

(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
2022 年 12 月 1 日 (01.12.2022)



(10) 国际公布号
WO 2022/247639 A1

(51) 国际专利分类号:
G06F 21/79 (2013.01)

湖街道红荔西路8089号深业中城6号楼A单元3401, Guangdong 518040 (CN)。

(21) 国际申请号: PCT/CN2022/092296

(22) 国际申请日: 2022 年 5 月 11 日 (11.05.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110566480.8 2021年5月24日 (24.05.2021) CN

(71) 申请人: 荣耀终端有限公司(HONOR DEVICE CO., LTD.) [CN/CN]; 中国广东省深圳市福田区香蜜湖街道红荔西路8089号深业中城6号楼A单元3401, Guangdong 518040 (CN)。

(72) 发明人: 于洪健(YU, Hongjian); 中国广东省深圳市福田区香蜜湖街道红荔西路8089号深业中城6号楼A单元3401, Guangdong 518040 (CN)。李霜(LI, Shuang); 中国广东省深圳市福田区香蜜湖街道红荔西路8089号深业中城6号楼A单元3401, Guangdong 518040 (CN)。王飞(WANG, Fei); 中国广东省深圳市福田区香蜜湖街道红荔西路8089号深业中城6号楼A单元3401, Guangdong 518040 (CN)。

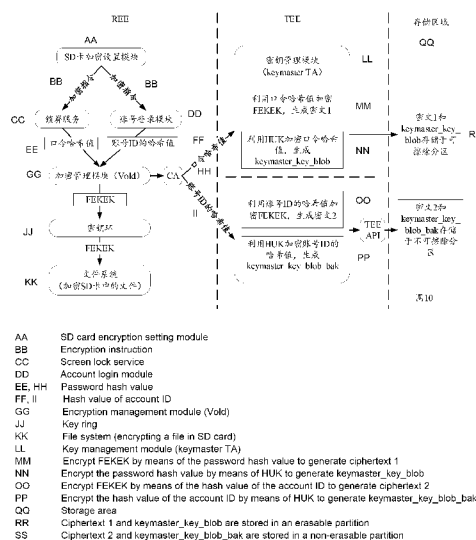
(74) 代理人: 深圳中一联合知识产权代理有限公司(SHENZHEN ZHONGYI UNION INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市福田区莲花街道紫荆社区深南大道6008号深圳特区报业大厦33层, Guangdong 518034 (CN)。

(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, IQ, IR, IS, IT, JM, JO, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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,

(54) Title: METHOD AND APPARATUS FOR STORING CIPHERTEXT

(54) 发明名称: 保存密文的方法和装置



(57) Abstract: A method and apparatus for storing ciphertext. The method comprises: obtaining an encryption instruction, the encryption instruction instructs to encrypt a file in an external memory; obtaining a feature value of a first account identifier according to the encryption instruction; encrypting a first key by means of the feature value of the first account identifier to generate first ciphertext, wherein the first key is used to encrypt a second key, and the second key is used to encrypt a first file in the external memory; encrypting the feature value of the first account identifier to generate second ciphertext; and storing the first ciphertext and the second ciphertext in a non-erasable partition. The method and apparatus can solve the problem that data in an external memory cannot be decrypted after an electronic device executes factory reset.

(57) 摘要: 一种保存密文的方法和装置, 方法包括: 获取加密指令, 加密指令指示加密外置存储器中的文件; 根据加密指令获取第一账号标识的特征值; 使用第一账号标识的特征值加密第一密钥, 生成第一密文, 其中, 第一密钥用于加密第二密钥, 第二密钥用于加密外置存储器中的第一文件; 加密第一账号标识的特征值, 生成第二密文; 将第一密文和第二密文存储于不可擦除分区。方法和装置能够解决电子设备执行工厂级重置后外置存储器中的数据无法解密的问题。

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))。

保存密文的方法和装置

本申请要求于2021年05月24日提交国家知识产权局、申请号为202110566480.8、
5 申请名称为“保存密文的方法和装置”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

本申请涉及终端领域，具体涉及一种保存密文的方法和装置。

背景技术

随着增强移动宽带（enhanced mobile broadband, eMBB）、高清视频等大数据量
业务的出现，电子设备面临存储空间不足的问题。与电子设备连接的外置存储器（如
安全数码（secure digital, SD）卡）能够解决存储空间不足的问题，为了保障数据安
15 全，外置存储器中的数据需要加密保存。

外置存储器的密钥被锁屏口令加密后存储在电子设备的可擦除分区中，当用户对电
子设备实施工厂级重置（factory reset）时，可擦除分区内加密的密钥（即，密文）来
不及保存即被删除，从而导致外置存储器中的数据无法解密。

发明内容

本申请提供了一种保存密文的方法和装置，能够解决电子设备执行工厂级重置后
外置存储器中的数据无法解密的问题。

第一方面，提供了一种保存密文的方法，包括：获取加密指令，所述加密指令指
示加密外置存储器中的文件；根据所述加密指令获取第一账号标识的特征值；使用所
25 述第一账号标识的特征值加密第一密钥，生成第一密文，其中，所述第一密钥用于加
密第二密钥，所述第二密钥用于加密所述外置存储器中的第一文件；加密所述第一账
号标识的特征值，生成第二密文；将所述第一密文和所述第二密文存储于不可擦除分
区。

加密指令为用户在加密设置界面加密外置存储器时触发的指令，电子设备获取加
30 密指令后生成第一密文和第二密文，并将第一密文和第二密文存储在电子设备的不可
擦除分区中，这样，在用户对电子设备实施工厂级重置前，电子设备已完成了第一密
文和第二密文的安全存储；电子设备完成了工厂级重置后，可以从不可擦除分区恢复
第一密钥，随后利用第一密钥解密出外置存储器中的第二密钥，并利用第二密钥解密
出外置存储器中的文件，从而解决了工厂级重置后外置存储器中的文件无法被解密的
35 问题。

可选地，所述方法还包括：获取切换账号的指示信息；根据所述指示信息校验所
述第一账号标识；所述第一账号标识校验通过后，获取第二账号标识的特征值；根据
所述第二账号标识的特征值更新所述第一密文和所述第二密文。

用户可以在账号登录界面切换当前登录的账号标识（如，第一账号标识），用户

在账号登录界面触发电子设备生成切换账号的指示信息后，电子设备可以要求用户输入第一账号标识对应的密码，对第一账号标识进行校验。第一账号标识校验通过后，说明切换账号标识的用户为合法用户，电子设备可以获取用户输入的第二账号标识，并计算第二账号标识的哈希值（特征值的一个示例），随后利用第二账号标识的哈希值更新所述第一密文和所述第二密文，其中，电子设备可以先解密出第一密钥，再使用第二账号标识的哈希值生成更新后的第一密文，随后加密第二账号标识的哈希值生成更新后的第二密文。上述方案在确定当前用户（切换账号标识的用户）为合法用户后，利用当前用户的账号标识（第二账号标识）更新第一密文和第二密文，解除了第一账号标识对应的加密和解密外置存储器的权限，从而确保了外置存储器中数据的安全性。

可选地，所述方法还包括：在工厂级重置完成后，校验所述第一账号标识；当所述第一账号标识校验成功时，解密所述第一密文和所述第二密文，生成所述第一密钥。

电子设备执行工厂级重置后会启动账号校验机制，该机制要求账号校验成功后才能正常使用电子设备。校验工厂级重置前最后登录的账号标识（如，第一账号标识），可以确保电子设备执行工厂级重置后的用户为合法用户，从而确保了外置存储器中数据的安全性。

可选地，所述校验所述第一账号标识，包括：

当工厂级重置保护（factory reset protection, FRP）状态已被触发时，校验所述第一账号标识。

可选地，所述方法还包括：使用默认值加密所述第一密钥，生成第三密文；加密所述默认值，生成第四密文；将所述第三密文和所述第四密文存储于所述不可擦除分区。

由于用户可能会切换账号，电子设备执行工厂级重置后继续使用第一账号标识或者第二账号标识加密保存第一密钥存在泄密风险，电子设备可以在解密出第一密钥后使用默认值加密保存第一密钥，从而确保了外置存储器中数据的安全性。

可选地，所述方法还包括：将所述第三密文和所述第四密文从所述不可擦除分区拷贝至可擦除分区；根据所述可擦除分区中的所述第三密文和所述第四密文生成所述第一密钥；根据所述第一密钥解密所述外置存储器中加密的第一文件。

可选地，所述校验所述第一账号标识之前，所述方法还包括：获取 recovery 界面触发的工厂级重置指令；根据所述工厂级重置指令格式化可擦除分区中的数据。

可选地，所述使用所述第一账号标识的特征值加密第一密钥，包括：调用密钥管理模块 keymaster TA 执行：使用所述第一账号标识的特征值加密所述第一密钥；所述加密所述第一账号标识的特征值，包括：调用所述 keymaster TA 执行：加密所述第一账号标识的特征值。

可选地，所述将所述第一密文和所述第二密文存储于不可擦除分区，包括：调用可信执行环境应用程序接口执行：将所述第一密文和所述第二密文存储于所述不可擦除分区。

可选地，所述第一密钥还用于加密第三密钥，所述第三密钥用于加密所述外置存储器中加密的第二文件。

可选地，所述方法还包括：根据所述加密指令获取锁屏口令的特征值；使用所述锁屏口令的特征值加密所述第一密钥，生成第五密文；加密所述锁屏口令的特征值，生成第六密文；将所述第五密文和所述第六密文存储于可擦除分区。

5 可选地，所述使用所述锁屏口令的特征值加密所述第一密钥，包括：调用 keymaster TA 执行：使用所述锁屏口令的特征值加密所述第一密钥；所述加密所述锁屏口令的特征值，包括：调用所述 keymaster TA 执行：加密所述锁屏口令的特征值。

可选地，所述方法还包括：获取设置界面触发的用户级重置指令；根据所述用户级重置指令将所述第五密文和所述第六密文备份至所述不可擦除分区。

10 可选地，所述根据所述用户级重置指令将所述第五密文和所述第六密文备份至所述不可擦除分区，包括：根据所述用户级重置指令从所述第五密文和所述第六密文中解密出所述第一密钥；使用默认值加密所述第一密钥，生成第七密文；加密所述默认值，生成第八密文；将所述第七密文和所述第八密文存储在所述不可擦除分区中。

15 可选地，所述方法还包括：在用户级重置完成后，将所述第七密文和所述第八密文从所述不可擦除分区拷贝至所述可擦除分区；从所述可擦除分区中的所述第七密文和所述第八密文中解密出所述第一密钥；根据所述第一密钥解密所述外置存储器中加密的所述第一文件。

可选地，所述可擦除分区为 data 分区，所述锁屏口令的特征值为所述锁屏口令的哈希值。

20 可选地，所述不可擦除分区为 sec_storage 分区，所述第一账号标识的特征值为所述第一账号标识的哈希值。

25 第二方面，提供了一种另一种保存密文的方法，包括：显示外置存储器的加密设置界面；接收用户在所述加密设置界面上进行的第一操作；响应于所述第一操作，加密所述外置存储器中的文件；接收所述用户的第二操作；响应于所述第二操作，显示工厂级重置设置界面；接收所述用户在所述工厂级重置设置界面进行的第三操作；响应于所述第三操作，进行工厂级重置；显示账号校验界面；接收所述用户在所述账号校验界面输入的校验信息；当所述校验信息校验通过时，并且，当接收到用户访问所述外置存储器中的文件的操作时，解密所述外置存储器中加密的文件。

30 加密指令为用户在加密设置界面加密外置存储器时触发的指令，电子设备获取加密指令后生成第一密文和第二密文，并将第一密文和第二密文存储在电子设备的不可擦除分区中，这样，在用户对电子设备实施工厂级重置前，电子设备已完成了第一密文和第二密文的安全存储；电子设备在完成了工厂级重置后，可以从不可擦除分区恢复第一密钥，随后利用第一密钥解密出外置存储器中的第二密钥，并利用第二密钥解密出外置存储器中的文件，从而解决了工厂级重置后外置存储器中的文件无法被解密的问题。

35 第三方面，提供了一种保存密文的装置，包括用于执行第一方面或第二方面中任一种方法的单元。该装置可以是终端设备，也可以是终端设备内的芯片。该装置可以包括输入单元和处理单元。

当该装置是终端设备时，该处理单元可以是处理器，该输入单元可以是通信接口；该终端设备还可以包括存储器，该存储器用于存储计算机程序代码，当该处理器执行

该存储器所存储的计算机程序代码时，使得该终端设备执行第一方面或第二方面中的任一种方法。

当该装置是终端设备内的芯片时，该处理单元可以是芯片内部的处理单元，该输入单元可以是输出接口、管脚或电路等；该芯片还可以包括存储器，该存储器可以是该芯片内的存储器（例如，寄存器、缓存等），也可以是位于该芯片外部的存储器（例如，只读存储器、随机存取存储器等）；该存储器用于存储计算机程序代码，当该处理器执行该存储器所存储的计算机程序代码时，使得该芯片执行第一方面或第二方面中的任一种方法。

第四方面，提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序代码，当所述计算机程序代码被保存密文的装置运行时，使得该装置执行第一方面或第二方面中的任一种方法。

第五方面，提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码被保存密文的装置运行时，使得该装置执行第一方面或第二方面中的任一种方法。

附图说明

图 1 是一种适用于本申请的装置的硬件系统的示意图；

图 2 是一种适用于本申请的装置的软件系统的示意图；

图 3 是本申请提供的一种加密设置界面的示意图；

图 4 是本申请提供的一种加密确认界面的示意图；

图 5 是本申请提供的一种加密过程界面的示意图；

图 6 是本申请提供的一种保存密钥的方法的示意图；

图 7 是本申请提供的一种加密流程的示意图；

图 8 是本申请提供的一种用户级重置场景中备份和恢复密钥的方法的示意图；

图 9 是本申请提供的一种用户级重置场景中存储区域的密文存储变化情况的示意图；

图 10 是本申请提供的一种工厂级重置场景中备份密钥的方法的示意图；

图 11 是本申请提供的一种账号登录界面的示意图；

图 12 是本申请提供的一种账号切换时存储区域的密文存储变化情况的示意图；

图 13 是本申请提供的一种工厂级重置设置界面的示意图；

图 14 是本申请提供的一种工厂级重置确认界面的示意图；

图 15 是本申请提供的一种工厂级重置过程界面的示意图；

图 16 是本申请提供的一种工厂级重置场景中恢复密钥的方法的示意图；

图 17 是本申请提供的一种账号校验界面示意图；

图 18 是本申请提供的一种工厂级重置场景中存储区域的密文存储变化情况的示意图；

图 19 是本申请提供的一种保存密文的装置的示意图；

图 20 是本申请提供的一种保存密文的电子设备的示意图。

具体实施方式

下面将结合附图，对本申请实施例中的技术方案进行描述。

图 1 示出了一种适用于本申请的装置的硬件系统。

5 装置 100 可以是手机、智慧屏、平板电脑、可穿戴电子设备、车载电子设备、增强现实（augmented reality, AR）设备、虚拟现实（virtual reality, VR）设备、笔记本电脑、超级移动个人计算机（ultra-mobile personal computer, UMPC）、上网本、个人数字助理（personal digital assistant, PDA）、投影仪等等，本申请实施例对装置 100 的具体类型不作任何限制。

