(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110140124 B
(45)授权公告日 2021.04.20

(21)申请号 201780082026.7
(22)申请日 2017.12.29
(65)同一申请的已公布的文献号
申请公布号 CN 110140124 A
(43)申请公布日 2019.08.16
(85)PCT国际申请进入国家阶段日
2019.07.04
(86)PCT国际申请的申请数据
PCT/CN2017/120132 2017.12.29
(87)PCT国际申请的公布数据
WO2019/127468 ZH 2019.07.04
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 杨李军 熊晟 王奇
(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健
(51)Int.Cl.
G06F 21/12(2006.01)
(56)对比文件
CN 107133498 A,2017.09.05
CN 104980269 A,2015.10.14
CN 1989472 A,2007.06.27
CN 103888252 A,2014.06.25
CN 106056000 A,2016.10.26
CN 107463823 A,2017.12.12
CN 105634740 A,2016.06.01
CN 106156557 A,2016.11.23
US 2017329823 A1,2017.11.16
CN 106650508 A,2017.05.10
李勇 等.用于移动设备应用程序的群密钥交换方案.《清华大学学报(自然科学版)》.2011,(第10期),
审查员 李华芳

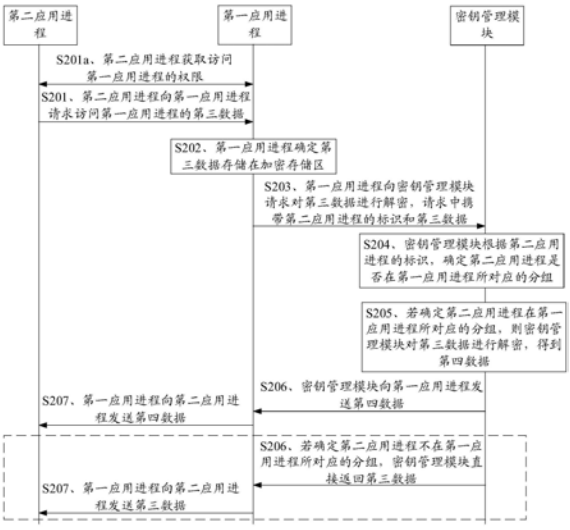
权利要求书3页 说明书17页 附图10页

(54)发明名称

分组应用使用同一密钥共享数据

(57)摘要

本申请提供的一种数据处理的方法及终端，涉及通信技术领域，有利于提高终端中应用程序中的数据的安全性。该方法运用于终端，该终端上运行有第一应用进程、第二应用进程和密钥管理进程，该方法具体包括：第二应用进程向第一应用进程发送访问请求，该访问请求用于请求访问所述第一应用进程的第三数据；密钥管理进程接收请求解密第三数据的解密请求；若密钥管理进程根据该解密请求确定第二应用进程是否在第一应用进程所在的进程分组中。若在，则密钥管理进程使用该进程分组对应的解密密钥解密第三数据，得到第四数据，返回第四数据。若不在，则密钥管理进程不进行解密，返回第三数据。



CN 110140124 B

1.一种数据处理的方法,其特征在于,应用于终端,所述终端运行第一应用进程、第二应用进程和密钥管理进程,所述方法包括:

所述第二应用进程向所述第一应用进程发送访问请求,所述访问请求用于请求访问所述第一应用进程的第三数据;

所述密钥管理进程接收请求解密所述第三数据的解密请求;

若所述密钥管理进程根据所述解密请求确定所述第二应用进程在所述第一应用进程所在的进程分组内,则所述密钥管理进程使用所述第一应用进程所在的进程分组对应的解密密钥解密所述第三数据,得到第四数据;

响应于所述解密请求,所述密钥管理进程返回所述第四数据;

其中,所述终端具有N个进程分组;所述N个进程分组中的每一个包含至少一个进程,并且至少有一个进程分组包含两个或两个以上的进程;其中,N为大于1或等于1的整数;所述N个进程分组对应M个解密密钥,且每一个进程分组对应一个解密密钥;其中,M为正整数,N>=M。

2.根据权利要求1所述的方法,其特征在于,所述密钥管理进程接收请求解密所述第三数据的解密请求具体为

所述密钥管理进程接收第一应用进程根据所述访问请求发送的所述解密请求;

所述密钥管理进程返回所述第四数据具体为:

所述密钥管理进程向所述第一应用进程返回所述第四数据;

所述方法还包括:

所述第一应用进程向所述第二应用进程发送所述第四数据。

3.根据权利要求1或2所述的方法,其特征在于,所述方法还包括:

若所述密钥管理进程确定所述第二应用进程不在所述第一应用进程所在的进程分组内,则所述密钥管理进程向所述第一应用进程发送所述第三数据;

所述第一应用进程向所述第二应用进程发送所述第三数据。

4.根据权利要求1所述的方法,其特征在于,所述第二应用进程向所述第一应用进程发送访问请求之后,所述密钥管理进程接收请求解密所述第三数据的解密请求之前,所述方法还包括:

所述第二应用进程接收所述第一应用进程发送的所述第三数据;

所述密钥管理进程接收请求解密所述第三数据的解密请求具体为:

所述密钥管理进程接收所述第二应用进程发送的所述解密请求;

所述密钥管理进程返回所述第四数据具体为:

所述密钥管理进程向所述第二应用进程返回所述第四数据。

5.根据权利要求4所述的方法,其特征在于,所述方法还包括:

若所述密钥管理进程确定所述第二应用进程不在所述第一应用进程所在的进程分组内,则所述密钥管理进程向所述第二应用进程发送所述第三数据。

6.根据权利要求1所述的方法,其特征在于,在所述密钥管理进程使用所述第一应用进程所在的进程分组对应的解密密钥解密所述第三数据,得到第四数据之前,所述方法还包括:

所述密钥管理进程获取所述第一应用进程的标识;

所述密钥管理进程根据所述第一应用进程的标识，确定所述第一应用进程所在的进程分组的标识；

所述密钥管理进程根据所述第一应用进程所在的进程分组的标识，获取所述第一应用进程所在的进程分组对应的解密密钥。

7.根据权利要求1所述的方法，其特征在于，所述方法还包括：

所述第一应用进程请求所述密钥管理进程对第一数据进行加密；

所述密钥管理进程根据所述请求确定所述第一应用进程所在的进程分组；

所述密钥管理进程使用所述第一应用进程所在的进程分组对应的加密密钥对所述第一数据进行加密，生成第二数据；所述N个进程分组对应M个加密密钥，且每一个进程分组对应一个与其解密密钥相对应的加密密钥；

所述密钥管理进程向所述第一应用进程发送所述第二数据。

8.根据权利要求7所述的方法，其特征在于，在所述密钥管理进程向所述第一应用进程发送所述第二数据之后，所述方法还包括：

所述第一应用进程保存所述第二数据。

9.根据权利要求8所述的方法，其特征在于，所述密钥管理进程根据所述请求确定所述第一应用进程所在的进程分组包括：

所述密钥管理进程获取所述第一应用进程的标识；

所述密钥管理进程根据所述第一应用进程的标识，确定所述第一应用进程所在的进程分组的标识；

所述密钥管理进程根据所述第一应用进程所在的进程分组的标识，获取所述第一应用进程所在的进程分组对应的加密密钥。

10.一种终端，其特征在于，包括第一应用程序模块、第二应用程序模块和密钥管理模块，

所述第二应用程序模块，用于向所述第一应用程序模块发送访问请求，所述访问请求用于请求访问第一应用进程的第三数据；

所述密钥管理模块，用于接收请求解密所述第三数据的解密请求；

所述密钥管理模块，还用于若所述密钥管理模块根据所述解密请求确定第二应用进程在所述第一应用进程所在的进程分组内，则使用所述第一应用进程所在的进程分组对应的解密密钥解密所述第三数据，得到第四数据；

所述密钥管理模块，还用于响应于所述解密请求，返回所述第四数据；

其中，所述终端具有N个进程分组；所述N个进程分组中的每一个包含至少一个进程，并且至少有一个进程分组包含两个或两个以上的进程；其中，N为大于1或等于1的整数；所述N个进程分组对应M个解密密钥，且每一个进程分组对应一个解密密钥；其中，M为正整数，N>=M。

11.根据权利要求10所述的终端，其特征在于，

所述密钥管理模块，还用于接收第一应用程序模块根据所述访问请求发送的所述解密请求；

所述密钥管理模块，还用于向所述第一应用程序模块返回所述第四数据；

所述第一应用程序模块，用于向所述第二应用程序模块发送所述第四数据。

12.根据权利要求10或11所述的终端，其特征在于，所述密钥管理模块，还用于若所述密钥管理模块确定所述第二应用进程不在所述第一应用进程所在的进程分组内，则向所述第一应用程序模块发送所述第三数据；

所述第一应用程序模块，还用于向所述第二应用程序模块发送所述第三数据。

13.根据权利要求10所述的终端，其特征在于，

所述第二应用程序模块，还用于接收所述第一应用程序模块发送的所述第三数据；

所述密钥管理模块，还用于接收所述第二应用程序模块发送的所述解密请求；

所述密钥管理模块，还用于向所述第二应用程序模块返回所述第四数据。

14.根据权利要求13所述的终端，其特征在于，所述密钥管理模块，还用于若所述密钥管理模块确定所述第二应用进程不在所述第一应用进程所在的进程分组内，则向所述第二应用程序模块发送所述第三数据。

15.根据权利要求10所述的终端，其特征在于，

所述密钥管理模块，还用于获取所述第一应用程序模块的标识；

所述密钥管理模块，还用于根据所述第一应用程序模块的标识，确定所述第一应用程序模块所在的进程分组的标识；

所述密钥管理模块，还用于根据所述第一应用程序模块所在的进程分组的标识，获取所述第一应用程序模块所在的进程分组对应的解密密钥。

16.根据权利要求10所述的终端，其特征在于，

所述第一应用程序模块，还用于请求所述密钥管理模块对第一数据进行加密；

所述密钥管理模块，还用于根据所述请求确定所述第一应用程序模块所在的进程分组；

所述密钥管理模块，还用于使用所述第一应用程序模块所在的进程分组对应的加密密钥对所述第一数据进行加密，生成第二数据；所述N个进程分组对应M个加密密钥，且每一个进程分组对应一个与其解密密钥相对应的加密密钥；

所述密钥管理模块，还用于向所述第一应用程序模块发送所述第二数据。

17.根据权利要求16所述的终端，其特征在于，

所述第一应用程序模块，还用于保存所述第二数据。

18.根据权利要求17所述的终端，其特征在于，

所述密钥管理模块，还用于获取所述第一应用程序模块的标识；

所述密钥管理模块，还用于根据所述第一应用程序模块的标识，确定所述第一应用程序模块所在的进程分组的标识；

所述密钥管理模块，还用于根据所述第一应用程序模块所在的进程分组的标识，获取所述第一应用程序模块所在的进程分组对应的加密密钥。

19.一种终端，其特征在于，包括：处理器、存储器和触摸屏，所述存储器、所述触摸屏与所述处理器耦合，所述存储器用于存储计算机程序代码，所述计算机程序代码包括计算机指令，当所述处理器从所述存储器中读取所述计算机指令，以执行如权利要求1-9中任一项所述数据处理的方法。

20.一种计算机存储介质，其特征在于，包括计算机指令，当所述计算机指令在终端上运行时，使得所述终端执行如权利要求1-9中任一项所述数据处理的方法。

分组应用使用同一密钥共享数据

技术领域

[0001] 本申请涉及通信技术领域，尤其涉及一种数据处理的方法及终端。

背景技术

[0002] 终端上的各个应用程序都是运行在各自独立的进程空间中，各个进程的数据和功能是相互隔离的。若进程之间需要通信，则被访问进程需先对访问进程进行权限校验。若校验成功，表明该访问进程具有访问权限，则允许该访问进程进行访问。否则，表明该访问进程不具有访问权限，则不允许该访问进程进行访问。

[0003] 可见，目前终端是通过权限机制来保证进程之间的通信安全。然而，在被访问进程授权的过程中，很容易出现误授权的情况。例如：用户可能会被诱导而安装了病毒应用，并对病毒应用进行了授权。那么，该病毒应用可以通过其他进程(被访问进程)的权限校验，即可以任意访问其他应用的数据，甚至是关键信息，这样会对用户造成危害。

