(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117592069 A
(43)申请公布日 2024.02.23

(21)申请号 202311549247.4

(22)申请日 2023.11.17

(71)申请人 中孚安全技术有限公司
地址 250101 山东省济南市高新区经十路7000号汉峪金谷A1-5号楼24层

(72)发明人 范小震 张雷 李本学

(74)专利代理机构 济南圣达知识产权代理有限公司 37221
专利代理师 王雪

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/79(2013.01)
G06F 21/80(2013.01)

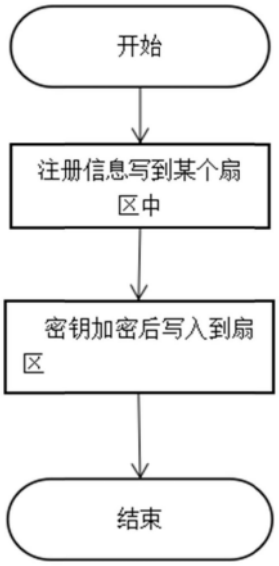
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种外接移动存储介质的加解密方法及系统

(57)摘要

本发明数据加解密技术领域,提供了一种外接移动存储介质的加解密方法及系统。该方法包括,根据移动存储介质的属性,选择保留扇区;将加密后的移动存储介质的注册信息和加密后的密钥写入保留扇区中;分别计算加密后的注册信息的校验码和加密后的密钥的校验码,并写入保留扇区中;对移动存储介质中除保留扇区的分区进行加密,分区加密成功后,将加密的分区密钥写入分区,注册成功。本发明能够对移动存储介质实现更精细化的控制,控制该移动存储介质可被哪些机器上识别;解密秘钥加密后存储在移动存储介质中,即使秘钥丢失也不会导致数据无法解密,解决了秘钥丢失导致数据无法恢复的问题。



CN 117592069 A

1.一种外接移动存储介质的加密方法,其特征在于,包括:

根据移动存储介质的属性,选择保留扇区;

将加密后的移动存储介质的注册信息和加密后的密钥写入保留扇区中;

分别计算加密后的注册信息的校验码和加密后的密钥的校验码,并写入保留扇区中;

对移动存储介质中除保留扇区的分区进行加密,分区加密成功后,注册成功。

2.根据权利要求1所述的外接移动存储介质的加密方法,其特征在于,所述移动存储介质的获取过程包括:通过UDEV事件获取移动存储介质接入系统时生成的设备节点;通过所述设备节点获取所述移动存储介质的属性。

3.根据权利要求1所述的外接移动存储介质的加密方法,其特征在于,所述属性包括分区表类型GPT或者MBR,分区表起始位置和分区大小。

4.一种外接移动存储介质的加密系统,其特征在于,包括:

扇区选择模块,其被配置为:根据移动存储介质的属性,选择保留扇区;

第一写入模块,其被配置为:将加密后的移动存储介质的注册信息和加密后的密钥写入保留扇区中;

第二写入模块,其被配置为:分别计算加密后的注册信息的校验码和加密后的密钥的校验码,并写入保留扇区中;

加密模块,其被配置为:对移动存储介质中除保留扇区的分区进行加密,分区加密成功后,注册成功。

5.一种外接移动存储介质的解密方法,其特征在于,包括:

根据移动存储介质的属性,选择移动存储介质的保留扇区;

找出保留扇区中加密后的注册信息、加密后的密钥和校验码的保存位置,在判定校验码正确时,对加密后的注册信息进行解密,得到注册信息;

将解密后的注册信息与移动存储介质接入的本机的注册信息进行比对,在注册信息一致时,读取加密的密钥,并进行解密;

通过解密后的密钥对移动存储介质的分区数据进行解密,挂载到系统上。

6.根据权利要求5所述的外接移动存储介质的解密方法,其特征在于,所述移动存储介质的获取过程包括:通过UDEV事件获取移动存储介质接入系统时生成的设备节点;通过所述设备节点获取所述移动存储介质的属性。

7.根据权利要求5所述的外接移动存储介质的解密方法,其特征在于,所述属性包括分区表类型GPT或者MBR,分区表起始位置和分区大小。

8.一种外接移动存储介质的解密系统,其特征在于,包括:

保留扇区选择模块,其被配置为:根据移动存储介质的属性,选择移动存储介质的保留扇区;

