(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
2019 年 12 月 19 日 (19.12.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/237304 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2018/091282

(22) 国际申请日: 2018 年 6 月 14 日 (14.06.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华 为 技 术 有 限 公 司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 潘 时 林 (**PAN, Shilin**); 中 国 广 东 省 深 圳 市 龙 岗 区 坂 田 华 为 总 部 办 公 楼, Guangdong 518129 (CN)。

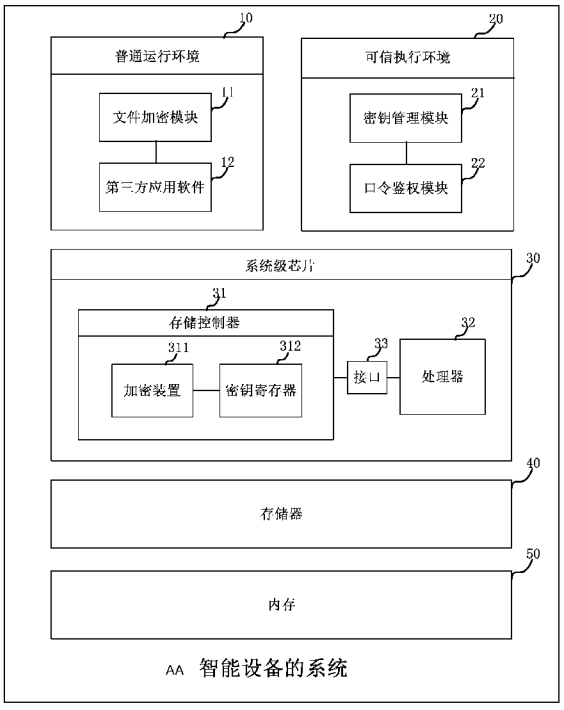
(74) 代理人: 北京弘权知识产权代理事务所（普通合伙）(**CHINABLE IP**); 中国北京市朝阳区安定路35号六层35-10-2内620室, Beijing 100029 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

WO 2019/237304 A1

(54) **Title:** KEY PROCESSING METHOD AND DEVICE

(54) 发明名称: 一种密钥处理方法及装置



10 Normal running environment
11 File encryption module
12 Third party application software
20 Trusted execution environment
21 Key management module
22 Password authentication module
30 System level chip
31 Storage controller
311 Encryption device
312 Key register
32 Processor
33 Interface
40 Memory
50 Internal memory
AA System of a smart device

图 1

(57) **Abstract:** Disclosed by the embodiments of the present application are a key processing method and device, the method comprising: in a trusted execution environment, receiving an initial key sent by a file encryption module which is in a normal running environment; decrypting the initial key in the trusted execution environment to obtain a file key; storing the file key in a key register of a storage controller in the trusted execution environment, the file encryption module which is in the normal running environment being prohibited from accessing the key register; obtaining a key index of the file key within the key register in the trusted execution environment, the

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：
— 包括国际检索报告(条约第21条(3))。

key index being used to indicate a storage location of the file key in the key register; and in the trusted execution environment, sending the key index to the file encryption module in the normal running environment, wherein the file encryption module which is in the normal running environment is prohibited from accessing the trusted execution environment and the key register, thus a file key is secure in a smart device during the processes of generating the file key, writing the file and reading the file.

(57) 摘要：本申请实施例公开了一种密钥处理方法及装置，该方法包括：在可信执行环境中接收普通运行环境中的文件加密模块发送的初始密钥；在可信执行环境中对初始密钥进行解密处理得到文件密钥；在可信执行环境中将文件密钥存储至存储控制器的密钥寄存器中，普通运行环境中的文件加密模块被禁止访问密钥寄存器；在可信执行环境中获取密钥寄存器中文件密钥的密钥索引，密钥索引用于指示文件密钥在密钥寄存器中的存储位置；在可信执行环境中将密钥索引发送给普通运行环境中的文件加密模块。其中，普通运行环境内的文件加密模块被禁止访问可信执行环境和密钥寄存器，所以在生成文件密钥、写入文件和读取文件的过程中，文件密钥在智能设备内均是安全的。

一种密钥处理方法及装置

技术领域

本申请实施例涉及密钥处理技术领域，更具体的说，涉及密钥处理方法及装置。

背景技术

目前，在智能设备写入文件时，需要使用文件密钥对文件进行加密，再将加密后的文件存储至存储器内，以保证文件在智能设备内的安全性。在智能设备读取文件时，需要使用文件密钥对存储器中加密后的文件进行解密以得到文件。由于文件密钥的安全与否直接影响到智能设备内文件的安全性，所以文件密钥在智能设备中的安全性更加重要，下面简要介绍一下现有技术中文件密钥的生成方法。

当前智能设备的系统主要包括普通运行环境和可信执行环境。在智能设备启动以后，可信执行环境的模块会对文件密钥的密文进行解密处理得到文件密钥，并将文件密钥发送给普通运行环境内的文件加密模块；然后，普通运行环境内的文件加密模块将文件密钥存储至内存中备用，以便于在智能设备需要写入文件或读取文件时，普通运行环境内的文件加密模块可以使用文件密钥对文件进行加密处理或解密处理。

普通运行环境内运行着很多用户安装的第三方应用软件，如果黑客利用这些第三方应用软件非法破解普通运行环境内的文件加密模块，那么便可通过文件加密模块的接口窃取内存中的文件密钥，进而通过该文件密钥解密智能设备内的文件。因此，现有技术提供的技术方案无法保证文件密钥在智能设备内的安全性。

发明内容

本申请实施例提供一种密钥处理方法及装置，以保证文件密钥在智能设备内的安全性。

本申请实施例是这样实现的：

第一方面，本申请实施例提供了一种密钥处理方法，该方法包括：在可信执行环境中接收普通运行环境中的文件加密模块发送的初始密钥；在可信执行环境中对初始密钥进行解密处理得到文件密钥，文件密钥用于加密文件；在可信执行环境中将文件密钥存储至存储控制器的密钥寄存器中，普通运行环境中的文件加密模块被禁止访问密钥寄存器；在可信执行环境中获取密钥寄存器中文件密钥的密钥索引，密钥索引用于指示文件密钥在密钥寄存器中的存储位置；在可信执行环境中将密钥索引发送给普通运行环境中的文件加密模块。

在第一方面中，普通运行环境内的文件加密模块被禁止访问可信执行环境内的模块或信息，在可信执行环境中生成文件密钥的过程中，普通运行环境内的文件加密模块无法窃取可信执行环境中生成的文件密钥，所以生成文件密钥的过程是安全的。而且，在可信执行环境中生成文件密钥以后，可信执行环境中将文件密钥存储至存储控制器的密钥寄存器中，由于普通运行环境中的文件加密模块被禁止访问密钥寄存器，普通运行环境中的文件加密模块无法窃取存储控制器的密钥寄存器中的文件密钥，所

以文件密钥的存储环境也是安全的。另外，可信执行环境中仅将文件密钥的密钥索引发送给普通运行环境中的文件加密模块，以使普通运行环境中的第三方应用软件或其他模块需要写入文件或读取文件的情况下，文件加密模块可以与存储控制器相互配合，文件加密模块将密钥索引发送给存储控制器，以使存储控制器实现对文件的加密或解密，进而实现对文件的写入操作或读取操作。

在一种可能的实现方式中，在可信执行环境中对初始密钥进行解密处理得到文件密钥包括：在可信执行环境中利用第一派生密钥对初始密钥进行解密得到文件密钥。

在一种可能的实现方式中，在可信执行环境中利用第一派生密钥对初始密钥进行解密得到文件密钥之前，方法还包括：在可信执行环境中获取个人识别密码的消息认证码；在可信执行环境中获取私有密钥；在可信执行环境中获取第一加密因子；在可信执行环境中利用私有密钥和第一加密因子对消息认证码进行加密得到第一派生密钥。

在一种可能的实现方式中，在可信执行环境中利用第一派生密钥对初始密钥进行解密得到文件密钥之前，方法还包括：在可信执行环境中获取第一加密因子；在可信执行环境中获取私有密钥；在可信执行环境中利用私有密钥对第一加密因子进行加密得到第一派生密钥。