发明内容

[0004] 本申请提供的一种数据处理的方法及终端，可以提高终端上应用进程中的数据安全性。

[0005] 第一方面，本申请提供的一种数据处理的方法，可应用于终端，该终端运行第一应用进程、第二应用进程和密钥管理进程。该方法具体包括：第二应用进程向第一应用进程发送访问请求，该访问请求用于请求访问所述第一应用进程的第三数据；密钥管理进程接收请求解密第三数据的解密请求；若密钥管理进程根据该解密请求确定第二应用进程在第一应用进程所在的进程分组内，则密钥管理进程使用第一应用进程所在的进程分组对应的解密密钥解密第三数据，得到第四数据；响应于该解密请求，密钥管理进程返回第四数据。

[0006] 其中，终端具有N个进程分组；N个进程分组中的每一个包含至少一个进程，并且至少有一个进程分组包含两个或两个以上的进程；其中，N为大于1或等于1的整数；N个进程分组对应M个解密密钥，且每一个进程分组对应一个解密密钥；其中，M为正整数，N＞＝M。

[0007] 其中，第一应用进程为第一应用程序运行的其中一个进程，而第一应用程序可以为终端上任一个应用，为可执行一定业务功能的程序和数据集合，例如：短信应用、美团应用、淘宝应用等。

[0008] 其中，第二应用进程可以为第一应用程序中另一个进程，不同于第一应用进程，第二应用进程也可以是第二应用程序中的一个进程，第二应用程序不同于第二应用程序。

[0009] 一些实施例中，第二应用进程需预先获取访问第一应用进程的权限。

[0010] 一些实施例中，第一数据可以是需要加密的数据，例如是根据第一应用进程或者第一应用程序的业务性质确定的数据，例如可以是第一应用进程或第一应用程序中重要的、关键的、敏感的数据。

[0011] 一些实施例中，密钥管理模块根据第三应用进程的业务类型、或下载来源等信息确定第三应用进程所对应的分组，并将第三应用进程的标识与该分组标识建立对应关系，

并保存在本地。

[0012] 由此可见，第二应用进程和第一应用进程属于同一进程分组时，密钥管理进程使用第一应用进程所在的进程分组对应的解密密钥对第三数据进行解密，使得第二应用进程获取到解密后的第三数据，即第四数据。实现了第二应用进程和第一应用进程属于同一进程分组时，才能访问第一应用进程的数据，有利于提高第一应用进程中的数据安全。

[0013] 在一种可能的设计中，密钥管理进程接收请求解密第三数据的解密请求具体为密钥管理进程接收第一应用进程根据访问请求发送的解密请求。密钥管理进程返回第四数据具体为：密钥管理进程向第一应用进程返回第四数据。第一应用进程向第二应用进程发送第四数据。

[0014] 可见，终端可以是第二应用进程访问第一应用进程，由第一应用进程向密钥管理进程请求对第三数据进行解密。在密钥管理进程对第三数据进行解密后，可通过第一应用进程将解密后的第三数据，即第四数据发送给第二应用进程。由此，本申请实施例提供了一种第二应用进程访问第一应用进程第三数据的方法。

[0015] 在一种可能的设计中，若密钥管理进程确定第二应用进程不在第一应用进程所在的进程分组内，则密钥管理进程向第一应用进程发送第三数据；第一应用进程向第二应用进程发送所述第三数据。

[0016] 可见，本申请实现了第二应用进程和第一应用进程不在同一进程分组时，密钥管理进程不对第三数据进行解密，通过第一应用进程将第三数据直接发送给第二应用进程，有利于包括第一应用进程的数据安全性。

[0017] 在一种可能的设计中，若第二应用进程不在分组中，则密钥管理模块也可以直接拒绝第一应用进程对第三数据的解密请求，结束流程。

[0018] 在一种可能的设计中，在第二应用进程向第一应用进程发送访问请求之后，密钥管理进程接收请求解密第三数据的解密请求之前，所述方法还包括：第二应用进程接收第一应用进程发送的第三数据；密钥管理进程接收请求解密第三数据的解密请求具体为：密钥管理进程接收第二应用进程发送的解密请求；密钥管理进程返回第四数据具体为：密钥管理进程向第二应用进程返回所述第四数据。

[0019] 可见，终端可以是第二应用进程访问第一应用进程的数据时，先获取到第一应用进程加密的数据，即第三数据，再由第二应用进程向密钥管理进程请求对第三数据进行解密。在密钥管理进程对第三数据进行解密后，可将解密后的第三数据，即第四数据发送给第二应用进程。由此，本申请实施例提供了一种第二应用进程访问第一应用进程第三数据的方法。

[0020] 在一种可能的设计中，若密钥管理进程确定第二应用进程不在第一应用进程所在的进程分组内，则密钥管理进程向第二应用进程发送第三数据。

[0021] 可见，本申请实现了第二应用进程和第一应用进程不在同一进程分组时，密钥管理进程不对第三数据进行解密，直接将第三数据发送给第二应用进程，有利于包括第一应用进程的数据安全性。

[0022] 在一种可能的设计中，在密钥管理进程使用第一应用进程所在的进程分组对应的解密密钥解密第三数据，得到第四数据之前，所述方法还包括：密钥管理进程获取第一应用进程的标识；密钥管理进程根据第一应用进程的标识，确定第一应用进程所在的进程分组

的标识;密钥管理进程根据第一应用进程所在的进程分组的标识,获取第一应用进程所在的进程分组对应的解密密钥。

[0023] 由此,本申请提供了一种终端获取第一应用进程所在的进程分组对应的解密密钥的方法。

[0024] 在一种可能的设计中,第一应用进程请求密钥管理进程对第一数据进行加密;密钥管理进程根据该请求确定第一应用进程所在的进程分组;密钥管理进程使用第一应用进程所在的进程分组对应的加密密钥对所述第一数据进行加密,生成第二数据;N个进程分组对应M个加密密钥,且每一个进程分组对应一个加密密钥;密钥管理进程向第一应用进程发送第二数据。

[0025] 由此,本申请实现了为同一进程分组中的应用进程使用相同的加密密钥进行加密的方法,有利于提升应用进程中的数据安全性。

[0026] 在一种可能的设计中,第一应用进程保存第二数据。

[0027] 一些实施例中,第一应用进程将第二数据保存在第一应用进程中的加密存储区。其中,加密存储区为第一应用进程中一片特定存储空间,专用于存储经过密钥管理模块加密后的数据。

[0028] 在一种可能的设计中,密钥管理进程根据该请求确定第一应用进程所在的进程分组包括:密钥管理进程获取第一应用进程的标识;密钥管理进程根据第一应用进程的标识,确定第一应用进程所在的进程分组的标识;密钥管理进程根据第一应用进程所在的进程分组的标识,获取第一应用进程所在的进程分组对应的加密密钥。

[0029] 第二方面,一种终端,包括第一应用程序模块、第二应用程序模块和密钥管理模块,第二应用程序模块,用于向第一应用程序模块发送访问请求,访问请求用于请求访问第一应用进程的第三数据;密钥管理模块,用于接收请求解密第三数据的解密请求;密钥管理模块,还用于若密钥管理模块根据解密请求确定第二应用进程在第一应用进程所在的进程分组内,则使用第一应用进程所在的进程分组对应的解密密钥解密所述第三数据,得到第四数据;密钥管理模块,还用于响应于解密请求,返回第四数据。

[0030] 其中,终端具有N个进程分组;N个进程分组中的每一个包含至少一个进程,并且至少有一个进程分组包含两个或两个以上的进程;其中,N为大于1或等于1的整数;N个进程分组对应M个解密密钥,且每一个进程分组对应一个解密密钥;其中,M为正整数,N>=M。

[0031] 一种可能的设计中,密钥管理模块,还用于接收第一应用程序模块根据访问请求发送的解密请求:密钥管理模块,还用于向第一应用程序模块返回第四数据;第一应用程序模块,用于向第二应用程序模块发送第四数据。

[0032] 一种可能的设计中,密钥管理模块,还用于若密钥管理模块确定第二应用进程不在第一进程所在的进程分组内,则向第一应用程序模块发送第三数据;第一应用程序模块,还用于向第二应用程序模块发送第三数据。

[0033] 一种可能的设计中,第二应用程序模块,还用于接收第一应用程序模块发送的第三数据;密钥管理模块,还用于接收第二应用程序模块发送的解密请求;密钥管理模块,还用于向第二应用程序模块返回第四数据。

[0034] 一种可能的设计中,密钥管理模块,还用于若密钥管理模块确定第二应用进程不在第一应用进程所在的进程分组内,则向第二应用程序模块发送第三数据。

[0035] 一种可能的设计中，密钥管理模块，还用于获取第一应用程序模块的标识；密钥管理模块，还用于根据第一应用程序模块的标识，确定第一应用程序模块所在的进程分组的标识；密钥管理模块，还用于根据第一应用程序模块所在的进程分组的标识，获取第一应用程序模块所在的进程分组对应的解密密钥。

[0036] 一种可能的设计中，第一应用程序模块，还用于请求密钥管理模块对第一数据进行加密；密钥管理模块，还用于根据该请求确定第一应用程序模块所在的进程分组；密钥管理模块，还用于使用第一应用程序模块所在的进程分组对应的加密密钥对第一数据进行加密，生成第二数据；N个进程分组对应M个加密密钥，且每一个进程分组对应一个加密密钥；密钥管理模块，还用于向第一应用程序模块发送第二数据。

[0037] 一种可能的设计中，第一应用程序模块，还用于保存第二数据。

[0038] 一种可能的设计中，密钥管理模块，还用于获取第一应用程序模块的标识；密钥管理模块，还用于根据第一应用程序模块的标识，确定第一应用程序模块所在的进程分组的标识；密钥管理模块，还用于根据第一应用程序模块所在的进程分组的标识，获取第一应用程序模块所在的进程分组对应的加密密钥。

[0039] 第三方面、一种终端，包括：处理器、存储器和触摸屏，存储器、触摸屏与处理器耦合，存储器用于存储计算机程序代码，计算机程序代码包括计算机指令，当处理器执行计算机指令时，终端执行如第一方面中任一任一种可能的设计方法中的数据处理的方法。

[0040] 第四方面、一种计算机存储介质，包括计算机指令，当计算机指令在终端上运行时，使得终端执行如第一方面中任一任一种可能的设计方法数据处理的方法。

[0041] 第五方面、一种计算机程序产品，当计算机程序产品在计算机上运行时，使得计算机执行如第一方面中任一任一种可能的设计方法数据处理的方法。

附图说明

[0042] 图1为本申请提供的一种终端的硬件结构示意图；

[0043] 图2为本申请提供的一种数据处理方法的流程示意图一；

[0044] 图3为本申请提供的一种进程的存储空间的示意图；

[0045] 图4为本申请提供的一种数据处理方法的流程示意图二；

[0046] 图5为本申请提供的一种数据处理方法的流程示意图三；

[0047] 图6为本申请提供的一种终端的软件结构示意图；

[0048] 图7为本申请提供的一种数据处理方法的流程示意图四；

[0049] 图8为本申请提供的一种数据处理方法的流程示意图五；

[0050] 图9为本申请提供的一种数据处理方法的流程示意图六；

[0051] 图10为本申请提供的一种数据处理方法的流程示意图七；

[0052] 图11为本申请提供的一种数据处理方法的流程示意图八；

[0053] 图12为本申请提供的一种终端的组成示意图一；

[0054] 图13为本申请提供的一种终端的组成示意图二。

具体实施方式

[0055] 以下，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性

或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括一个或者更多个该特征。在本申请的描述中，除非另有说明，“多个”的含义是两个或两个以上。

[0056] 首先，为了更好的理解本申请的技术方案，先对应用程序之间的通信机制进行简要介绍。

[0057] 终端在安装应用程序时，为每个应用程序都分配了唯一的用户标识(user Identifier，UID)或者进程标识(Process Identifier，PID)，并永久保持。在不同应用程序之间进行通信时，采用粘合剂(Binder)机制。Binder机制是基于客户端/服务端(Client/Sever，C/S)架构的。具体的，被访问的应用程序作为服务(Sever)端，访问的应用程序作为客户(Client)端。Client端将访问的任务发送给Server端，Server端会根据权限控制策略，根据UID/PID判断Client端是否满足访问权限。只有申请了特定权限的Client端才能访问Server端。

[0058] 目前，权限控制很多时候是通过弹出权限询问对话框，让用户选择是否运行。权限分为安装权限和动态权限。安装权限是指应用程序在第一次安装时，会将整个应用程序所涉及的所有权限一次询问，例如：在Android 6.0，也称为Android M，之前版本的安卓系统。动态权限则是在应用程序运行过程中，需要哪个权限再弹框询问用户是否给相应的权限，例如：Android M及之后版本的安卓系统。