第一解密模块,其被配置为:找出保留扇区中加密后的注册信息、加密后的密钥和校验码的保存位置,在判定校验码正确时,对加密后的注册信息进行解密,得到注册信息;

比对模块,其被配置为:将解密后的注册信息与移动存储介质接入的本机的注册信息进行比对,在注册信息一致时,读取加密的密钥,并进行解密;

第二解密模块,其被配置为:通过解密后的密钥对移动存储介质的分区数据进行解密,挂载到系统上。

9.一种计算机可读移动存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1-3中任一项所述的外接移动存储介质的加密方法中的步骤,或,实现如权利要求5-7中任一项所述的外接移动存储介质的解密方法中的步骤。

10.一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现如权利要求1-3中任一项所述的外接移动存储介质的加密方法中的步骤,或,实现如权利要求5-7中任一项所述的外接移动存储介质的解密方法中的步骤。

一种外接移动存储介质的加解密方法及系统

技术领域

[0001] 本发明数据加解密技术领域,尤其涉及一种外接移动存储介质的加解密方法及系统。

背景技术

[0002] 本部分的陈述仅仅是提供了与本发明相关的背景技术信息,不必然构成在先技术。

[0003] 可移动保密介质发生丢失或者被盗的情况下,都会面临数据泄露的风险,未加密的数据可以轻松被未经授权的人访问,而加密后的数据则需要相应的密钥或密码才能解锁。

[0004] 公司的商业机密,研发成果,客户数据库等重要信息需要受到保护,以防止竞争对手获取这些敏感数据。泄漏这些信息可能导致商业竞争劣势。

[0005] 当前linux移动介质加密大多使用密钥对移动介质内的数据进行加密,密码管理复杂,如果用户丢失了密码或者密钥文件,那么数据可能会永远无法恢复。

[0006] 针对越来越复杂的环境,有时特定的移动存储介质只允许特定的机器识别和访问,目前的方案无法实现该功能。

发明内容

[0007] 为了解决上述背景技术中存在的技术问题,本发明提供一种外接移动存储介质的加解密方法及系统,本发明将注册信息(可包含用户组织信息、密级等)写入到介质中,写入成功后再将key信息加密后写入到移动存储介质中。在识别时,系统先读取移动存储介质中的注册信息,注册信息和本系统一致时,才能继续读取key信息,key信息正确才能继续对移动存储介质中的加密数据进行解密,并挂载到操作系统上。

[0008] 为了实现上述目的,本发明采用如下技术方案:

[0009] 本发明的第一个方面提供一种外接移动存储介质的加密方法。

[0010] 一种外接移动存储介质的加密方法,包括:

[0011] 根据移动存储介质的属性,选择保留扇区;

[0012] 将加密后的移动存储介质的注册信息和加密后的密钥写入保留扇区中;

[0013] 分别计算加密后的注册信息的校验码和加密后的密钥的校验码,并写入保留扇区中;

[0014] 对移动存储介质中除保留扇区的分区进行加密,分区加密成功后,注册成功。

[0015] 进一步地,所述移动存储介质的获取过程包括:通过UDEV事件获取移动存储介质接入系统时生成的设备节点;通过所述设备节点获取所述移动存储介质的属性。

[0016] 进一步地,所述属性包括分区表类型GPT或者MBR,分区表起始位置和分区大小。

[0017] 本发明的第二个方面提供一种外接移动存储介质的加密系统。

[0018] 一种外接移动存储介质的加密系统,包括:

[0019] 扇区选择模块,其被配置为:根据移动存储介质的属性,选择保留扇区;

[0020] 第一写入模块,其被配置为:将加密后的移动存储介质的注册信息和加密后的密钥写入保留扇区中;

[0021] 第二写入模块,其被配置为:分别计算加密后的注册信息的校验码和加密后的密钥的校验码,并写入保留扇区中;

[0022] 加密模块,其被配置为:对移动存储介质中除保留扇区的分区进行加密,分区加密成功后,注册成功。

[0023] 本发明的第三个方面提供一种外接移动存储介质的解密方法。

[0024] 一种外接移动存储介质的解密方法,包括:

[0025] 根据移动存储介质的属性,选择移动存储介质的保留扇区;