在一种可能的实现方式中，在可信执行环境中将密钥索引发送给普通运行环境中的文件加密模块以后，方法还包括：在普通运行环境中的文件加密模块接收文件的处理指令；在普通运行环境中的文件加密模块获取文件的密钥类型；在普通运行环境中的文件加密模块获取密钥类型对应的密钥索引；在普通运行环境中的文件加密模块获取初始向量，初始向量用于与文件密钥联合加密文件；在普通运行环境中的文件加密模块根据密钥索引和初始向量生成基于文件的处理请求；在普通运行环境中的文件加密模块向存储控制器发送处理请求。

在一种可能的实现方式中，在普通运行环境中文件加密模块向存储控制器发送处理请求以后，方法还包括：存储控制器接收普通运行环境中的文件加密模块发送的处理请求；存储控制器获取密钥寄存器中的密钥索引对应的文件密钥；存储控制器利用文件密钥和初始向量对文件进行加密得到文件的密文，并将文件的密文存储到存储器中；或者，存储控制器获取存储器中的文件的密文，利用文件密钥和初始向量对文件的密文进行解密得到文件。

其中，由于普通运行环境中的模块或软件被禁止访问密钥寄存器，在写入文件或读取文件的过程中，普通运行环境中的模块或软件无法窃取到密钥寄存器中存储的文件密钥，而且普通运行环境中的模块或软件也无法窃取到存储控制器在加密文件或解密文件的过程中所使用的文件密钥，因此，本申请实施例可以保证在写入文件或读取文件的过程中文件密钥是安全的。

在一种可能的实现方式中，在普通运行环境中获取初始向量包括：在普通运行环境中的文件加密模块获取存储器中初始向量的密文；在普通运行环境中的文件加密模块获取元数据密钥；在普通运行环境中的文件加密模块利用元数据密钥对初始向量的密文进行解密得到初始向量。

在一种可能的实现方式中，在普通运行环境中的文件加密模块获取初始向量后，方法还包括：在所述普通运行环境中的所述文件加密模块获取元数据密钥；在普通运

行环境中的文件加密模块利用元数据密钥对初始向量进行加密得到初始向量的密文；在普通运行环境中的文件加密模块将初始向量的密文存储至存储器中。

在一种可能的实现方式中，方法还包括：在可信执行环境中对初始密钥进行解密处理得到元数据密钥；在可信执行环境中将元数据密钥发送给普通运行环境中的文件加密模块。

在一种可能的实现方式中，在可信执行环境中对初始密钥进行解密处理得到元数据密钥包括：在可信执行环境中利用第二派生密钥对初始密钥进行解密得到元数据密钥。

在一种可能的实现方式中，在可信执行环境中利用第二派生密钥对初始密钥进行解密得到元数据密钥之前，方法还包括：在可信执行环境中获取个人识别密码的消息认证码；在可信执行环境中获取私有密钥；在可信执行环境中获取第二加密因子；在可信执行环境中利用私有密钥和第二加密因子对消息认证码进行加密得到第二派生密钥。

在一种可能的实现方式中，在可信执行环境中利用第二派生密钥对初始密钥进行解密得到元数据密钥之前，方法还包括：在可信执行环境中获取第二加密因子；在可信执行环境中获取私有密钥；在可信执行环境中利用私有密钥对第二加密因子进行加密得到第二派生密钥。

第二方面，本申请实施例提供了一种密钥处理方法，该方法包括：存储控制器接收普通运行环境中的文件加密模块发送的基于文件的处理请求，处理请求包括密钥索引，密钥索引用于指示文件密钥存储控制器的密钥寄存器中的存储位置；存储控制器获取密钥寄存器中的密钥索引对应的文件密钥，普通运行环境中的文件加密模块被禁止访问密钥寄存器；存储控制器利用文件密钥对文件进行加密得到文件的密文，并将文件的密文存储到存储器中；或者，存储控制器获取存储器中的文件的密文，利用文件密钥对文件的密文进行解密得到文件。

在第二方面中，由于普通运行环境中的模块或软件被禁止访问密钥寄存器，在写入文件或读取文件的过程中，普通运行环境中的模块或软件无法窃取到密钥寄存器中存储的文件密钥，而且普通运行环境中的模块或软件也无法窃取到存储控制器在加密文件或解密文件的过程中所使用的文件密钥，因此，本申请实施例可以保证在写入文件或读取文件的过程中文件密钥是安全的。

在一种可能的实现方式中，处理请求还包括初始向量；存储控制器利用文件密钥对文件进行加密得到文件的密文包括：存储控制器利用文件密钥和初始向量对文件进行加密得到文件的密文。

在一种可能的实现方式中，处理请求还包括初始向量；存储控制器利用文件密钥对文件的密文进行解密得到文件包括：存储控制器利用文件密钥和初始向量对文件的密文进行解密得到文件。

第三方面，本申请实施例提供了一种密钥处理装置，该装置包括处理器和接口，接口与存储控制器和处理器连接；处理器，用于运行软件指令以产生可信执行环境和普通运行环境并在普通运行环境中实现文件加密模块的功能，并进一步执行以下操作：在可信执行环境中接收普通运行环境中的文件加密模块发送的初始密钥；在可信执行

环境中对初始密钥进行解密处理得到文件密钥，文件密钥用于加密文件；在可信执行环境中通过接口将文件密钥存储至存储控制器的密钥寄存器中，普通运行环境中的文件加密模块被禁止访问密钥寄存器；在可信执行环境中通过接口获取密钥寄存器中文件密钥的密钥索引，密钥索引用于指示文件密钥在密钥寄存器中的存储位置；在可信执行环境中将密钥索引发送给普通运行环境中的文件加密模块。

在第三方面中，普通运行环境内的文件加密模块被禁止访问可信执行环境内的模块或信息，在可信执行环境中生成文件密钥的过程中，普通运行环境内的文件加密模块无法窃取可信执行环境中生成的文件密钥，所以生成文件密钥的过程是安全的。而且，在可信执行环境中生成文件密钥以后，可信执行环境中将文件密钥存储至存储控制器的密钥寄存器中，由于普通运行环境中的文件加密模块被禁止访问密钥寄存器，普通运行环境中的文件加密模块无法窃取存储控制器的密钥寄存器中的文件密钥，所以文件密钥的存储环境也是安全的。另外，可信执行环境中仅将文件密钥的密钥索引发送给普通运行环境中的文件加密模块，以使普通运行环境中的第三方应用软件或其他模块需要写入文件或读取文件的情况下，文件加密模块可以与存储控制器相互配合，文件加密模块将密钥索引发送给存储控制器，以使存储控制器实现对文件的加密或解密，进而实现对文件的写入操作或读取操作。

在一种可能的实现方式中，处理器，具体用于在可信执行环境中利用第一派生密钥对初始密钥进行解密得到文件密钥。

在一种可能的实现方式中，处理器，还用于在可信执行环境中获取个人识别密码的消息认证码；在可信执行环境中获取私有密钥；在可信执行环境中获取第一加密因子；在可信执行环境中利用私有密钥和第一加密因子对消息认证码进行加密得到第一派生密钥。

在一种可能的实现方式中，处理器，还用于在可信执行环境中获取第一加密因子；在可信执行环境中获取私有密钥；在可信执行环境中利用私有密钥对第一加密因子进行加密得到第一派生密钥。

在一种可能的实现方式中，处理器，还用于在普通运行环境中实现文件加密模块的如下功能：接收文件的处理指令；获取文件的密钥类型；获取密钥类型对应的密钥索引；获取初始向量，初始向量用于与文件密钥联合加密文件；根据密钥索引和初始向量生成基于文件的处理请求；向存储控制器发送处理请求。

在一种可能的实现方式中，装置还包括存储控制器，存储控制器包括加密装置和密钥寄存器；存储控制器的加密装置，用于接收普通运行环境中的文件加密模块发送的处理请求；获取密钥寄存器中的密钥索引对应的文件密钥；利用文件密钥和初始向量对文件进行加密得到文件的密文，并将文件的密文存储到存储器中；或者，获取存储器中的文件的密文，利用文件密钥和初始向量对文件的密文进行解密得到文件。

在一种可能的实现方式中，处理器，还用于在普通运行环境中实现文件加密模块的如下功能：获取存储器中初始向量的密文；获取元数据密钥；利用元数据密钥对初始向量的密文进行解密得到初始向量。