[0059] 需要说明的是，对于某些恶意应用，可能会通过申明为不支持动态权限的应用程序，而避开用户的同意而直接获取某些重要应用程序的访问权限，获取这些重要应用程序的关键数据，给用户带来损失。为此，本申请提供了一种数据处理的方法，通过终端对安装在其上的应用程序进行分组，同一分组内的应用程序在运行时，使用相同的密钥对关键数据进行加密。这样，同一分组内的应用程序加密后的数据，只能由该分组内其他的应用程序进行解密。那么，即使恶意应用程序获得了该应用程序的访问权限，由于不在同一分组内，也不能对加密的数据进行解密，有利于保证用户的数据安全。

[0060] 示例性的，本申请中的终端可以为可以安装应用程序并显示应用程序图标的手机(如图1所示的手机100)、平板电脑、个人计算机(Personal Computer，PC)、个人数字助理(personal digital assistant，PDA)、智能手表、上网本、可穿戴电子设备、增强现实技术(Augmented Reality，AR)设备、虚拟现实(Virtual Reality，VR)设备等，本申请对该终端的具体形式不做特殊限制。

[0061] 如图1所示，以手机100作为上述终端举例，手机100具体可以包括：

[0062] 处理器101是手机100的控制中心，利用各种接口和线路连接手机100的各个部分，通过运行或执行存储在存储器103内的应用程序，以及调用存储在存储器103内的数据，执行手机100的各种功能和处理数据。在一些实施例中，处理器101可包括一个或多个处理单元；举例来说，处理器101可以是华为技术有限公司制造的麒麟960芯片。

[0063] 射频电路102可用于在收发信息或通话过程中，无线信号的接收和发送。特别地，射频电路102可以将基站的下行数据接收后，给处理器101处理；另外，将涉及上行的数据发送给基站。通常，射频电路包括但不限于天线、至少一个放大器、收发信机、耦合器、低噪声放大器、双工器等。此外，射频电路102还可以通过无线通信和其他设备通信。所述无线通信可以使用任一通信标准或协议，包括但不限于全球移动通讯系统、通用分组无线服务、码分

多址、宽带码分多址、长期演进、电子邮件、短消息服务等。

[0064] 存储器103用于存储应用程序以及数据，处理器101通过运行存储在存储器103的应用程序以及数据，执行手机100的各种功能以及数据处理。存储器103主要包括存储程序区以及存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)；存储数据区可以存储根据使用手机100时所创建的数据(比如音频数据、电话本等)。此外，存储器103可以包括高速随机存取存储器(Random Access Memory，RAM)，还可以包括非易失存储器，例如磁盘存储器件、闪存器件或其他易失性固态存储器件等。存储器103可以存储各种操作系统，例如，苹果公司所开发的iOS®操作系统，谷歌公司所开发的Android®操作系统等。上述存储器103可以是独立的，通过上述通信总线与处理器101相连接；存储器103也可以和处理器101集成在一起。

[0065] 触摸屏104具体可以包括触控板104-1和显示器104-2。

[0066] 其中，触控板104-1可采集手机100的用户在其上或附近的触摸事件(比如用户使用手指、触控笔等任何适合的物体在触控板104-1上或在触控板104-1附近的操作)，并将采集到的触摸信息发送给其他器件(例如处理器101)。其中，用户在触控板104-1附近的触摸事件可以称之为悬浮触控；悬浮触控可以是指，用户无需为了选择、移动或拖动目标(例如图标等)而直接接触触控板，而只需用户位于设备附近以便执行所想要的功能。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型来实现触控板104-1。

[0067] 显示器(也称为显示屏)104-2可用于显示由用户输入的信息或提供给用户的信息以及手机100的各种菜单。可以采用液晶显示器、有机发光二极管等形式来配置显示器104-2。触控板104-1可以覆盖在显示器104-2之上，当触控板104-1检测到在其上或附近的触摸事件后，传送给处理器101以确定触摸事件的类型，随后处理器101可以根据触摸事件的类型在显示器104-2上提供相应的视觉输出。虽然在图1中，触控板104-1与显示屏104-2是作为两个独立的部件来实现手机100的输入和输出功能，但是在某些实施例中，可以将触控板104-1与显示屏104-2集成而实现手机100的输入和输出功能。可以理解的是，触摸屏104是由多层的材料堆叠而成，本申请实施例中只展示出了触控板(层)和显示屏(层)，其他层在本申请实施例中不予记载。另外，触控板104-1可以以全面板的形式配置在手机100的正面，显示屏104-2也可以以全面板的形式配置在手机100的正面，这样在手机的正面就能够实现无边框的结构。

[0068] 另外，手机100还可以具有指纹识别功能。例如，可以在手机100的背面(例如后置摄像头的下方)配置指纹识别器112，或者在手机100的正面(例如触摸屏104的下方)配置指纹识别器112。又例如，可以在触摸屏104中配置指纹采集器件112来实现指纹识别功能，即指纹采集器件112可以与触摸屏104集成在一起来实现手机100的指纹识别功能。在这种情况下，该指纹采集器件112配置在触摸屏104中，可以是触摸屏104的一部分，也可以以其他方式配置在触摸屏104中。本申请实施例中的指纹采集器件112的主要部件是指纹传感器，该指纹传感器可以采用任何类型的感测技术，包括但不限于光学式、电容式、压电式或超声波传感技术等。

[0069] 手机100还可以包括蓝牙装置105，用于实现手机100与其他短距离的设备(例如手机、智能手表等)之间的数据交换。

[0070] 手机100还可以包括至少一种传感器106，比如光传感器、运动传感器以及其他传

感器。具体地，光传感器可包括环境光传感器及接近传感器，其中，环境光传感器可根据环境光线的明暗来调节触摸屏104的显示器的亮度，接近传感器可在手机100移动到耳边时，关闭显示器的电源。作为运动传感器的一种，加速计传感器可检测各个方向上(一般为三轴)加速度的大小，静止时可检测出重力的大小及方向，可用于识别手机姿态的应用(比如横竖屏切换、相关游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等；至于手机100还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。

[0071] WiFi装置107，用于为手机100提供遵循WiFi相关标准协议的网络接入，手机100可以通过WiFi装置107接入到WiFi接入点，进而帮助用户收发电子邮件、浏览网页和访问流媒体等，它为用户提供了无线的宽带互联网访问。在其他一些实施例中，该WiFi装置107也可以作为WiFi无线接入点，可以为其他设备提供WiFi网络接入。

[0072] 定位装置108，用于为手机100提供地理位置。可以理解的是，该定位装置108具体可以是全球定位系统(Global Positioning System，GPS)或北斗卫星导航系统、俄罗斯GLONASS等定位系统的接收器。定位装置108在接收到上述定位系统发送的地理位置后，将该信息发送给处理器101进行处理，或者发送给存储器103进行保存。在另外的一些实施例中，该定位装置108还可以是辅助全球卫星定位系统(Assisted Global Positioning System，AGPS)的接收器，AGPS系统通过作为辅助服务器来协助定位装置108完成测距和定位服务，在这种情况下，辅助定位服务器通过无线通信网络与设备例如手机100的定位装置108(即GPS接收器)通信而提供定位协助。在另外的一些实施例中，该定位装置108也可以是基于WiFi接入点的定位技术。由于每一个WiFi接入点都有一个全球唯一的(Media Access Control，MAC)地址，设备在开启WiFi的情况下即可扫描并收集周围的WiFi接入点的广播信号，因此可以获取到WiFi接入点广播出来的MAC地址；设备将这些能够标示WiFi接入点的数据(例如MAC地址)通过无线通信网络发送给位置服务器，由位置服务器检索出每一个WiFi接入点的地理位置，并结合WiFi广播信号的强弱程度，计算出该设备的地理位置并发送到该设备的定位装置108中。

[0073] 音频电路109、扬声器113、麦克风114可提供用户与手机100之间的音频接口。音频电路109可将接收到的音频数据转换后的电信号，传输到扬声器113，由扬声器113转换为声音信号输出；另一方面，麦克风114将收集的声音信号转换为电信号，由音频电路109接收后转换为音频数据，再将音频数据输出至RF电路102以发送给比如另一手机，或者将音频数据输出至存储器103以便进一步处理。

[0074] 外设接口110，用于为外部的输入/输出设备(例如键盘、鼠标、外接显示器、外部存储器、用户识别模块卡等)提供各种接口。例如通过通用串行总线(Universal Serial Bus，USB)接口与鼠标连接，通过用户识别模块卡卡槽上的金属触点与电信运营商提供的用户识别模块卡(Subscriber Identification Module，SIM)卡进行连接。外设接口110可以被用来将上述外部的输入/输出外围设备耦接到处理器101和存储器103。

[0075] 手机100还可以包括给各个部件供电的电源装置111(比如电池和电源管理芯片)，电池可以通过电源管理芯片与处理器101逻辑相连，从而通过电源装置111实现管理充电、放电、以及功耗管理等功能。

[0076] 尽管图1未示出，手机100还可以包括摄像头(前置摄像头和/或后置摄像头)、闪光

灯、微型投影装置、近场通信(Near Field Communication,NFC)装置等,在此不再赘述。

[0077] 以下实施例中的方法均可以在具有上述硬件结构的手机100中实现。

[0078] 如图2所示,为本申请提供的一种数据处理的方法流程图,该方法包括对数据的加密过程,该方法可应用于终端,该终端运行第一应用进程和密钥管理进程,该方法具体包括:

[0079] S101、第一应用进程生成第一数据。

[0080] 其中,第一应用进程为第一应用程序运行的其中一个进程,而第一应用程序可以为终端上任一个应用,为可执行一定业务功能的程序和数据集合,例如:短信应用、美团应用、淘宝应用等。

[0081] 一些实施例中,第一数据可以是需要加密的数据,例如是根据第一应用进程或者第一应用程序的业务性质确定的数据,例如可以是第一应用进程或第一应用程序中重要的、关键的、敏感的数据。举例说明,若第一应用程序是短信应用,则第一数据可以是账号、密码、验证码、短信内容等信息。具体的,第一数据可以是包含关键数据的整条短信内容,也可以是一条短信内容中部分内容,仅关键数据,本申请实施例不做限定。若第一数据是这类需要加密的数据,则第一应用进程需要向密钥管理模块请求对第一数据进行加密,即执行步骤S102。

[0082] 一些实施例中,第一数据可以是不需要加密的数据,例如是根据第一应用进程或第一应用程序的业务性质确定不需要加密的数据,则第一应用进程直接存储第一数据即可,即不需执行下面步骤。

[0083] S102、第一应用进程向密钥管理模块请求对第一数据进行加密,请求消息中携带第一数据。

[0084] 其中,密钥管理模块主要用于执行对各个应用进程中的特定数据进行加解密过程,以及创建与管理各个分组的加解密密钥等。密钥管理模块在运行时,也可以称为密钥管理进程。

[0085] S103、密钥管理模块对第一数据进行加密,生成第二数据。

[0086] 具体的,密钥管理模块被第一应用进程调用时,基于binder的进程间通信机制可知,密钥管理模块可获取调用者的标识,即第一应用进程的标识。第一应用进程的标识可以是第一应用进程的PID,也可以是第一应用程序的UID。那么,密钥管理模块可根据第一应用进程的标识确定第一应用进程所对应的分组,获取第一应用进程所对应的分组的标识。然后,根据第一应用进程所对应的分组的标识获取第一应用进程对应的加密密钥。最后,密钥管理模块根据获取的加密密钥对第一数据进行加密,得到第二数据。其中,第二数据为第一数据加密后的数据,为密文。

[0087] 需要说明的是,第一应用进程可以对应一个分组,这一个分组对应一个加密密钥,那么第一应用进程对应一个加密密钥。于是,密钥管理模块采用这一个加密密钥对第一数据进行加密。第一应用进程也可以对应多个分组,这多个分组对应多个加密密钥,那么第一应用进程对应多个加密密钥。于是,密钥管理模块采用这多个加密密钥对第一数据进行加密。本申请实施例不做限定。

[0088] 还需要说明的是,这里的分组,也可称为进程分组。终端中运行的一个或多个进程可以对应一个或多个进程分组。而这一个或多个进程分组分别对应一个或多个加密密钥。

[0089] 举例说明，假设终端上运行的应用进程可以划分为三个进程分组，分别为进程分组A、进程分组B和进程分组C。那么，进程分组A、进程分组B和进程分组C可以分别对应不同的加密密钥，也可以进程分组A和进程分组B对应一个相同的加密密钥，进程分组C对应另一个不同的加密密钥，还可以是进程分组A、进程分组B和进程分组C分别对应一个相同的加密密钥。本申请实施例对进程分组和加密密钥的对应关系不做限定。