[0026] 找出保留扇区中加密后的注册信息、加密后的密钥和校验码的保存位置,在判定校验码正确时,对加密后的注册信息进行解密,得到注册信息;

[0027] 将解密后的注册信息与移动存储介质接入的本机的注册信息进行比对,在注册信息一致时,读取加密的密钥,并进行解密;

[0028] 通过解密后的密钥对移动存储介质的分区数据进行解密,挂载到系统上。

[0029] 进一步地,所述移动存储介质的获取过程包括:通过UDEV事件获取移动存储介质接入系统时生成的设备节点;通过所述设备节点获取所述移动存储介质的属性。

[0030] 进一步地,所述属性包括分区表类型GPT或者MBR,分区表起始位置和分区大小。

[0031] 本发明的第四个方面提供一种外接移动存储介质的解密系统。

[0032] 一种外接移动存储介质的解密系统,包括:

[0033] 保留扇区选择模块,其被配置为:根据移动存储介质的属性,选择移动存储介质的保留扇区;

[0034] 第一解密模块,其被配置为:找出保留扇区中加密后的注册信息、加密后的密钥和校验码的保存位置,在判定校验码正确时,对加密后的注册信息进行解密,得到注册信息;

[0035] 比对模块,其被配置为:将解密后的注册信息与移动存储介质接入的本机的注册信息进行比对,在注册信息一致时,读取加密的密钥,并进行解密;

[0036] 第二解密模块,其被配置为:通过解密后的密钥对移动存储介质的分区数据进行解密,挂载到系统上。

[0037] 本发明的第五个方面提供一种计算机可读移动存储介质,其上存储有计算机程序,该程序被处理器执行时实现如第一个方面所述的外接移动存储介质的加密方法中的步骤,或,实现如第三个方面所述的外接移动存储介质的解密方法中的步骤。

[0038] 本发明的第六个方面提供一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现如第一个方面所述的外接移动存储介质的加密方法中的步骤,或,实现如第三个方面所述的外接移动存储介质的解密方法中的步骤。

[0039] 与现有技术相比,本发明的有益效果是:

[0040] 本发明能够对移动存储介质实现更精细化的控制,控制该移动存储介质可被哪些机器上识别;解密秘钥加密后存储在移动存储介质中,即使秘钥丢失也不会导致数据无法解密,解决了秘钥丢失导致数据无法恢复的问题。

[0041] 本发明将注册信息(可包含用户组织信息、密级等)写入到介质中,写入成功后再将key信息加密后写入到移动存储介质中。在识别时,系统先读取移动存储介质中的注册信息,注册信息和本系统一致时,才能继续读取key信息,key信息正确才能继续对移动存储介质中的加密数据进行解密,并挂载到操作系统上,提高了移动存储介质的安全等级。

附图说明

[0042] 构成本发明的一部分的说明书附图用来提供对本发明的进一步理解,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。

[0043] 图1是本发明示出的外接移动存储介质的加密方法的流程图;

[0044] 图2是本发明示出的外接移动存储介质的解密方法的流程图。

具体实施方式

[0045] 下面结合附图与实施例对本发明作进一步说明。

[0046] 应该指出,以下详细说明都是例示性的,旨在对本发明提供进一步的说明。除非另有指明,本文使用的所有技术和科学术语具有与本发明所属技术领域的普通技术人员通常理解的相同含义。

[0047] 需要注意的是,这里所使用的术语仅是为了描述具体实施方式,而非意图限制根据本发明的示例性实施方式。如在这里所使用的,除非上下文另外明确指出,否则单数形式也意图包括复数形式,此外,还应当理解的是,当在本说明书中使用术语“包含”和/或“包括”时,其指明存在特征、步骤、操作、器件、组件和/或它们的组合。

[0048] 需要注意的是,附图中的流程图和框图示出了根据本公开的各种实施例的方法和系统的可能实现的体系架构、功能和操作。应当注意,流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分,所述模块、程序段、或代码的一部分可以包括一个或多个用于实现各个实施例中所规定的逻辑功能的可执行指令。也应当注意,在有些作为备选的实现中,方框中所标注的功能也可以按照不同于附图中所标注的顺序发生。例如,两个接连地表示的方框实际上可以基本并行地执行,或者它们有时也可以按照相反的顺序执行,这取决于所涉及的功能。同样应当注意的是,流程图和/或框图中的每个方框、以及流程图和/或框图中的方框的组合,可以使用执行规定的功能或操作的专用的基于硬件的系统来实现,或者可以使用专用硬件与计算机指令的组合来实现。