10 装置 100 可以包括处理器 110，外部存储器接口 120，内部存储器 121，通用串行总线（universal serial bus, USB）接口 130，充电管理模块 140，电源管理模块 141，电池 142，天线 1，天线 2，移动通信模块 150，无线通信模块 160，音频模块 170，扬声器 170A，受话器 170B，麦克风 170C，耳机接口 170D，传感器模块 180，按键 190，马达 191，指示器 192，摄像头 193，显示屏 194，以及用户标识模块（subscriber identification module, SIM）卡接口 195 等。其中传感器模块 180 可以包括压力传感器 15 180A，陀螺仪传感器 180B，气压传感器 180C，磁传感器 180D，加速度传感器 180E，距离传感器 180F，接近光传感器 180G，指纹传感器 180H，温度传感器 180J，触摸传感器 180K，环境光传感器 180L，骨传导传感器 180M 等。

需要说明的是，图 1 所示的结构并不构成对装置 100 的具体限定。在本申请另一些 20 实施例 中，装置 100 可以包括比图 1 所示的部件更多或更少的部件，或者，装置 100 可以包括图 1 所示的部件中某些部件的组合，或者，装置 100 可以包括图 1 所示的部件中某些部件的子部件。图 1 示的部件可以以硬件、软件、或软件和硬件的组合实现。

处理器 110 可以包括一个或多个处理单元。例如，处理器 110 可以包括以下处理 25 单元中的至少一个：应用处理器（application processor, AP）、调制解调处理器、图形处理器（graphics processing unit, GPU）、图像信号处理器（image signal processor, ISP）、控制器、视频编解码器、数字信号处理器（digital signal processor, DSP）、基带处理器、神经网络处理器（neural-network processing unit, NPU）。其中，不同的处理单元可以是独立的器件，也可以是集成的器件。

控制器可以根据指令操作码和时序信号，产生操作控制信号，完成取指令和执行 30 指令的控制。

处理器 110 中还可以设置存储器，用于存储指令和数据。在一些实施例中，处理器 110 中的存储器为高速缓冲存储器。该存储器可以保存处理器 110 刚用过或循环使用的指令或数据。如果处理器 110 需要再次使用该指令或数据，可从所述存储器中直接调用。避免了重复存取，减少了处理器 110 的等待时间，因而提高了系统的效率。

35 在一些实施例中，处理器 110 可以包括一个或多个接口。例如，处理器 110 可以包括以下接口中的至少一个：内部集成电路（inter-integrated circuit, I2C）接口、内部集成电路音频（inter-integrated circuit sound, I2S）接口、脉冲编码调制（pulse code modulation, PCM）接口、通用异步接收传输器（universal asynchronous receiver/transmitter, UART）接口、移动产业处理器接口（mobile industry processor interface, MIPI）、通用输入输出（general-purpose input/output, GPIO）接口、SIM 接

口、USB 接口。

I2C 接口是一种双向同步串行总线，包括一根串行数据线（serial data line, SDA）和一根串行时钟线（serial clock line, SCL）。在一些实施例中，处理器 110 可以包含多组 I2C 总线。处理器 110 可以通过不同的 I2C 总线接口分别耦合触摸传感器 180K、充电器、闪光灯、摄像头 193 等。例如：处理器 110 可以通过 I2C 接口耦合触摸传感器 180K，使处理器 110 与触摸传感器 180K 通过 I2C 总线接口通信，实现装置 100 的触摸功能。

I2S 接口可以用于音频通信。在一些实施例中，处理器 110 可以包含多组 I2S 总线。处理器 110 可以通过 I2S 总线与音频模块 170 耦合，实现处理器 110 与音频模块 170 之间的通信。在一些实施例中，音频模块 170 可以通过 I2S 接口向无线通信模块 160 传递音频信号，实现通过蓝牙耳机接听电话的功能。

PCM 接口也可以用于音频通信，将模拟信号抽样、量化和编码。在一些实施例中，音频模块 170 与无线通信模块 160 可以通过 PCM 接口耦合。在一些实施例中，音频模块 170 也可以通过 PCM 接口向无线通信模块 160 传递音频信号，实现通过蓝牙耳机接听电话的功能。所述 I2S 接口和所述 PCM 接口都可以用于音频通信。

UART 接口是一种通用串行数据总线，用于异步通信。该总线可以为双向通信总线。它将要传输的数据在串行通信与并行通信之间转换。在一些实施例中，UART 接口通常被用于连接处理器 110 与无线通信模块 160。例如：处理器 110 通过 UART 接口与无线通信模块 160 中的蓝牙模块通信，实现蓝牙功能。在一些实施例中，音频模块 170 可以通过 UART 接口向无线通信模块 160 传递音频信号，实现通过蓝牙耳机播放音乐的功能。

MIPI 接口可以被用于连接处理器 110 与显示屏 194 和摄像头 193 等外围器件。MIPI 接口包括摄像头串行接口（camera serial interface, CSI）、显示屏串行接口（display serial interface, DSI）等。在一些实施例中，处理器 110 和摄像头 193 通过 CSI 接口通信，实现装置 100 的拍摄功能。处理器 110 和显示屏 194 通过 DSI 接口通信，实现装置 100 的显示功能。

GPIO 接口可以通过软件配置。GPIO 接口可以被配置为控制信号接口，也可被配置为数据信号接口。在一些实施例中，GPIO 接口可以用于连接处理器 110 与摄像头 193，显示屏 194、无线通信模块 160、音频模块 170 和传感器模块 180。GPIO 接口还可以被配置为 I2C 接口、I2S 接口、UART 接口或 MIPI 接口。

USB 接口 130 是符合 USB 标准规范的接口，例如可以是迷你（Mini）USB 接口、微型（Micro）USB 接口或 C 型 USB（USB Type C）接口。USB 接口 130 可以用于连接充电器为装置 100 充电，也可以用于装置 100 与外围设备之间传输数据，还可以用于连接耳机以通过耳机播放音频。USB 接口 130 还可以用于连接其他装置 100，例如 AR 设备。

图 1 所示的各模块间的连接关系只是示意性说明，并不构成对装置 100 的各模块间的连接关系的限定。可选地，装置 100 的各模块也可以采用上述实施例中多种连接方式的组合。

充电管理模块 140 用于从充电器接收电力。其中，充电器可以是无线充电器，也

可以是有线充电器。在一些有线充电的实施例中，充电管理模块 140 可以通过 USB 接口 130 接收有线充电器的电流。在一些无线充电的实施例中，充电管理模块 140 可以通过装置 100 的无线充电线圈接收电磁波（电流路径如虚线所示）。充电管理模块 140 为电池 142 充电的同时，还可以通过电源管理模块 141 为装置 100 供电。

5 电源管理模块 141 用于连接电池 142，充电管理模块 140 与处理器 110。电源管理模块 141 接收电池 142 和/或充电管理模块 140 的输入，为处理器 110，内部存储器 121，显示屏 194，摄像头 193，和无线通信模块 160 等供电。电源管理模块 141 还可以用于监测电池容量、电池循环次数和电池健康状态（例如，漏电、阻抗）等参数。可选地，电源管理模块 141 可以设置于处理器 110 中，或者，电源管理模块 141 和充电管理模块 140 可以设置于同一个器件中。

10 装置 100 的无线通信功能可以通过天线 1、天线 2、移动通信模块 150、无线通信模块 160、调制解调处理器以及基带处理器等器件实现。

15 天线 1 和天线 2 用于发射和接收电磁波信号。装置 100 中的每个天线可用于覆盖单个或多个通信频带。不同的天线还可以复用，以提高天线的利用率。例如：可以将天线 1 复用为无线局域网的分集天线。在另外一些实施例中，天线可以和调谐开关结合使用。

移动通信模块 150 可以提供应用在装置 100 上的无线通信的解决方案，例如下列方案中的至少一个：第二代（2th generation, 2G）移动通信解决方案、第三代（3th generation, 3G）移动通信解决方案、第四代（4th generation, 4G）移动通信解决方案、
20 第五代（5th generation, 5G）移动通信解决方案。移动通信模块 150 可以包括至少一个滤波器，开关，功率放大器，低噪声放大器（low noise amplifier, LNA）等。移动通信模块 150 可以由天线 1 接收电磁波，并对接收的电磁波进行滤波和放大等处理，随后传送至调制解调处理器进行解调。移动通信模块 150 还可以放大经调制解调处理器调制后的信号，放大后的该信号经天线 1 转变为电磁波辐射出去。在一些实施例中，
25 移动通信模块 150 的至少部分功能模块可以被设置于处理器 110 中。在一些实施例中，移动通信模块 150 的至少部分功能模块可以与处理器 110 的至少部分模块被设置在同一个器件中。

调制解调处理器可以包括调制器和解调器。其中，调制器用于将待发送的低频基带信号调制成中高频信号。解调器用于将接收的电磁波信号解调为低频基带信号。随后解调器将解调得到的低频基带信号传送至基带处理器处理。低频基带信号经基带处理器处理后，被传递给应用处理器。应用处理器通过音频设备（例如，扬声器 170A、受话器 170B）输出声音信号，或通过显示屏 194 显示图像或视频。在一些实施例中，调制解调处理器可以是独立的器件。在另一些实施例中，调制解调处理器可以独立于处理器 110，与移动通信模块 150 或其他功能模块设置在同一个器件中。

35 与移动通信模块 150 类似，无线通信模块 160 也可以提供应用在装置 100 上的无线通信解决方案，例如下列方案中的至少一个：无线局域网（wireless local area networks, WLAN）、蓝牙（bluetooth, BT）、蓝牙低功耗（bluetooth low energy, BLE）、超宽带（ultra wide band, UWB）、全球导航卫星系统（global navigation satellite system, GNSS）、调频（frequency modulation, FM）、近场通信（near field communication, NFC）、红

外 (infrared, IR) 技术。无线通信模块 160 可以是集成至少一个通信处理模块的一个或多个器件。无线通信模块 160 经由天线 2 接收电磁波, 将电磁波信号调频以及滤波处理, 并将处理后的信号发送到处理器 110。无线通信模块 160 还可以从处理器 110 接收待发送的信号, 对其进行调频和放大, 该信号经天线 2 转变为电磁波辐射出去。

5 在一些实施例中, 装置 100 的天线 1 和移动通信模块 150 耦合, 装置 100 的天线 2 和无线通信模块 160 耦合, 使得电子设备 100 可以通过无线通信技术与网络和其他电子设备通信。该无线通信技术可以包括以下通信技术中的至少一个: 全球移动通讯系统 (global system for mobile communications, GSM), 通用分组无线服务 (general packet radio service, GPRS), 码分多址接入 (code division multiple access, CDMA),
10 宽带码分多址 (wideband code division multiple access, WCDMA), 时分码分多址 (time-division code division multiple access, TD-SCDMA), 长期演进 (long term evolution, LTE), BT, GNSS, WLAN, NFC, FM, IR 技术。该 GNSS 可以包括以下定位技术中的至少一个: 全球卫星定位系统 (global positioning system, GPS), 全球导航卫星系统 (global navigation satellite system, GLONASS), 北斗卫星导航系统
15 (beidou navigation satellite system, BDS), 准天顶卫星系统 (quasi-zenith satellite system, QZSS), 星基增强系统 (satellite based augmentation systems, SBAS)。

装置 100 可以通过 GPU、显示屏 194 以及应用处理器实现显示功能。GPU 为图像处理的微处理器, 连接显示屏 194 和应用处理器。GPU 用于执行数学和几何计算, 用于图形渲染。处理器 110 可包括一个或多个 GPU, 其执行程序指令以生成或改变显示
20 信息。

显示屏 194 可以用于显示图像或视频。显示屏 194 包括显示面板。显示面板可以采用液晶显示屏 (liquid crystal display, LCD)、有机发光二极管 (organic light-emitting diode, OLED)、有源矩阵有机发光二极体 (active-matrix organic light-emitting diode, AMOLED)、柔性发光二极管 (flex light-emitting diode, FLED)、迷你发光二极管 (mini
25 light-emitting diode, Mini LED)、微型发光二极管 (micro light-emitting diode, Micro LED)、微型 OLED (Micro OLED) 或量子点发光二极管 (quantum dot light emitting diodes, QLED)。在一些实施例中, 装置 100 可以包括 1 个或 N 个显示屏 194, N 为大于 1 的正整数。

装置 100 可以通过 ISP、摄像头 193、视频编解码器、GPU、显示屏 194 以及应用
30 处理器等实现拍摄功能。

ISP 用于处理摄像头 193 反馈的数据。例如, 拍照时, 打开快门, 光线通过镜头被传递到摄像头感光元件上, 光信号转换为电信号, 摄像头感光元件将所述电信号传递给 ISP 处理, 转化为肉眼可见的图像。ISP 可以对图像的噪点、亮度和色彩进行算法优化, ISP 还可以优化拍摄场景的曝光和色温等参数。在一些实施例中, ISP 可以设
35 置在摄像头 193 中。

摄像头 193 用于捕获静态图像或视频。物体通过镜头生成光学图像投射到感光元件。感光元件可以是电荷耦合器件 (charge coupled device, CCD) 或互补金属氧化物半导体 (complementary metal-oxide-semiconductor, CMOS) 光电晶体管。感光元件把光信号转换成电信号, 之后将电信号传递给 ISP 转换成数字图像信号。ISP 将数字图

像信号输出到 DSP 加工处理。DSP 将数字图像信号转换成标准的红绿蓝(red green blue, RGB), YUV 等格式的图像信号。在一些实施例中, 装置 100 可以包括 1 个或 N 个摄像头 193, N 为大于 1 的正整数。

5 数字信号处理器用于处理数字信号, 除了可以处理数字图像信号, 还可以处理其他数字信号。例如, 当装置 100 在频点选择时, 数字信号处理器用于对频点能量进行傅里叶变换等。

视频编解码器用于对数字视频压缩或解压缩。装置 100 可以支持一种或多种视频编解码器。这样, 装置 100 可以播放或录制多种编码格式的视频, 例如: 动态图像专家组(moving picture experts group, MPEG) 1、MPEG2、MPEG3 和 MPEG4。

10 NPU 是一种借鉴生物神经网络结构的处理器, 例如借鉴人脑神经元之间传递模式对输入信息快速处理, 还可以不断地自学习。通过 NPU 可以实现装置 100 的智能认知等功能, 例如: 图像识别、人脸识别、语音识别和文本理解。

15 外部存储器接口 120 可以用于连接外部存储卡, 例如安全数码(secure digital, SD)卡, 实现扩展装置 100 的存储能力。外部存储卡通过外部存储器接口 120 与处理器 110 通信, 实现数据存储功能。例如将音乐, 视频等文件保存在外部存储卡中。

内部存储器 121 可以用于存储计算机可执行程序代码, 所述可执行程序代码包括指令。内部存储器 121 可以包括存储程序区和存储数据区。其中, 存储程序区可存储操作系统, 至少一个功能(例如, 声音播放功能和图像播放功能)所需的应用程序。存储数据区可存储装置 100 使用过程中所创建的数据(例如, 音频数据和电话本)。此外, 内部存储器 121 可以包括高速随机存取存储器, 还可以包括非易失性存储器, 例如: 至少一个磁盘存储器件、闪存器件和通用闪存存储器(universal flash storage, UFS)等。处理器 110 通过运行存储在内部存储器 121 的指令和/或存储在设置于处理器中的存储器的指令, 执行装置 100 的各种处理方法。

25 装置 100 可以通过音频模块 170、扬声器 170A、受话器 170B、麦克风 170C、耳机接口 170D 以及应用处理器等实现音频功能, 例如, 音乐播放和录音。

音频模块 170 用于将数字音频信息转换成模拟音频信号输出, 也可以用于将模拟音频输入转换为数字音频信号。音频模块 170 还可以用于对音频信号编码和解码。在一些实施例中, 音频模块 170 或者音频模块 170 的部分功能模块可以设置于处理器 110 中。