[0090] S104、密钥管理模块将第二数据发送给第一应用进程。

[0091] S105、第一应用进程保存第二数据。

[0092] 具体的，第一应用进程将第二数据保存在第一应用进程中的加密存储区。其中，加密存储区为第一应用进程中一片特定存储空间，专用于存储经过密钥管理模块加密后的数据。

[0093] 示例性的，如图3所示，为第一应用进程的空间示意图。第一应用进程的空间包括：栈(stack)、堆(heap)、BBS(Block Started by Symbol)段、数据段(data segment)段、代码段(code/text segment)。

[0094] 其中，BBS段、数据段和代码段都属于静态内存分配，用于保存代码、全局变量和静态变量的，是具有固定作用的。stack是由操作系统自动分配和释放的，用于存放第一应用进程的局部变量，还可以用于传递参数和返回值。

[0095] heap为由第一应用进程分配和释放的，用于存放第一应用进程运行中被动态分配的内存空间段。在本申请实施例中，第一应用进程可以在第一次运行时，在heap分配一段内存空间，用于专门存储经密钥加密模块加密后的数据，即加密存储区。

[0096] 可见，在本申请实施例中，第一应用进程在运行过程中，先确定第一应用进程对应的分组，再获取该分组对应的加密密钥，使用该加密密钥对第一应用进程的数据进行加密，并存储于特定的加密存储区，有利于提高应用程序的关键数据的安全性。

[0097] 如图4所示，为本申请实施例提供的一种数据处理的方法流程图，该方法包括对数据的解密过程，具体包括：

[0098] S201、第二应用进程向第一应用进程请求访问第一应用进程的第三数据。

[0099] 其中，第二应用进程可以为第一应用程序中另一个进程，不同于第一应用进程，第二应用进程也可以是第二应用程序中的一个进程，第二应用程序不同于第二应用程序。

[0100] 一些实施例中，第二应用进程需预先获取访问第一应用进程的权限，图中以S201a示出。具体的，可以是第二应用进程向第一应用进程发送申请访问权限的请求，第一应用进程对第二应用进程进行授权。也可以是第一应用进程直接向第二应用进程进行授权，允许第二应用进程访问第一应用进程的数据。还可以是第一应用进程默认第二应用进程具有访问第一应用进程的权限，本申请实施例不做限定。

[0101] 然后，第二应用进程可读取第一应用进程的数据，包括第三数据。示例性的，第二应用进程可以读取第一应用进程中全部数据，也可以读取到与第二应用进程相关联的数据，本申请实施例不做限定。

[0102] 示例性，假设第一应用进程为短信应用中的进程，第二应用进程为美团应用中的进程，美团应用具有短信应用的访问权限。那么美团应用可以读取到短信应用中的全部短信内容，或者美团应用可以读取到短信应用中的，与美团应用相关联的短信内容，例如：美团应用发送给短信应用的验证码信息等。

[0103] S202、第一应用进程确定第三数据存储在加密存储区。

[0104] 具体的，第一应用进程根据获取到第三数据所对应的索引确定第三数据是否存储在加密存储区。若第三数据没有存储在加密存储区，则第三数据为明文，第一应用进程将第三数据发送给第二应用进程即可。若第三数据存储在加密存储区，则第三数据为密文，第一应用进程还需要对第三数据进行解密，即执行步骤S203。

[0105] S203、第一应用进程向密钥管理模块请求对第三数据进行解密，请求中携带第二应用进程的标识和第三数据。

[0106] 具体的，第一应用进程被第二应用进程调用时，第一应用进程可获取调用程序的标识，即第二应用进程的标识。

[0107] S204、密钥管理模块根据第二应用进程的标识，确定第二应用进程是否在第一应用进程所对应的分组，若是，则执行S205；否则，则密钥管理模块不对第三数据进行解密，直接返回第三数据。

[0108] 具体的，密钥管理模块被第一应用进程调用时，密钥管理模块可获取调用者的标识，即第一应用进程的标识。密钥管理模块可以根据第一应用进程的标识确定第一应用进程所对应的分组，以及该分组中包含的应用程序的标识。进一步的，密钥管理模块可以根据第二应用进程的标识确定第二应用进程是否在该分组中。若第二应用进程在分组中，则密钥管理模块对第三数据进行解密，即执行步骤S205。若第二应用进程不在分组中，则密钥管理模块不对第三数据进行解密，直接向第一应用进程返回第三数据。若第二应用进程不在分组中，则密钥管理模块也可以直接拒绝第一应用进程对第三数据的解密请求，结束流程。

[0109] 换句话来说，第二应用进程访问第一应用进程时，即使第二应用进程具有访问权限，但第二应用进程和第一应用进程并不属于同一个分组，第二应用进程也不能获得第一应用进程存储在加密存储区的数据的明文。这样，若第二应用进程为恶意程序时，即使诱导用户对第二应用进程访问第一应用进程进行授权，第二应用进程也不能获得第一应用进程加密的数据，提高了第一应用进程中加密数据的安全性。

[0110] S205、密钥管理模块对第三数据进行解密，得到第四数据。

[0111] 具体的，密钥管理模块根据第一应用进程对应的分组，获取该分组对应的解密密钥。采用获取到的解密密钥对第三数据进行解密，得到第四数据。其中，第四数据为第三数据解密后的数据，为明文。

[0112] 还需要说明的是，第一应用进程可以对应一个分组，这一个分组对应一个解密密钥，那么第一应用进程对应一个解密密钥。于是，密钥管理模块采用这一个解密密钥对第三数据进行解密。第一应用进程也可以对应多个分组，这多个分组中每一个分组又对应一个解密密钥，那么第一应用进程对应多个解密密钥。于是，密钥管理模块采用这多个解密密钥对第三数据进行解密。本申请实施例不做限定。

[0113] S206、密钥管理模块向第一应用进程发送第四数据。

[0114] S207、第一应用进程向第二应用进程发送第四数据。

[0115] 可见，在本申请实施例中，第二应用进程需要访问第一应用进程的加密数据时，需要第一应用进程申请密钥管理模块对加密数据进行解密。而密钥管理模块需先确定第二应用进程是否在第一应用进程的对应的分组内，若在，则对加密数据进行解密，并向第一应用进程返回解密后数据。由此，避免了第二应用进程在误获取访问第一应用进程的权限后，就

直接能读取第一应用进程的数据的情况发生，提升了第一应用进程的数据的安全性。

[0116] 还需要说明的是，在本申请实施例中，第二应用进程可以通过第一应用进程向密钥管理模块申请解密第三数据的。第二应用进程也可以直接向密钥管理模块申请解密第三数据，即步骤S202～S207可替换为步骤S301～S305。

[0117] 如图5所示，为本申请实施例提供的一种数据处理的方法流程图，该方法包括步骤S201、S301～S305，具体如下：

[0118] S301、第一应用进程向第二应用进程返回第三数据。

[0119] 其中，若第三数据存储在第一应用进程的加密存储区中，则第三数据为密文，则需要第一应用进程需要对第三数据进行解密，即执行步骤S302。若第三数据存储在第一应用进程的非加密存储区中，则第三数据为明文，即为第一应用进程最终要获取的数据。

[0120] S302、第二应用进程向密钥管理模块请求解密第三数据，该请求中携带第三数据和第一应用进程的标识。

[0121] 需要说明的是，第二应用进程被第一应用进程调用时，第二应用进程可获取调用者的标识，即第一应用进程的标识。

[0122] S303、密钥管理模块根据确定第二应用进程是否在第一应用进程所对应的分组。若是，则执行S304；否则，密钥管理模块不对第三数据进行解密，直接向第一应用进程返回第三数据。

[0123] 具体的，密钥管理模块被第二应用进程调用时，密钥管理模块也可获取第二应用进程的标识。那么，密钥管理模块根据请求中携带的第一应用进程的标识，确定第一应用进程所对应的分组以及该分组中包含的应用进程的标识。进一步的，密钥管理模块可以根据第二应用进程的标识确定第二应用进程是否在该分组中。若第二应用进程在分组中，则密钥管理模块对第三数据进行解密，即执行步骤S304。若第二应用进程不在分组中，则密钥管理模块不对第三数据进行解密，直接向第一应用进程返回第三数据。若第二应用进程不在分组中，则密钥管理模块也可以直接拒绝第二应用进程对第三数据的解密请求，结束流程。

[0124] S304、密钥管理模块对第三数据进行解密，得到第四数据。

[0125] 本步骤可参考步骤S205，不再重复赘述。

[0126] S305、密钥管理模块向第二应用进程发送第四数据。

[0127] 由此，本申请实施例中，第二应用进程在获取到第一应用进程加密数据后，可向密钥管理模块申请对该加密数据进行解密。而密钥管理模块需先确定第二应用进程是否在第一应用进程的对应的分组内，若在，则对加密数据进行解密，并向第一应用进程返回解密后数据。由此，避免了第二应用进程在误获取访问第一应用进程的权限后，就直接能读取第一应用进程的数据的情况发生，提升了第一应用进程的数据的安全性。

[0128] 示例性的，如图6所示，为本申请实施例提供的一种终端的组成示意图，该终端包括多个应用进程601～604、密钥管理模块605和安全存储模块606。

[0129] 其中，终端对这多个应用进程进行了分组，同一分组内的应用进程采用相同的密钥对特定数据进行加解密，即同一分组内的应用进程之间可以相互访问特定数据。其中，分组方法将在下文具体介绍。例如：应用进程601和应用进程602为第一分组的进程。应用进程603和应用进程604为第二分组的进程。

[0130] 密钥管理模块605，用于执行对各个应用进程中的特定数据进行加解密过程，以及

创建与管理各个分组的加解密密钥等。具体的，密钥管理模块605还包括分组管理模块60501和加密模块60502。

[0131] 其中，分组管理模块60501，用于按照分组策略对应用进程进行分组，分组管理模块60502可以自动生成分组策略，也可以接收用户的设置，更新分组策略，本申请对分组策略不做限定。分组管理模块60502还可以请求加密模块60502为分组创建密钥，建立应用与分组、和/或密钥的对应关系等。其中加密模块60502，用于为分组创建新的密钥对，对应用进程的数据进行加密、解密等。

[0132] 安全存储模块606，用于存储密钥管理模块605生成的加解密的密钥，保证密钥存储的安全。

[0133] 下面以本申请提供的数据处理方法运用于如图6所示的终端为例，对本申请提供的技术方案进行详细阐述。

[0134] 首先，对于应用进程的分组策略进行说明。终端可以根据应用进程对应的应用程序的来源、业务类型等，对应用进程进行分组。

[0135] 示例性的，分组策略可以是根据应用程序的下载来源进行分组。具体的，从终端中的应用市场中下载的应用程序，由于这些应用程序是通过上架审核的，可认为是可信的应用程序，可划分到为一个分组。从其他的方式下载的，不是通过应用市场下载的，可认为是不可信的应用程序，可划分到另一个分组。

[0136] 示例性的，分组策略还可以是根据应用程序的具体业务类型进行分组。具体的，从应用市场下载的应用程序在上架时，应用市场会对这些应用程序进行分类，例如：办公、购物、社交、娱乐、新闻等。那么，可以根据这些分类对应用程序进行分组，例如同一类型的应用程序划分到一个分组内，也可以是几个类型的应用程序划分到一个分组内，本申请实施例不做限定。

[0137] 需要说明的是，应用市场在终端下载应用程序时，也将该应用程序的来源信息、业务类型下发给终端，以便终端根据这些信息进行分组，或者应用市场将其对应用程序的分类信息发送给终端。如图7所示，为应用程序的发布、上架审核、分类、下载的流程示意图。

[0138] 在一些实施例中，当应用开发者或用户发现应用程序有恶意行为后，可以上报给应用市场，应用市场重新进行审核，重新分组。如图8所示，为应用程序被重新审核上架的流程示意图。

[0139] 示例性的，分组策略还可以是根据用户的设置，指定将某些应用程序划分到一个分组内。分组策略还可以是以上各种分组策略的组合，本申请实施例不做限定。

[0140] 在终端确定分组策略后，终端根据分组策略对各个应用程序进行分组，以及为各个分组确定密钥。具体的，如图9所示，为本申请实施例提供的一种数据处理的方法流程示意图，该方法具体包括：

