实施例涉及数据安全技术领域，尤其涉及一种终端文件加密方法、终端文件解密方法和终端。

背景技术

目前，随着手机等移动终端中大量交流软件的应用，使得用户在手机中留下的信息越来越多。如果手机丢失，用户最关心的是手机中的隐私是否被泄露；如果手机被其他人使用，用户最关心的也是手机中的重要信息是否已泄露。

所以，用户在使用手机过程中，希望对文件、图片等用户比较敏感的内容进行加密来保护。相关技术方案中，往往通过用户设置的密码进行加密，但密码容易遗失。因此，需要一种新的用于保护终端文件的加解密方案，不依赖用户进行密码输入，并保障终端文件的安全性。

发明内容

有鉴于此，本发明实施例提供了一种终端文件加密方法、终端文件解密方法和终端,以至少实现不需要用户设置密码，并保证终端文件的安全性。

本发明实施例解决上述技术问题所采用的技术方案如下：

根据本发明的一个实施例，提供的一种终端文件加密方法，包括：读取终端中的一项或多项数据信息；根据所述一项或多项数据信息生成唯一标识并发送到服务器，供所述服务器根据所述唯一标识生成密钥；获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行加密。

可选地，前述的方法，读取终端中的一项或多项数据信息，具体包括：读取所述终端中身份识别卡的标识信息、所述终端的标识信息、所述终端的网络信息和/或所述文件的存储时间信息。

可选地，前述的方法，在获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行加密之前，还包括：获取所述终端的地域信息，根据所述地域信息从所述终端中选择待加密的文件。

可选地，前述的方法，在读取终端中的一项或多项数据信息之前，还包括：获取用户输入的信息，判断所述用户输入的信息终端的与所述用户身份识别卡对应的个人密码是否相同，在判断结果为是时执行读取终端中的一项或多项数据信息。

依据本发明的另一实施例，提供的一种终端，包括：数据读取模块，设置为读取终端中的一项或多项数据信息；唯一标识生成模块，设置为根据所述一项或多项数据信息生成唯一标识并发送到服务器，供所述服务器根据所述唯一标识生成密钥；加密处理模块，设置为获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行加密。

可选地，前述的终端，所述数据读取模块包括身份识别卡读取模块、终端标识读取模块、网络信息读取模块和/或存储时间读取模块，所述身份识别卡读取模块设置为读取所述终端中身份识别卡的标识信息；所述终端标识读取模块设置为读取所述终端的标识信息；所述网络信息读取模块设置为读取所述终端的网络信息；所述存储时间读取模块设置为读取所述文件的存储时间信息。

可选地，前述的终端，还包括：文件选择模块，设置为获取所述终端的地域信息，根据所述地域信息从所述终端中选择待加密的文件。

可选地，前述的终端，还包括：判断模块，设置为获取用户输入的信息，判断所述用户输入的信息终端的与所述用户身份识别卡对应的个人密码是否相同，在判断结果为是时执行读取终端中的一项或多项数据信息。

依据本发明的另一实施例，提供的一种终端文件解密方法，包括：读取终端中的一项或多项数据信息；根据所述一项或多项数据信息生成唯一标识并发送到服务器，供所述服务器根据所述唯一标识查找预存储的根据所述唯一标识生成的密钥；获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行解密。

可选地，前述的方法，读取终端中的一项或多项数据信息，具体包括：读取所述终端中身份识别卡的标识信息、所述终端的标识信息、所述终端的网络

信息和/或所述文件的存储时间信息。

可选地，前述的方法，在获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行解密之前，还包括：获取所述终端的地域信息，根据所述地域信息从所述终端中选择待解密的文件。

可选地，前述的方法，在读取终端中的一项或多项数据信息之前，还包括：获取用户输入的信息，判断所述用户输入的信息与所述终端的用户身份识别卡对应的个人密码是否相同，在判断结果为是时执行读取终端中的一项或多项数据信息。

依据本发明的另一实施例，提供的一种终端，包括：数据读取模块，设置为读取终端中的一项或多项数据信息；唯一标识生成模块，设置为根据所述一项或多项数据信息生成唯一标识并发送到服务器，供所述服务器根据所述唯一标识查找预存储的根据所述唯一标识生成的密钥；解密处理模块，设置为获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行解密。

可选地，前述的终端，所述数据读取模块包括身份识别卡读取模块、终端标识读取模块、网络信息读取模块和/或存储时间读取模块，所述身份识别卡读取模块设置为读取所述终端中身份识别卡的标识信息；所述终端标识读取模块设置为读取所述终端的标识信息；所述网络信息读取模块设置为读取所述终端的网络信息；所述存储时间读取模块设置为读取所述文件的存储时间信息。

可选地，前述的终端，还包括：文件选择模块，设置为获取所述终端的地域信息，根据所述地域信息从所述终端中选择待解密的文件。

可选地，前述的终端，还包括：判断模块，设置为获取用户输入的信息，判断所述用户输入的信息与所述终端的用户身份识别卡对应的个人密码是否相同，在判断结果为是时执行读取终端中的一项或多项数据信息。

根据以上技术方案，本发明实施例的终端文件加密方法、终端文件解密方法和终端至少具有以下优点：

在本发明实施例的技术方案中，收集终端中的数据信息并生成唯一标识，发送给服务器并由服务器根据唯一标识生成密钥，终端从服务器获取密钥进行对终端文件的加解密；可见不同于相关技术的用户自行设置密码进行加解密的方案，本发明实施例在不依赖用户设置密码的情况下，通过服务器按终端的唯

一标识生成密钥发送给终端进行加解密，则密钥位于服务器中难以被非法获取，有利于保证终端文件的安全性。

附图说明

图1为本发明实施例的一个实施例的终端文件加密方法的流程图；

图2为本发明实施例的一个实施例的终端文件加密方法的流程图；

图3为本发明实施例的一个实施例的终端文件加密方法的工作流程图；

图4为本发明实施例的一个实施例的终端的框图；

图5为本发明实施例的一个实施例的终端的框图；

图6为本发明实施例的一个实施例的终端文件解密方法的流程图；

图7为本发明实施例的一个实施例的终端文件解密方法的流程图；

图8为本发明实施例的一个实施例的终端文件解密方法的工作流程图；

图9为本发明实施例的一个实施例的终端的框图；

图10为本发明实施例的一个实施例的终端的框图。

本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

为了使本发明所要解决的技术问题、技术方案及有益效果更加清楚、明白，以下结合附图和实施例，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，并不用于限定本发明。

如图 1 所示，本发明的一个实施例中提供了一种终端文件加密方法，包括:

步骤 S110，读取终端中的一项或多项数据信息。在本实施例中，对数据信息的类型不进行限制，例如，本实施例中终端的软硬件信息均可以使用。终端包括不限于手机、平板电脑等。

步骤 S120，根据一项或多项数据信息生成唯一标识并发送到服务器，供服务器根据唯一标识生成密钥。在本实施例中，该唯一标识可以是全球唯一标识;

在本实施例中，进一步地，为了保证唯一标识的唯一性，要求一项或多项数据信息具有唯一性，例如可以是终端中存储的用户账号信息等。

步骤 S130，获取服务器生成的密钥，并使用密钥对终端中的文件进行加密。

根据本实施例的技术方案，收集终端中的数据信息并生成唯一标识，发送给服务器并由服务器根据唯一标识生成密钥，终端从服务器获取密钥进行对终端文件的加解密；可见不同于相关技术的用户自行设置密码进行加解密的方案，本发明实施例在不依赖用户设置密码的情况下，通过服务器按终端的唯一标识生成密钥发送给终端进行加解密，则密钥位于服务器中难以被非法获取，有利于保证终端文件的安全性。

如图 2 所示，本发明的一个实施例中提供了一种终端文件加密方法，包括:

步骤 S210，获取用户输入的信息，判断用户输入的信息终端的与用户身份识别卡对应的个人密码是否相同，在判断结果为是时执行步骤 S220。在本实施例中，由于对文件进行加解密为较重要的操作，此时需要验证用户的身份，其中 SIM 卡（用户身份识别卡）的 PIN 码（Personal Identification Number，个人密码）能够指示用户的身份，所以在本实施例中利用 PIN 码对用户身份进行验证。