在一种可能的实现方式中，处理器，还用于在普通运行环境中实现文件加密模块的如下功能：获取元数据密钥；利用元数据密钥对初始向量进行加密得到初始向量的

密文；将初始向量的密文存储至存储器中。

在一种可能的实现方式中，处理器，还用于在可信执行环境中对初始密钥进行解密处理得到元数据密钥；在可信执行环境中将元数据密钥发送给普通运行环境中的文件加密模块。

在一种可能的实现方式中，处理器，具体用于在可信执行环境中利用第二派生密钥对初始密钥进行解密得到元数据密钥。

在一种可能的实现方式中，处理器，还用于在可信执行环境中获取个人识别密码的消息认证码；在可信执行环境中获取私有密钥；在可信执行环境中获取第二加密因子；在可信执行环境中利用私有密钥和第二加密因子对消息认证码进行加密得到第二派生密钥。

在一种可能的实现方式中，处理器，还用于在可信执行环境中获取第二加密因子；在可信执行环境中获取私有密钥；在可信执行环境中利用私有密钥对第二加密因子进行加密得到第二派生密钥。

第四方面，本申请实施例提供了一种存储控制器，包括加密装置和密钥寄存器；密钥寄存器用于存储文件密钥；加密装置，用于接收普通运行环境中的文件加密模块发送的基于文件的处理请求，处理请求包括密钥索引，密钥索引用于指示文件密钥在密钥寄存器中的存储位置；获取密钥寄存器中的密钥索引对应的文件密钥，普通运行环境中的文件加密模块被禁止访问密钥寄存器；利用文件密钥对文件进行加密得到文件的密文，并将文件的密文存储到存储器中；或者，获取存储器中的文件的密文，利用文件密钥对文件的密文进行解密得到文件。

在第四方面中，由于普通运行环境中的模块或软件被禁止访问密钥寄存器，在写入文件或读取文件的过程中，普通运行环境中的模块或软件无法窃取到密钥寄存器中存储的文件密钥，而且普通运行环境中的模块或软件也无法窃取到加密装置在加密文件或解密文件的过程中所使用的文件密钥，因此，本申请实施例可以保证在写入文件或读取文件的过程中文件密钥是安全的。

在一种可能的实现方式中，处理请求还包括初始向量；加密装置，具体用于利用文件密钥和初始向量对文件进行加密得到文件的密文。

在一种可能的实现方式中，处理请求还包括初始向量；加密装置，具体用于利用文件密钥和初始向量对文件的密文进行解密得到文件。

第五方面，本申请实施例提供了一种密钥处理装置，包括：接收模块，用于在可信执行环境中接收普通运行环境中的文件加密模块发送的初始密钥；第一解密模块，用于在可信执行环境中对初始密钥进行解密处理得到文件密钥，文件密钥用于加密文件；存储模块，用于在可信执行环境中将文件密钥存储至存储控制器的密钥寄存器中，普通运行环境中的文件加密模块被禁止访问密钥寄存器；获取模块，用于在可信执行环境中获取密钥寄存器中文件密钥的密钥索引，密钥索引用于指示文件密钥在密钥寄存器中的存储位置；发送模块，用于在可信执行环境中将密钥索引发送给普通运行环境中的文件加密模块。

在第五方面中，普通运行环境内的文件加密模块被禁止访问可信执行环境内的模块或信息，在可信执行环境中生成文件密钥的过程中，普通运行环境内的文件加密模

块无法窃取可信执行环境中生成的文件密钥，所以生成文件密钥的过程是安全的。而且，在可信执行环境中生成文件密钥以后，可信执行环境中将文件密钥存储至存储控制器的密钥寄存器中，由于普通运行环境中的文件加密模块被禁止访问密钥寄存器，普通运行环境中的文件加密模块无法窃取存储控制器的密钥寄存器中的文件密钥，所以文件密钥的存储环境也是安全的。另外，可信执行环境中仅将文件密钥的密钥索引发送给普通运行环境中的文件加密模块，以使普通运行环境中的第三方应用软件或其他模块需要写入文件或读取文件的情况下，文件加密模块可以与存储控制器相互配合，文件加密模块将密钥索引发送给存储控制器，以使存储控制器实现对文件的加密或解密，进而实现对文件的写入操作或读取操作。

在一种可能的实现方式中，第一解密模块，具体用于在可信执行环境中利用第一派生密钥对初始密钥进行解密得到文件密钥。

在一种可能的实现方式中，装置还包括第一加密模块；第一加密模块，用于在可信执行环境中获取个人识别密码的消息认证码；在可信执行环境中获取私有密钥；在可信执行环境中获取第一加密因子；在可信执行环境中利用私有密钥和第一加密因子对消息认证码进行加密得到第一派生密钥。

在一种可能的实现方式中，装置还包括第二加密模块；第二加密模块，用于在可信执行环境中获取第一加密因子；在可信执行环境中获取私有密钥；在可信执行环境中利用私有密钥对第一加密因子进行加密得到第一派生密钥。

在一种可能的实现方式中，装置还包括文件加密模块；文件加密模块，用于在普通运行环境中接收文件的处理指令；在普通运行环境中获取文件的密钥类型；在普通运行环境中获取密钥类型对应的密钥索引；在普通运行环境中获取初始向量；在普通运行环境中根据密钥索引和初始向量生成基于文件的处理请求；在普通运行环境中向存储控制器发送处理请求。

在一种可能的实现方式中，文件加密模块，具体用于在普通运行环境中获取存储器中初始向量的密文；在普通运行环境中获取元数据密钥；在普通运行环境中利用元数据密钥对初始向量的密文进行解密得到初始向量。

在一种可能的实现方式中，文件加密模块，还用于在所述普通运行环境中获取元数据密钥；在普通运行环境中利用元数据密钥对初始向量进行加密得到初始向量的密文；在普通运行环境中将初始向量的密文存储至存储器中。

在一种可能的实现方式中，装置还包括第二解密模块：第二解密模块，用于在可信执行环境中对初始密钥进行解密处理得到元数据密钥；发送模块，还用于在可信执行环境中将元数据密钥发送给普通运行环境中的文件加密模块。

在一种可能的实现方式中，第二解密模块，具体用于在可信执行环境中利用第二派生密钥对初始密钥进行解密得到元数据密钥。

在一种可能的实现方式中，装置还包括第三加密模块；第三加密模块，用于在可信执行环境中获取个人识别密码的消息认证码；在可信执行环境中获取私有密钥；在可信执行环境中获取第二加密因子；在可信执行环境中利用私有密钥和第二加密因子对消息认证码进行加密得到第二派生密钥。

在一种可能的实现方式中，装置还包括第四加密模块；第四加密模块，用于在可

信执行环境中获取第二加密因子；在可信执行环境中获取私有密钥；在可信执行环境中利用私有密钥对第二加密因子进行加密得到第二派生密钥。

第六方面，本申请实施例提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机或处理器上运行时，使得计算机或处理器执行上述第一方面或第一方面的任一种可能实现方式中的方法。

第七方面，本申请实施例提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机或处理器上运行时，使得计算机或处理器执行上述第二方面或第二方面的任一种可能实现方式中的方法。

第八方面，本申请实施例提供了一种包含指令的计算机程序产品，当其在计算机或处理器上运行时，使得计算机或处理器执行上述第一方面或第一方面的任一种可能实现方式中的方法。

第九方面，本申请实施例提供了一种包含指令的计算机程序产品，当其在计算机或处理器上运行时，使得计算机或处理器执行上述第二方面或第二方面的任一种可能实现方式中的方法。

附图说明

图 1 所示的为本申请实施例提供的智能设备的系统的示意图；

图 2A 所示的为本申请实施例提供的智能设备生成文件密钥的示意图；

图 2B 所示的为一种生成文件密钥的示意图；

图 2C 所示的为另一种生成文件密钥的示意图；

图 2D 所示的为一种生成元数据密钥的示意图；

图 2E 所示的为另一种生成元数据密钥的示意图；

图 3A 所示的为本申请实施例提供的智能设备写入文件的示意图；

图 3B 所示的为一种生成写入请求的示意图；

图 3C 所示的为一种加密文件的示意图；

图 4A 所示的为本申请实施例提供的智能设备读取文件的示意图；

图 4B 所示的为一种生成读取请求的示意图；

图 4C 所示的为一种解密文件的示意图；

图 5 所示的为本申请实施例提供的密钥处理方法的信令交互图；

图 6 所示的为本申请实施例提供的密钥处理方法的信令交互图；

图 7 所示的为本申请实施例提供的密钥处理方法的信令交互图；

图 8 所示的为本申请实施例提供的一种密钥处理装置的示意图。

具体实施方式

请参见图 1 所示，图 1 所示的为本申请实施例提供的智能设备的系统的示意图。该智能设备的系统包括普通运行环境 10、可信执行环境 20、系统级芯片 30、存储器 40 和内存 50。其中，文件加密模块 11 和第三方应用软件 12 可在普通运行环境 10 内运行，密钥管理模块 21 和口令鉴权模块 22 可在可信执行环境 20 内运行，系统级芯片 30 包括存储控制器 31、处理器 32 和接口 33，处理器 32 通过接口 33 与存储控制器 31 相连接，接口 33 可以是用于连接处理器 32 和存储控制器 31 的总线或其他连接器件，