30 扬声器 170A, 也称为喇叭, 用于将音频电信号转换为声音信号。装置 100 可以通过扬声器 170A 收听音乐或免提通话。

受话器 170B, 也称为听筒, 用于将音频电信号转换成声音信号。当用户使用装置 100 接听电话或语音信息时, 可以通过将受话器 170B 靠近耳朵接听语音。

35 麦克风 170C, 也称为话筒或传声器, 用于将声音信号转换为电信号。当用户拨打电话或发送语音信息时, 可以通过靠近麦克风 170C 发声将声音信号输入麦克风 170C。装置 100 可以设置至少一个麦克风 170C。在另一些实施例中, 装置 100 可以设置两个麦克风 170C, 以实现降噪功能。在另一些实施例中, 装置 100 还可以设置三个、四个或更多麦克风 170C, 以实现识别声音来源和定向录音等功能。处理器 110 可以对麦克风 170C 输出的电信号进行处理, 例如, 音频模块 170 与无线通信模块 160 可以通过

PCM 接口耦合, 麦克风 170C 将环境声音转换为电信号 (如 PCM 信号) 后, 通过 PCM 接口将该电信号传输至处理器 110; 从处理器 110 对该电信号进行音量分析和频率分析, 确定环境声音的音量和频率。

5 耳机接口 170D 用于连接有线耳机。耳机接口 170D 可以是 USB 接口 130, 也可以是 3.5mm 的开放移动装置 100 平台 (open mobile terminal platform, OMTP) 标准接口, 美国蜂窝电信工业协会 (cellular telecommunications industry association of the USA, CTIA) 标准接口。

10 压力传感器 180A 用于感受压力信号, 可以将压力信号转换成电信号。在一些实施例中, 压力传感器 180A 可以设置于显示屏 194。压力传感器 180A 的种类很多, 例如可以是电阻式压力传感器、电感式压力传感器或电容式压力传感器。电容式压力传感器可以是包括至少两个具有导电材料的平行板, 当力作用于压力传感器 180A, 电极之间的电容改变, 装置 100 根据电容的变化确定压力的强度。当触摸操作作用于显示屏 194 时, 装置 100 根据压力传感器 180A 检测所述触摸操作。装置 100 也可以根据压力传感器 180A 的检测信号计算触摸的位置。在一些实施例中, 作用于相同触摸位置, 但不同触摸操作强度的触摸操作, 可以对应不同的操作指令。例如: 当触摸操作强度小于第一压力阈值的触摸操作作用于短消息应用图标时, 执行查看短消息的指令; 当触摸操作强度大于或等于第一压力阈值的触摸操作作用于短消息应用图标时, 执行新建短消息的指令。

20 陀螺仪传感器 180B 可以用于确定装置 100 的运动姿态。在一些实施例中, 可以通过陀螺仪传感器 180B 确定装置 100 围绕三个轴 (即, x 轴、y 轴和 z 轴) 的角速度。陀螺仪传感器 180B 可以用于拍摄防抖。例如, 当快门被按下时, 陀螺仪传感器 180B 检测装置 100 抖动的角度, 根据角度计算出镜头模组需要补偿的距离, 让镜头通过反向运动抵消装置 100 的抖动, 实现防抖。陀螺仪传感器 180B 还可以用于导航和体感游戏等场景。

25 气压传感器 180C 用于测量气压。在一些实施例中, 装置 100 通过气压传感器 180C 测得的气压值计算海拔高度, 辅助定位和导航。

30 磁传感器 180D 包括霍尔传感器。装置 100 可以利用磁传感器 180D 检测翻盖皮套的开合。在一些实施例中, 当装置 100 是翻盖机时, 装置 100 可以根据磁传感器 180D 检测翻盖的开合。装置 100 可以根据检测到的皮套的开合状态或翻盖的开合状态, 设置翻盖自动解锁等特性。

加速度传感器 180E 可检测装置 100 在各个方向上 (一般为 x 轴、y 轴和 z 轴) 加速度的大小。当装置 100 静止时可检测出重力的大小及方向。加速度传感器 180E 还可以用于识别装置 100 的姿态, 作为横竖屏切换和计步器等应用程序的输入参数。

35 距离传感器 180F 用于测量距离。装置 100 可以通过红外或激光测量距离。在一些实施例中, 例如在拍摄场景中, 装置 100 可以利用距离传感器 180F 测距以实现快速对焦。

接近光传感器 180G 可以包括例如发光二极管 (light-emitting diode, LED) 和光检测器, 例如, 光电二极管。LED 可以是红外 LED。装置 100 通过 LED 向外发射红外光。装置 100 使用光电二极管检测来自附近物体的红外反射光。当检测到反射光时,

装置 100 可以确定附近存在物体。当检测不到反射光时，装置 100 可以确定附近没有物体。装置 100 可以利用接近光传感器 180G 检测用户是否手持装置 100 贴近耳朵通话，以便自动熄灭屏幕达到省电的目的。接近光传感器 180G 也可用于皮套模式或口袋模式的自动解锁与自动锁屏。

5 环境光传感器 180L 用于感知环境光亮度。装置 100 可以根据感知的环境光亮度自适应调节显示屏 194 亮度。环境光传感器 180L 也可用于拍照时自动调节白平衡。环境光传感器 180L 还可以与接近光传感器 180G 配合，检测装置 100 是否在口袋里，以防误触。

10 指纹传感器 180H 用于采集指纹。装置 100 可以利用采集的指纹特性实现解锁、访问应用锁、拍照和接听来电等功能。

温度传感器 180J 用于检测温度。在一些实施例中，装置 100 利用温度传感器 180J 检测的温度，执行温度处理策略。例如，当温度传感器 180J 上报的温度超过阈值，装置 100 执行降低位于温度传感器 180J 附近的处理器的性能，以便降低功耗实施热保护。在另一些实施例中，当温度低于另一阈值时，装置 100 对电池 142 加热，以避免低温导致装置 100 异常关机。在其他一些实施例中，当温度低于又一阈值时，装置 100 对电池 142 的输出电压执行升压，以避免低温导致的异常关机。

20 触摸传感器 180K，也称为触控器件。触摸传感器 180K 可以设置于显示屏 194，由触摸传感器 180K 与显示屏 194 组成触摸屏，触摸屏也称为触控屏。触摸传感器 180K 用于检测作用于其上或其附近的触摸操作。触摸传感器 180K 可以将检测到的触摸操作传递给应用处理器，以确定触摸事件类型。可以通过显示屏 194 提供与触摸操作相关的视觉输出。在另一些实施例中，触摸传感器 180K 也可以设置于装置 100 的表面，并且与显示屏 194 设置于不同的位置。

25 骨传导传感器 180M 可以获取振动信号。在一些实施例中，骨传导传感器 180M 可以获取人体声部振动骨块的振动信号。骨传导传感器 180M 也可以接触人体脉搏，接收血压跳动信号。在一些实施例中，骨传导传感器 180M 也可以设置于耳机中，结合成骨传导耳机。音频模块 170 可以基于所述骨传导传感器 180M 获取的声部振动骨块的振动信号，解析出语音信号，实现语音功能。应用处理器可以基于所述骨传导传感器 180M 获取的血压跳动信号解析心率信息，实现心率检测功能。

30 按键 190 包括开机键和音量键。按键 190 可以是机械按键，也可以是触摸式按键。装置 100 可以接收按键输入信号，实现于案件输入信号相关的功能。

35 马达 191 可以产生振动。马达 191 可以用于来电提示，也可以用于触摸反馈。马达 191 可以对作用于不同应用程序的触摸操作产生不同的振动反馈效果。对于作用于显示屏 194 的不同区域的触摸操作，马达 191 也可产生不同的振动反馈效果。不同的应用场景（例如，时间提醒、接收信息、闹钟和游戏）可以对应不同的振动反馈效果。触摸振动反馈效果还可以支持自定义。

指示器 192 可以是指示灯，可以用于指示充电状态和电量变化，也可以用于指示消息、未接来电和通知。

SIM 卡接口 195 用于连接 SIM 卡。SIM 卡可以插入 SIM 卡接口 195 实现与装置 100 的接触，也可以从 SIM 卡接口 195 拔出实现与装置 100 的分离。装置 100 可以支

持 1 个或 N 个 SIM 卡接口，N 为大于 1 的正整数。同一个 SIM 卡接口 195 可以同时插入多张卡，所述多张卡的类型可以相同，也可以不同。SIM 卡接口 195 也可以兼容外部存储卡。装置 100 通过 SIM 卡和网络交互，实现通话以及数据通信等功能。在一些实施例中，装置 100 采用嵌入式 SIM (embedded-SIM, eSIM) 卡，eSIM 卡可以嵌在装置 100 中，不能和装置 100 分离。

上文详细描述了装置 100 的硬件系统，下面介绍装置 100 的软件系统。软件系统可以采用分层架构、事件驱动架构、微核架构、微服务架构或云架构，本申请实施例以分层架构为例，示例性地描述装置 100 的软件系统。

如图 2 所示，采用分层架构的软件系统分成若干个层，每一层都有清晰的角色和分工。层与层之间通过软件接口通信。在一些实施例中，软件系统可以分为四层，从上至下分别为应用程序层、应用程序框架层、安卓运行时 (Android Runtime) 和系统库、以及内核层。

应用程序层可以包括相机、图库、日历、通话、地图、导航、WLAN、蓝牙、音乐、视频、短信息等应用程序。

应用程序框架层为应用程序层的应用程序提供应用程序编程接口 (application programming interface, API) 和编程框架。应用程序框架层可以包括一些预定义的函数。

例如，应用程序框架层包括窗口管理器、内容提供者、视图系统、电话管理器、资源管理器和通知管理器。

窗口管理器用于管理窗口程序。窗口管理器可以获取显示屏大小，判断是否有状态栏、锁定屏幕和截取屏幕。

内容提供者用来存放和获取数据，并使这些数据可以被应用程序访问。所述数据可以包括视频、图像、音频、拨打和接听的电话、浏览历史和书签、以及电话簿。

视图系统包括可视控件，例如显示文字的控件和显示图片的控件。视图系统可用于构建应用程序。显示界面可以由一个或多个视图组成，例如，包括短信通知图标的显示界面，可以包括显示文字的视图以及显示图片的视图。

电话管理器用于提供装置 100 的通信功能，例如通话状态 (接通或挂断) 的管理。

资源管理器为应用程序提供各种资源，比如本地化字符串、图标、图片、布局文件和视频文件。

通知管理器使应用程序可以在状态栏中显示通知信息，可以用于传达告知类型的消息，可以短暂停留后自动消失，无需用户交互。比如通知管理器被用于下载完成告知和消息提醒。通知管理器还可以管理以图表或者滚动条文本形式出现在系统顶部状态栏的通知，例如后台运行的应用程序的通知。通知管理器还可以管理以对话框形式出现在屏幕上的通知，例如在状态栏提示文本信息、发出提示音、电子设备振动以及指示灯闪烁。

Android Runtime 包括核心库和虚拟机。Android runtime 负责安卓系统的调度和管理。

核心库包含两部分：一部分是 java 语言需要调用的功能函数，另一部分是安卓的核心库。

应用程序层和应用程序框架层运行在虚拟机中。虚拟机将应用程序层和应用程序

框架层的 java 文件执行为二进制文件。虚拟机用于执行对象生命周期的管理、堆栈管理、线程管理、安全和异常的管理、以及垃圾回收等功能。

系统库可以包括多个功能模块，例如：表面管理器（surface manager），媒体库（Media Libraries），三维图形处理库（例如：针对嵌入式系统的开放图形库（open graphics library for embedded systems, OpenGL ES）和 2D 图形引擎（例如：skia 图形库（skia graphics library, SGL））。

表面管理器用于对显示子系统进行管理，并且为多个应用程序提供了 2D 图层和 3D 图层的融合。

媒体库支持多种音频格式的回放和录制、多种视频格式回放和录制以及静态图像文件。媒体库可以支持多种音视频编码格式，例如：MPEG4、H.264、动态图像专家组音频层面 3（moving picture experts group audio layer III, MP3）、高级音频编码（advanced audio coding, AAC）、自适应多码率（adaptive multi-rate, AMR）、联合图像专家组（joint photographic experts group, JPG）和便携式网络图形（portable network graphics, PNG）。

三维图形处理库可以用于实现三维图形绘图、图像渲染、合成和图层处理。

二维图形引擎是 2D 绘图的绘图引擎。

内核层是硬件和软件之间的层。内核层可以包括显示驱动、摄像头驱动、音频驱动和传感器驱动等驱动模块。

下面结合显示拍照场景，示例性说明装置 100 的软件系统和硬件系统的工作流程。

当用户在触摸传感器 180K 上进行触摸操作时，相应的硬件中断被发送至内核层，内核层将触摸操作加工成原始输入事件，原始输入事件例如包括触摸坐标和触摸操作的时间戳等信息。原始输入事件被存储在内核层，应用程序框架层从内核层获取原始输入事件，识别出原始输入事件对应的控件，并通知该控件对应的应用程序（application, APP）。例如，上述触摸操作为单击操作，上述控件对应的 APP 为相机 APP，相机 APP 被单击操作唤醒后，可以通过 API 调用内核层的摄像头驱动，通过摄像头驱动控制摄像头 193 进行拍摄。

下面以装置 100 为例介绍本申请提供的保存密文的方法。

为了保障外置存储器中的文件的安全，可以对外置存储器中的文件加密后存储在外置存储器中，解密这些文件的密钥存储在装置 100 的内部存储器中，这样，外置存储器中的内容只能在装置 100 中作为明文被读出，当外置存储器与其他电子设备连接时，由于其他电子设备未存储密钥，外置存储器中的内容无法被其他电子设备解密，从而保障了外置存储器中的文件的安全。

外置存储器可以是 SD 卡，也可以是 U 盘或其他类型的存储器，外置存储器可以通过插入的方式与装置 100 建立数据连接，也可以通过有线或无线方式与装置 100 建立数据连接，本申请对外置存储器的具体类型和外置存储器与装置 100 的连接方式不做限定。下面以 SD 为例进行说明。

用户可以在图 3 所示的加密设置界面触发对 SD 卡的加密过程。用户可以点击图 3 中的“加密存储卡”，进入图 4 所示的加密设置确认界面，随后，用户点击图 4 中的“加密存储卡”，确认对 SD 卡中的文件进行加密，加密过程的界面如图 5 所示。本申请对加密过程中

采用的加密算法不做限定。

SD 卡中的文件完成加密后，文件加密密钥（file encryption key, FEK）需要被妥善保存。一种保存 FEK 的方法是对 FEK 进行多次加密后再存储于可擦除分区，该方法如图 6 所示。

5 用户在图 3 所示的加密设置界面触发对 SD 卡的加密过程后，SD 卡加密设置模块生成加密指令，基于锁屏口令的设置情况，加密指令调用的模块有两种情况。

情况一：锁屏口令未设置。

SD 卡加密模块通过该加密指令调用加密管理模块（Vold）对 FEK 进行加密，在用户未设置锁屏口令的情况下，后续可以使用默认值（empty auth）对加密 FEK 的密钥（file encryption key encryption key, FEKEK）进行加密，下文会详细介绍加密 FEK 的过程。