步骤 S220，读取终端中身份识别卡的标识信息、终端的标识信息、终端的网络信息和/或文件的存储时间信息。在本实施例中， SIM 卡的标识信息可以是 ICCID（Integrate circuit card identity，集成电路卡识别码）或 IMSI（International Mobile Subscriber Identification Number，国际移动用户识别码），终端的标识信息可以是 IMEI（International Mobile Equipment Identity，国际移动设备标识），网络信息可以是 GUTI（Globally Unique Temporary UE Identity，全球唯一临时 UE 标识）或 TMSI（Temporary Mobile Subscriber Identity，临时识别码）。利用上述数据信息的优点在于：在终端正常使用过程中，必然可以从终端中获取到上述数据信息，不需要用户进行设置。

步骤 S230，根据终端中身份识别卡的标识信息、终端的标识信息、终端的网络信息和/或文件的存储时间信息生成唯一标识并发送到服务器，供服务器根

据唯一标识生成密钥。在本实施例中，对于生成唯一标识的方式不进行限制，例如，可以直接将上述信息串联，也可以利用其它函数对上述信息进行运算得到唯一标识。基于上述信息，服务器生成密钥的方式包括但不限于:

密钥的生成公式可以表示为:

Key=ICCID⊕IMSI⊕TMSI⊕TIME

加密文件过程公式为:

FileEncrypted=Key⊕FileByte

其中，Key 是密钥，FileEncrypted 是加密后的文件字节流，表示读取原始文件的按照字节的 FileByte 的字节流后，按 Key 进行加密。⊕表示运算，Key 值是经过多次运算的，因此反向破解也是非常难的。

步骤 S240，获取终端的地域信息，根据地域信息从终端中选择待加密的文件。在本实施例中，地域信息可以是前述的 GUTI，在加密过程中可以通过读取不同小区标识的 GUTI 值实现在不同地域加密不同的文件。

步骤 S250，获取服务器生成的密钥，并使用密钥对终端中的文件进行加密。在本实施例中，为进一步保证文件安全，还对加密后的数据进行隐藏。

本实施例的技术方案的一个具体应用场景如图 3 所示:

1、用户办理 SIM 卡，运营商告知用户 SIM 卡的 PIN 码;

2、用户选择要加密和隐藏的文件。

3、终端读取 SIM 卡标识，例如 ICCID 信息，并临时启用 PIN 校验功能，提示用户输入 PIN 码。

4、如果 PIN 码错误，则 SIM 卡被锁死，用户需到运营商进行解锁和重置 PIN 码，如果 PIN 码正确将读取 ICCID、IMSI,终端标识 IMEI、小区标识 GUTI 和 TMSI 和加密文件存储时间标识等。

5、终端根据如上信息串联或者采用其他混合函数生成一个临时全球唯一标识，并发送此临时全球唯一标识到网络侧的服务器。

6、网络侧服务器接收到此临时全球唯一标识后，对该用户进行身份合法校验（包括不限于此手机和卡有没有被挂失等等），并询问用户是否生成并存储新的密钥或是否更改已有的密钥，如果该用户不存储该密钥或不更改已有的密钥，

服务器向终端用户返回失败信息，终端显示更改提示或错误提示；如果用户需要生成密钥，服务器根据临时的唯一标识生成密钥，按照预先设定的算法生成临时密钥，存储该密钥并向终端侧返回成功信息，同时终端根据该密钥，按照预先设定的算法加密文件并隐藏文件。

如图 4 所示，本发明的一个实施例中提供了一种终端，包括:

数据读取模块 410，读取终端中的一项或多项数据信息。在本实施例中，对数据信息的类型不进行限制，例如，本实施例中终端的软硬件信息均可以使用。

唯一标识生成模块 420，根据一项或多项数据信息生成唯一标识并发送到服务器，供服务器根据唯一标识生成密钥。在本实施例中，该唯一标识可以是全球唯一标识；在本实施例中，进一步地，为了保证唯一标识的唯一性，要求一项或多项数据信息具有唯一性，例如可以是终端中存储的用户账号信息等。

加密处理模块 430，获取服务器生成的密钥，并使用密钥对终端中的文件进行加密。

根据本实施例的技术方案，收集终端中的数据信息并生成唯一标识，发送给服务器并由服务器根据唯一标识生成密钥，终端从服务器获取密钥进行对终端文件的加解密；可见不同于相关技术的用户自行设置密码进行加解密的方案，本发明实施例在不依赖用户设置密码的情况下，通过服务器按终端的唯一标识生成密钥发送给终端进行加解密，则密钥位于服务器中难以被非法获取，有利于保证终端文件的安全性。

如图 5 所示，本发明的一个实施例中提供了一种终端，包括:

判断模块 510，获取用户输入的信息，判断用户输入的信息终端的与用户身份识别卡对应的个人密码是否相同，在判断结果为是时数据读取模块 520 进入工作。在本实施例中，由于对文件进行加解密为较重要的操作，此时需要验证用户的身份，其中 SIM 卡(用户身份识别卡)的 PIN 码(Personal Identification Number，个人密码）能够指示用户的身份，所以在本实施例中利用 PIN 码对用户身份进行验证。

数据读取模块 520，包括身份识别卡读取模块、终端标识读取模块、网络信

息读取模块和/或存储时间读取模块，身份识别卡读取模块设置为读取终端中身份识别卡的标识信息；终端标识读取模块设置为读取终端的标识信息；网络信息读取模块设置为读取终端的网络信息；存储时间读取模块设置为读取文件的存储时间信息。在本实施例中，SIM卡的标识信息可以是ICCID（Integrate circuit card identity，集成电路卡识别码）或IMSI（International Mobile Subscriber Identification Number，国际移动用户识别码），终端的标识信息可以是IMEI（International Mobile Equipment Identity，国际移动设备标识），网络信息可以是GUTI（Globally Unique Temporary UE Identity，全球唯一临时UE标识）或TMSI（Temporary Mobile Subscriber Identity，临时识别码）。利用上述数据信息的优点在于：在终端正常使用过程中，必然可以从终端中获取到上述数据信息，不需要用户进行设置。

唯一标识生成模块530，根据终端中身份识别卡的标识信息、终端的标识信息、终端的网络信息和/或文件的存储时间信息生成唯一标识并发送到服务器，供服务器根据唯一标识生成密钥。在本实施例中，对于生成唯一标识的方式不进行限制，例如，可以直接将上述信息串联，也可以利用其它函数对上述信息进行运算得到唯一标识。基于上述信息，服务器生成密钥的方式包括但不限于：

密钥的生成公式可以表示为：

Key=ICCID⊕IMSI⊕TMSI⊕TIME

加密文件过程公式为：

FileEncrypted=Key⊕FileByte

其中，Key是密钥，FileEncrypted是加密后的文件字节流，表示读取原始文件的按照字节的FileByte的字节流后，按Key进行加密。⊕表示运算，Key值是经过多次运算的，因此反向破解也是非常难的。

文件选择模块540，获取终端的地域信息，根据地域信息从终端中选择待加密的文件。在本实施例中，地域信息可以是前述的GUTI，在加密过程中可以通过读取不同小区标识的GUTI值实现在不同地域加密不同的文件。

加密处理模块550，获取服务器生成的密钥，并使用密钥对终端中的文件进行加密。在本实施例中，为进一步保证文件安全，还对加密后的数据进行隐藏。

本实施例的技术方案的一个具体应用场景如图3所示：

1、用户办理SIM卡，运营商告知用户SIM卡的PIN码;

2、用户选择要加密和隐藏的文件。

3、终端读取SIM卡标识，例如ICCID信息，判断模块临时启用PIN校验功能，提示用户输入PIN码;

4、如果PIN码错误，则SIM卡被锁死，用户需到运营商进行解锁和重置PIN码，如果PIN码正确身份识别卡读取模块、终端标识读取模块、网络信息读取模块、存储时间读取模块将读取ICCID、IMSI,终端标识IMEI、小区标识GUTI和TMSI和加密文件存储时间标识等;