[0141] S401、终端检测到第三应用程序安装完成后，通知分组管理模块为第三应用程序对应的第三应用进程分组。

[0142] 其中，第三应用程序为终端需要安装的新的应用程序，第三应用程序不同于第一应用程序和第二应用程序。

[0143] 需要说明的是，终端也可以是检测到用户要求安装第三应用程序的操作后，就通知分组管理模块，本申请实施例不做限定。

[0144] 还需要说明的是，终端上安装应用程序通常有两类，一类是终端预置的应用程序，例如短信应用、照相应用、浏览器应用等。这些应用程序可以是终端首次开机时，由系统触发终端自行安装的。另一类是用户自己下载安装的，例如：美团应用、支付宝应用等，这些应用是有用户的操作触发终端安装的。无论是哪种安装方式，终端都可以在应用程序安装完成后，或开始安装后，通知分组管理模块。

[0145] S402、分组管理模块根据分组策略将第三应用进程进行分组。

[0146] 具体的，分组管理根据第三应用进程的业务类型、或下载来源等信息确定第三应用进程所对应的分组，并将第三应用进程的标识与该分组标识建立对应关系，并保存在本地。

[0147] 进一步的，若第三应用进程为该分组中的第一个安装的应用程序时，分组管理模块请求加密模块为该分组创建新的分组密钥对，即执行步骤S403。若第三应用进程不是该分组中的第一个安装的应用程序时，分组管理模块直接建立第三应用进程与分组、密钥之间的对应关系，即执行步骤S406。

[0148] 举例说明，假设第三应用进程为美团应用，第三应用进程所对应的分组为购物分组。那么，在美团应用安装完成时，或者在终端接收用户要求安装美团应用时，通知分组管理模块。分组管理模块将美团应用划分到购物分组。若美团应用是购物分组内的第一个安装的应用程序，在分组管理模块请求加密模块为该购物分组创建密钥对。若美团应用不是购物分组中第一个安装的应用程序，则分组管理模块直接将美团应用与购物分组及购物分组的密钥建立对应关系。

[0149] S403、分组管理模块向加密模块发送请求为第三应用进程所对应的分组创建密钥对。

[0150] 其中，该请求中携带第三应用进程所对应的分组的标识。

[0151] S403a、加密模块为第三应用进程所对应的分组创建密钥对。

[0152] S404、加密模块将创建的密钥对存储在安全存储模块中。

[0153] 示例的，在安卓系统中，安全存储模块可以包括密钥库(keystore)和keymaster。其中，keystore用于存储的是密钥对的索引，用于提供其他应用使用密钥对的接口。keymaster用于存储密钥对的内容、及对数据进行加密解密处理。具体的，加密模块可以通过keystore将创建的密钥对存储在keymaster，由于keymaster与keystore物理隔离，能够提高密钥对的存储安全。

[0154] S405、加密模块将创建的密钥对的信息返回给分组管理模块。

[0155] 其中，密钥对的信息可以包括分组标识和密钥对的索引的对应关系。

[0156] 示例性的，加密模块可以将分组标识和密钥对的索引的对应关系返回给分组管理模块。当加密模块需要加密时，可以根据密钥对的索引从安全存储模块中查找到对应的加密密钥，采用查找到的加密密钥进行加密。当加密模块需要解密时，可以根据密钥对的索引从安全存储模块中查找到对应的解密密钥，采用查找到的解密密密钥进行解密。

[0157] 其中，步骤S405也可以在S404之前或同时执行，本申请实施例不限定步骤S404和S405之间的顺序关系。

[0158] S406、分组管理模块将第三应用进程与分组、密钥对建立对应关系。

[0159] 示例性的，分组管理模块根据加密模块返回的分组标识和密钥对索引的对应关

系，以及本地已有的第三应用进程的标识与分组标识的对应关系，建立第三应用进程的标识、分组标识和密钥对索引的对应关系。

[0160] 需要说明的是，如果某个分组中的应用程序发送变化，例如某个应用程序从一个分组变化到另一分组，分组管理模块需要更新应用程序与分组、密钥对的对应关系。

[0161] 举例说明，假设在某个分组内发送有恶意应用，可以将该恶意应用从该分组中剔除，换到另一个分组，不再允许该恶意应用访问本分组内其他应用的数据。或者，经过对业务性质的评估，发现某个应用可不必在某个分组内，则也可以从该分组中剔除，换到另一个分组。

[0162] 由此，本申请实施例提供一种数据处理的方法，能够对应用程序进行分组，并为该分组创建密钥对，建立应用程序与分组、密钥对的对应关系，从而能够实现同一分组内的应用程序使用同一密钥进行加解密。

[0163] 进一步的，对数据的加密过程中步骤S102～S104进行细化，那么，步骤S102～S104可替换为S501～S507，如图10所示，本申请实施例提供的数据处理方法还具体包括：

[0164] S501、分组管理模块接收第一应用进程发送的第一数据。

[0165] 具体的，分组管理模块被第一应用进程调用，分组管理模块可以获取第一应用进程的标识。

[0166] S502、分组管理模块根据第一应用进程的标识，获取第一应用进程对应的加密密钥或密钥对的索引。

[0167] 示例的，分组管理模块根据第一应用进程的标识，查找第一应用进程的标识对应的分组标识，进一步根据该分组标识确定该分组标识对应的加密密钥或密钥对的索引。而查找到的加密密钥或密钥对的索引对应着第一应用进程对应的加密密钥或密钥对。

[0168] S503、分组管理模块将第一数据和获取到的加密密钥或密钥对的索引发送给加密模块。

[0169] S504、加密模块根据加密密钥或密钥对的索引，从安全存储模块读取第一应用进程对应的加密密钥。

[0170] S505、加密模块根据获取的加密密钥对第一数据进行加密，得到第二数据。

[0171] S506、加密模块将得到的第二数据发送给分组管理模块。

[0172] S507、分组管理模块将第二数据发送给第一应用进程。

[0173] 进一步的，对数据的解密过程中步骤S203～S206进行细化，那么，步骤S203～S206可替换为S601～S607，如图11所示，本申请实施例提供的数据处理方法还具体包括：

[0174] S601、第一应用进程向分组管理模块请求对第三数据进行解密，请求中携带第二应用进程的标识和第三数据。

[0175] 具体的，第一应用进程被第二应用进程调用时，第一应用进程可获取调用程序的标识，即第二应用进程的标识。

[0176] S602、分组管理模块根据第二应用进程的标识，确定第二应用进程是否在第一应用进程所对应的分组。若是，则执行步骤S603。否则，分组管理模块不请求加密模块对第三数据进行解密，而是直接向第一应用进程返回第三数据。

[0177] 具体的，分组管理模块被第一应用进程调用时，分组管理模块可获取调用者的标识，即第一应用进程的标识。分组管理模块可以根据第一应用进程的标识确定第一应用进

程所对应的分组，以及该分组中包含的应用程序的标识。进一步的，分组管理模块可以根据第二应用进程的标识确定第二应用进程是否在该分组中。若第二应用进程在分组中，则分组管理模块请求加密模块对第三数据进行解密，即执行步骤S603。若第二应用进程不在分组中，则分组管理模块不请求加密模块对第三数据进行解密，而是直接向第一应用进程返回第三数据，而第一应用进程向第二应用进程返回第三数据。

[0178] S603、分组管理模块根据第一应用进程的标识，获取第一应用进程对应的解密密钥或密钥对的索引。

[0179] 示例的，分组管理模块根据第一应用进程的标识，查找第一应用进程的标识对应的分组标识，进一步根据该分组标识确定该分组标识对应的解密密钥或密钥对的索引。而查找到的解密密钥或密钥对的索引对应着第一应用进程对应的加密密钥或密钥对。

[0180] S604、分组管理模块将第三数据和获取到的解密密钥或密钥对的索引发送给加密模块。

[0181] S605、加密模块根据解密密钥或密钥对的索引，从安全存储模块读取第一应用进程对应的解密密钥。

[0182] S606、加密模块根据获取的解密密钥对第三数据进行解密，得到第四数据。

[0183] 其中，第四数据为第三数据解密后的数据，为明文。

[0184] S607、加密模块将得到的第四数据发送给分组管理模块。

[0185] S608、分组管理模块将第四数据发送给第一应用进程。

[0186] 可以理解的是，上述终端等为了实现上述功能，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，本申请实施例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发明实施例的范围。

[0187] 本申请实施例可以根据上述方法示例对上述终端等进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。需要说明的是，本发明实施例中对模块的划分是示意性的，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。

[0188] 在采用对应各个功能划分各个功能模块的情况下，图12示出了上述实施例中所涉及的终端的一种可能的结构示意图。如图12所示，终端1200包括：第一应用程序模块1201、第二应用程序模块1202和密钥管理模块1203。

[0189] 其中，第一应用程序模块1201用于支持终端执行图2中的S101、S102和S105，图4中的S202、S203和S207，图5中的S302，图10中的S501，图11中的S601和/或用于本文所描述的技术的其它过程。第二应用程序模块1202用于支持终端执行图4中的S201a和S201，和/或用于本文所描述的技术的其它过程。密钥管理模块1203用于支持终端执行图2中的S103和S104，图4中的S204-S206，图5中的S303-S305，图9中的S402-S406，图10中的S502-S507，图11中的S602-S608，和/或用于本文所描述的技术的其它过程。

[0190] 其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块

的功能描述，在此不再赘述。

[0191] 当然，终端1200还可以包括安全存储单元1204，用于存储本申请中的分组信息、加密密钥和解密密钥等。终端1200还可以包括通信单元，用于终端与其他设备进行交互。并且，上述功能单元的具体所能够实现的功能也包括但不限于上述实例所述的方法步骤对应的功能，终端1200的其他单元的详细描述可以参考其所对应方法步骤的详细描述，本申请实施例这里不再赘述。

[0192] 在采用集成的单元的情况下，上述第一应用程序模块1201、第二应用程序模块1202和密钥管理模块1203可以集成在一起，可以是终端的处理模块。上述的通信单元可以是终端的通信模块，如RF电路、WiFi模块或者蓝牙模块。上述安全存储单元可以是终端的存储模块。

[0193] 图13示出了上述实施例中所涉及的终端的一种可能的结构示意图。该终端1300包括：处理模块1301、存储模块1302和通信模块1303。处理模块1301用于对终端的动作进行控制管理。存储模块1302，用于保存终端的程序代码和数据。通信模块1303用于与其他终端通信。其中，处理模块1301可以是处理器或控制器，例如可以是中央处理器(Central Processing Unit,CPU)，通用处理器，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)或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本发明公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP和微处理器的组合等等。通信模块1303可以是收发器、收发电路或通信接口等。存储模块1302可以是存储器。

[0194] 当处理模块1301为处理器(如图1所示的处理器101)，通信模块1303为RF收发电路(如图1所示的射频电路102)，存储模块1302为存储器(如图1所示的存储器103)时，本申请实施例所提供的终端可以为图1所示的终端100。其中，上述通信模块1303不仅可以包括RF电路，还可以包括WiFi模块和蓝牙模块。RF电路、WiFi模块和蓝牙模块等通信模块可以统称为通信接口。其中，上述处理器、通信接口和存储器可以通过总线耦合在一起。

[0195] 通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0196] 在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块或单元的划分，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，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0197] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个

网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0198] 另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。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。

[0199] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或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)或处理器执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：快闪存储器、移动硬盘、只读存储器、随机存取存储器、磁碟或者光盘等各种可以存储程序代码的介质。

[0200] 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何在本申请揭露的技术范围内的变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