[0049] 实施例一

[0050] 本实施例提供了一种外接移动存储介质的加密方法。

[0051] 一种外接移动存储介质的加密方法,包括:

[0052] 根据移动存储介质的属性,选择保留扇区;

[0053] 将加密后的移动存储介质的注册信息和加密后的密钥写入保留扇区中;

[0054] 分别计算加密后的注册信息的校验码和加密后的密钥的校验码,并写入保留扇区中;

[0055] 对移动存储介质中除保留扇区的分区进行加密,分区加密成功后,注册成功。

[0056] 本实施例所述的加密过程发生在注册过程中,如图1所示,具体步骤包括:

[0057] 步骤1:将移动存储介质插入到系统上,在系统上会生成一个设备节点

[0058] /dev/sd*。

[0059] 步骤2:通过UDEV事件获取到该移动存储介质在系统上的设备节点。

[0060] 步骤3:通过设备节点获取到插入的移动存储介质的属性,包括分区表类型GPT或者MBR,分区表起始位置和分区大小等。

[0061] 步骤4:通过步骤3中获取到的移动存储介质属性,选择保留的扇区。选择保留扇区的原因为保留扇区不会被分区使用,避免后续在对分区进行加密时造成注册信息丢失。

[0062] 步骤5:将注册信息加密写入到保留扇区中。采用AES算法对注册信息进行加密。

[0063] 步骤6:在注册信息(包括用户识别码,密级等)写入成功后,用户将密钥写入到保留扇区中,该密钥在写入过程中会进行加密,避免泄露。采用AES算法对密钥进行加密,加密后再写入保留扇区中。这里的密钥指的是用户手动输入的密钥,是多个字符的组合,用该密钥对分区进行加密。

[0064] 步骤7:在注册信息和密钥写入完成后,生成crc校验码写入到保留扇区中。注册信息和密钥写入到保留扇区后,通过crc算法计算加密的注册信息和加密的密钥的校验码,并写到保留扇区中,供载体识别时校验使用。其中,加密的注册信息和加密的密钥可以使用crc算法生成两个校验码,在读取时,可以先判断crc校验密钥和注册信息中的至少一个有没有被篡改过,如果没有被篡改,再继续读取使用。

[0065] 步骤8:在密钥写入扇区成功后,使用cryptsetup并传入密钥对移动存储介质中的各个分区进行加密。此处的密钥是用户第6步用户手动输入的密钥,该文档中所有的密钥,指的都是同一个,该密钥的作用为对分区进行加密和解密,cryptsetup是linux下的一个分区加密工具,通过传入密钥和分区地址,可以对分区进行加解密。

[0066] 步骤9:分区加密成功后返回注册成功。

[0067] 实施例二

[0068] 本实施例提供了一种外接移动存储介质的加密系统。

[0069] 一种外接移动存储介质的加密系统,包括:

[0070] 扇区选择模块,其被配置为:根据移动存储介质的属性,选择保留扇区;

[0071] 第一写入模块,其被配置为:将加密后的移动存储介质的注册信息和加密后的密钥写入保留扇区中;

[0072] 第二写入模块,其被配置为:分别计算加密后的注册信息的校验码和加密后的密钥的校验码,并写入保留扇区中;

[0073] 加密模块,其被配置为:对移动存储介质中除保留扇区的分区进行加密,分区加密成功后,注册成功。

[0074] 此处需要说明的是,上述扇区选择模块、第一写入模块、第二写入模块和加密模块与实施例一中的步骤所实现的示例和应用场景相同,但不限于上述实施例一所公开的内容。需要说明的是,上述模块作为系统的一部分可以在诸如一组计算机可执行指令的计算机系统中执行。

[0075] 实施例三

[0076] 本实施例提供了一种外接移动存储介质的解密方法。

[0077] 一种外接移动存储介质的解密方法,包括:

[0078] 根据移动存储介质的属性,选择移动存储介质的保留扇区;