5、唯一标识生成模块根据如上信息串联或者采用其他混合函数生成一个临时全球唯一标识，并发送此临时全球唯一标识到网络侧的服务器。

6、网络侧服务器接收到此临时全球唯一标识后，对该用户进行身份合法校验，并询问用户是否生成并存储新的密钥或是否更改已有的密钥，如果该用户不存储该密钥或不更改已有的密钥，服务器向终端用户返回失败信息，终端显示不更改提示或错误提示；如果用户需要生成密钥，服务器根据临时的唯一标识生成密钥，按照预先设定的算法生成临时密钥，存储该密钥并向终端侧返回成功信息，同时加密处理模块根据该密钥，按照预先设定的算法加密文件并隐藏文件。

如图6所示，本发明的一个实施例中提供了一种终端文件解密方法，包括:

步骤S610，读取终端中的一项或多项数据信息。在本实施例中，对数据信息的类型不进行限制，例如，本实施例中终端的软硬件信息均可以使用。终端包括不限于手机、平板电脑等。

步骤S620，根据一项或多项数据信息生成唯一标识并发送到服务器，供服务器根据唯一标识查找预存储的根据唯一标识生成的密钥。在本实施例中，该唯一标识可以是全球唯一标识；在本实施例中，进一步地，为了保证唯一标识的唯一性，要求一项或多项数据信息具有唯一性，例如可以是终端中存储的用户账号信息等。

步骤S630，获取服务器生成的密钥，并使用密钥对终端中的文件进行解密。

根据本实施例的技术方案，收集终端中的数据信息并生成唯一标识，发送

给服务器，并由服务器查找已根据该唯一标识生成的密钥，终端从服务器获取密钥进行对终端文件的解密；可见不同于相关技术的用户自行设置密码进行加解密的方案，本发明实施例在不依赖用户设置密码的情况下，通过服务器按终端的唯一标识生成密钥发送给终端进行加解密，则密钥位于服务器中难以被非法获取，有利于保证终端文件的安全性。

如图 7 所示，本发明的一个实施例中提供了一种终端文件解密方法，包括:

步骤 S710，获取用户输入的信息，判断用户输入的信息与终端的用户身份识别卡对应的个人密码是否相同，在判断结果为是时执行步骤 720。在本实施例中，由于对文件进行加解密为较重要的操作，此时需要验证用户的身份，其中 SIM 卡（用户身份识别卡）的 PIN 码（Personal Identification Number，个人密码）能够指示用户的身份，所以在本实施例中利用 PIN 码对用户身份进行验证。

步骤 S720，读取终端中身份识别卡的标识信息、终端的标识信息、终端的网络信息和/或文件的存储时间信息。在本实施例中， SIM 卡的标识信息可以是 ICCID（Integrate circuit card identity，集成电路卡识别码）或 IMSI（International Mobile Subscriber Identification Number，国际移动用户识别码），终端的标识信息可以是 IMEI（International Mobile Equipment Identity，国际移动设备标识），网络信息可以是 GUTI（Globally Unique Temporary UE Identity，全球唯一临时 UE 标识）或 TMSI（Temporary Mobile Subscriber Identity，临时识别码）。利用上述数据信息的优点在于：在终端正常使用过程中，必然可以从终端中获取到上述数据信息，不需要用户进行设置。

步骤 S730，根据身份识别卡的标识信息、终端的标识信息、终端的网络信息和/或文件的存储时间信息生成唯一标识并发送到服务器，供服务器根据唯一标识查找预存储的根据唯一标识生成的密钥。在本实施例中，对于生成唯一标识的方式不进行限制，例如，可以直接将上述信息串联，也可以利用其它函数对上述信息进行运算得到唯一标识。基于上述信息，服务器生成密钥的方式包括但不限于:

密钥的生成公式可以表示为:

Key=ICCID⊕IMSI⊕TMSI⊕TIME

加密文件过程公式为:

FileEncrypted=Key⊕FileByte

其中，Key 是密钥，FileEncrypted 是加密后的文件字节流，表示读取原始文件的按照字节的 FileByte 的字节流后，按 Key 进行加密。⊕表示运算，Key 值是经过多次运算的，因此反向破解也是非常难的。

步骤 S740，获取终端的地域信息，根据地域信息从终端中选择待解密的文件。在本实施例中，地域信息可以是前述的 GUTI，在解密过程中可以通过读取不同小区标识的 GUTI 值实现在不同地域解密不同的文件。

步骤 S750，获取服务器生成的密钥，并使用密钥对终端中的文件进行解密。在本实施例中，如文件被隐藏，还需要解除文件的隐藏状态；在本实施例中，假定 Keyserver 是从网络侧服务器获取到的密钥，那么解密过程可以简单的用如下公式算出来:

File=Keyserver⊕FileEncryptedByte

FileEncryptedByte 是加密文件的字节流，Keyserver 是从加密服务器获取到密钥，⊕表示解密运算。

本实施例的技术方案的一个具体应用场景如图 8 所示:

1、用户执行解密动作。

2、终端读取卡标识，例如 ICCID 信息，并且临时启用 PIN 码校验功能提示用户输入 PIN 码。

3、如果输入 PIN 码错误，错误 3 次后 SIM 卡被锁死，用户需到运营商进行解锁和重置 PIN 码；如果 PIN 码正确将读取 ICCID、IMSI,终端标识 IMEI、小区标识 GUTI 和 TMSI 和加密文件存储时间标识等。

4、终端根据如上信息串联或者采用其他混合函数生成一个临时全球唯一标识，并发送此临时全球唯一标识到网络侧服务器。

5、网络侧接收到此临时全球唯一标识后，对该用户进行身份合法校验（包括不限于此手机和卡有没有被挂失等等），如果该用户为非合法用户，网络侧向终端用户返回失败信息，终端显示失败提示；如果用户身份合法，服务器根据

临时标识码检索之前生成和存储的密钥。

6、如果检索密钥失败，网络侧服务器向终端用户返回失败信息，终端显示失败提示，如果密钥检索成功，服务器发送此密钥，并向终端侧返回密钥检索成功的信息。

7、解密处理模块根据收到的密钥尝试解密显示文件，文件解密成功，正常显示被加密或隐藏的文件，文件解密失败提示错误信息。

如图 9 所示，本发明的一个实施例中提供了一种终端，包括:

数据读取模块 910，读取终端中的一项或多项数据信息。在本实施例中，对数据信息的类型不进行限制，例如，本实施例中终端的软硬件信息均可以使用。

唯一标识生成模块 920，根据一项或多项数据信息生成唯一标识并发送到服务器，供服务器根据唯一标识查找预存储的根据唯一标识生成的密钥。在本实施例中，该唯一标识可以是全球唯一标识；在本实施例中，进一步地，为了保证唯一标识的唯一性，要求一项或多项数据信息具有唯一性，例如可以是终端中存储的用户账号信息等。

解密处理模块 930，获取服务器生成的密钥，并使用密钥对终端中的文件进行解密。

根据本实施例的技术方案，收集终端中的数据信息并生成唯一标识，发送给服务器，并由服务器查找已根据该唯一标识生成的密钥，终端从服务器获取密钥进行对终端文件的解密；可见不同于相关技术的用户自行设置密码进行加解密的方案，本发明实施例在不依赖用户设置密码的情况下，通过服务器按终端的唯一标识生成密钥发送给终端进行加解密，则密钥位于服务器中难以被非法获取，有利于保证终端文件的安全性。

如图 10 所示，本发明的一个实施例中提供了一种终端，包括:

判断模块 1010，获取用户输入的信息，判断用户输入的信息与终端的用户身份识别卡对应的个人密码是否相同，在判断结果为是时执行步骤 720。在本实施例中，由于对文件进行加解密为较重要的操作，此时需要验证用户的身份，其中 SIM 卡（用户身份识别卡）的 PIN 码（Personal Identification Number，