存储控制器 31 包括加密装置 311 和密钥寄存器 312。例如，存储器 40 用于永久存储数据，如果关闭电源或断电，存储器 40 内的数据不会丢失，例如，存储器 40 可以为非易失性存储器（non-volatile memory，NVM）。例如，内存 50 用于暂时存放数据，如果关闭电源或断电，内存 50 内的数据会丢失，例如，内存 50 可以为易失性存储器（random access memory，RAM）。而且，存储器 40 的数量可以为 1 个或多个，本申请实施例可以使用 1 个或多个存储器 40 存储数据。

在图 1 所示的实施例中，普通运行环境 10 内的模块或软件被禁止访问可信执行环境 20 内的模块或信息，普通运行环境 10 内的文件加密模块 11 可将初始密钥发送给可信执行环境 20 内的密钥管理模块 21；而且，普通运行环境 10 中的模块或软件被禁止访问存储控制器 31 中的密钥寄存器 312，普通运行环境 10 内的文件加密模块 11 可将处理请求发送给存储控制器 31 的加密装置 311，其中，处理请求可以为写入请求和读取请求。

在图 1 所示的实施例中，需要注意的是，本申请实施例中的处理器 32 可以是一种集成电路或其部分，具有信号的处理能力。上述的处理器 32 可以是通用处理器、数字信号处理器（digital signal processor，DSP）、人工智能处理器、微控制器或微处理器，能够读取并运行存储器 40 中的软件指令实现相关功能。当然，处理器 32 也可以读取并运行其他的存储器中的软件指令实现相关功能，并不局限于存储器 40。

在图 1 所示的实施例中，处理器 32 用于运行软件指令以产生普通运行环境 10 和可信执行环境 20，并在普通运行环境 10 中实现文件加密模块 11 的功能，以及在可信执行环境 20 中实现密钥管理模块 21 的功能。

存储控制器 31 可以是一个包括逻辑电路、晶体管或其他硬件的装置，用于实现对存储器 40 的访问和控制，并可以进一步实现对内存 40 的访问和控制。其中的加密装置 311 可以是硬件加速装置或是运行软件的处理器使得该处理器通过运行软件来实现加密装置 311 的相关功能。密钥寄存器 312 则是用于实现数据临时存储的寄存器单元。

请参见图 2A 所示，图 2A 所示的为本申请实施例提供的智能设备生成文件密钥的示意图。下面介绍本申请实施例生成文件密钥的过程：首先，普通运行环境 10 中的文件加密模块 11 将初始密钥发送给可信执行环境 20 中的密钥管理模块 21，其中，初始密钥可以为预先生成的随机数；然后，密钥管理模块 21 对初始密钥进行解密处理得到文件密钥；其次，密钥管理模块 21 将该文件密钥存储至系统级芯片 30 的存储控制器 31 的密钥寄存器 312 中，普通运行环境 10 中的文件加密模块 11 被禁止访问存储控制器 31 中的密钥寄存器 312；再次，密钥管理模块 21 获取密钥寄存器 312 中文件密钥的密钥索引，该密钥索引用于指示文件密钥在密钥寄存器 312 中的存储位置；再次，密钥管理模块 21 将密钥索引发送给文件加密模块 11；最后，文件加密模块 11 将该文件密钥对应的密钥索引存储至内存 50 中。

在图 2A 所示的实施例中，普通运行环境 10 内的模块或软件被禁止访问可信执行环境 20 内的模块或信息，在密钥管理模块 21 生成文件密钥的过程中，普通运行环境 10 内的模块或软件无法窃取密钥管理模块 21 生成的文件密钥，所以生成文件密钥的过程是安全的。而且，在密钥管理模块 21 生成文件密钥以后，密钥管理模块 21 将文件密钥存储至存储控制器 31 的密钥寄存器 312 中，由于普通运行环境 10 中的模块或

软件被禁止访问存储控制器 31 中的密钥寄存器 312，普通运行环境 10 中的模块或软件无法窃取存储控制器 31 的密钥寄存器 312 中的文件密钥，所以文件密钥的存储环境也是安全的。另外，可信执行环境 20 中的密钥管理模块 21 仅将文件密钥的密钥索引发送给普通运行环境 10 中的文件加密模块 11，以使普通运行环境 10 中的第三方应用软件 12 或其他模块需要写入文件或读取文件的情况下，文件加密模块 11 可以与存储控制器 31 相互配合，文件加密模块 11 将密钥索引发送给存储控制器 31，以使存储控制器 31 实现对文件的加密或解密，进而实现对文件的写入操作或读取操作。

在图 2A 所示的实施例中，在普通运行环境 10 中的文件加密模块 11 将初始密钥发送给可信执行环境 20 中的密钥管理模块 21 以前，普通运行环境 10 中的文件加密模块 11 便已经与可信执行环境 20 中的密钥管理模块 21 协商好当前生成的文件密钥的密钥类型，所以在文件加密模块 11 将该文件密钥对应的密钥索引存储至内存 50 中以后，文件加密模块 11 可以建立文件的密钥索引与密钥类型的映射关系，并将密钥索引与密钥类型的映射关系存储在内存 50 中。

其中，文件的密钥类型指的是加密不同文件的文件密钥。例如，文件的密钥类型可以为用户文件密钥，用户文件密钥用于加密用户文件；又如，文件的密钥类型还可以为系统文件密钥，系统文件密钥用于加密系统文件。

请参见表 1 所示，表 1 所示的为一示例中文件加密模块 11 在内存 50 中存储的密钥索引与密钥类型的映射关系表。

密钥索引	密钥类型
Key1	用户文件密钥
Key2	系统文件密钥
…	…

表 1

请参见表 2 所示，表 2 所示的为一示例中密钥寄存器 312 存储的密钥索引与文件密钥的映射关系表。

密钥索引	文件密钥
Key1	11111111
Key2	22222222
…	…

表 2

在图 2A 所示的实施例中，对于智能设备的系统首次启动或恢复出厂设置的技术场景而言，在普通运行环境 10 中的文件加密模块 11 将初始密钥发送给可信执行环境 20 中的密钥管理模块 21 之前，普通运行环境 10 中的文件加密模块 11 会先利用随机数产生器生成初始密钥；然后，普通运行环境 10 中的文件加密模块 11 将初始密钥存入存储器 40 中。其中，在智能设备的系统首次启动或恢复出厂设置的技术场景中，智能设备的系统内并不存在初始密钥，所以普通运行环境 10 中的文件加密模块 11 需要生成一个初始密钥，并将初始密钥存入存储器 40 中，以便于智能设备在重启以后能够在存储器 40 中获取到初始密钥。

在图 2A 所示的实施例中，对于智能设备的系统开机或重启的技术场景而言，在普

通运行环境 10 中的文件加密模块 11 将初始密钥发送给可信执行环境 20 中的密钥管理模块 21 之前，普通运行环境 10 中的文件加密模块 11 可以直接在存储器 40 中获取初始密钥。其中，在智能设备的系统开机或重启的技术场景中，智能设备的系统的存储器 40 中已经存储有初始密钥，所以普通运行环境 10 中的文件加密模块 11 可以直接在存储器 40 中获取初始密钥。

在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 可以利用第一派生密钥对初始密钥进行解密得到文件密钥。具体的，在可信执行环境 20 中的密钥管理模块 21 可以利用高级加密标准（advanced encryption standard，AES）的密码分组链接模式（cipher block chaining ，CBC)和第一派生密钥对初始密钥进行解密得到文件密钥。