[0079] 找出保留扇区中加密后的注册信息、加密后的密钥和校验码的保存位置,在判定校验码正确时,对加密后的注册信息进行解密,得到注册信息;

[0080] 将解密后的注册信息与移动存储介质接入的本机的注册信息进行比对,在注册信息一致时,读取加密的密钥,并进行解密;

[0081] 通过解密后的密钥对移动存储介质的分区数据进行解密,挂载到系统上。

[0082] 本实施例所述的加密过程发生在载体识别过程中,如图2所示,具体步骤包括:

[0083] 步骤1:将移动存储介质插入到系统上,在系统上会生成一个设备节点

[0084] /dev/sd*。

[0085] 步骤2:通过系统的UDEV事件获取到移动存储介质在系统上的设备节点。

[0086] 步骤3:通过设备节点获取到插入的移动存储介质的属性,包括分区表类型,分区表起始位置和分区大小等。

[0087] 步骤4:查找移动存储介质的保留扇区,并找到注册信息的保存位置,读取注册信息,并解密。读取移动存储介质的保留扇区,找到注册信息,密钥,crc校验码所在的位置,首先通过crc校验数据正确,再通过使用AES算法对注册信息部分进行解密。crc校验码有两个,一个是加密的注册信息的校验码和加密的密钥的校验码。

[0088] 步骤5:在系统中读取本机的注册信息,与步骤4获取到的注册信息,密级(注册信息包括密级和用户识别码)进行对比。

[0089] 步骤6:若步骤5一致,则继续读取密钥数据,不一致则直接返回,拒绝识别。

[0090] 步骤7:读取到密钥后,对密钥解密。

[0091] 步骤8:通过密钥对移动存储介质内的分区数据进行解密并挂载到系统上,完成整个识别过程。在获取到密钥后,使用cryptset指令并传入密钥对各个分区进行解密,并挂载到操作系统上。

[0092] 实施例四

[0093] 本实施例提供了一种外接移动存储介质的解密系统。

[0094] 一种外接移动存储介质的解密系统,包括:

[0095] 保留扇区选择模块,其被配置为:根据移动存储介质的属性,选择移动存储介质的保留扇区;

[0096] 第一解密模块,其被配置为:找出保留扇区中加密后的注册信息、加密后的密钥和校验码的保存位置,在判定校验码正确时,对加密后的注册信息进行解密,得到注册信息;

[0097] 比对模块,其被配置为:将解密后的注册信息与移动存储介质接入的本机的注册信息进行比对,在注册信息一致时,读取加密的密钥,并进行解密;

[0098] 第二解密模块,其被配置为:通过解密后的密钥对移动存储介质的分区数据进行解密,挂载到系统上。

[0099] 此处需要说明的是,上述保留扇区选择模块、第一解密模块、比对模块和第二解密模块与实施例三中的步骤所实现的示例和应用场景相同,但不限于上述实施例三所公开的内容。需要说明的是,上述模块作为系统的一部分可以在诸如一组计算机可执行指令的计算机系统中执行。

[0100] 实施例五

[0101] 本实施例提供了一种计算机可读移动存储介质,其上存储有计算机程序,该程序

被处理器执行时实现如实施例一所述的外接移动存储介质的加密方法中的步骤,或,实现如实施例三所述的外接移动存储介质的解密方法中的步骤。

[0102] 实施例六

[0103] 本实施例提供了一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现如实施例一所述的外接移动存储介质的加密方法中的步骤,或,实现如实施例三所述的外接移动存储介质的解密方法中的步骤。

[0104] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用硬件实施例、软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用移动存储介质(包括但不限于磁盘存储器和光学存储器等)上实施的计算机程序产品的形式。

[0105] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0106] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0107] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0108] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的程序可存储于一计算机可读取移动存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,所述的移动存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory,ROM)或随机存储记忆体(Random AccessMemory,RAM)等。

[0109] 以上所述仅为本发明的优选实施例而已,并不用于限制本发明,对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本发明的保护范围之内。