个人密码）能够指示用户的身份，所以在本实施例中利用 PIN 码对用户身份进行验证。

数据读取模块 1020，包括身份识别卡读取模块、终端标识读取模块、网络信息读取模块和/或存储时间读取模块，身份识别卡读取模块设置为读取终端中身份识别卡的标识信息；终端标识读取模块设置为读取终端的标识信息；网络信息读取模块设置为读取终端的网络信息；存储时间读取模块设置为读取文件的存储时间信息。在本实施例中， SIM 卡的标识信息可以是 ICCID（Integrate circuit card identity，集成电路卡识别码）或 IMSI（International Mobile Subscriber Identification Number，国际移动用户识别码），终端的标识信息可以是 IMEI（International Mobile Equipment Identity，国际移动设备标识），网络信息可以是 GUTI（Globally Unique Temporary UE Identity，全球唯一临时 UE 标识）或 TMSI（Temporary Mobile Subscriber Identity，临时识别码）。利用上述数据信息的优点在于：在终端正常使用过程中，必然可以从终端中获取到上述数据信息，不需要用户进行设置。

唯一标识生成模块 1030，根据身份识别卡的标识信息、终端的标识信息、终端的网络信息和/或文件的存储时间信息生成唯一标识并发送到服务器，供服务器根据唯一标识查找预存储的根据唯一标识生成的密钥。在本实施例中，对于生成唯一标识的方式不进行限制，例如，可以直接将上述信息串联，也可以利用其它函数对上述信息进行运算得到唯一标识。基于上述信息，服务器生成密钥的方式包括但不限于：

密钥的生成公式可以表示为：

$$Key=ICCID\oplus IMSI\oplus TMSI\oplus TIME$$

加密文件过程公式为：

$$FileEncrypted=Key\oplus FileByte$$

其中，Key 是密钥，FileEncrypted 是加密后的文件字节流，表示读取原始文件的按照字节的 FileByte 的字节流后，按 Key 进行加密。⊕表示运算，Key 值是经过多次运算的，因此反向破解也是非常难的。

文件选择模块 1040，获取终端的地域信息，根据地域信息从终端中选择待解密的文件。在本实施例中，地域信息可以是前述的 GUTI，在解密过程中可以

通过读取不同小区标识的 GUTI 值实现在不同地域解密不同的文件。

解密处理模块 1050，获取服务器生成的密钥，并使用密钥对终端中的文件进行解密。在本实施例中，如文件被隐藏，还需要解除文件的隐藏状态；在本实施例中，假定 Keyserver 是从网络侧服务器获取到的密钥，那么解密过程可以简单的用如下公式算出来:

File=Keyserver⊕FileEncryptedByte

FileEncryptedByte 是加密文件的字节流，Keyserver 是从加密服务器获取到密钥，⊕表示解密运算。

本实施例的技术方案的一个具体应用场景如图 8 所示:

1、用户执行解密动作。

2、终端读取卡标识，例如 ICCID 信息，判断模块启用 PIN 码校验功能提示用户输入 PIN 码。

3、如果输入 PIN 码错误，错误 3 次后 SIM 卡被锁死，用户需到运营商进行解锁和重置 PIN 码；如果 PIN 码正确数据读取模块将读取 ICCID、IMSI,终端标识 IMEI、小区标识 GUTI 和 TMSI 和加密文件存储时间标识等。

4、唯一标识生成模块根据如上信息串联或者采用其他混合函数生成一个临时全球唯一标识，并发送此临时全球唯一标识到网络侧服务器。

5、网络侧接收到此临时全球唯一标识后，对该用户进行身份合法校验，如果该用户为非合法用户，网络侧向终端用户返回失败信息，终端显示失败提示；如果用户身份合法，服务器根据临时标识码检索之前生成和存储的密钥。

6、如果检索密钥失败，网络侧服务器向终端用户返回失败信息，终端显示失败提示，如果密钥检索成功，服务器发送此密钥，并向终端侧返回密钥检索成功的信息。

7、解密处理模块根据收到的密钥尝试解密显示文件，文件解密成功，正常显示被加密或隐藏的文件，文件解密失败提示错误信息。

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根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现

出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可以是手机，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。

本发明的实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以被设置为存储用于执行以下步骤的程序代码:

步骤 S110，读取终端中的一项或多项数据信息。在本实施例中，对数据信息的类型不进行限制，例如，本实施例中终端的软硬件信息均可以使用。终端包括不限于手机、平板电脑等。

步骤 S120，根据一项或多项数据信息生成唯一标识并发送到服务器，供服务器根据唯一标识生成密钥。在本实施例中，该唯一标识可以是全球唯一标识; 在本实施例中，进一步地，为了保证唯一标识的唯一性，要求一项或多项数据信息具有唯一性，例如可以是终端中存储的用户账号信息等。

步骤 S130，获取服务器生成的密钥，并使用密钥对终端中的文件进行加密。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码:

步骤 S610，读取终端中的一项或多项数据信息。在本实施例中，对数据信息的类型不进行限制，例如，本实施例中终端的软硬件信息均可以使用。终端包括不限于手机、平板电脑等。

步骤 S620，根据一项或多项数据信息生成唯一标识并发送到服务器，供服务器根据唯一标识查找预存储的根据唯一标识生成的密钥。在本实施例中，该唯一标识可以是全球唯一标识; 在本实施例中，进一步地，为了保证唯一标识的唯一性，要求一项或多项数据信息具有唯一性，例如可以是终端中存储的用户账号信息等。

步骤 S630，获取服务器生成的密钥，并使用密钥对终端中的文件进行解密。

可选地，在本实施例中，上述存储介质可以包括但不限于: U 盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

可选地，本实施例中的具体示例可以参考上述实施例及可选实施方式中所描述的示例，本实施例在此不再赘述。

显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以

用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

以上参照附图说明了本发明的优选实施例，并非因此局限本发明的权利范围。本领域技术人员不脱离本发明的范围和实质，可以有多种变型方案实现本发明，比如作为一个实施例的特征可用于另一实施例而得到又一实施例。凡在运用本发明的技术构思之内所作的任何修改、等同替换和改进，均应在本发明的权利范围之内。

工业实用性

如上所述，本发明实施例提供的一种终端文件加密方法、终端文件解密方法和终端，具有以下有益效果：收集终端中的数据信息并生成唯一标识，发送给服务器并由服务器根据唯一标识生成密钥，终端从服务器获取密钥进行对终端文件的加解密；可见不同于相关技术的用户自行设置密码进行加解密的方案，本发明实施例在不依赖用户设置密码的情况下，通过服务器按终端的唯一标识生成密钥发送给终端进行加解密，则密钥位于服务器中难以被非法获取，有利于保证终端文件的安全性。

权 利 要 求 书

1.一种终端文件加密方法，包括:

读取终端中的一项或多项数据信息;

根据所述一项或多项数据信息生成唯一标识并发送到服务器，供所述服务器根据所述唯一标识生成密钥;

获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行加密。

2.根据权利要求 1 所述的方法，其中，读取终端中的一项或多项数据信息，具体包括:

读取所述终端中身份识别卡的标识信息、所述终端的标识信息、所述终端的网络信息和/或所述文件的存储时间信息。

3.根据权利要求 1 所述的方法，其中，在获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行加密之前，还包括:

获取所述终端的地域信息，根据所述地域信息从所述终端中选择待加密的文件。

4.根据权利要求 1 至 3 任一项所述的方法，其中，在读取终端中的一项或多项数据信息之前，还包括:

获取用户输入的信息，判断所述用户输入的信息终端的与所述用户身份识别卡对应的个人密码是否相同，在判断结果为是时执行读取终端中的一项或多项数据信息。

5.一种终端，包括:

数据读取模块，设置为读取终端中的一项或多项数据信息;

唯一标识生成模块，设置为根据所述一项或多项数据信息生成唯一标识并发送到服务器，供所述服务器根据所述唯一标识生成密钥;

加密处理模块，设置为获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行加密。

6.根据权利要求 5 所述的终端，其中，所述数据读取模块包括身份识别卡读取模块、终端标识读取模块、网络信息读取模块和/或存储时间读取模块，

所述身份识别卡读取模块设置为读取所述终端中身份识别卡的标识信息;