情况二：锁屏口令已设置。

SD 卡加密模块通过该加密指令调用锁屏服务（LockSettingsService）获取口令哈希值，随后，锁屏服务将口令哈希值传输至加密管理模块（Vold），以便于后续使用口令哈希值对加密 FEK 的密钥进行加密。上述口令哈希值是基于锁屏口令生成的信息，例如，锁屏服务在用户设置锁屏口令时对锁屏口令进行哈希计算生成口令哈希值，在用户触发 SD 卡的加密后获取先前保存的口令哈希值并将口令哈希值传输至加密管理模块。

Vold 负责加密解密核心功能的实现，Vold 通过调用加密库或解密库，触发针对 SD 卡的加密逻辑或解密逻辑。

当文件系统（如，eCryptfs）在 SD 卡中创建文件时，文件系统针对每个文件生成一个随机数，例如，当 eCryptfs 创建一个新文件时，利用内核提供的随机函数创建一个随机数，该随机数即 FEK。FEK 用于加密 SD 卡中的文件，以及用于解密 SD 卡中被加密的文件。

可选地，eCryptfs 采用开放优良保密协议（open pretty good privacy, OpenPGP）的文件格式存放加密文件，加密文件可以被分成多个逻辑块（extent），每个逻辑块的大小是可调的，但每个逻辑块的大小通常不会大于物理页的尺寸。

SD 卡中的文件被加密后，FEK 需要被加密保存。Vold 在用户设置 SD 卡加密时卸载文件系统，并重新挂载文件系统，此时生成一个随机数，该随机数即 FEKEK（第一密钥的一个示例）。FEKEK 用于加密 FEK（第二密钥的一个示例），其中，FEKEK 由 Vold 设置到内核的密钥环（keyring），文件系统在对 FEK 进行加密时从 keyring 中获取 FEKEK。加密后的 FEK 存储于加密文件的元数据（meta data）中。

FEK 被加密后，FEKEK 也需要被加密保存。由于 Vold 属于富执行环境（rich execution environment, REE）中的模块，安全性不满足要求，无法对 FEKEK 进行加密，Vold 可以通过客户应用（client application, CA）调用可信执行环境（trust execution environment, TEE）中的密钥管理模块，即，keymaster 可信应用（trust application, TA），由 keymaster TA 完成对 FEKEK 的加密。

keymaster TA 可以利用口令哈希值并根据高级加密标准（advanced encryption standard, AES）对 FEKEK 进行加密，生成密文 1（第五密文的一个示例）。随后，keymaster TA 可以利用硬件唯一密钥（hardware unique key, HUK）并根据 AES 对口令哈希值进行加密，生成 keymaster_key_blob（第六密文的一个示例）。keymaster TA 将密文 1 和 keymaster_key_blob 存储在可擦除分区（/data 路径）中。

由于不同装置的 HUK 具有唯一性，使用 HUK 对口令哈希值进行加密，保证了上述 keymaster_key_blob 只能在装置 100 上解密，从而确保了 SD 卡中加密文件的安全性。

图 6 涉及的加密流程如图 7 所示。

5 若当前 SD 卡存在两个待加密的文件（文件 1 和文件 2），文件系统针对这两个文件生成两个随机数，即，FEK1 和 FEK2；随后，文件系统使用 FEK1 加密文件 1，并使用 FEK2 加密文件 2。

文件 1 和文件 2 完成加密后，文件系统从 keyring 中获取 FEKEK，并使用 FEKEK 分别对 FEK1 和 FEK2 进行加密，加密后的 FEK1 保存在文件 1 的元数据中，加密后的 FEK2 保存在文件 2 的元数据中。

10 随后，Vold 通过 CA 调用 keymaster TA，由 keymaster TA 使用口令哈希值对 FEKEK 进行加密；随后，keymaster TA 使用硬件 HUK 对口令哈希值进行加密。

当需要解密 SD 卡中的加密文件时，装置 100 执行图 7 所示的加密流程的逆过程，例如，Vold 通过 CA 调用 keymaster TA 执行下列解密步骤：keymaster TA 从可擦除分区中获取 keymaster_key_blob 和密文 1，首先利用 HUK 解密 keymaster_key_blob，获得口令哈希值，随后利用口令哈希值解密密文 1，获得 FEKEK。Vold 从 keymaster TA 获取 FEKEK 后，
15 将 FEKEK 设置到 keyring，文件系统从 keyring 获取 FEKEK，解密出 FEK，再利用 FEK 解密出 SD 卡中的解密文件。

例如，eCryptfs 打开一个加密文件时，通过下层文件系统读取该加密文件头部的元数据，将该元数据交予 Keystore 模块（包含 keymaster TA 的模块）；Keystore 模块从 keyring 获取 FEKEK，利用 FEKEK 对元数据中加密后的 FEK 进行解密，生成 FEK；随后，eCryptfs 利用 FEK 解密该加密文件。在对加密文件进行解密时，加密文件的各个逻辑块（extent）
20 被读入缓存页（page cache），通过 Kernel Crypto API 进行解密。

当装置 100 执行第一类重置（也称为“用户级重置”，即，用户从系统设置菜单对装置 100 进行重置）时，可擦除区的数据将被清空，此时，装置 100 可以备份密文 1 和
25 keymaster_key_blob，从而避免密文 1 和 keymaster_key_blob 被删除导致 SD 卡中的文件无法解密。用户级重置的备份流程如图 8 所示。

用户通过设置界面控制装置 100 恢复出厂设置。装置 100 校验用户输入的锁屏口令，例如，装置 100 对用户输入的锁屏口令进行计算，得到口令哈希值，随后将计算得到的口令哈希值与保存的口令哈希值进行对比，若这两个口令哈希值相同，则确定校验通过。

30 校验通过后，应用程序框架层（framework）发送恢复出厂设置的广播消息。Vold 收到该广播消息后启动备份密钥流程，通过 CA 调用 keymaster TA 从可擦除分区解密出 FEKEK，随后使用默认值（empty auth）加密 FEKEK，并使用 HUK 加密该默认值，加密后的 FEKEK 和默认值（第七密文和第八密文的一个示例）被保存在不可擦除分区。

本申请中，不可擦除分区指的是第二类重置（也称为“工厂级重置”，即，用户不通过
35 系统设置菜单对装置 100 进行重置）过程中不会被擦除数据的存储区域，不可擦除分区可以是/sec_storage，也可以是 TEE 中其他安全存储区域，如重放保护内存块（replay protected memory block，RPMB）。

装置 100 恢复出厂设置并重启后，检测 SD 卡是否在位。当 SD 在位时，keymaster TA 将加密后的 FEKEK 和默认值从不可擦除分区拷贝至可擦除分区，从而可以利用加密后的

FEKEK 和默认值恢复 FEK，解密 SD 卡中的文件。

综上所述，装置 100 执行用户级重置前后，存储区域存储的密钥变化情况如图 9 所示。

用户指示装置 100 进行用户级重置后，触发装置 100 执行密钥备份。在密钥备份阶段，可擦除分区中存储有密文 1 和 keymaster_key_blob，密文 1 和 keymaster_key_blob 经过解密和加密，以“默认值加密的 FEKEK 和 HUK 加密的默认值”的形式存储于不可擦除分区。

密钥备份完成后，装置 100 进入格式化阶段。在格式化阶段，可擦除分区内的数据被清除，不可擦除分区内的数据被保留。

格式化完成后，装置 100 进入密钥恢复阶段。在密钥恢复阶段，不可擦除分区内的密文（默认值加密的 FEKEK 和 HUK 加密的默认值）被拷贝至可擦除分区，从而完成了密钥恢复。

上述用户级重置过程中，用户需要通过系统设置菜单对装置 100 进行格式化，装置 100 有机会备份可擦除分区中的密文（加密后的 FEKEK），使得 SD 卡中的文件在装置 100 格式化后仍能被解密。然而，当用户不通过系统设置菜单对装置 100 实施第二类重置（即，工厂级重置）时，可擦除分区内的密文会在未拷贝至不可擦除分区的情况下被删除，从而导致装置 100 格式化后 SD 卡中的文件无法解密。

下面介绍本申请提供的保存密文的方法的另一实施例，能够使装置 100 经过工厂级重置后 SD 卡中的文件仍可以被解密。该实施例可以与上文所述的“用户级重置”实施例共同应用于装置 100 上，也可以单独应用于装置 100 上。

用户在图 3 所示的设置界面触发对 SD 卡的加密后，装置 100 执行图 10 所示的密钥备份流程。如图 10 所示，SD 卡加密设置模块通过加密指令调用账号登录模块进行后续处理。基于账号登录情况，账号登录模块的处理方式有以下两种。

情况三：用户未登录账号。

账号登录模块显示图 11 所示的账号登录界面，提示用户登录账号（如荣耀账号）。账号登录成功后，账号登录模块计算账号标识（identifier，ID）的哈希值，随后，将账号 ID 的哈希值传输至 Vold。

情况四：用户已登录账号。

账号登录模块获取账号 ID 的哈希值，并将账号 ID 的哈希值传输至 Vold。可选地，若账号登录模块在用户触发 SD 卡加密前未计算账号 ID 的哈希值，则账号登录模块在用户触发 SD 卡加密时计算账号 ID 的哈希值；若账号登录模块在用户触发 SD 卡加密前已计算账号 ID 的哈希值，则账号登录模块在用户触发 SD 卡加密时直接获取账号 ID 的哈希值。

Vold 获取账号 ID 的哈希值后，通过 CA 调用 keymaster TA，由 keymaster TA 对 FEKEK 进行加密和备份。

keymaster TA 可以利用账号 ID 的哈希值并根据 AES 对 FEKEK 进行加密，生成密文 2（第一密文的一个示例）。随后，keymaster TA 可以利用 HUK 并根据 AES 对账号 ID 的哈希值进行加密，生成 keymaster_key_blob_bak（第二密文的一个示例）。keymaster TA 调用 TEE API 将密文 2 和 keymaster_key_blob_bak 存储在不可擦除分区（/sec_storage 路径）中，从而完成了 FEKEK 的备份。

由于不同装置的 HUK 具有唯一性，使用 HUK 对账号 ID 的哈希值进行加密，保证了上述 keymaster_key_blob_bak 只能在装置 100 上解密，从而确保了 SD 卡中加密文件的安全。

全性。

图 10 所示的方法中，用户通过设置界面触发对 SD 卡的加密后，装置 100 可以在执行工厂级重置前的任一时刻备份 FEKEK，即使后续装置 100 执行了工厂级重置，也能够重启后恢复 FEKEK，从而解决了工厂级重置后 SD 卡中的文件无法被解密的问题。

5 可选地，装置 100 执行图 10 所示的方法后，若用户切换了登录的账号 ID，则 Vold 获取新的账号 ID 的哈希值，并利用新的账号 ID 的哈希值更新密文 2 和 keymaster_key_blob_bak，更新过程如图 12 所示。

下面说明装置 100 执行工厂级重置后解密 SD 卡中的文件的过程。

10 用户先将装置 100 锁屏（或关机），然后可以按组合键（如，“音量键”+“电源键”）使装置 100 进入 recovery 模式，显示如图 13 所示的工厂级重置设置界面。随后，用户点击“恢复出厂设置”后装置 100 显示图 14 所示的确认界面。用户在图 13 所示的界面点击“恢复出厂设置”后，装置 100 执行工厂级重置，显示图 15 所示的工厂级重置界面。

装置 100 完成工厂级重置后重启，运行开机向导程序，执行图 16 所示的密钥恢复流程。

15 开机向导程序调用手机找回模块确定工厂级重置保护（factory reset protection, FRP）状态是否已触发。手机找回模块通过防盗 CA 调用防盗 TA 确定 FRP 状态是否已触发，若 FRP 状态已触发，则手机找回模块显示图 17 所示的账号校验界面，该账号校验界面所校验的账号为 FRP 状态关联的账号（即，装置 100 执行工厂级重置前最后一次登录的账号）。用户在该界面输入正确的密码后，手机找回模块通知 Vold 账号校验成功。随后，Vold 通过 CA 调用 keymaster TA 执行下列密钥恢复步骤。

keymaster TA 从不可擦除分区中获取 keymaster_key_blob_bak 和密文 2，首先利用 HUK 解密 keymaster_key_blob_bak，获得账号 ID 的哈希值，随后利用账号 ID 的哈希值解密密文 2，获得 FEKEK。

25 keymaster TA 使用默认值（empty auth）重新加密 FEKEK，生成第三密文，并使用 HUK 加密该默认值，生成第四密文。加密后的 FEKEK 和默认值作为备份密钥被保存在不可擦除分区（/sec_storage 路径）。随后，keymaster TA 将加密后的 FEKEK 和默认值拷贝至可擦除分区（/data 路径），以便于对 SD 卡中的文件进行加密或解密时使用。装置 100 执行工厂级重置后旧的锁屏口令被清除，上述实施例使得装置 100 可以在未设置新的锁屏口令的情况下使用默认值作为密钥解密 SD 卡。

30 可选地，keymaster TA 可以不使用默认值加密 FEKEK，直接将 keymaster_key_blob_bak 和密文 2 从不可擦除分区拷贝到可擦除分区，在这种情况下，装置 100 可以提示用户设置新的锁屏口令，以便于使用新的锁屏口令加密 FEKEK。

当需要对 SD 卡中的文件进行加密时，keymaster TA 从可擦除分区解密出 FEKEK，通过 Vold 将该 FEKEK 传输至密钥环。文件系统使用 FEK 对 SD 卡中的文件加密后，从密钥环中获取 FEKEK，使用 FEKEK 对 FEK 进行加密，加密后的 FEK 保存在文件的元数据中。

当需要对 SD 卡中的文件进行解密时，keymaster TA 从可擦除分区解密出 FEKEK，通过 Vold 将该 FEKEK 传输至密钥环。文件系统使用 FEKEK 从 SD 卡的文件的元数据中解密出 FEK，随后使用 FEK 解密该文件。

综上所述，装置 100 执行工厂级重置前后，存储区域存储的密钥变化情况如图 18 所

示。

用户指示装置 100 对 SD 卡中的文件进行加密时, 触发装置 100 执行密钥备份。在密钥备份阶段, 可擦除分区中存储有密文 1 和 keymaster_key_blob, 不可擦除分区内存储有密文 2 和 keymaster_key_blob_bak, 其中, 密文 1 是使用口令哈希值加密的 FEKEK, keymaster_key_blob 是使用 HUK 加密的口令哈希值, 密文 2 是使用账号 ID 的哈希值加密的 FEKEK, keymaster_key_blob_bak 是使用 HUK 加密的账号 ID 的哈希值。

用户指示装置 100 执行工厂级重置后, 装置 100 进入工厂级重置阶段, 并执行格式化。在工厂级重置阶段, 可擦除分区内的数据被清除, 不可擦除分区内的数据被保留。

格式化完成后, 装置 100 进入密钥恢复阶段。在密钥恢复阶段, 不可擦除分区内的密文(密文 2 和 keymaster_key_blob_bak)经过解密和加密, 以“默认值加密的 FEKEK 和 HUK 加密的默认值”的形式被拷贝至可擦除分区, 从而完成了密钥恢复。

上文详细介绍了本申请提供的保存密文的方法的示例。可以理解的是, 相应的装置为了实现上述功能, 其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到, 结合本文中所公开的实施例描述的各示例的单元及算法步骤, 本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行, 取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能, 但是这种实现不应认为超出本申请的范围。

本申请可以根据上述方法示例对保存密文的装置进行功能单元的划分, 例如, 可以将各个功能划分为各个功能单元, 也可以将两个或两个以上的功能集成在一个单元中。上述集成的单元既可以采用硬件的形式实现, 也可以采用软件功能单元的形式实现。需要说明的是, 本申请中对单元的划分是示意性的, 仅仅为一种逻辑功能划分, 实际实现时可以有另外的划分方式。