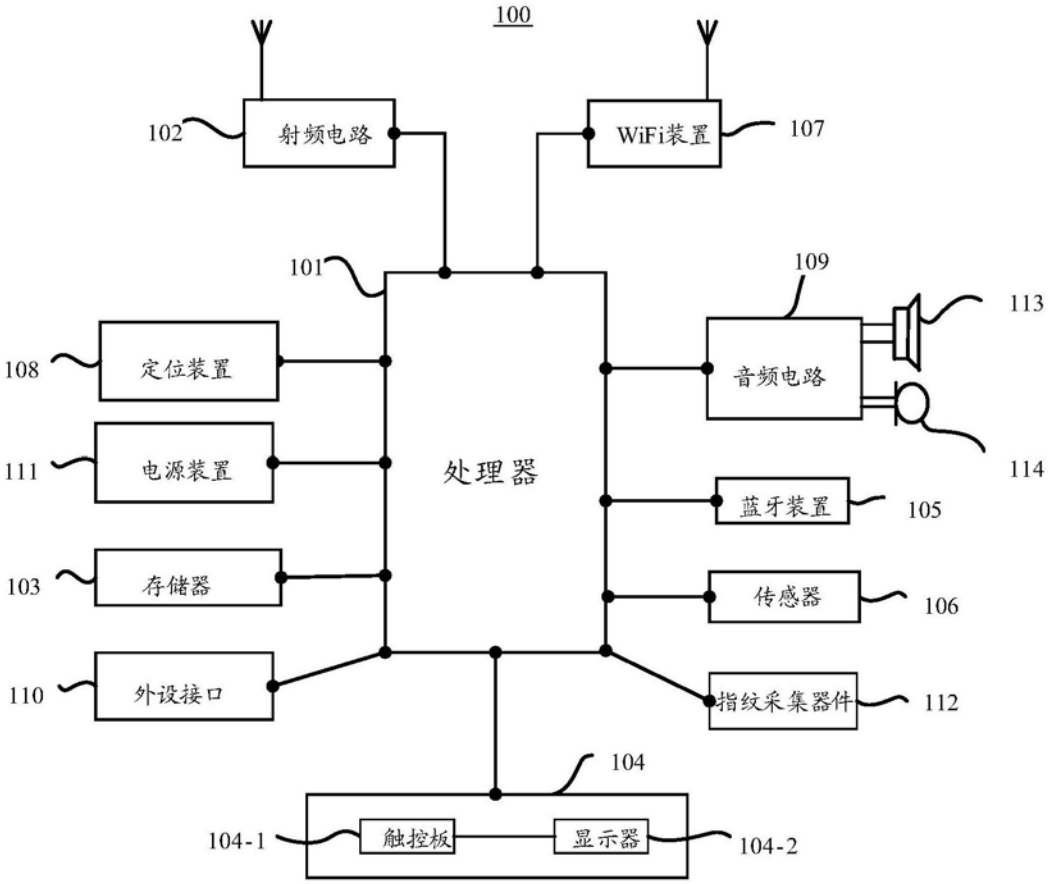

100
102
射频电路
WiFi装置
107
101
109
113
108
定位装置
音频电路
111
电源装置
处理器
114
蓝牙装置
105
103
存储器
传感器
106
110
外设接口
指纹采集器件
112
104
104-1
触控板
显示器
104-2

图1

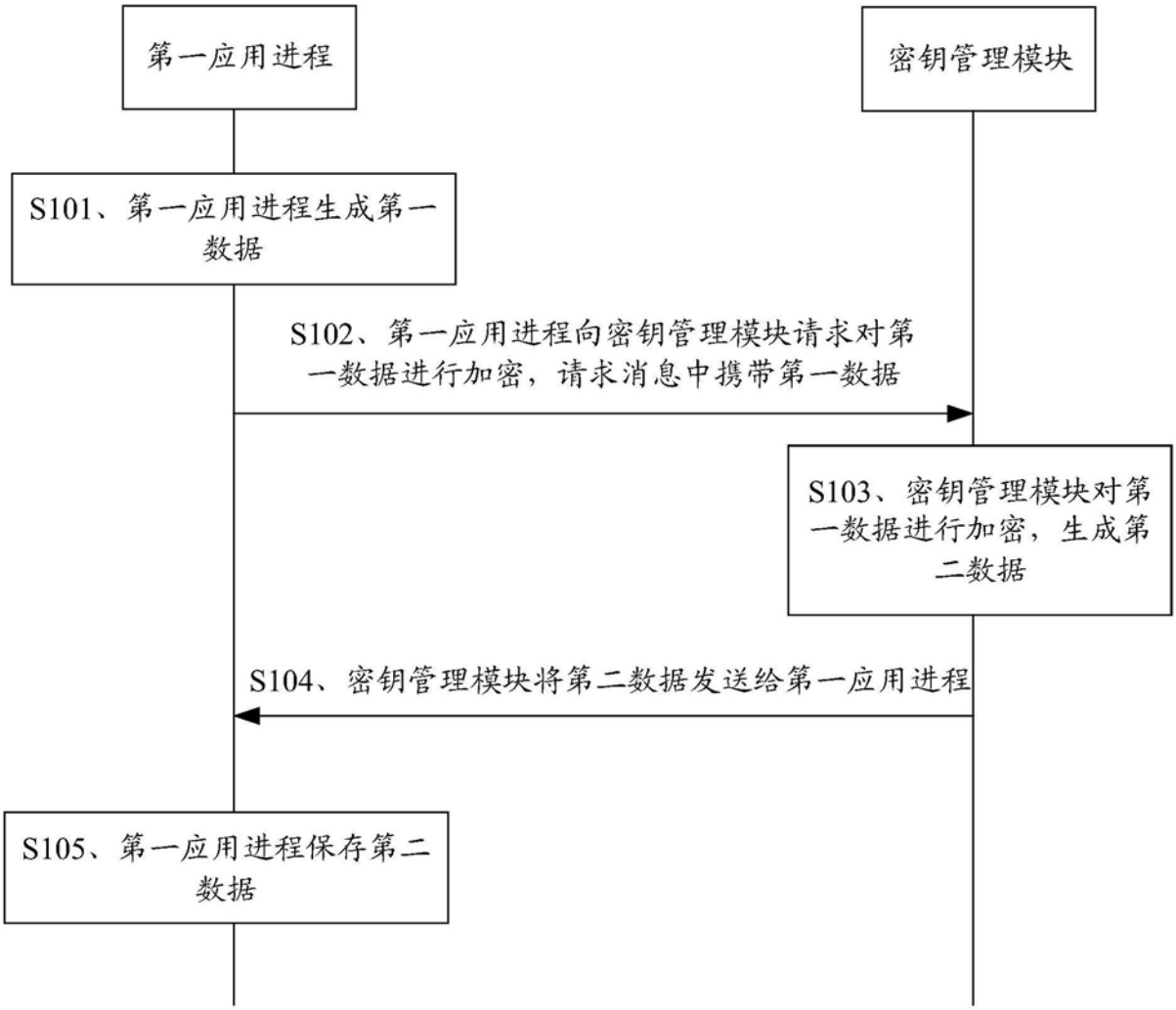

第一应用进程
密钥管理模块
S101、第一应用进程生成第一数据
S102、第一应用进程向密钥管理模块请求对第一数据进行加密，请求消息中携带第一数据
S103、密钥管理模块对第一数据进行加密，生成第二数据
S104、密钥管理模块将第二数据发送给第一应用进程
S105、第一应用进程保存第二数据

图2

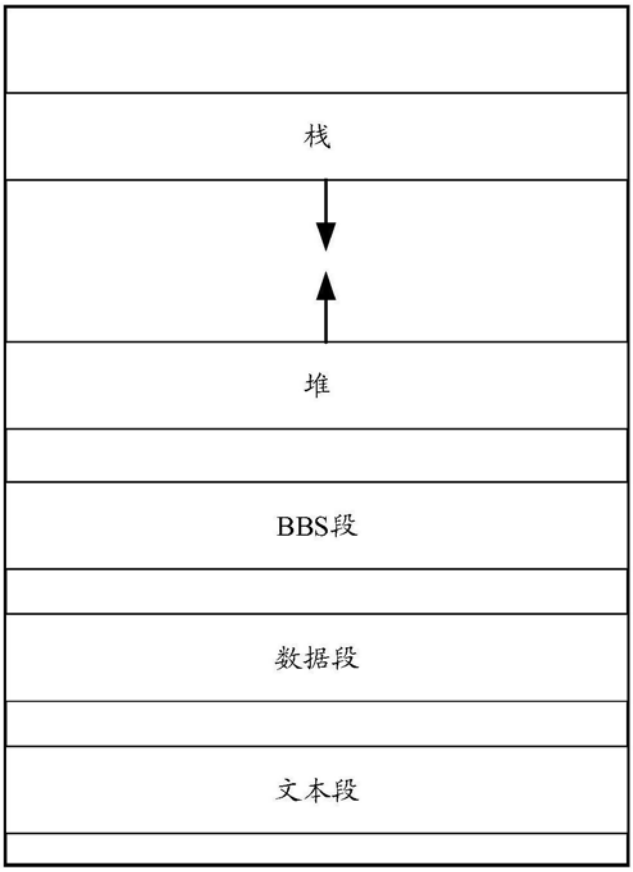


图3

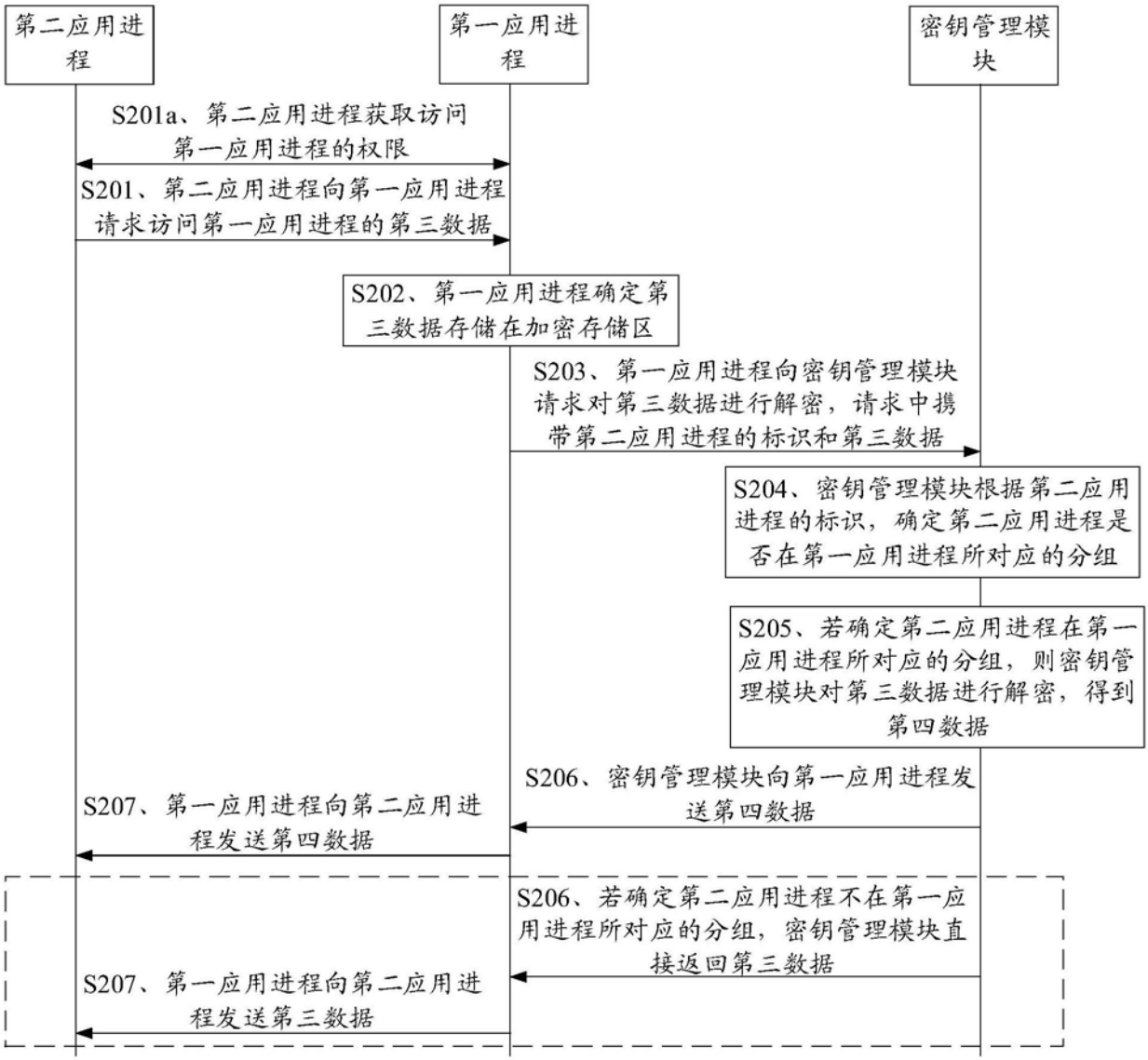

第二应用进程
第一应用进程
密钥管理模块
S201a、第二应用进程获取访问第一应用进程的权限
S201、第二应用进程向第一应用进程请求访问第一应用进程的第三数据
S202、第一应用进程确定第三数据存储在加密存储区
S203、第一应用进程向密钥管理模块请求对第三数据进行解密，请求中携带第二应用进程的标识和第三数据
S204、密钥管理模块根据第二应用进程的标识，确定第二应用进程是否在第一应用进程所对应的分组
S205、若确定第二应用进程在第一应用进程所对应的分组，则密钥管理模块对第三数据进行解密，得到第四数据
S206、密钥管理模块向第一应用进程发送第四数据
S207、第一应用进程向第二应用进程发送第四数据
S206、若确定第二应用进程不在第一应用进程所对应的分组，密钥管理模块直接返回第三数据
S207、第一应用进程向第二应用进程发送第三数据