所述终端标识读取模块设置为读取所述终端的标识信息;

所述网络信息读取模块设置为读取所述终端的网络信息;

所述存储时间读取模块设置为读取所述文件的存储时间信息。

7.根据权利要求 5 所述的终端，其中，还包括:

文件选择模块，设置为获取所述终端的地域信息，根据所述地域信息从所述终端中选择待加密的文件。

8.根据权利要求 5 至 7 任一项所述的终端，其中，还包括:

判断模块，设置为获取用户输入的信息，判断所述用户输入的信息终端的与所述用户身份识别卡对应的个人密码是否相同，在判断结果为是时执行读取终端中的一项或多项数据信息。

9.一种终端文件解密方法，包括:

读取终端中的一项或多项数据信息;

根据所述一项或多项数据信息生成唯一标识并发送到服务器，供所述服务器根据所述唯一标识查找预存储的根据所述唯一标识生成的密钥;

获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行解密。

10.一种终端，包括:

数据读取模块，设置为读取终端中的一项或多项数据信息;

唯一标识生成模块，设置为根据所述一项或多项数据信息生成唯一标识并发送到服务器，供所述服务器根据所述唯一标识查找预存储的根据所述唯一标识生成的密钥;

解密处理模块，设置为获取所述服务器生成的密钥，并使用所述密钥对所述终端中的文件进行解密。

11.一种存储介质，设置为存储用于执行如权利要求 1 至 4 中任一项所述的终端文件加密方法的计算机程序。

12.一种存储介质，设置为存储用于执行如权利要求 9 所述的终端文件解密方法的计算机程序。

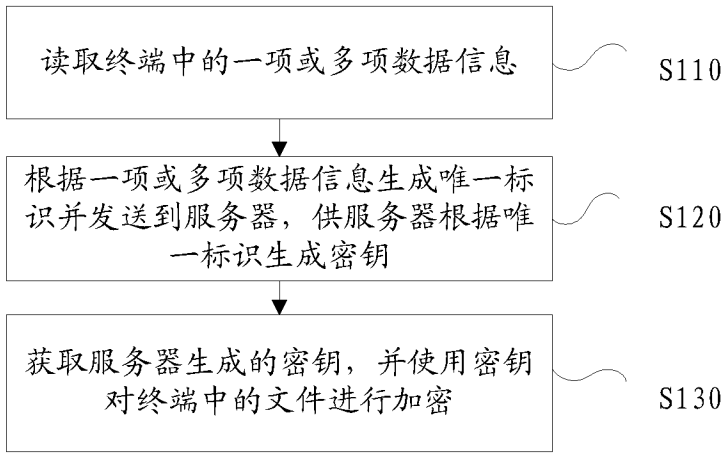
读取终端中的一项或多项数据信息
S110
根据一项或多项数据信息生成唯一标识并发送到服务器，供服务器根据唯一标识生成密钥
S120
获取服务器生成的密钥，并使用密钥对终端中的文件进行加密
S130

图 1

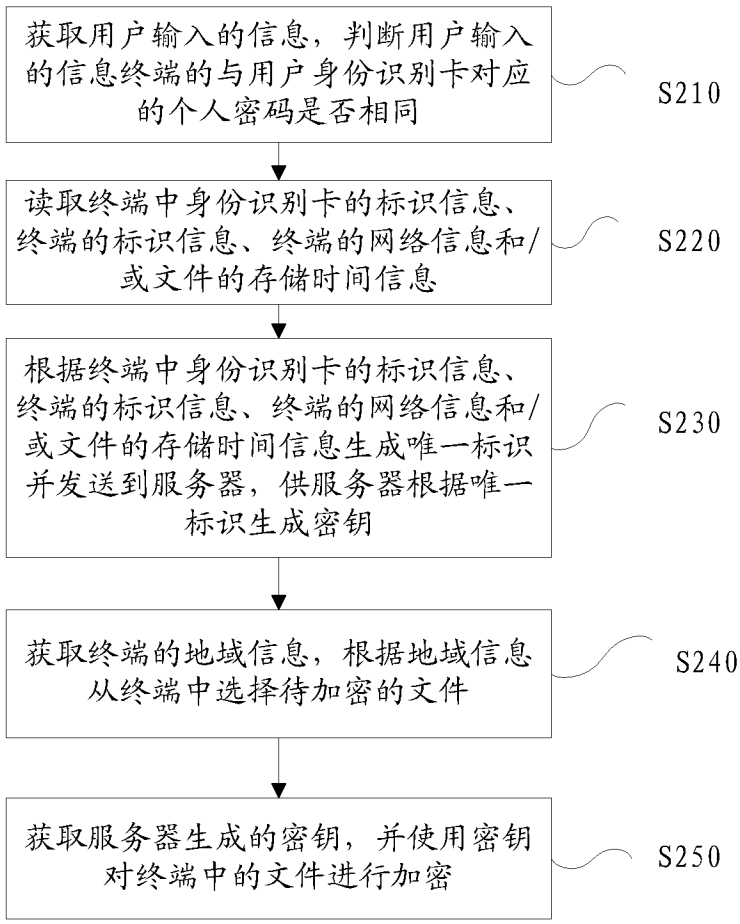
获取用户输入的信息，判断用户输入的信息终端的与用户身份识别卡对应的个人密码是否相同
S210
读取终端中身份识别卡的标识信息、终端的标识信息、终端的网络信息和/或文件的存储时间信息
S220
根据终端中身份识别卡的标识信息、终端的标识信息、终端的网络信息和/或文件的存储时间信息生成唯一标识并发送到服务器，供服务器根据唯一标识生成密钥
S230
获取终端的地域信息，根据地域信息从终端中选择待加密的文件
S240
获取服务器生成的密钥，并使用密钥对终端中的文件进行加密
S250