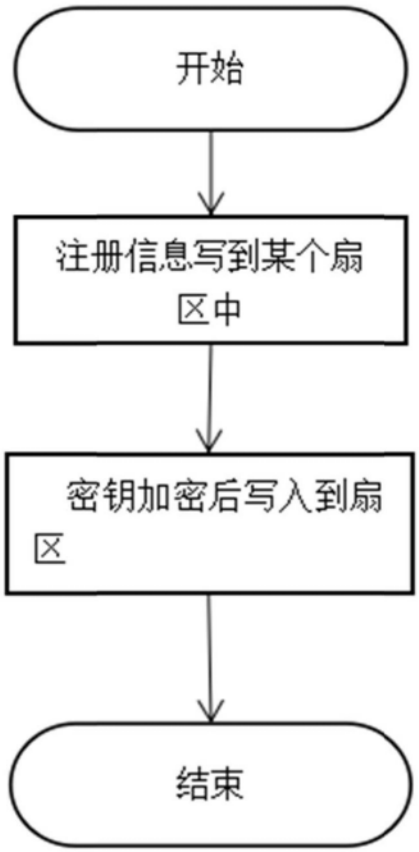


图1

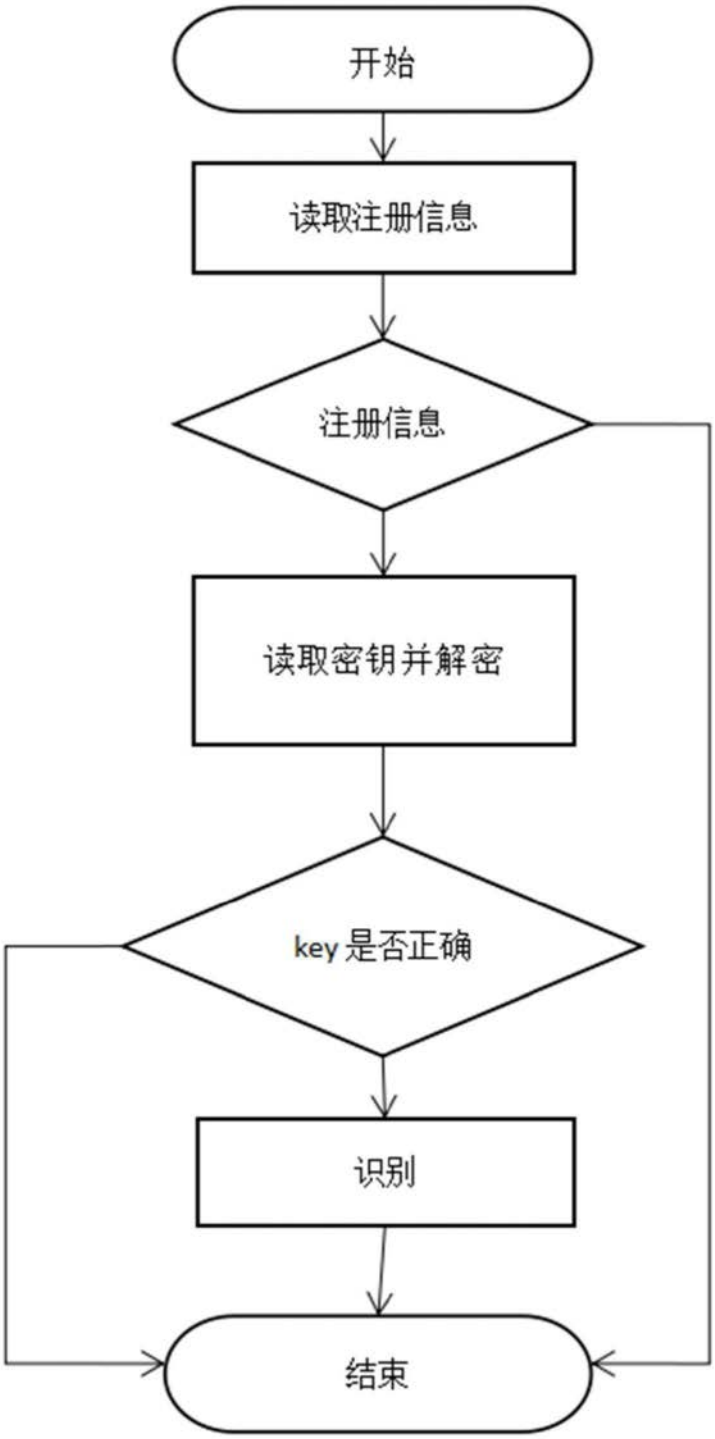


图2