图 19 是本申请提供的一种保存密文的装置的结构示意图。该装置 1900 包括处理单元 1910 和输入单元 1920。

输入单元 1920 用于: 获取加密指令, 所述加密指令指示加密外置存储器中的文件;

处理单元 1910 用于: 根据所述加密指令获取第一账号标识的特征值; 使用所述第一账号标识的特征值加密第一密钥, 生成第一密文, 其中, 所述第一密钥用于加密第二密钥, 所述第二密钥用于加密所述外置存储器中的第一文件; 加密所述第一账号标识的特征值, 生成第二密文; 将所述第一密文和所述第二密文存储于不可擦除分区。

可选地, 输入单元 1920 还用于: 获取切换账号的指示信息;

处理单元 1910 还用于: 根据所述指示信息校验所述第一账号标识; 所述第一账号标识校验通过后, 获取第二账号标识的特征值; 根据所述第二账号标识的特征值更新所述第一密文和所述第二密文。

可选地, 处理单元 1910 还用于: 确定 FRP 状态是否已被触发; 当所述 FRP 状态已被触发时, 校验所述第一账号标识; 当所述第一账号标识校验成功时, 解密所述第一密文和所述第二密文, 生成所述第一密钥。

可选地, 处理单元 1910 还用于: 使用默认值加密所述第一密钥, 生成第三密文; 加密所述默认值, 生成第四密文; 将所述第三密文和所述第四密文存储于所述不可擦

除分区。

可选地，处理单元 1910 还用于：将所述第三密文和所述第四密文从所述不可擦除分区拷贝至可擦除分区；根据所述可擦除分区中的所述第三密文和所述第四密文生成所述第一密钥；根据所述第一密钥解密所述外置存储器中的文件。

5 装置 1900 执行保存密文的方法的具体方式以及产生的有益效果可以参见方法实施例中的相关描述。

图 20 示出了本申请提供的一种电子设备的结构示意图。图 20 中的虚线表示该单元或该模块为可选的。设备 2000 可用于实现上述方法实施例中描述的方法。

设备 2000 包括一个或多个处理器 2001，该一个或多个处理器 2001 可支持设备
10 2000 实现方法实施例中的方法。处理器 2001 可以是通用处理器或者专用处理器。例如，处理器 2001 可以是中央处理器（central processing unit, CPU）、数字信号处理器（digital signal processor, DSP）、专用集成电路（application specific integrated circuit, ASIC）、现场可编程门阵列（field programmable gate array, FPGA）或者其它可编程逻辑器件，如分立门、晶体管逻辑器件或分立硬件组件。

15 处理器 2001 可以用于对设备 2000 进行控制，执行软件程序，处理软件程序的数据。设备 2000 还可以包括通信单元 2005，用以实现信号的输入（接收）和输出（发送）。

例如，设备 2000 可以是芯片，通信单元 2005 可以是该芯片的输入和/或输出电路，
20 或者，通信单元 2005 可以是该芯片的通信接口，该芯片可以作为终端设备或其它电子设备的组成部分。

又例如，设备 2000 可以是终端设备，通信单元 2005 可以是该终端设备的收发器，或者，通信单元 2005 可以是该终端设备的收发电路。

设备 2000 中可以包括一个或多个存储器 2002，其上存有程序 2004，程序 2004
25 可被处理器 2001 运行，生成指令 2003，使得处理器 2001 根据指令 2003 执行上述方法实施例中描述的方法。可选地，存储器 2002 中还可以存储有数据。可选地，处理器 2001 还可以读取存储器 2002 中存储的数据（如，第一密文和第二密文），该数据可以与程序 2004 存储在相同的存储地址，该数据也可以与程序 2004 存储在不同的存储地址。

处理器 2001 和存储器 2002 可以单独设置，也可以集成在一起，例如，集成在终端设备的系统级芯片（system on chip, SOC）上。

本申请还提供了一种计算机程序产品，该计算机程序产品被处理器 2001 执行时实现本申请中任一方法实施例所述的方法。

该计算机程序产品可以存储在存储器 2002 中，例如是程序 2004，程序 2004 经过
35 预处理、编译、汇编和链接等处理过程最终被转换为能够被处理器 2001 执行的可执行目标文件。

本申请还提供了一种计算机可读存储介质，其上存储有计算机程序，该计算机程序被计算机执行时实现本申请中任一方法实施例所述的方法。该计算机程序可以是高级语言程序，也可以是可执行目标程序。

该计算机可读存储介质例如是存储器 2002。存储器 2002 可以是易失性存储器或

非易失性存储器，或者，存储器 2002 可以同时包括易失性存储器和非易失性存储器。其中，非易失性存储器可以是只读存储器（read-only memory, ROM）、可编程只读存储器（programmable ROM, PROM）、可擦除可编程只读存储器（erasable PROM, EPROM）、电可擦除可编程只读存储器（electrically EPROM, EEPROM）或闪存。易失性存储器可以是随机存取存储器（random access memory, RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（static RAM, SRAM）、动态随机存取存储器（dynamic RAM, DRAM）、同步动态随机存取存储器（synchronous DRAM, SDRAM）、双倍数据速率同步动态随机存取存储器（double data rate SDRAM, DDR SDRAM）、增强型同步动态随机存取存储器（enhanced SDRAM, ESDRAM）、同步连接动态随机存取存储器（synchlink DRAM, SLDRAM）和直接内存总线随机存取存储器（direct rambus RAM, DR RAM）。

本领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的装置和设备的具体工作过程以及产生的技术效果，可以参考前述方法实施例中对应的过程和技术效果，在此不再赘述。

在本申请所提供的几个实施例中，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的方法实施例的一些特征可以忽略，或不执行。以上所描述的装置实施例仅仅是示意性的，单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，多个单元或组件可以结合或者可以集成到另一个系统。另外，各单元之间的耦合或各个组件之间的耦合可以是直接耦合，也可以是间接耦合，上述耦合包括电的、机械的或其它形式的连接。

应理解，在本申请的各种实施例中，各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请的实施例的实施过程构成任何限定。

另外，本文中术语“系统”和“网络”在本文中常被可互换使用。本文中的术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

总之，以上所述仅为本申请技术方案的较佳实施例而已，并非用于限定本申请的保护范围。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权利要求书

1. 一种保存密文的方法，其特征在于，包括：

获取加密指令，所述加密指令指示加密外置存储器中的文件；

根据所述加密指令获取第一账号标识的特征值；

5 使用所述第一账号标识的特征值加密第一密钥，生成第一密文，其中，所述第一密钥用于加密第二密钥，所述第二密钥用于加密所述外置存储器中的第一文件；

加密所述第一账号标识的特征值，生成第二密文；

将所述第一密文和所述第二密文存储于不可擦除分区。

2. 根据权利要求1所述的方法，其特征在于，所述方法还包括：

10 获取切换账号的指示信息；

根据所述指示信息校验所述第一账号标识；

所述第一账号标识校验通过后，获取第二账号标识的特征值；

根据所述第二账号标识的特征值更新所述第一密文和所述第二密文。

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：

15 在工厂级重置完成后，校验所述第一账号标识；

当所述第一账号标识校验成功时，解密所述第一密文和所述第二密文，生成所述第一密钥。

4. 根据权利要求3所述的方法，其特征在于，所述校验所述第一账号标识，包括：

当工厂级重置保护 FRP 状态已被触发时，校验所述第一账号标识。

20 5. 根据权利要求3或4所述的方法，其特征在于，所述方法还包括：

使用默认值加密所述第一密钥，生成第三密文；

加密所述默认值，生成第四密文；

将所述第三密文和所述第四密文存储于所述不可擦除分区。

6. 根据权利要求5所述的方法，其特征在于，所述方法还包括：

25 将所述第三密文和所述第四密文从所述不可擦除分区拷贝至可擦除分区；

根据所述可擦除分区中的所述第三密文和所述第四密文生成所述第一密钥；

根据所述第一密钥解密所述外置存储器中加密的所述第一文件。

7. 根据权利要求3至6中任一项所述的方法，其特征在于，所述校验所述第一账号标识之前，所述方法还包括：

30 获取 recovery 界面触发的工厂级重置指令；

根据所述工厂级重置指令格式化可擦除分区中的数据。

8. 根据权利要求1至7中任一项所述的方法，其特征在于，

所述使用所述第一账号标识的特征值加密第一密钥，包括：

35 调用密钥管理模块 keymaster TA 执行：使用所述第一账号标识的特征值加密所述第一密钥；

所述加密所述第一账号标识的特征值，包括：

调用所述 keymaster TA 执行：加密所述第一账号标识的特征值。

9. 根据权利要求1至8中任一项所述的方法，其特征在于，所述将所述第一密文和所述第二密文存储于不可擦除分区，包括：

调用可信执行环境应用程序接口 TEE API 执行：将所述第一密文和所述第二密文存储于所述不可擦除分区。

10. 根据权利要求 1 至 9 中任一项所述的方法，其特征在于，所述第一密钥还用于加密第三密钥，所述第三密钥用于加密所述外置存储器中加密的第二文件。

5 11. 根据权利要求 1 至 10 中任一项所述的方法，其特征在于，所述方法还包括：
根据所述加密指令获取锁屏口令的特征值；
使用所述锁屏口令的特征值加密所述第一密钥，生成第五密文；
加密所述锁屏口令的特征值，生成第六密文；
将所述第五密文和所述第六密文存储于可擦除分区。

10 12. 根据权利要求 11 所述的方法，其特征在于，
所述使用所述锁屏口令的特征值加密所述第一密钥，包括：
调用 keymaster TA 执行：使用所述锁屏口令的特征值加密所述第一密钥；
所述加密所述锁屏口令的特征值，包括：
调用所述 keymaster TA 执行：加密所述锁屏口令的特征值。

15 13. 根据权利要求 11 或 12 所述的方法，其特征在于，所述方法还包括：
获取设置界面触发的用户级重置指令；
根据所述用户级重置指令将所述第五密文和所述第六密文备份至所述不可擦除分区。

20 14. 根据权利要求 13 所述的方法，其特征在于，所述根据所述用户级重置指令将
所述第五密文和所述第六密文备份至所述不可擦除分区，包括：
根据所述用户级重置指令从所述第五密文和所述第六密文中解密出所述第一密钥；
使用默认值加密所述第一密钥，生成第七密文；
加密所述默认值，生成第八密文；
将所述第七密文和所述第八密文存储在所述不可擦除分区中。

25 15. 根据权利要求 14 所述的方法，其特征在于，所述方法还包括：
在用户级重置完成后，将所述第七密文和所述第八密文从所述不可擦除分区拷贝
至所述可擦除分区；

从所述可擦除分区中的所述第七密文和所述第八密文中解密出所述第一密钥；
根据所述第一密钥解密所述外置存储器中加密的所述第一文件。

30 16. 根据权利要求 11 至 15 中任一项所述的方法，其特征在于，所述可擦除分区
为 data 分区，所述锁屏口令的特征值为所述锁屏口令的哈希值。

17. 根据权利要求 1 至 16 中任一项所述的方法，其特征在于，所述不可擦除分区
为 sec_storage 分区，所述第一账号标识的特征值为所述第一账号标识的哈希值。

35 18. 一种保存密文的方法，其特征在于，包括：
显示外置存储器的加密设置界面；
接收用户在所述加密设置界面上进行的第一操作；
响应于所述第一操作，加密所述外置存储器中的文件；
接收所述用户的第二操作；
响应于所述第二操作，显示工厂级重置设置界面；