图 2

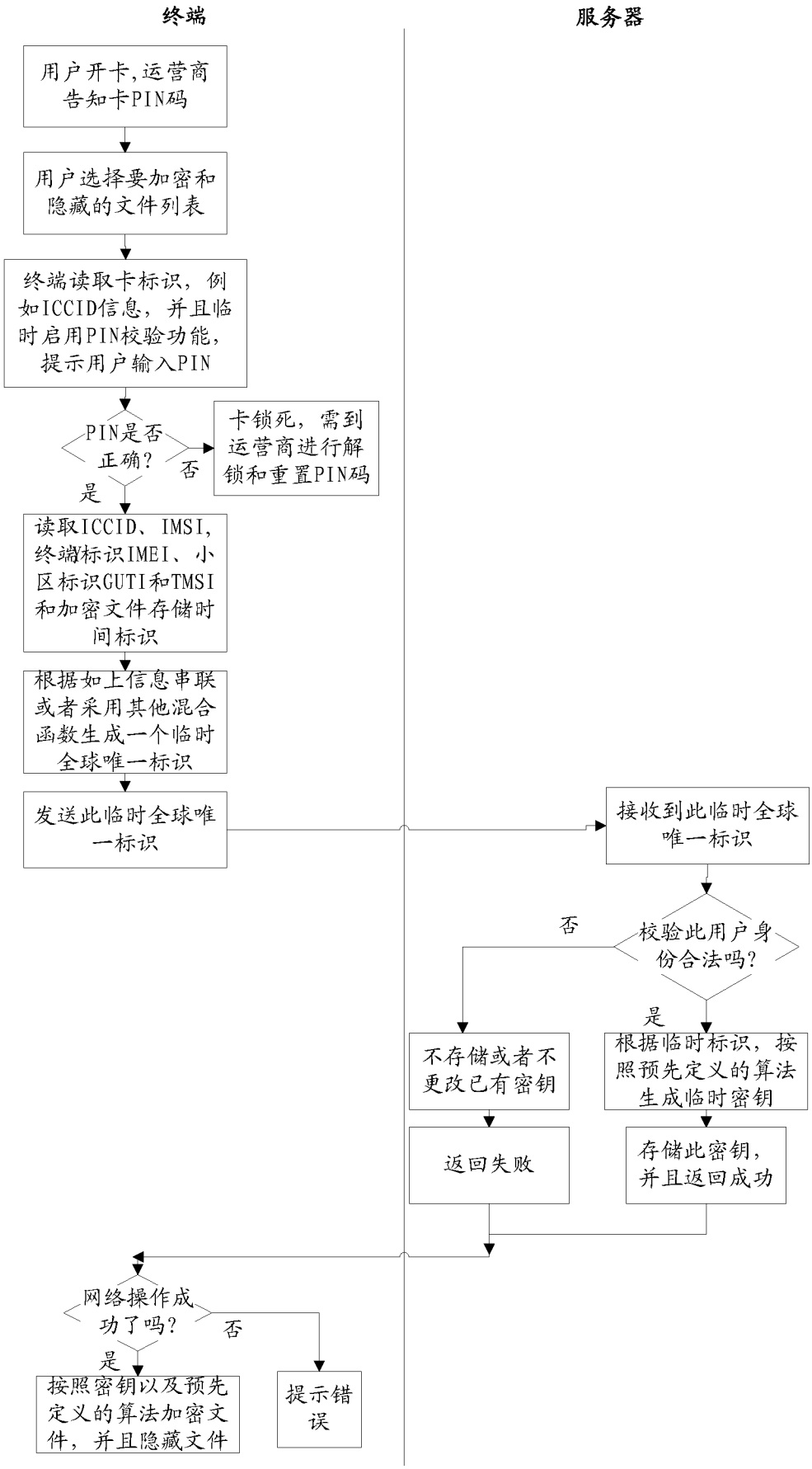
终端
服务器
用户开卡,运营商告知卡PIN码
用户选择要加密和隐藏的文件列表
终端读取卡标识，例如ICCID信息，并且临时启用PIN校验功能，提示用户输入PIN
PIN是否正确？
否
卡锁死，需到运营商进行解锁和重置PIN码
是
读取ICCID、IMSI，终端标识IMEI、小区标识GUTI和TMSI和加密文件存储时间标识
根据如上信息串联或者采用其他混合函数生成一个临时全球唯一标识
发送此临时全球唯一标识
接收到此临时全球唯一标识
校验此用户身份合法吗？
否
是
不存储或者不更改已有密钥
根据临时标识，按照预先定义的算法生成临时密钥
返回失败
存储此密钥，并且返回成功
网络操作成功了吗？
否
是
按照密钥以及预先定义的算法加密文件，并且隐藏文件
提示错误

图 3

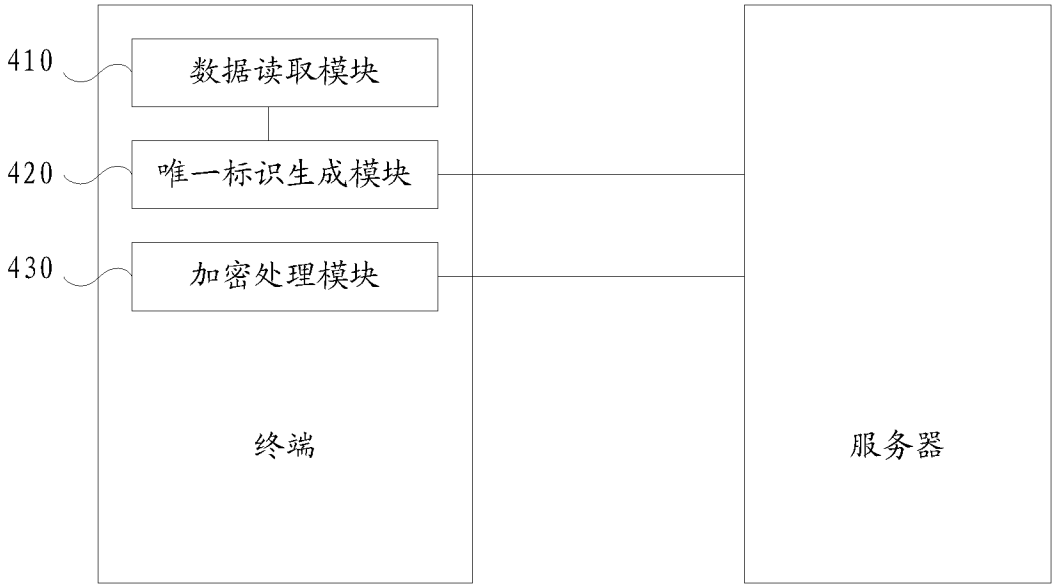
410
数据读取模块
420
唯一标识生成模块
430
加密处理模块
终端
服务器

图 4

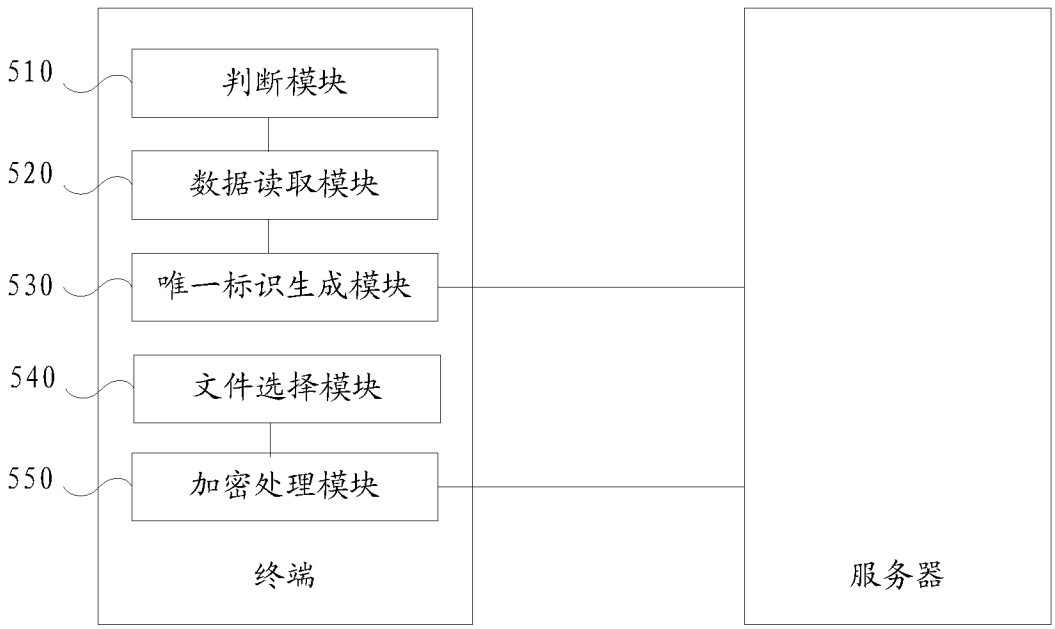
510
判断模块
520
数据读取模块
530
唯一标识生成模块
540
文件选择模块
550
加密处理模块
终端
服务器

图 5

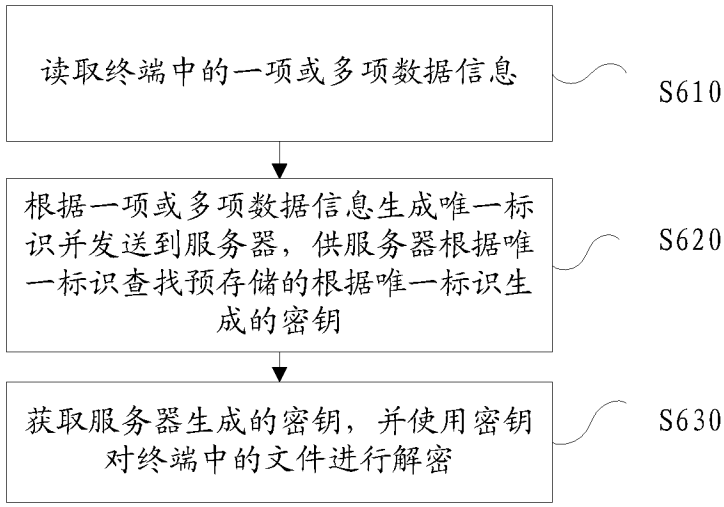
读取终端中的一项或多项数据信息
S610
根据一项或多项数据信息生成唯一标识并发送到服务器，供服务器根据唯一标识查找预存储的根据唯一标识生成的密钥
S620
获取服务器生成的密钥，并使用密钥对终端中的文件进行解密
S630