图4


第二应用进程
第一应用进程
密钥管理模块
S201a、第二应用进程获取访问第一应用进程的权限
S201、第二应用进程向第一应用进程请求访问第一应用进程的第三数据
S301、第一应用进程向第二应用进程返回第三数据
S302、第二应用进程向密钥管理模块请求解密第三数据，该请求中携带第三数据和第一应用进程的标识
S303、密钥管理模块根据第二应用进程的标识，确定第二应用进程是否在第一应用进程所对应的分组
S304、若确定第二应用进程在第一应用进程所对应的分组，则密钥管理模块对第三数据进行解密，得到第四数据
S305、密钥管理模块向第二应用进程发送第四数据
S206、若确定第二应用进程不在第一应用进程所对应的分组，密钥管理模块直接返回第三数据

图5

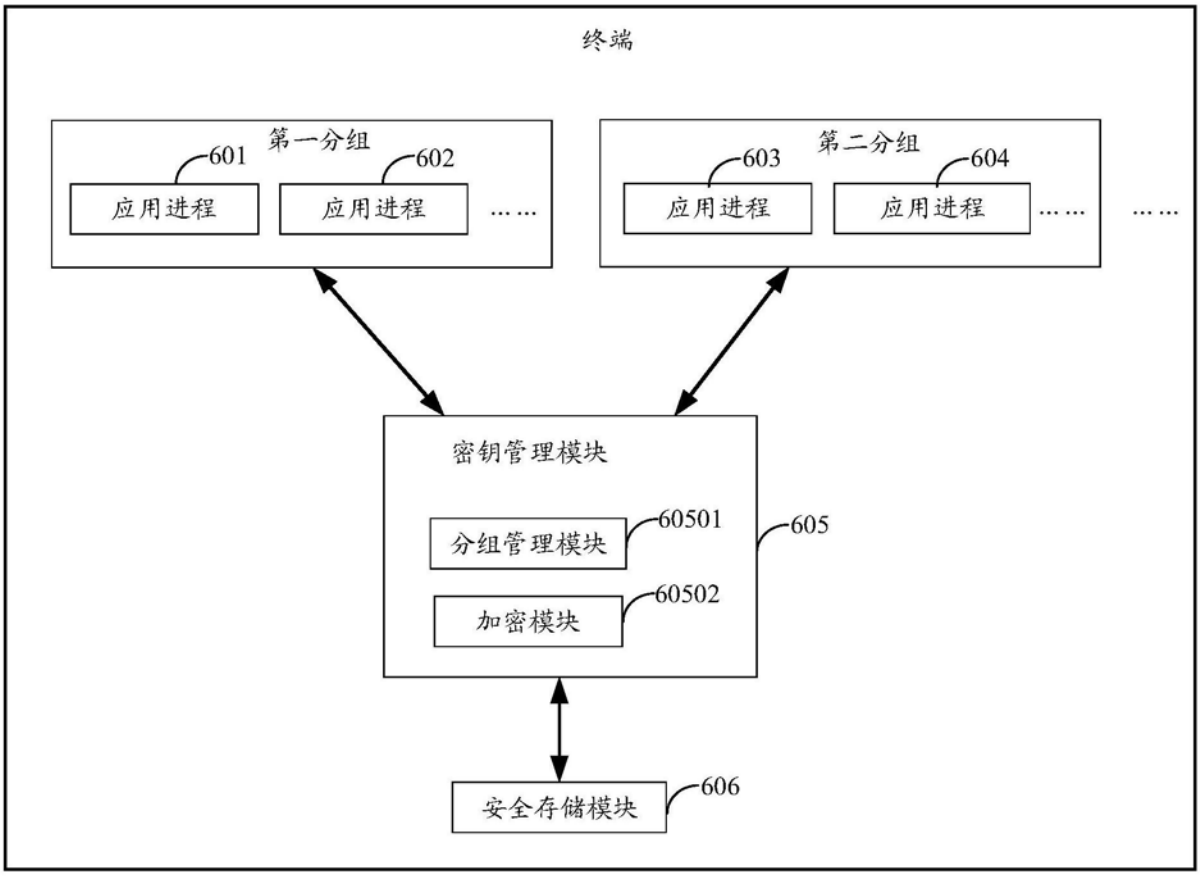

终端
第一分组
601
602
应用进程
应用进程
……
第二分组
603
604
应用进程
应用进程
……
……
密钥管理模块
分组管理模块
60501
605
加密模块
60502
安全存储模块
606

图6

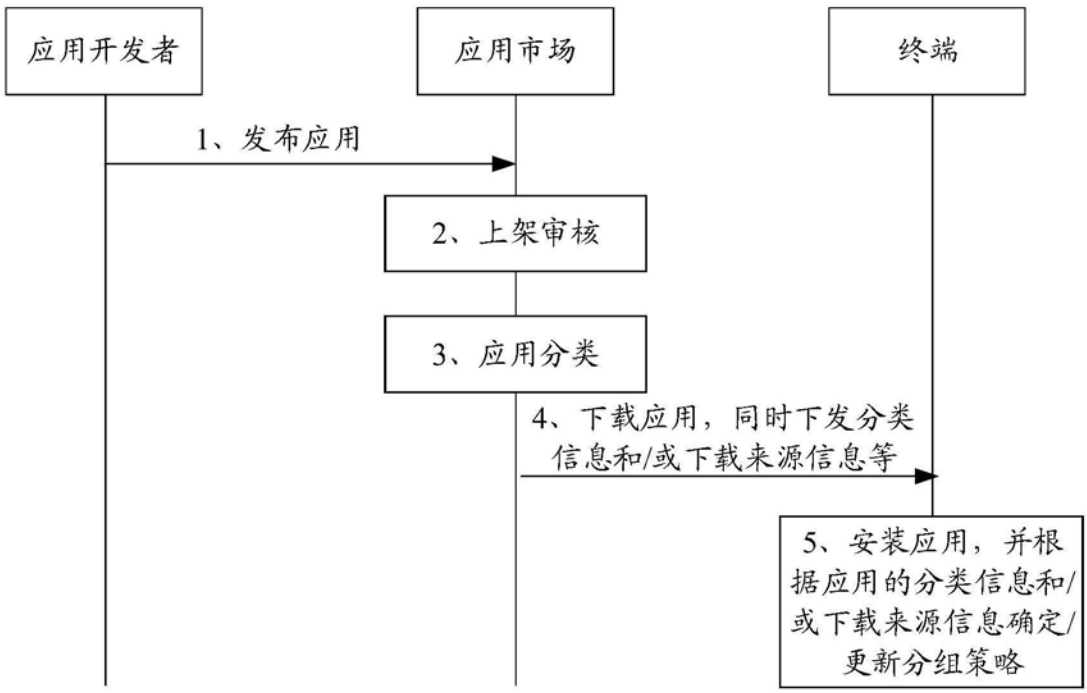

应用开发者
应用市场
终端
1、发布应用
2、上架审核
3、应用分类
4、下载应用，同时下发分类信息和/或下载来源信息等
5、安装应用，并根据应用的分类信息和/或下载来源信息确定/更新分组策略

图7

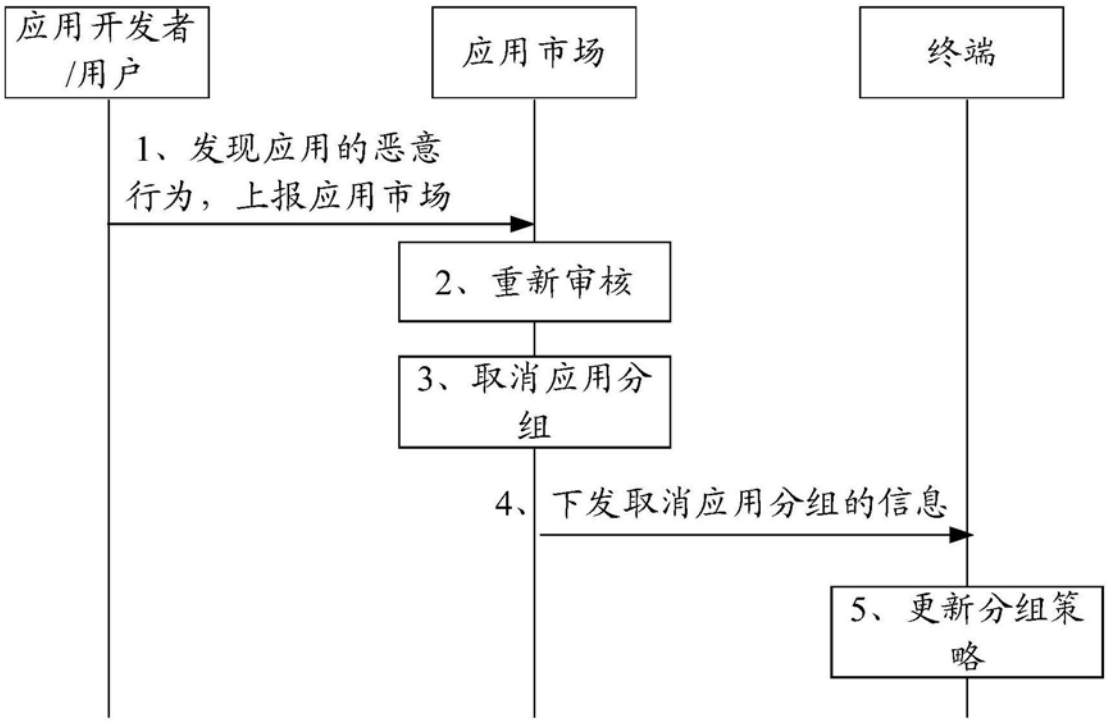

应用开发者/用户
应用市场
终端
1、发现应用的恶意行为，上报应用市场
2、重新审核
3、取消应用分组
4、下发取消应用分组的信息
5、更新分组策略

图8

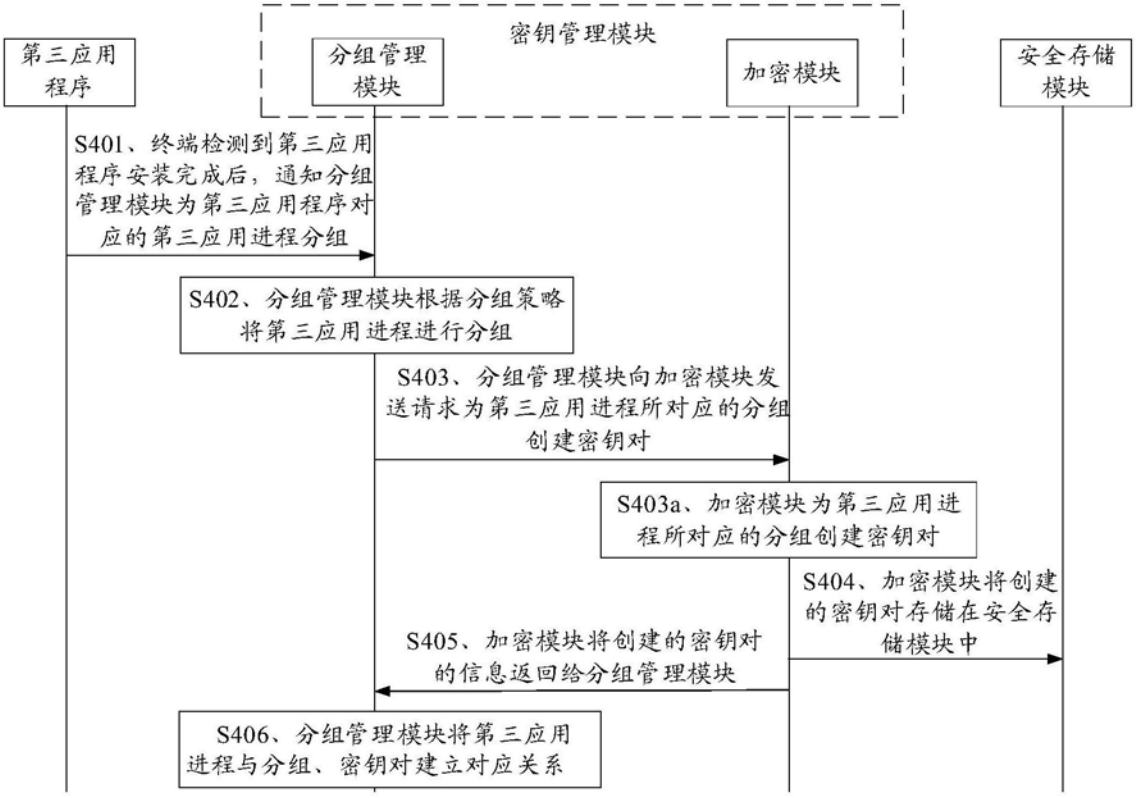

第三应用程序
密钥管理模块
分组管理模块
加密模块
安全存储模块
S401、终端检测到第三应用程序安装完成后，通知分组管理模块为第三应用程序对应的第三应用进程分组
S402、分组管理模块根据分组策略将第三应用进程进行分组
S403、分组管理模块向加密模块发送请求为第三应用进程所对应的分组创建密钥对
S403a、加密模块为第三应用进程所对应的分组创建密钥对
S404、加密模块将创建的密钥对存储在安全存储模块中
S405、加密模块将创建的密钥对的信息返回给分组管理模块
S406、分组管理模块将第三应用进程与分组、密钥对建立对应关系