在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 利用第一派生密钥对初始密钥进行解密得到文件密钥以前，需要先生成第一派生密钥，下面简要介绍一种生成第一派生密钥的具体方式：首先，在可信执行环境 20 中的密钥管理模块 21 获取口令鉴权模块 22 内的个人识别密码（personal identification number，PIN）的消息认证码（message authentication code，MAC）；然后，在可信执行环境 20 中的密钥管理模块 21 获取系统级芯片 30 内的私有密钥，其中，私有密钥可以为系统级芯片 30 内一次性编程（one time program，OTP）的 HUK（芯片自己的私有对称密钥），该私有密钥无法被普通运行环境 10 内的软件或模块读取；其次，在可信执行环境 20 中的密钥管理模块 21 获取第一加密因子，其中，第一加密因子可以为由系统级芯片 30 中的随机数产生器生成的随机数，当然，第一加密因子也可以为预先生成的固定值；最后，在可信执行环境 20 中的密钥管理模块 21 利用私有密钥和第一加密因子对消息认证码进行加密得到第一派生密钥，具体的，在可信执行环境 20 中的密钥管理模块 21 可以利用 AES-CBC、私有密钥和第一加密因子对消息认证码进行加密得到第一派生密钥。

其中，在可信执行环境 20 中的密钥管理模块 21 获取口令鉴权模块 22 内的个人识别密码的消息认证码之前，可信执行环境 20 中的口令鉴权模块 22 会获取用户输入的个人识别密码，个人识别密码可以例如为智能设备的开机密码；然后，可信执行环境 20 中的口令鉴权模块 22 会基于个人识别密码生成消息认证码。另外，用户输入个人识别密码的方式有很多。例如，通过数字键盘输入个人识别密码；又如，通过指纹识别的方式输入个人识别密码；再如，通过脸部识别的方式输入个人识别密码。

请参见图 2B 所示，图 2B 所示的为一种生成文件密钥的示意图。请结合图 2A 和图 2B 所示，首先，可信执行环境 20 中的密钥管理模块 21 获取口令鉴权模块 22 的 PIN 的 MAC，密钥管理模块 21 获取存储器 40 中的第一加密因子，密钥管理模块 21 获取系统级芯片 30 内的 OTP 中的私有密钥 HUK；然后，密钥管理模块 21 将 PIN 的 MAC、私有密钥 HUK 和第一加密因子作为 AES-CBC 加密函数的参数输入，那么 AES-CBC 加密函数会输出第一派生密钥；其次，密钥管理模块 21 将第一派生密钥和初始密钥作为 AES-CBC 解密函数的参数输入，那么 AES-CBC 解密函数会输出文件密钥。

在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 利用第一派生密钥对初始密钥进行解密得到文件密钥以前，需要先生成第一派生密钥，下面简要

介绍另一种生成第一派生密钥的具体方式：首先，在可信执行环境 20 中的密钥管理模块 21 获取第一加密因子，其中，第一加密因子可以为由系统级芯片 30 中的随机数产生器生成的随机数，当然，第一加密因子也可以为预先生成的固定值；然后，在可信执行环境 20 中的密钥管理模块 21 获取私有密钥，其中，私有密钥可以为系统级芯片 30 内的私有对称密钥，该私有密钥无法被普通运行环境 10 内的软件或模块读取；最后，在可信执行环境 20 中的密钥管理模块 21 利用私有密钥对第一加密因子进行加密得到第一派生密钥。

请参见图 2C 所示，图 2C 所示的为另一种生成文件密钥的示意图。请结合图 2A 和图 2C 所示，首先，可信执行环境 20 中的密钥管理模块 21 获取存储器 40 中的第一加密因子，密钥管理模块 21 获取系统级芯片 30 内的 OTP 中的私有密钥 HUK；然后，密钥管理模块 21 将私有密钥 HUK 和第一加密因子作为 AES-CBC 加密函数的参数输入，那么 AES-CBC 加密函数会输出第一派生密钥；其次，密钥管理模块 21 将第一派生密钥和初始密钥作为 AES-CBC 解密函数的参数输入，那么 AES-CBC 解密函数会输出文件密钥。

在一种可实现的实施例中，为了保证初始向量的安全性，在可信执行环境 20 中的密钥管理模块 21 还可以对初始密钥进行解密处理得到元数据密钥，其中，元数据密钥用于加密初始向量，初始向量用于与文件密钥联合加密文件；然后，密钥管理模块 21 将元数据密钥发送给普通运行环境 10 中的文件加密模块 11；其次，普通运行环境 10 中的文件加密模块 11 建立密钥索引与元数据密钥的映射关系；最后，普通运行环境 10 中的文件加密模块 11 将密钥索引与元数据密钥的映射关系存储在内存 50 中。

请参见表 3 所示，表 3 所示的为一示例中文件加密模块 11 在内存 50 中存储的密钥索引与元数据密钥的映射关系表。

密钥索引	元数据密钥
Key3	33333333
Key4	44444444
…	…

表 3

在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 还可以利用第二派生密钥对初始密钥进行解密得到元数据密钥。具体的，在可信执行环境 20 中的密钥管理模块 21 可以利用 AES-CBC 和第二派生密钥对初始密钥进行解密得到文件密钥。

在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 利用第二派生密钥对初始密钥进行解密得到元数据密钥以前，需要先生成第二派生密钥，下面简要介绍一种生成第二派生密钥的具体方式：首先，在可信执行环境 20 中的密钥管理模块 21 获取个人识别密码的消息认证码；然后，在可信执行环境 20 中的密钥管理模块 21 系统级芯片 30 内的私有密钥，其中，私有密钥可以为系统级芯片 30 内 OTP 的 HUK，该私有密钥无法被普通运行环境 10 内的软件或模块读取；其次，在可信执行环境 20 中的密钥管理模块 21 获取第二加密因子，其中，第二加密因子可以为由系统级芯片 30 中的随机数产生器生成的随机数，当然，第二加密因子也可以为预先生成的固定值；最后，在可信执行环境 20 中的密钥管理模块 21 利用私有密钥和第二加密因子对消息

认证码进行加密得到第二派生密钥，具体的，在可信执行环境 20 中的密钥管理模块 21 可以利用 AES-CBC、私有密钥和第二加密因子对消息认证码进行加密得到第二派生密钥。

请参见图 2D 所示，图 2D 所示的为一种生成元数据密钥的示意图。请结合图 2A 和图 2D 所示，首先，可信执行环境 20 中的密钥管理模块 21 获取口令鉴权模块 22 的 PIN 的 MAC，密钥管理模块 21 获取存储器 40 中的第二加密因子，密钥管理模块 21 获取系统级芯片 30 内的 OTP 中的私有密钥 HUK；然后，密钥管理模块 21 将 PIN 的 MAC、私有密钥 HUK 和第二加密因子作为 AES-CBC 加密函数的参数输入，那么 AES-CBC 加密函数会输出第二派生密钥；其次，密钥管理模块 21 将第二派生密钥和初始密钥作为 AES-CBC 解密函数的参数输入，那么 AES-CBC 解密函数会输出元数据密钥。

在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 利用第二派生密钥对初始密钥进行解密得到元数据密钥以前，需要先生成第二派生密钥，下面简要介绍生成第二派生密钥的具体方式：在可信执行环境 20 中的密钥管理模块 21 获取第二加密因子，其中，第二加密因子可以为由系统级芯片 30 中的随机数产生器生成的随机数，当然，第二加密因子也可以为预先生成的固定值；在可信执行环境 20 中的密钥管理模块 21 获取私有密钥，其中，私有密钥可以为系统级芯片 30 内的私有对称密钥，该私有密钥无法被普通运行环境 10 内的软件或模块读取；在可信执行环境 20 中的密钥管理模块 21 利用私有密钥对第二加密因子进行加密得到第二派生密钥。

请参见图 2E 所示，图 2E 所示的为另一种生成元数据密钥的示意图。请结合图 2A 和图 2E 所示，首先，可信执行环境 20 中的密钥管理模块 21 获取存储器 40 中的第二加密因子，密钥管理模块 21 获取系统级芯片 30 内的 OTP 中的私有密钥 HUK；然后，密钥管理模块 21 将私有密钥 HUK 和第二加密因子作为 AES-CBC 加密函数的参数输入，那么 AES-CBC 加密函数会输出第二派生密钥；其次，密钥管理模块 21 将第二派生密钥和初始密钥作为 AES-CBC 解密函数的参数输入，那么 AES-CBC 解密函数会输出元数据密钥。