图 6

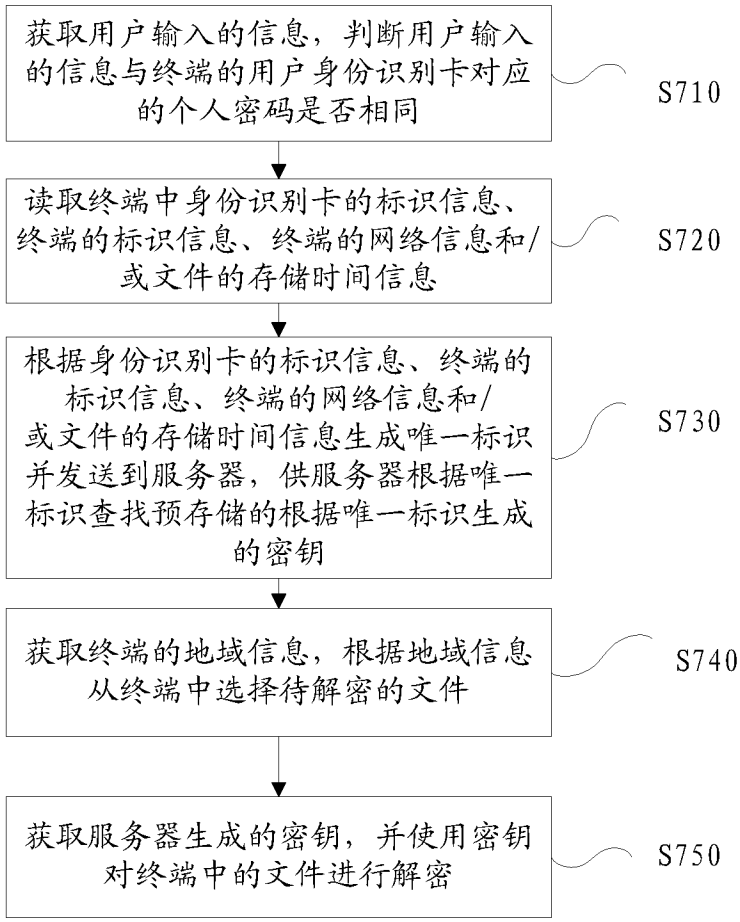
获取用户输入的信息，判断用户输入的信息与终端的用户身份识别卡对应的个人密码是否相同
S710
读取终端中身份识别卡的标识信息、终端的标识信息、终端的网络信息和/或文件的存储时间信息
S720
根据身份识别卡的标识信息、终端的标识信息、终端的网络信息和/或文件的存储时间信息生成唯一标识并发送到服务器，供服务器根据唯一标识查找预存储的根据唯一标识生成的密钥
S730
获取终端的地域信息，根据地域信息从终端中选择待解密的文件
S740
获取服务器生成的密钥，并使用密钥对终端中的文件进行解密
S750

图 7

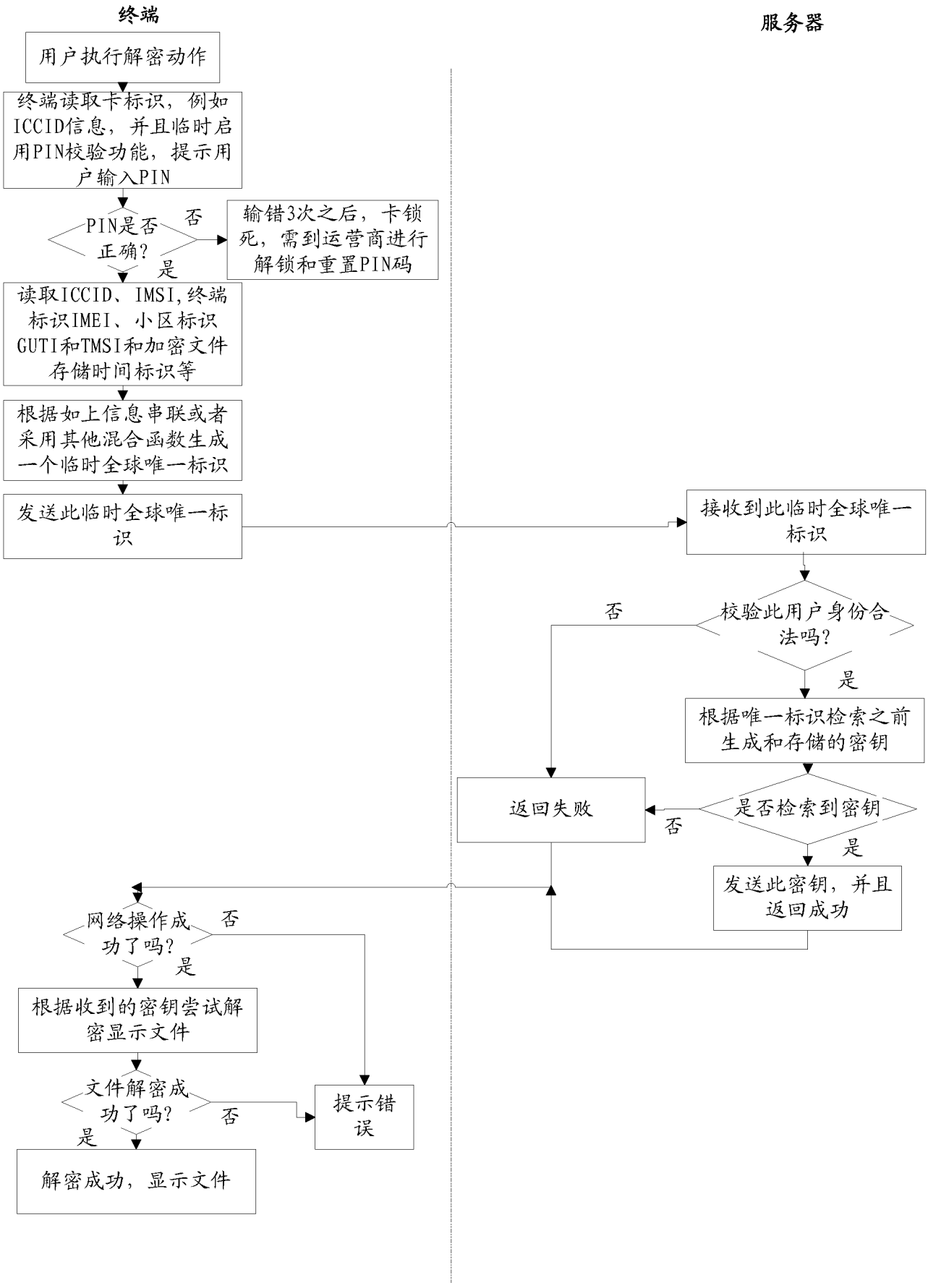
终端
服务器
用户执行解密动作
终端读取卡标识，例如ICCID信息，并且临时启用PIN校验功能，提示用户输入PIN
PIN是否正确?
否
是
输错3次之后，卡锁死，需到运营商进行解锁和重置PIN码
读取ICCID、IMSI,终端标识IMEI、小区标识GUTI和TMSI和加密文件存储时间标识等
根据如上信息串联或者采用其他混合函数生成一个临时全球唯一标识
发送此临时全球唯一标识
接收到此临时全球唯一标识
校验此用户身份合法吗?
否
是
根据唯一标识检索之前生成和存储的密钥
返回失败
是否检索到密钥
否
是
发送此密钥，并且返回成功
网络操作成功了吗?
否
是
根据收到的密钥尝试解密显示文件
文件解密成功了吗?
否
是
提示错误
解密成功，显示文件