图9

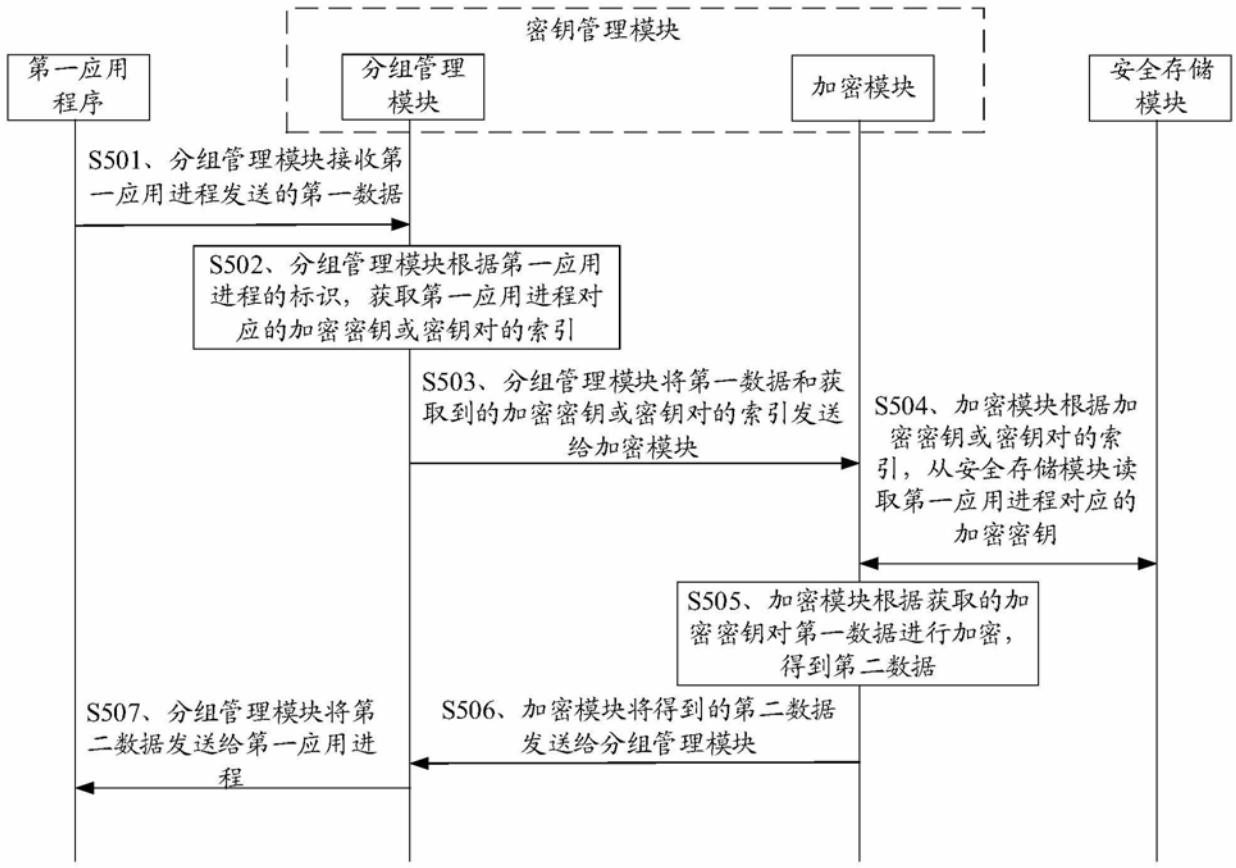

密钥管理模块
第一应用程序
分组管理模块
加密模块
安全存储模块
S501、分组管理模块接收第一应用进程发送的第一数据
S502、分组管理模块根据第一应用进程的标识，获取第一应用进程对应的加密密钥或密钥对的索引
S503、分组管理模块将第一数据和获取到的加密密钥或密钥对的索引发送给加密模块
S504、加密模块根据加密密钥或密钥对的索引，从安全存储模块读取第一应用进程对应的加密密钥
S505、加密模块根据获取的加密密钥对第一数据进行加密，得到第二数据
S506、加密模块将得到的第二数据发送给分组管理模块
S507、分组管理模块将第二数据发送给第一应用进程

图10

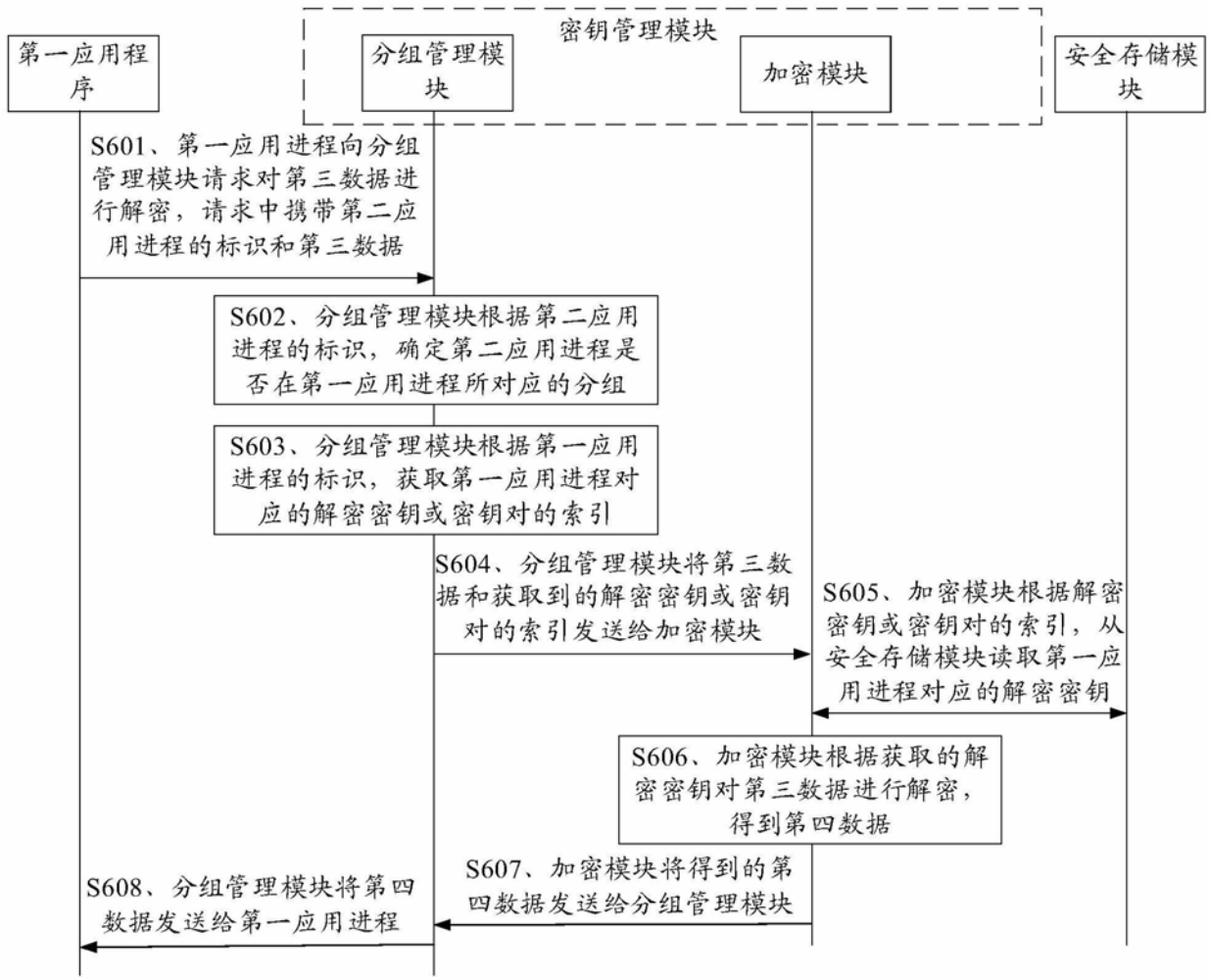

密钥管理模块
第一应用程序
分组管理模块
加密模块
安全存储模块
S601、第一应用进程向分组管理模块请求对第三数据进行解密，请求中携带第二应用进程的标识和第三数据
S602、分组管理模块根据第二应用进程的标识，确定第二应用进程是否在第一应用进程所对应的分组
S603、分组管理模块根据第一应用进程的标识，获取第一应用进程对应的解密密钥或密钥对的索引
S604、分组管理模块将第三数据和获取到的解密密钥或密钥对的索引发送给加密模块
S605、加密模块根据解密密钥或密钥对的索引，从安全存储模块读取第一应用进程对应的解密密钥
S606、加密模块根据获取的解密密钥对第三数据进行解密，得到第四数据
S607、加密模块将得到的第四数据发送给分组管理模块
S608、分组管理模块将第四数据发送给第一应用进程

图11

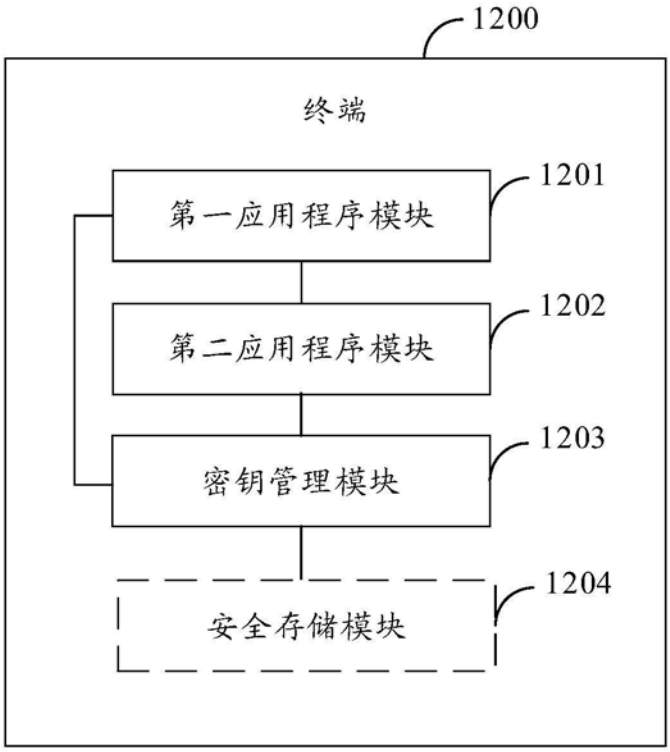

1200
终端
第一应用程序模块
1201
第二应用程序模块
1202
密钥管理模块
1203
安全存储模块
1204

图12

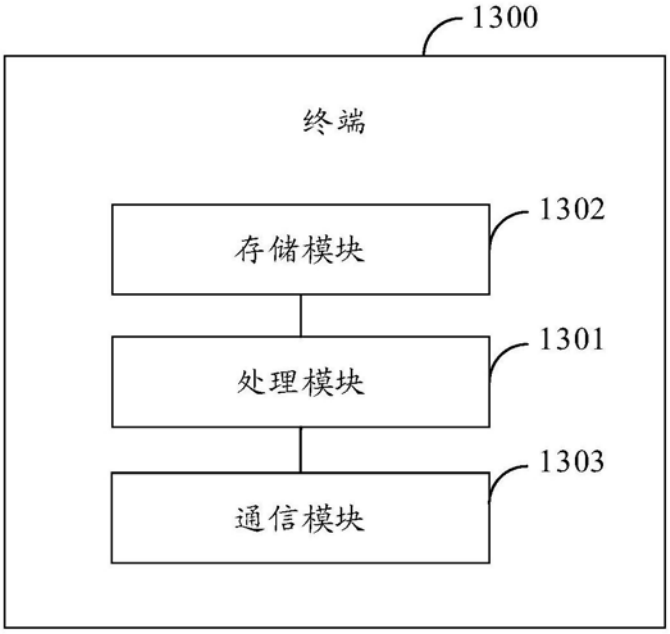

1300
终端
存储模块
1302
处理模块
1301
通信模块
1303

图13