请参见图 3A 所示，图 3A 所示的为本申请实施例提供的智能设备写入文件的示意图。下面介绍本申请实施例写入文件的过程：首先，普通运行环境 10 中的文件加密模块 11 接收普通运行环境 10 中的第三方应用软件 12 或其他模块发送的基于文件的写入指令；然后，文件加密模块 11 在内存 50 中获取密钥索引与密钥类型的映射关系，并根据密钥索引与密钥类型的映射关系获取文件的密钥类型对应的密钥索引；其次，文件加密模块 11 会利用随机数产生器生成一个随机数，并将该随机数作为文件的初始向量，其中，每个文件的初始向量是不同的，随机数产生器可以设置在普通运行环境 10、可信执行环境 20 或系统级芯片 30 内；再次，文件加密模块 11 将初始向量存储至存储器 40 中文件的数据头内，其中，文件包括数据头和数据区，文件的数据头用于存储初始向量等数据，文件的数据区用于存储文件的内容；再次，文件加密模块 11 根据密钥索引和初始向量生成基于文件的写入请求，文件加密模块 11 再将写入请求发送至存储控制器 31 的加密装置 311 中；再次，存储控制器 31 内的加密装置 311 获取写入请求中的密钥索引和初始向量，加密装置 311 获取密钥寄存器 312 中的密钥索引对应的文件密钥；最后，加密装置 311 利用文件密钥和初始向量对文件进行加密得到文件的密

文，并将文件的密文存储到存储器 40 中文件的数据区内。

在图 3A 所示的实施例中，由于普通运行环境 10 中的模块或软件被禁止访问存储控制器 31 中的密钥寄存器 312，在写入文件的过程中，普通运行环境 10 中的模块或软件无法窃取到密钥寄存器 312 中存储的文件密钥，而且普通运行环境 10 中的模块或软件也无法窃取到加密装置 311 在加密文件的过程中所使用的文件密钥，因此，本申请实施例可以保证在写入文件的过程中文件密钥是安全的。

在一种可实现的实施例中，为了保证初始向量的安全性，在文件加密模块 11 生成初始向量以后，文件加密模块 11 还可以利用元数据密钥对初始向量进行加密得到初始向量的密文，然后，文件加密模块 11 会将初始向量的密文存储至存储器 40 中文件的数据头内。当然，初始向量并不是文件加密或解密所必须的，在加密过程中，加密装置 311 可以仅使用文件密钥对文件进行加密得到文件的密文，在解密过程中，加密装置 311 可以仅使用文件密钥对文件的密文进行解密得到文件。

其中，如果初始向量的密文被存储至存储器 40 中文件的数据头内，在文件加密模块 11 接收普通运行环境 10 中的第三方应用软件 12 或其他模块发送的基于文件的读取指令时，那么文件加密模块 11 需要先在存储器 40 中该文件的数据头内获取到初始向量的密文；然后，文件加密模块 11 需要基于密钥索引与元数据密钥的映射关系获取密钥索引对应的元数据密钥；其次，文件加密模块 11 利用元数据密钥对初始向量的密文进行解密得到初始向量。此时，文件加密模块 11 便可以获取到初始向量。

请参见图 3B 所示，图 3B 所示的为一种生成写入请求的示意图。请结合图 3A 和图 3B 所示，首先，普通运行环境 10 中的文件加密模块 11 接收普通运行环境 10 中的第三方应用软件 12 或其他模块发送的基于文件的写入指令，文件加密模块 11 基于密钥类型与密钥索引的映射关系获取文件的密钥类型对应的密钥索引；然后，文件加密模块 11 利用随机数产生器生成一个随机数，并将该随机数作为文件的初始向量，再将初始向量存储至存储器 40 中文件的数据头内；最后，文件加密模块 11 根据密钥索引和初始向量生成基于文件的写入请求。

请参见图 3C 所示，图 3C 所示的为一种加密文件的示意图。请结合图 3A 和图 3C 所示，首先，文件加密模块 11 将写入请求发送至存储控制器 31 的加密装置 311 中；然后，存储控制器 31 内的加密装置 311 获取写入请求中的密钥索引和初始向量；其次，加密装置 311 获取密钥寄存器 312 中的密钥索引对应的文件密钥；再次，加密装置 311 将文件、文件密钥和初始向量作为 AES 加密函数的参数输入，那么 AES 加密函数会输出文件的密文；最后，加密装置 311 将文件的密文存储到存储器 40 中文件的数据区内。

请参见图 4A 所示，图 4A 所示的为本申请实施例提供的智能设备读取文件的示意图。下面介绍本申请实施例读取文件的过程：首先，普通运行环境 10 中的文件加密模块 11 接收普通运行环境 10 中的第三方应用软件 12 或其他模块发送的基于文件的读取指令；然后，文件加密模块 11 在内存 50 中获取密钥索引与密钥类型的映射关系，并根据密钥索引与密钥类型的映射关系获取文件的密钥类型对应的密钥索引；其次，文件加密模块 11 在存储器 40 中文件的数据头内获取初始向量，其中，文件包括数据头和数据区，文件的数据头用于存储初始向量等数据，文件的数据区用于存储文件的内容；再次，文件加密模块 11 根据密钥索引和初始向量生成基于文件的读取请求，文件

加密模块 11 再将读取请求发送至存储控制器 31 的加密装置 311 中；再次，加密装置 311 获取读取请求中的密钥索引和初始向量，加密装置 311 获取密钥寄存器 312 中的密钥索引对应的文件密钥；再次，加密装置 311 利用文件密钥和初始向量对存储器中的文件的密文进行解密得到文件，再将解密得到的文件存入内存 50 中；最后，普通运行环境 10 中的第三方应用软件 12 或其他模块在内存 50 中读取该文件。

在一种可实现的实施例中，由于普通运行环境 10 中的模块或软件被禁止访问存储控制器 31 中的密钥寄存器 312，在读取文件的过程中，普通运行环境 10 中的模块或软件无法窃取到密钥寄存器 312 中存储的文件密钥，普通运行环境 10 中的模块或软件也无法窃取到加密装置 311 在解密文件的过程中所使用的文件密钥，因此，本申请实施例可以保证在读取文件的过程中文件密钥是安全性的。

在一种可实现的实施例中，如果文件加密模块 11 预先利用元数据密钥对初始向量加密得到初始向量的密文，且将初始向量的密文存储到存储器 40 中文件的数据头内，那么文件加密模块 11 需要先获取存储器 40 中文件的数据头内的初始向量的密文；然后，文件加密模块 11 会基于密钥索引与元数据密钥的映射关系获取密钥索引对应的元数据密钥，并利用元数据密钥对初始向量的密文进行解密得到初始向量，进而得到初始向量。

请参见图 4B 所示，图 4B 所示的为一种生成读取请求的示意图。请结合图 4A 和图 4B 所示，首先，普通运行环境 10 中的文件加密模块 11 接收普通运行环境 10 中的第三方应用软件 12 或其他模块发送的基于文件的读取指令；然后，文件加密模块 11 在内存 50 中获取密钥索引与密钥类型的映射关系，并根据密钥索引与密钥类型的映射关系获取文件的密钥类型对应的密钥索引；其次，文件加密模块 11 在存储器 40 中文件的数据头内获取初始向量；再次，文件加密模块 11 根据密钥索引和初始向量生成基于文件的读取请求。

请参见图 4C 所示，图 4C 所示的为一种解密文件的示意图。请结合图 4A 和图 4C 所示，首先，文件加密模块 11 再将读取请求发送至存储控制器 31 的加密装置 311 中；然，存储控制器 31 内的加密装置 311 获取读取请求中的密钥索引和初始向量；其次，加密装置 311 获取密钥寄存器 312 中的密钥索引对应的文件密钥；再次，加密装置 311 将文件的密文、文件密钥和初始向量作为 AES 解密函数的参数输入，那么 AES 解密函数会输出文件；再次，加密装置 311 将文件存储到内存 50 中；最后，普通运行环境 10 中的第三方应用软件 12 或其他模块在内存 50 中读取该文件。

请参见图 2A 和图 5 所示，图 5 所示的为本申请实施例提供的密钥处理方法的信令交互图，图 2A 所示的智能设备可以执行图 5 所示的方法。图 5 所示的方法可以保证生成文件密钥的过程是安全的，该方法包括以下步骤。

步骤 S11、在普通运行环境 10 中的文件加密模块 11 将初始密钥发送给可信执行环境 20 中的密钥管理模块 21。其中，初始密钥可以为预先生成的随机数。例如，假设初始密钥为 2068134157937。