图 8

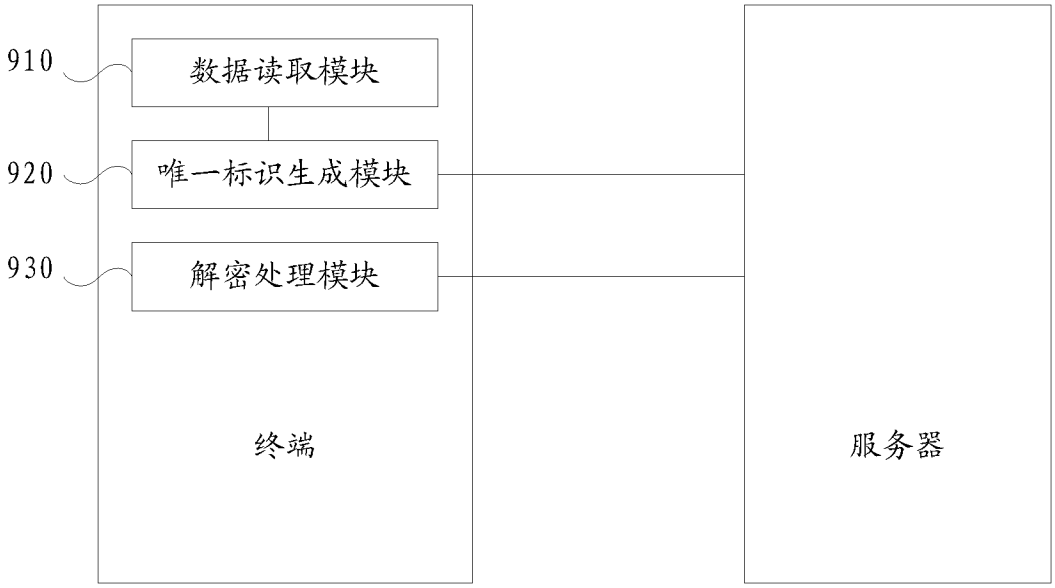
910
数据读取模块
920
唯一标识生成模块
930
解密处理模块
终端
服务器

图 9

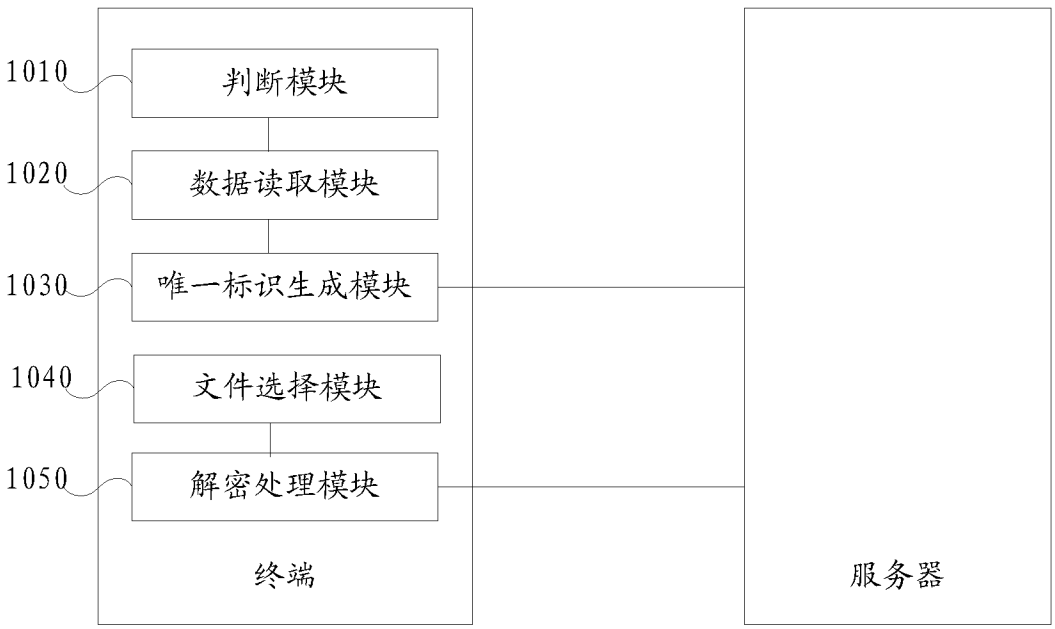
1010
判断模块
1020
数据读取模块
1030
唯一标识生成模块
1040
文件选择模块
1050
解密处理模块
终端
服务器

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/000057

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/02 (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)

H04W; H04Q

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)

CNPAT, CNKI, WPI, EPODOC: communication terminal, application, encrypt+, decrypt+, secret key, match+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104378203 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 25 February 2015 (25.02.2015) description, paragraphs [0033]-[0055]	1-12
A	CN 102938032 A (ZTE CORPORATION) 20 February 2013 (20.02.2013) the whole document	1-12
A	CN 104102858 A (ZTE CORPORATION) 15 October 2014 (15.10.2014) the whole document	1-12
A	CN 103813314 A (HUAWEI TECHNOLOGIES CO., LTD.) 21 May 2014 (21.05.2014) the whole document	1-12
A	US 2015281224 A1 (VERIFONE, INC.) 01 October 2015 (01.10.2015) the whole document	1-12

☐ 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
09 March 2017	29 March 2017
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 PENG, Liang Telephone No. (86-10) 62413350

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/000057

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104378203 A	25 February 2015	None	
CN 102938032 A	20 February 2013	US 2015288685 A1	08 October 2015
		JP 2015535151 A	07 December 2015
		WO 2013182154 A1	12 December 2013
		EP 2905715 A1	12 August 2015
CN 104102858 A	15 October 2014	EP 2985712 A1	17 February 2016
		JP 2016515778 A	30 May 2016
		US 2016055339 A1	25 February 2016
		WO 2014166193 A1	16 October 2014
CN 103813314 A	21 May 2014	EP 2919497 A1	16 September 2015
		US 2015245195 A1	27 August 2015
		WO 2014071725 A1	15 May 2014
US 2015281224 A1	01 October 2015	US 2011239000 A1	29 September 2011
		US 2013304594 A1	14 November 2013

国际检索报告

国际申请号
PCT/CN2017/000057

A. 主题的分类

H04W 12/02(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)

H04W; H04Q

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））

CNPAT,CNKI,WPI,EPODOC:通讯终端，移动终端，应用程序，加密，解密，密钥，匹配；communication terminal, application, encrypt+, decrypt+, secret key, match+

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
X	CN 104378203 A (腾讯科技深圳有限公司) 2015年 2月 25日 (2015-02-25) 说明书第0033-0055段	1-12
A	CN 102938032 A (中兴通讯股份有限公司) 2013年 2月 20日 (2013-02-20) 全文	1-12
A	CN 104102858 A (中兴通讯股份有限公司) 2014年 10月 15日 (2014-10-15) 全文	1-12
A	CN 103813314 A (华为技术有限公司) 2014年 5月 21日 (2014-05-21) 全文	1-12
A	US 2015281224 A1 (VERIFONE, INC.) 2015年 10月 1日 (2015-10-01) 全文	1-12

☐ 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
2017年 3月 9日	2017年 3月 29日
ISA/CN的名称和邮寄地址 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 传真号 (86-10)62019451	受权官员 彭亮 电话号码 (86-10)62413350

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/000057

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	104378203	A	2015年 2月 25日	无			
CN	102938032	A	2013年 2月 20日	US	2015288685	A1	2015年 10月 8日
				JP	2015535151	A	2015年 12月 7日
				WO	2013182154	A1	2013年 12月 12日
				EP	2905715	A1	2015年 8月 12日
CN	104102858	A	2014年 10月 15日	EP	2985712	A1	2016年 2月 17日
				JP	2016515778	A	2016年 5月 30日
				US	2016055339	A1	2016年 2月 25日
				WO	2014166193	A1	2014年 10月 16日
CN	103813314	A	2014年 5月 21日	EP	2919497	A1	2015年 9月 16日
				US	2015245195	A1	2015年 8月 27日
				WO	2014071725	A1	2014年 5月 15日
US	2015281224	A1	2015年 10月 1日	US	2011239000	A1	2011年 9月 29日
				US	2013304594	A1	2013年 11月 14日