接收所述用户在所述工厂级重置设置界面进行的第三操作；

响应于所述第三操作，进行工厂级重置；

显示账号校验界面；

接收所述用户在所述账号校验界面输入的校验信息；

- 5 当所述校验信息校验通过时，并且，当接收到用户访问所述外置存储器中的文件的操作时，解密所述外置存储器中加密的文件。

19. 根据权利要求 18 所述的方法，其特征在于，所述方法还包括：

接收所述用户在所述加密设置界面上进行的第四操作；

响应于所述第四操作，加密所述外置存储器中的文件；

- 10 接收所述用户的第五操作；

响应于所述第五操作，显示用户级重置设置界面；

接收所述用户在所述用户级重置设置界面进行的第六操作；

响应于所述第六操作，进行用户级重置；

显示锁屏口令校验界面；

- 15 接收所述用户在所述锁屏口令界面输入的锁屏口令；

当所述锁屏口令校验通过时，并且，当接收到用户访问所述外置存储器中的文件的操作时，解密所述外置存储器中加密的文件。

20. 根据权利要求 18 或 19 所述的方法，其特征在于，

所述接收用户在所述加密设置界面上进行的第一操作，包括

- 20 获取加密指令，所述加密指令指示加密外置存储器中的文件；

所述方法还包括：

根据所述加密指令获取第一账号标识的特征值；

使用所述第一账号标识的特征值加密第一密钥，生成第一密文，其中，所述第一密钥用于加密第二密钥，所述第二密钥用于加密所述外置存储器中的第一文件；

- 25 加密所述第一账号标识的特征值，生成第二密文；

将所述第一密文和所述第二密文存储于不可擦除分区。

21. 根据权利要求 20 所述的方法，其特征在于，所述方法还包括：

获取切换账号的指示信息；

根据所述指示信息校验所述第一账号标识；

- 30 所述第一账号标识校验通过后，获取第二账号标识的特征值；

根据所述第二账号标识的特征值更新所述第一密文和所述第二密文。

22. 根据权利要求 20 所述的方法，其特征在于，所述解密所述外置存储器中加密的文件之前，所述方法还包括：

在所述工厂级重置完成后，根据所述校验信息校验所述第一账号标识；

- 35 当所述第一账号标识校验成功时，解密所述第一密文和所述第二密文，生成所述第一密钥。

23. 根据权利要求 22 所述的方法，其特征在于，所述根据所述校验信息校验所述第一账号标识，包括：

当工厂级重置保护 FRP 状态已被触发时，根据所述校验信息校验所述第一账号标

识。

24. 根据权利要求 22 或 23 所述的方法，其特征在于，所述方法还包括：

使用默认值加密所述第一密钥，生成第三密文；

加密所述默认值，生成第四密文；

5 将所述第三密文和所述第四密文存储于所述不可擦除分区。

25. 根据权利要求 24 所述的方法，其特征在于，所述方法还包括：

将所述第三密文和所述第四密文从所述不可擦除分区拷贝至可擦除分区；

根据所述可擦除分区中的所述第三密文和所述第四密文生成所述第一密钥；

根据所述第一密钥解密所述外置存储器中加密的所述第一文件。

10 26. 根据权利要求 20 至 25 中任一项所述的方法，其特征在于，所述响应于所述第三操作，进行工厂级重置，包括：

获取所述第三操作在所述工厂级重置设置界面触发的工厂级重置指令；

根据所述工厂级重置指令格式化可擦除分区中的数据。

27. 根据权利要求 20 至 26 中任一项所述的方法，其特征在于，

15 所述使用所述第一账号标识的特征值加密第一密钥，包括：

调用密钥管理模块执行：使用所述第一账号标识的特征值加密所述第一密钥；

所述加密所述第一账号标识的特征值，包括：

调用所述密钥管理模块执行：加密所述第一账号标识的特征值。

20 28. 根据权利要求 20 至 27 中任一项所述的方法，其特征在于，所述将所述第一密文和所述第二密文存储于不可擦除分区，包括：

调用可信执行环境应用程序接口执行：将所述第一密文和所述第二密文存储于所述不可擦除分区。

29. 根据权利要求 20 至 28 中任一项所述的方法，其特征在于，所述第一密钥还用于加密第三密钥，所述第三密钥用于加密所述外置存储器中加密的第二文件。

25 30. 根据权利要求 20 至 29 中任一项所述的方法，其特征在于，所述方法还包括：

根据所述加密指令获取锁屏口令的特征值；

使用所述锁屏口令的特征值加密所述第一密钥，生成第五密文；

加密所述锁屏口令的特征值，生成第六密文；

将所述第五密文和所述第六密文存储于可擦除分区。

30 31. 根据权利要求 30 所述的方法，其特征在于，

所述使用所述锁屏口令的特征值加密所述第一密钥，包括：

调用密钥管理模块执行：使用所述锁屏口令的特征值加密所述第一密钥；

所述加密所述锁屏口令的特征值，包括：

调用所述密钥管理模块执行：加密所述锁屏口令的特征值。

35 32. 根据权利要求 30 或 31 所述的方法，其特征在于，所述方法还包括：

获取设置界面触发的用户级重置指令；

根据所述用户级重置指令将所述第五密文和所述第六密文备份至所述不可擦除分区。

33. 根据权利要求 32 所述的方法，其特征在于，所述根据所述用户级重置指令将

所述第五密文和所述第六密文备份至所述不可擦除分区，包括：

根据所述用户级重置指令从所述第五密文和所述第六密文中解密出所述第一密钥；

使用默认值加密所述第一密钥，生成第七密文；

加密所述默认值，生成第八密文；

5 将所述第七密文和所述第八密文存储在所述不可擦除分区中。

34. 根据权利要求 33 所述的方法，其特征在于，所述方法还包括：

在用户级重置完成后，将所述第七密文和所述第八密文从所述不可擦除分区拷贝至所述可擦除分区；

从所述可擦除分区中的所述第七密文和所述第八密文中解密出所述第一密钥；

10 根据所述第一密钥解密所述外置存储器中加密的所述第一文件。

35. 根据权利要求 30 至 34 中任一项所述的方法，其特征在于，所述可擦除分区为数据分区，所述锁屏口令的特征值为所述锁屏口令的哈希值。

36. 根据权利要求 20 至 35 中任一项所述的方法，其特征在于，所述不可擦除分区为安全存储分区，所述第一账号标识的特征值为所述第一账号标识的哈希值。

15 37. 一种保存密文的装置，其特征在于，所述装置包括处理器和存储器，所述存储器用于存储计算机程序，所述处理器用于从所述存储器中调用并运行所述计算机程序，使得所述装置执行权利要求 1 至 17 中任一项所述的方法，或者，使得所述装置执行权利要求 18 至 36 中任一项所述的方法。

20 38. 一种芯片，其特征在于，包括处理器，当所述处理器执行指令时，所述处理器执行如权利要求 1 至 17 中任一项所述的方法，或者，使得所述处理器执行权利要求 18 至 36 中任一项所述的方法。

25 39. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储了计算机程序，当所述计算机程序被处理器执行时，使得所述处理器执行权利要求 1 至 17 中任一项所述的方法，或者，使得所述处理器执行权利要求 18 至 36 中任一项所述的方法。