步骤 S12、在可信执行环境 20 中的密钥管理模块 21 对初始密钥进行解密处理得到文件密钥，文件密钥用于加密文件。其中，密钥管理模块 21 对初始密钥进行解密处理得到文件密钥具体可以包括以下步骤：在可信执行环境 20 中的密钥管理模块 21 利

用第一派生密钥对初始密钥进行解密得到文件密钥。在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 利用第一派生密钥对初始密钥进行解密得到文件密钥以前，需要先生成第一派生密钥，下面简要介绍生成第一派生密钥的具体方式：在可信执行环境 20 中的密钥管理模块 21 获取个人识别密码的消息认证码；在可信执行环境 20 中的密钥管理模块 21 获取私有密钥，其中，私有密钥可以为系统级芯片 30 内的私有对称密钥，该私有密钥无法被普通运行环境 10 内的文件加密模块 11 读取；在可信执行环境 20 中的密钥管理模块 21 获取第一加密因子，其中，第一加密因子可以为预先生成的随机数；在可信执行环境 20 中的密钥管理模块 21 利用私有密钥和第一加密因子对消息认证码进行加密得到第一派生密钥。

在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 利用第一派生密钥对初始密钥进行解密得到文件密钥以前，需要先生成第一派生密钥，下面简要介绍生成第一派生密钥的具体方式：在可信执行环境 20 中的密钥管理模块 21 获取第一加密因子，其中，第一加密因子可以为预先生成的随机数；在可信执行环境 20 中的密钥管理模块 21 获取私有密钥，其中，私有密钥可以为系统级芯片 30 内的私有对称密钥，该私有密钥无法被普通运行环境 10 内的文件加密模块 11 读取；在可信执行环境 20 中的密钥管理模块 21 利用私有密钥对第一加密因子进行加密得到第一派生密钥。

步骤 S13、在可信执行环境 20 中的密钥管理模块 21 将文件密钥存储至存储控制器 31 的密钥寄存器 312 中。其中，普通运行环境 10 中的文件加密模块 11 被禁止访问存储控制器 31 中的密钥寄存器 312。另外，存储控制器 31 可以为系统级芯片 30 内的一个装置。

步骤 S14、在可信执行环境 20 中的密钥管理模块 21 获取密钥寄存器 312 中文件密钥的密钥索引。其中，密钥索引用于指示文件密钥在密钥寄存器 312 中的存储位置，存储控制器 31 可以根据密钥索引获取到密钥寄存器 312 中的文件密钥。

步骤 S15、在可信执行环境 20 中的密钥管理模块 21 将密钥索引发送给普通运行环境 10 中的文件加密模块 11。其中，由于普通运行环境 10 中的文件加密模块 11 被禁止访问存储控制器 31 中的密钥寄存器 312，所以普通运行环境 10 中的文件加密模块 11 无法根据密钥索引获取到密钥寄存器 312 中的文件密钥。

步骤 S16、在普通运行环境 10 中的文件加密模块 11 将该文件密钥的密钥索引存储至内存 50 中。

其中，文件加密模块 11 将该文件密钥的密钥索引存储至内存 50 中的目的在于，如果普通运行环境 10 中的第三方应用软件 12 或其他模块需要写入文件或读取文件，那么文件加密模块 11 可以将内存 50 中的密钥索引发送给存储控制器 31，以使存储控制器 31 实现对文件的加密或解密，进而实现对文件的写入操作或读取操作。

在图 5 所示的实施例中，普通运行环境 10 内的文件加密模块 11 被禁止访问可信执行环境 20 内的模块或信息，在密钥管理模块 21 生成文件密钥的过程中，普通运行环境 10 内的文件加密模块 11 无法窃取密钥管理模块 21 生成的文件密钥，所以生成文件密钥的过程是安全的。而且，在密钥管理模块 21 生成文件密钥以后，密钥管理模块 21 将文件密钥存储至存储控制器 31 的密钥寄存器 312 中，由于普通运行环境 10 中的文件加密模块 11 被存储控制器 31 禁止访问存储控制器 31 中的密钥寄存器 312，普通

运行环境 10 中的文件加密模块 11 无法窃取存储控制器 31 的密钥寄存器 312 中的文件密钥，所以文件密钥的存储环境也是安全的。另外，可信执行环境 20 中的密钥管理模块 21 仅将文件密钥的密钥索引发送给普通运行环境 10 中的文件加密模块 11，以使普通运行环境 10 中的第三方应用软件 12 或其他模块需要写入文件或读取文件的情况下，文件加密模块 11 可以与存储控制器 31 相互配合，文件加密模块 11 将密钥索引发送给存储控制器 31，以使存储控制器 31 实现对文件的加密或解密，进而实现对文件的写入操作或读取操作。

在一种可实现的实施例中，为了保证初始向量的安全性，在可信执行环境 20 中的密钥管理模块 21 还可以对初始密钥进行解密处理得到元数据密钥，其中，元数据密钥用于加密初始向量，初始向量用于与文件密钥联合加密文件；在可信执行环境 20 中的密钥管理模块 21 将元数据密钥发送给普通运行环境 10 中的文件加密模块 11。

在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 对初始密钥进行解密处理得到元数据密钥具体可以包括以下步骤：在可信执行环境 20 中的密钥管理模块 21 利用第二派生密钥对初始密钥进行解密得到元数据密钥。

在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 利用第二派生密钥对初始密钥进行解密得到元数据密钥以前，需要先生成第二派生密钥，下面简要介绍生成第二派生密钥的具体方式：在可信执行环境 20 中的密钥管理模块 21 获取个人识别密码的消息认证码；在可信执行环境 20 中的密钥管理模块 21 获取私有密钥，其中，私有密钥可以为系统级芯片 30 内的私有对称密钥，该私有密钥无法被普通运行环境 10 内的文件加密模块 11 读取；在可信执行环境 20 中的密钥管理模块 21 获取第二加密因子，其中，第二加密因子可以为预先生成的随机数；在可信执行环境 20 中的密钥管理模块 21 利用私有密钥和第二加密因子对消息认证码进行加密得到第二派生密钥。

在一种可实现的实施例中，在可信执行环境 20 中的密钥管理模块 21 利用第二派生密钥对初始密钥进行解密得到元数据密钥以前，需要先生成第二派生密钥，下面简要介绍生成第二派生密钥的具体方式：在可信执行环境 20 中的密钥管理模块 21 获取第二加密因子，其中，第二加密因子可以为预先生成的随机数；在可信执行环境 20 中的密钥管理模块 21 获取私有密钥，其中，私有密钥可以为系统级芯片 30 内的私有对称密钥，该私有密钥无法被普通运行环境 10 内的文件加密模块 11 读取；在可信执行环境 20 中的密钥管理模块 21 利用私有密钥对第二加密因子进行加密得到第二派生密钥。

请参见图 3A 和图 6 所示，图 6 所示的为本申请实施例提供的密钥处理方法的信令交互图，图 3A 所示的智能设备可以执行图 6 所示的方法。图 6 所示的方法可以保证在写入文件的过程中文件密钥是安全的，该方法包括以下步骤。

步骤 S21、在普通运行环境 10 中的文件加密模块 11 接收文件的写入指令。其中，写入指令可以是普通运行环境 10 中的第三方应用软件 12 或其他模块生成的。

步骤 S22、在普通运行环境 10 中的文件加密模块 11 获取文件的密钥类型。其中，文件加密模块 11 预先设置好每个文件的密钥类型。例如，对于用户文件，密钥类型为 A 类型；又如，对于系统文件，密钥类型为 B 类型。

步骤 S23、在普通运行环境 10 中的文件加密模块 11 获取密钥类型对应的密钥索引；其中，在普通运行环境 10 中的文件加密模块 11 接收到可信执行环境 20 的密钥管理模块 21 发送的密钥索引时，便建立了密钥索引与密钥类型的映射关系，所以在普通运行环境 10 中的文件加密模块 11 可以基于密钥索引与密钥类型的映射关系，获取密钥类型对应的密钥索引。

步骤 S24、在普通运行环境 10 中的文件加密模块 11 获取初始向量。其中，在普通运行环境 10 中的文件加密模块 11 每次接收到文件的写入指令时，文件加密模块 11 均会生成一个新的初始向量，该初始向量可以为随机数。