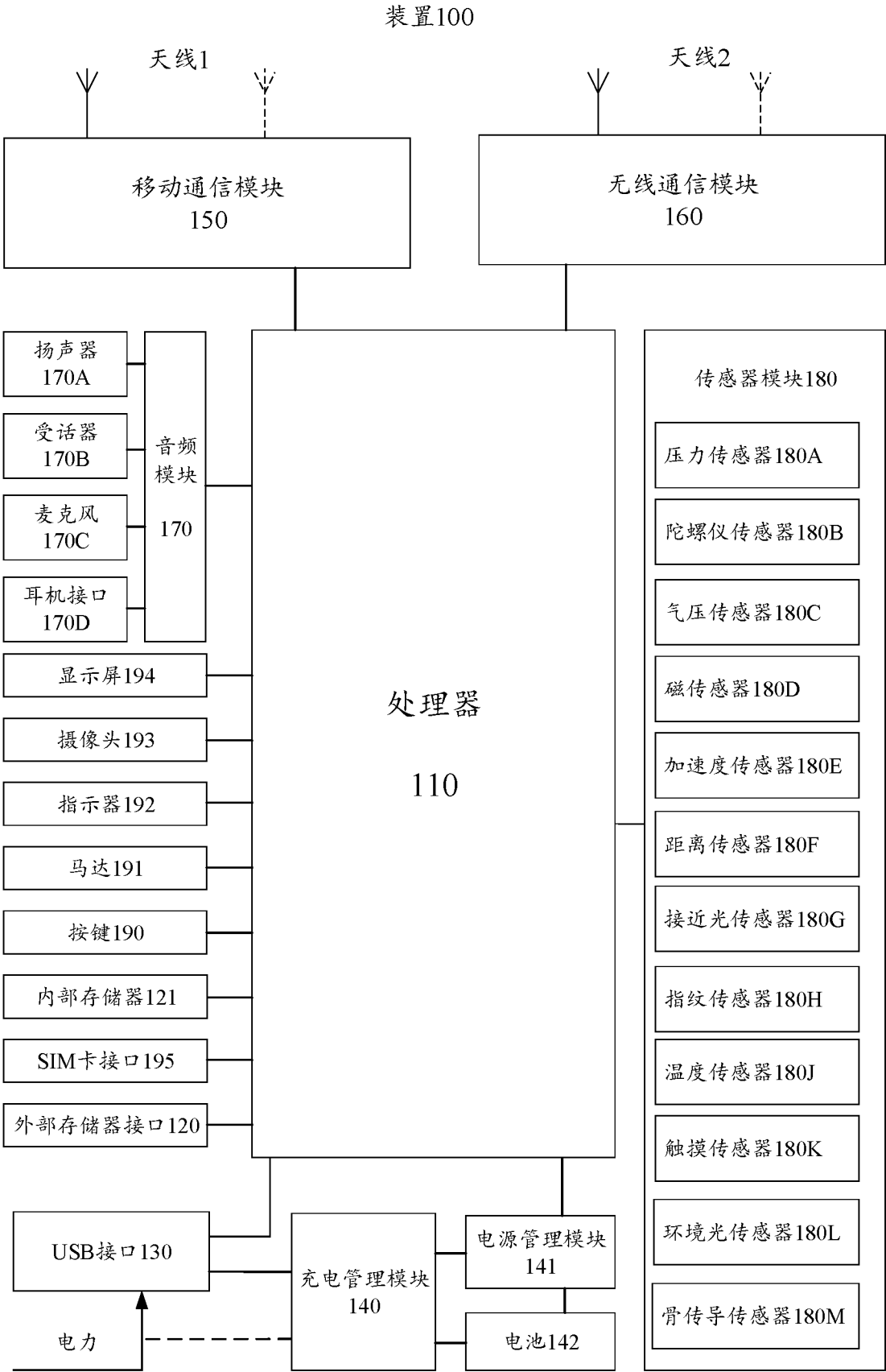


图1

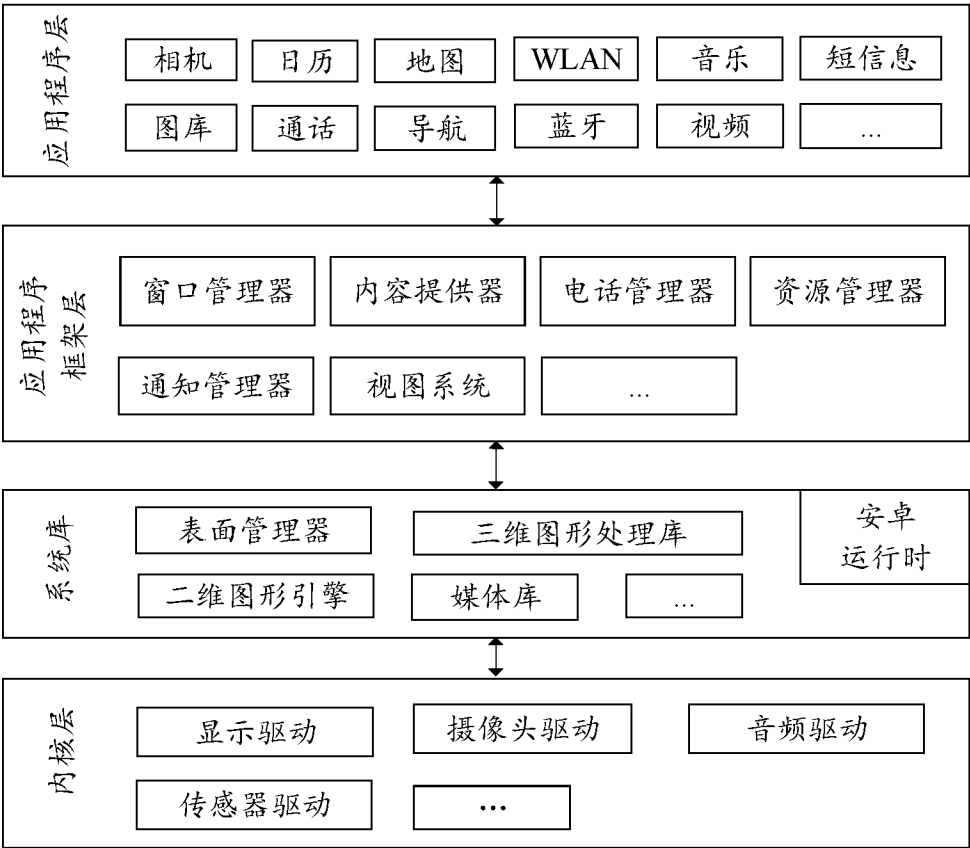


图2



图3

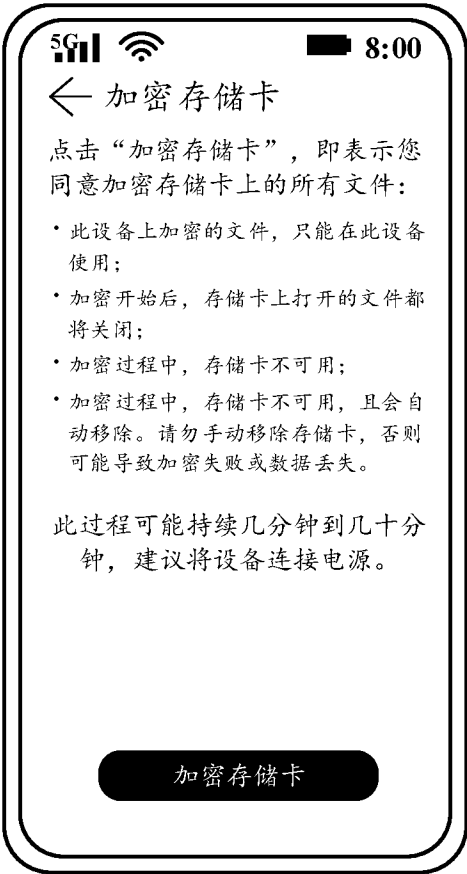


图4

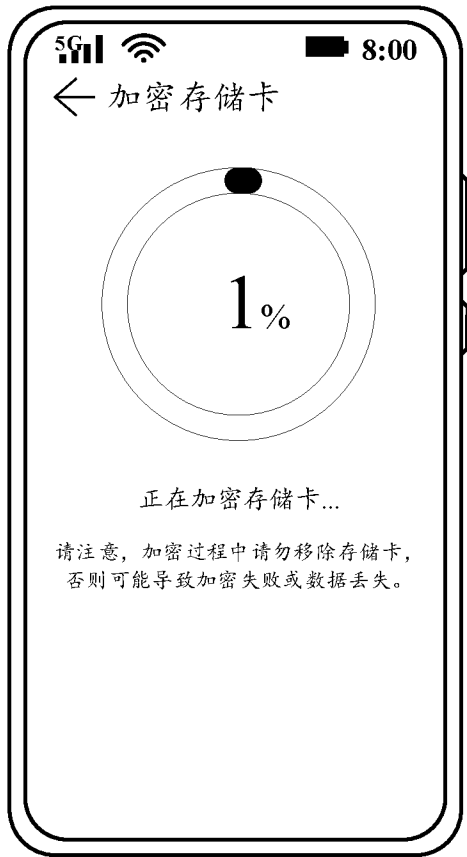


图5

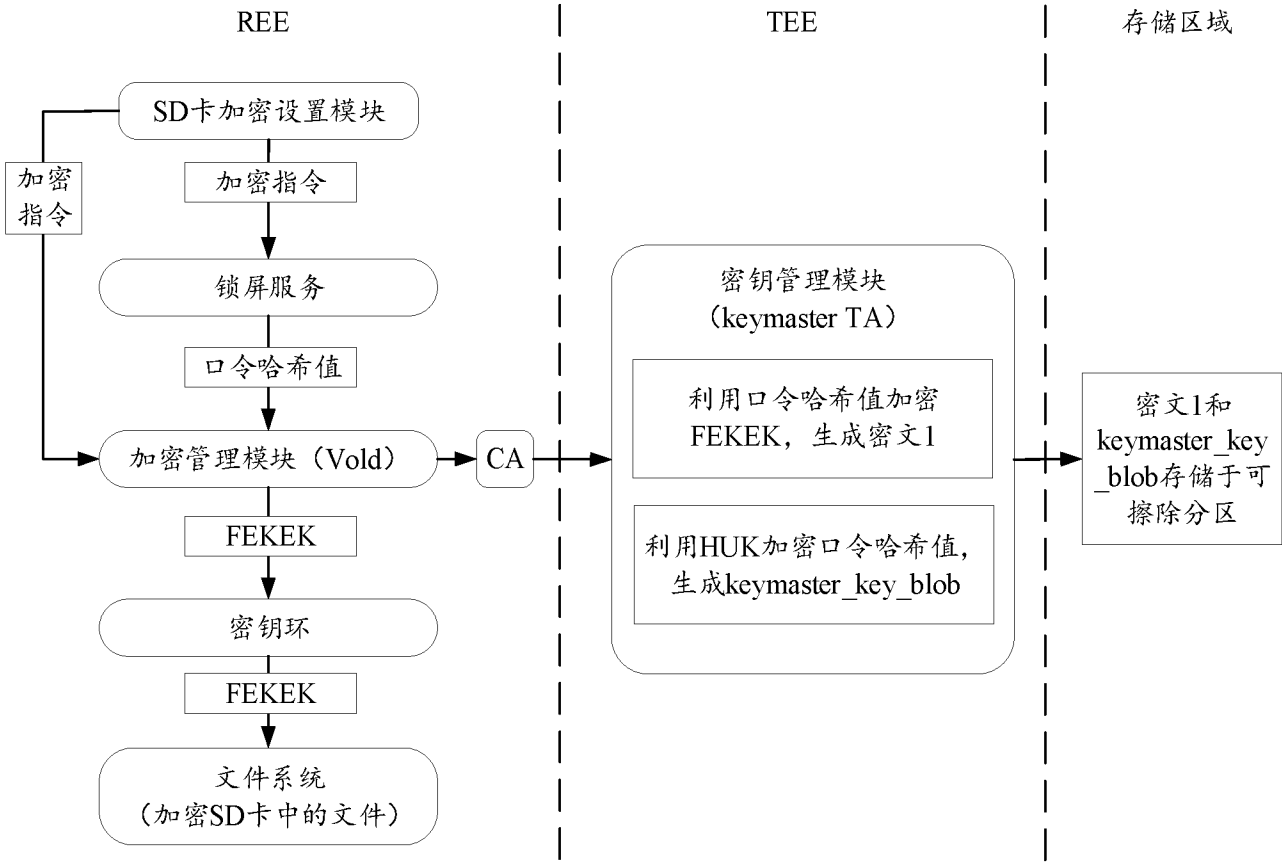


图6

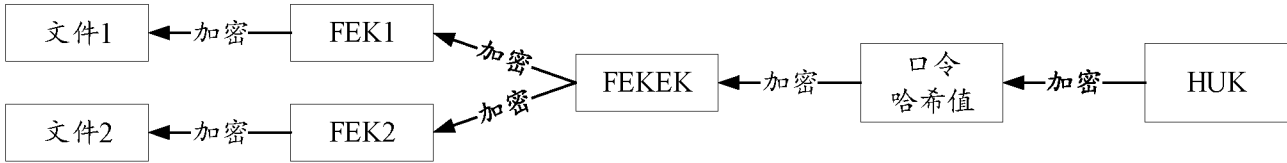


图7

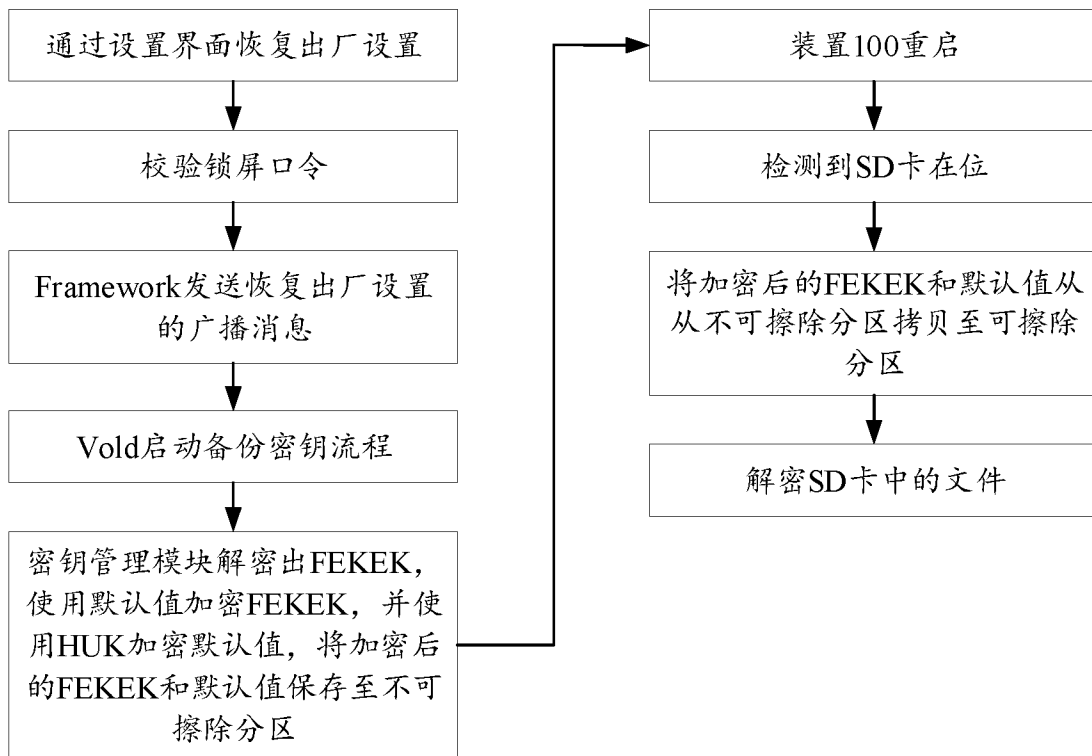


图8

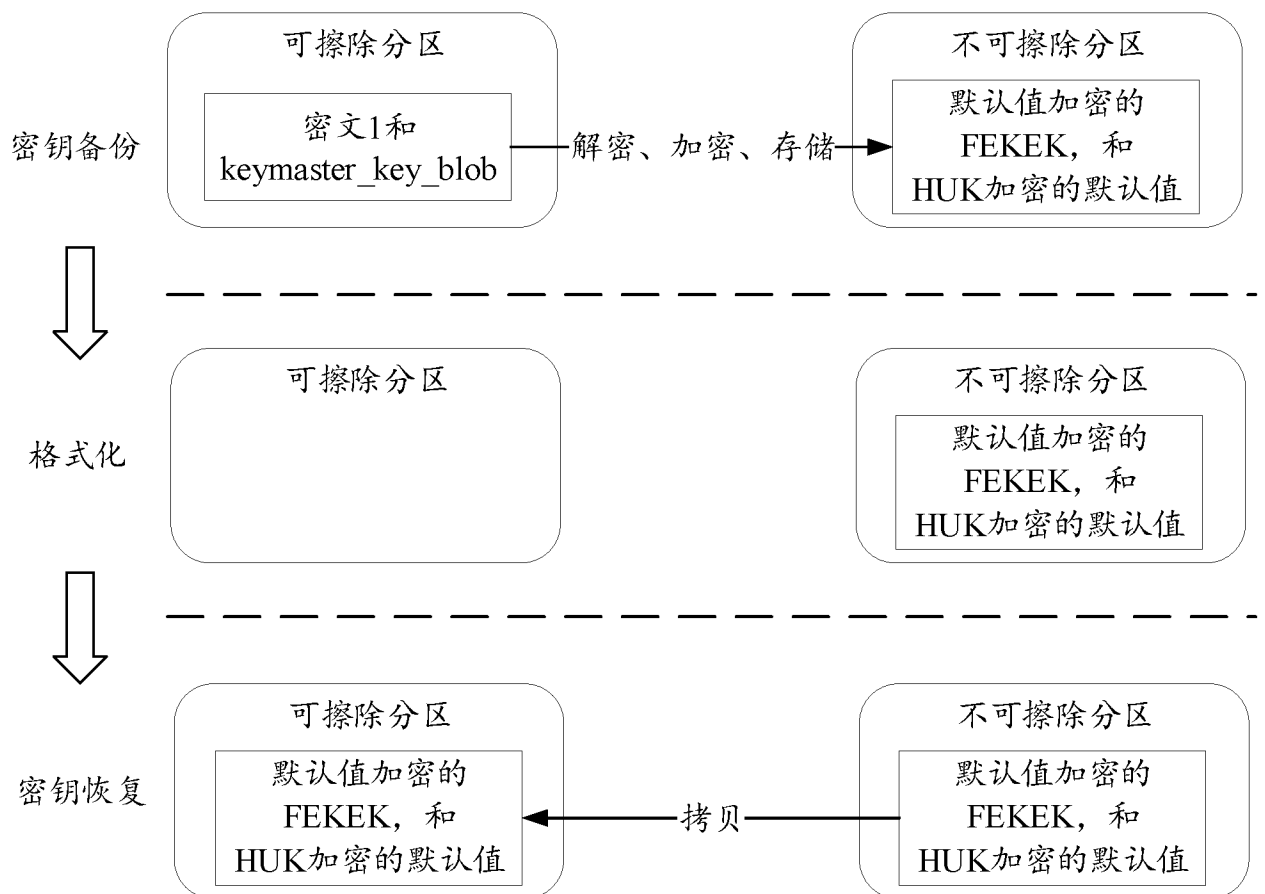


图9

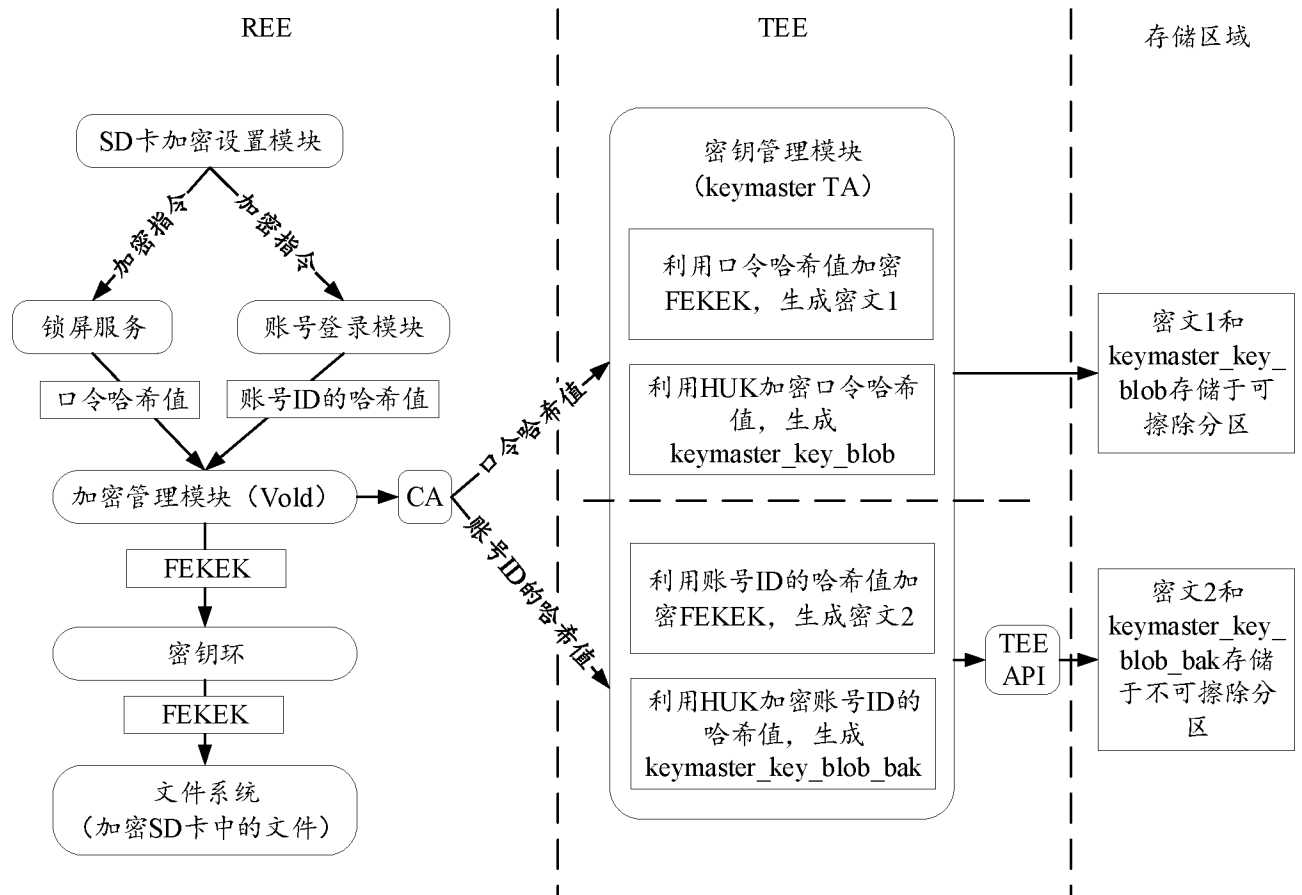


图10

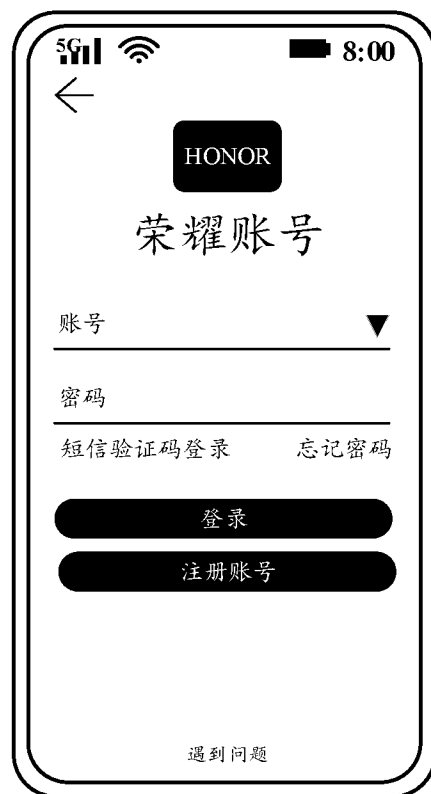


图11

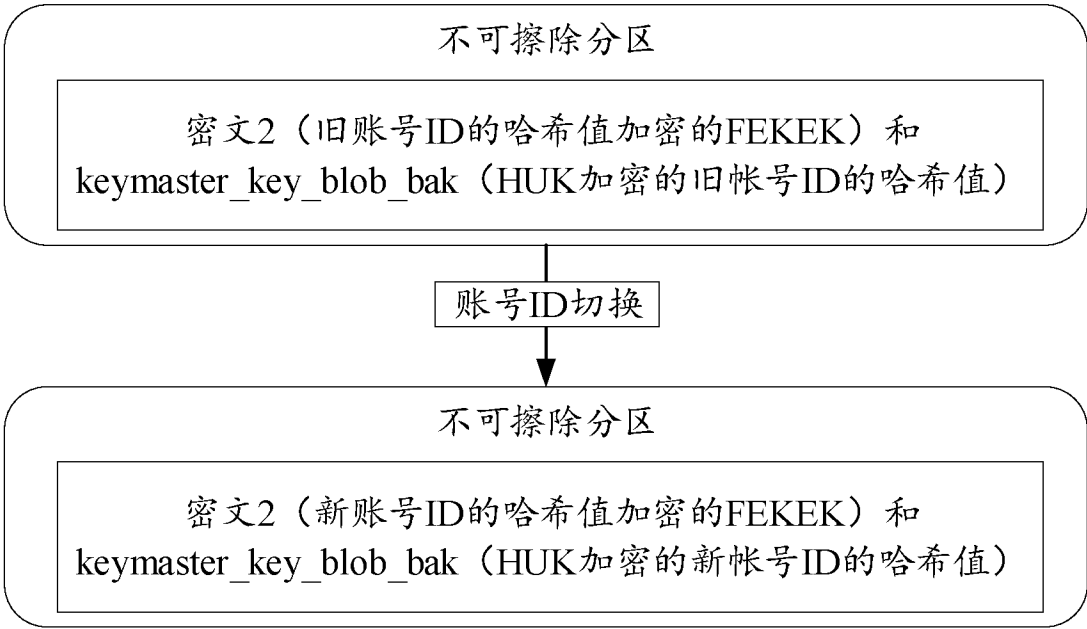


图12



图13



图14



图15

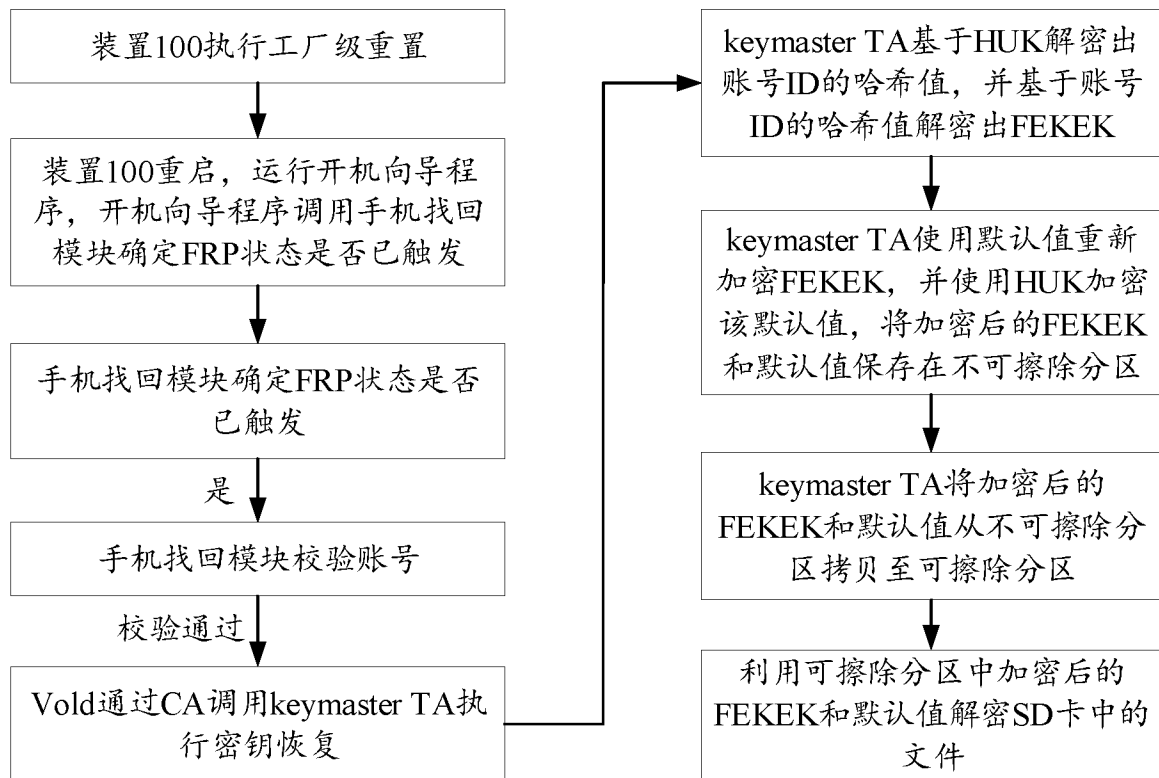


图16

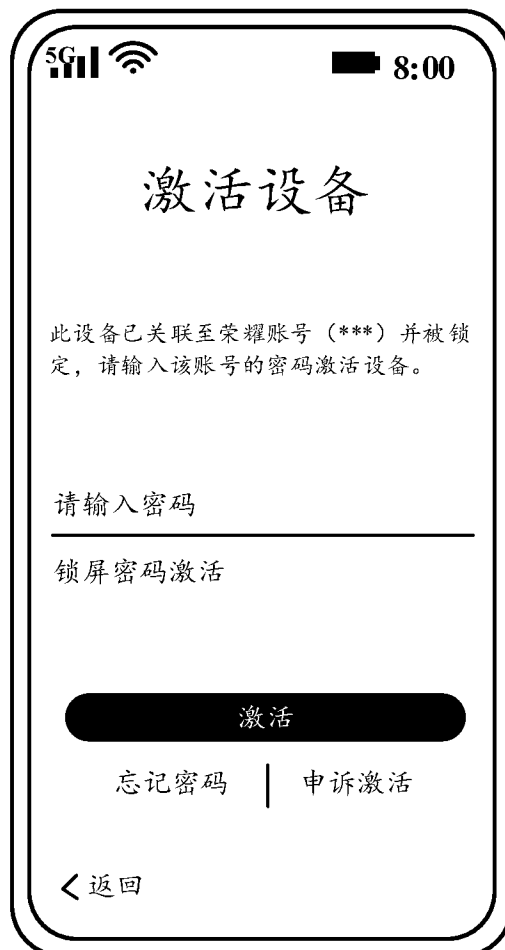


图17

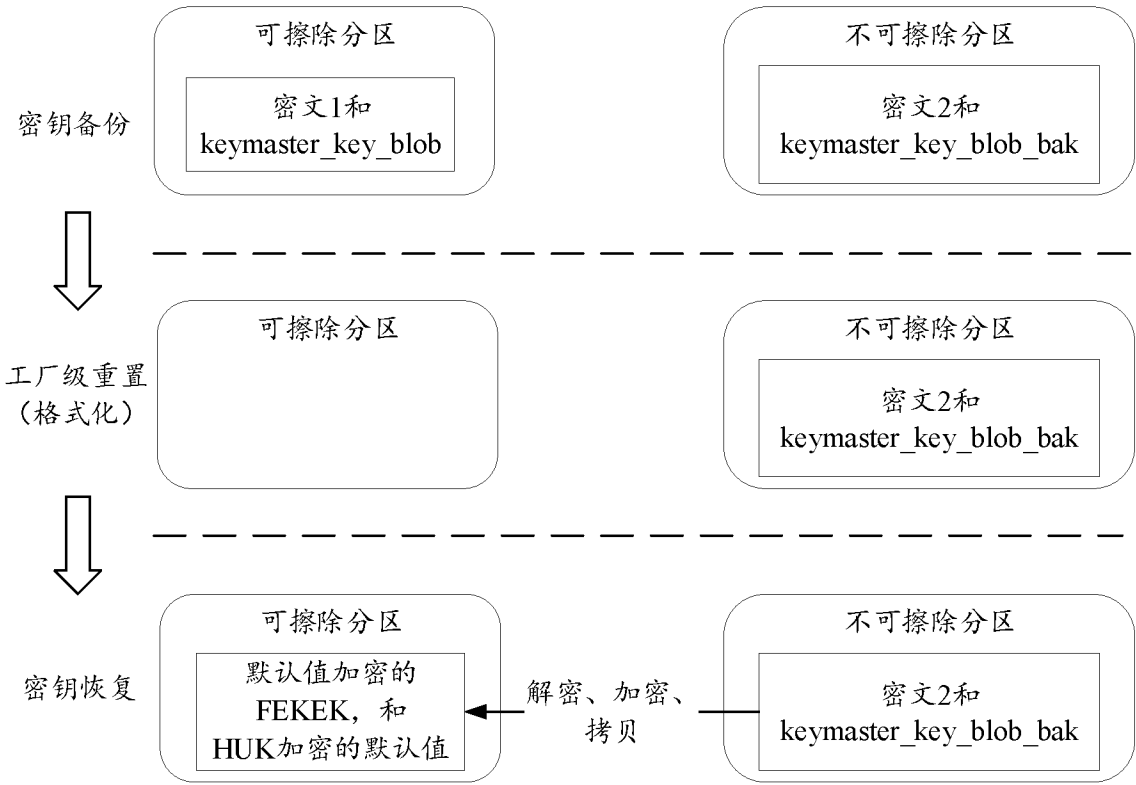


图18

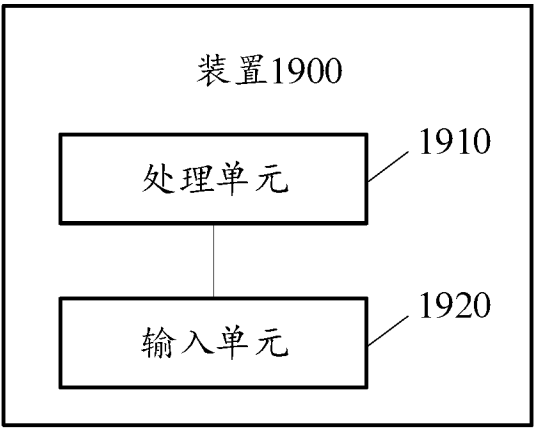


图19

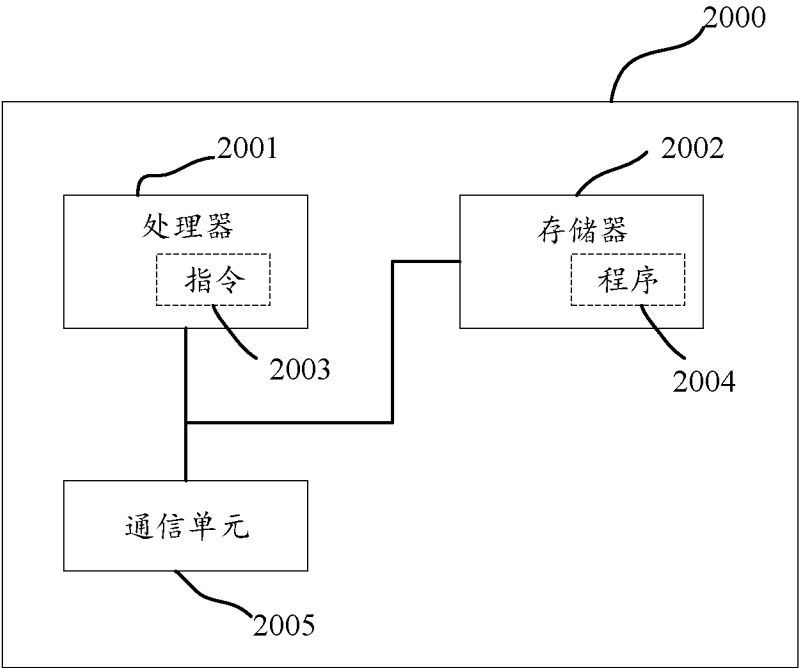


图20

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/092296

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/79(2013.01)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)

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)

CNABS; CNTXT; ENTXTC; DWPI; VEN; WPABS; USTXT; CNKI; IEEE: 不可擦除, 密文, 特征值, 第二类, 工厂级, 用户级, 重置, 密钥, 分区, 外置, 解密, 校验, 账户, 标识, erasable, PROME, PROM, non-erasable, recovery, encrypt+, key, identifier, FEK, erasable, reset, hash

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 113408016 A (HONOR TERMINAL CO., LTD.) 17 September 2021 (2021-09-17) description, paragraphs 4-216	1-39
X	CN 111614698 A (LI LIPING) 01 September 2020 (2020-09-01) description, paragraphs [0006]-[0060]	18-19, 37-39
A	US 2020151356 A1 (DUALITY TECHNOLOGIES INC.) 14 May 2020 (2020-05-14) entire document	1-39
A	US 10164955 B1 (GOOGLE INC. et al.) 25 December 2018 (2018-12-25) entire document	1-39
A	CN 112262548 A (HUAWEI TECHNOLOGIES CO., LTD.) 22 January 2021 (2021-01-22) entire document	1-39
A	US 2012185759 A1 (BALINSKY, H. et al.) 19 July 2012 (2012-07-19) entire document	1-39
A	CN 105809045 A (QINGDAO HISENCE MOBILE COMMUNICATIONS TECHNOLOGY CO., LTD.) 27 July 2016 (2016-07-27) entire document	1-39



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

23 June 2022

Date of mailing of the international search report

18 August 2022

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088, China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/092296

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 111966373 A (OPPO (CHONGQING) INTELLIGENT TECHNOLOGY CO., LTD.) 20 November 2020 (2020-11-20) entire document	1-39

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/092296

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	113408016	A	17 September 2021	None			
CN	111614698	A	01 September 2020	None			
US	2020151356	A1	14 May 2020	None			
US	10164955	B1	25 December 2018	None			
CN	112262548	A	22 January 2021	WO	2020172874	A1	03 September 2020
				KR	20210116644	A	27 September 2021
				IN	202117035602	A	17 December 2021
				EP	3907930	A1	10 November 2021
				CN	112262548	B	14 January 2022
				EP	3907930	A4	19 January 2022
US	2012185759	A1	19 July 2012	None			
CN	105809045	A	27 July 2016	None			
CN	111966373	A	20 November 2020	None			

国际检索报告

国际申请号

PCT/CN2022/092296

A. 主题的分类 G06F 21/79 (2013.01) 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) 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)) CNABS; CNTXT; ENTXT; DWPI; VEN; WPABS; USTXT; CNKI; IEEE: 不可擦除, 密文, 特征值, 第二类, 工厂级, 用户级, 重置, 密钥, 分区, 外置, 解密, 校验, 账户, 标识, erasable, PROME, PROM, non-erasable, recovery, encrypt+, key, identifier, FEK, erasable, reset, hash																										
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 113408016 A (荣耀终端有限公司) 2021年9月17日 (2021 - 09 - 17) 说明书第4-216段</td> <td>1-39</td> </tr> <tr> <td>X</td> <td>CN 111614698 A (李丽萍) 2020年9月1日 (2020 - 09 - 01) 说明书第6-60段</td> <td>18-19、37-39</td> </tr> <tr> <td>A</td> <td>US 2020151356 A1 (DUALITY TECH INC) 2020年5月14日 (2020 - 05 - 14) 全文</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>US 10164955 B1 (GOOGLE INC et al.) 2018年12月25日 (2018 - 12 - 25) 全文</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>CN 112262548 A (华为技术有限公司) 2021年1月22日 (2021 - 01 - 22) 全文</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>US 2012185759 A1 (BALINSKY HELEN et al.) 2012年7月19日 (2012 - 07 - 19) 全文</td> <td>1-39</td> </tr> <tr> <td>A</td> <td>CN 105809045 A (青岛海信移动通信技术股份有限公司) 2016年7月27日 (2016 - 07 - 27) 全文</td> <td>1-39</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 113408016 A (荣耀终端有限公司) 2021年9月17日 (2021 - 09 - 17) 说明书第4-216段	1-39	X	CN 111614698 A (李丽萍) 2020年9月1日 (2020 - 09 - 01) 说明书第6-60段	18-19、37-39	A	US 2020151356 A1 (DUALITY TECH INC) 2020年5月14日 (2020 - 05 - 14) 全文	1-39	A	US 10164955 B1 (GOOGLE INC et al.) 2018年12月25日 (2018 - 12 - 25) 全文	1-39	A	CN 112262548 A (华为技术有限公司) 2021年1月22日 (2021 - 01 - 22) 全文	1-39	A	US 2012185759 A1 (BALINSKY HELEN et al.) 2012年7月19日 (2012 - 07 - 19) 全文	1-39	A	CN 105809045 A (青岛海信移动通信技术股份有限公司) 2016年7月27日 (2016 - 07 - 27) 全文	1-39
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																								
PX	CN 113408016 A (荣耀终端有限公司) 2021年9月17日 (2021 - 09 - 17) 说明书第4-216段	1-39																								
X	CN 111614698 A (李丽萍) 2020年9月1日 (2020 - 09 - 01) 说明书第6-60段	18-19、37-39																								
A	US 2020151356 A1 (DUALITY TECH INC) 2020年5月14日 (2020 - 05 - 14) 全文	1-39																								
A	US 10164955 B1 (GOOGLE INC et al.) 2018年12月25日 (2018 - 12 - 25) 全文	1-39																								
A	CN 112262548 A (华为技术有限公司) 2021年1月22日 (2021 - 01 - 22) 全文	1-39																								
A	US 2012185759 A1 (BALINSKY HELEN et al.) 2012年7月19日 (2012 - 07 - 19) 全文	1-39																								
A	CN 105809045 A (青岛海信移动通信技术股份有限公司) 2016年7月27日 (2016 - 07 - 27) 全文	1-39																								
☒ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																										
<table border="0"> <tr> <td> * 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 </td> <td> “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 </td> </tr> </table>			* 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																						
* 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 2022年6月23日		国际检索报告邮寄日期 2022年8月18日																								
ISA/CN的名称和邮寄地址 中国国家知识产权局 (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 李婧雯 电话号码 (86-27)-59371911																								

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
A	CN 111966373 A (OPPO重庆智能科技有限公司) 2020年11月20日 (2020 - 11 - 20) 全文	1-39

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/092296

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	113408016	A	2021年9月17日	无	
CN	111614698	A	2020年9月1日	无	
US	2020151356	A1	2020年5月14日	无	
US	10164955	B1	2018年12月25日	无	
CN	112262548	A	2021年1月22日	WO 2020172874 A1	2020年9月3日
				KR 20210116644 A	2021年9月27日
				IN 202117035602 A	2021年12月17日
				EP 3907930 A1	2021年11月10日
				CN 112262548 B	2022年1月14日
				EP 3907930 A4	2022年1月19日
US	2012185759	A1	2012年7月19日	无	
CN	105809045	A	2016年7月27日	无	
CN	111966373	A	2020年11月20日	无	