步骤 S25、在普通运行环境 10 中的文件加密模块 11 根据密钥索引和初始向量生成基于文件的写入请求。步骤 S26、在普通运行环境 10 中的文件加密模块 11 向存储控制器 31 的加密装置 311 发送写入请求。步骤 S27、在存储控制器 31 内的加密装置 311 获取写入请求中的密钥索引和初始向量。步骤 S28、在存储控制器 31 中的加密装置 311 获取密钥寄存器 312 中的密钥索引对应的文件密钥。步骤 S29、在存储控制器 31 中的加密装置 311 利用文件密钥和初始向量对文件进行加密得到文件的密文。步骤 S30、在存储控制器 31 中的加密装置 311 将文件的密文存储到存储器 40 中。

在图 6 所示的实施例中，由于普通运行环境 10 中的模块或软件被存储控制器 31 禁止访问存储控制器 31 中的密钥寄存器 312，在写入文件的过程中，普通运行环境 10 中的模块或软件无法窃取到密钥寄存器 312 中存储的文件密钥，而且普通运行环境 10 中的模块或软件也无法窃取到加密装置 311 在加密文件的过程中所使用的文件密钥，因此，本申请实施例可以保证在写入文件的过程中文件密钥是安全的。

在一种可实现的实施例中，为了保证初始向量的安全性，在普通运行环境 10 中的文件加密模块 11 可以利用元数据密钥对初始向量进行加密得到初始向量的密文；在普通运行环境 10 中的文件加密模块 11 将初始向量的密文存储至存储器 40 中。

请参见图 4A 和图 7 所示，图 7 所示的为本申请实施例提供的密钥处理方法的信令交互图，图 4A 所示的智能设备可以执行图 5 所示的方法。图 7 所示的方法可以保证在读取文件的过程中文件密钥是安全的，该方法包括以下步骤。

步骤 S31、在普通运行环境 10 中的文件加密模块 11 接收文件的读取指令。其中，读取指令可以是普通运行环境 10 中的第三方应用软件 12 或其他模块生成的。

步骤 S32、在普通运行环境 10 中的文件加密模块 11 获取文件的密钥类型。其中，文件加密模块 11 预先设置好每个文件的密钥类型。例如，对于用户文件，密钥类型为 A 类型；又如，对于系统文件，密钥类型为 B 类型。

步骤 S33、在普通运行环境 10 中的文件加密模块 11 获取密钥类型对应的密钥索引；其中，在普通运行环境 10 中的文件加密模块 11 接收到可信执行环境 20 的密钥管理模块 21 发送的密钥索引时，便建立了密钥索引与密钥类型的映射关系，所以在普通运行环境 10 中的文件加密模块 11 可以基于密钥索引与密钥类型的映射关系，获取密钥类型对应的密钥索引。

步骤 S34、在普通运行环境 10 中的文件加密模块 11 获取初始向量。其中，在普通运行环境 10 中的文件加密模块 11 每次接收到文件的写入指令时，文件加密模块 11 均会生成一个新的初始向量，该初始向量可以为随机数。

步骤 S35、在普通运行环境 10 中的文件加密模块 11 根据密钥索引和初始向量生成基于文件的读取请求。步骤 S36、在普通运行环境 10 中的文件加密模块 11 向存储控制器 31 的加密装置 311 发送读取请求。步骤 S37、在存储控制器 31 内的加密装置 311 获取读取请求中的密钥索引和初始向量。步骤 S38、在存储控制器 31 中的加密装置 311 获取密钥寄存器 312 中的密钥索引对应的文件密钥。步骤 S39、在存储控制器 31 中的加密装置 311 获取存储器 40 中的文件的密文。步骤 S40、在存储控制器 31 中的加密装置 311 利用文件密钥和初始向量对文件的密文进行解密得到文件。

在一种可实现的实施例中，由于普通运行环境 10 中的模块或软件被存储控制器 31 禁止访问存储控制器 31 中的密钥寄存器 312，在读取文件的过程中，普通运行环境 10 中的模块或软件无法窃取到密钥寄存器 312 中存储的文件密钥，普通运行环境 10 中的模块或软件也无法窃取到加密装置 311 在解密文件的过程中所使用的文件密钥，因此，本申请实施例可以保证在读取文件的过程中文件密钥是安全性的。

在一种可实现的实施例中，如果普通运行环境 10 中的文件加密模块 11 预先利用元数据密钥对初始向量加密得到初始向量的密文，且将初始向量的密文存储到存储器 40 中，那么普通运行环境 10 中的文件加密模块 11 获取初始向量的具体过程包括以下步骤：在普通运行环境 10 中的文件加密模块 11 获取存储器 40 中初始向量的密文；在普通运行环境 10 中的文件加密模块 11 获取元数据密钥；在普通运行环境 10 中的文件加密模块 11 利用元数据密钥对初始向量的密文进行解密得到初始向量。

请参见图 8 所示，图 8 所示的为本申请实施例提供的一种密钥处理装置的示意图。该密钥处理装置包括以下模块：

接收模块 101，用于在可信执行环境中接收普通运行环境中的文件加密模块发送的初始密钥；具体详细的实现方式，请参考上述图 5 所示的方法实施例中步骤 S11 的详细描述。结合图 1，接收模块 101 位于图 1 的密钥管理模块 21 中。

第一解密模块 102，用于在可信执行环境中对初始密钥进行解密处理得到文件密钥，文件密钥用于加密文件；具体详细的实现方式，请参考上述图 5 所示的方法实施例中步骤 S12 的详细描述。结合图 1，第一解密模块 102 位于图 1 的密钥管理模块 21 中。

存储模块 103，用于在可信执行环境中将文件密钥存储至存储控制器的密钥寄存器中，普通运行环境中的文件加密模块被禁止访问存储控制器中的密钥寄存器；具体详细的实现方式，请参考上述图 5 所示的方法实施例中步骤 S13 的详细描述。结合图 1，存储模块 103 位于图 1 的密钥管理模块 21 中。

获取模块 104，用于在可信执行环境中获取密钥寄存器中文件密钥的密钥索引，密钥索引用于指示文件密钥在密钥寄存器中的存储位置；具体详细的实现方式，请参考上述图 5 所示的方法实施例中步骤 S14 的详细描述。结合图 1，获取模块 104 位于图 1 的密钥管理模块 21 中。

发送模块 105，用于在可信执行环境中将密钥索引发送给普通运行环境中的文件加密模块；具体详细的实现方式，请参考上述图 5 所示的方法实施例中步骤 S15 的详细描述。结合图 1，发送模块 105 位于图 1 的密钥管理模块 21 中。

在一种可实现的实施例中，第一解密模块 102，具体用于在可信执行环境中利用

第一派生密钥对初始密钥进行解密得到文件密钥。具体详细的实现方式，请参考上述图 5 所示的方法实施例中对应的详细描述。

在一种可实现的实施例中，密钥处理装置还包括第一加密模块 106；第一加密模块 106，用于在可信执行环境中获取个人识别密码的消息认证码；在可信执行环境中获取私有密钥；在可信执行环境中获取第一加密因子；在可信执行环境中利用私有密钥和第一加密因子对消息认证码进行加密得到第一派生密钥。具体详细的实现方式，请参考上述图 5 所示的方法实施例中对应的详细描述。结合图 1，第一加密模块 106 位于图 1 的密钥管理模块 21 中。

在一种可实现的实施例中，密钥处理装置还包括第二加密模块 107；第二加密模块 107，用于在可信执行环境中获取第一加密因子；在可信执行环境中获取私有密钥；在可信执行环境中利用私有密钥对第一加密因子进行加密得到第一派生密钥。具体详细的实现方式，请参考上述图 5 所示的方法实施例中对应的详细描述。结合图 1，第二加密模块 107 位于图 1 的密钥管理模块 21 中。

在一种可实现的实施例中，密钥处理装置还包括第二解密模块 108：第二解密模块，用于在可信执行环境中对初始密钥进行解密处理得到元数据密钥，元数据密钥用于加密初始向量，初始向量用于与文件密钥联合加密文件；发送模块 105，还用于在可信执行环境中将元数据密钥发送给普通运行环境中的文件加密模块。具体详细的实现方式，请参考上述图 5 所示的方法实施例中对应的详细描述。结合图 1，第二解密模块 108 位于图 1 的密钥管理模块 21 中。

在一种可实现的实施例中，第二解密模块 108，具体用于在可信执行环境中利用第二派生密钥对初始密钥进行解密得到元数据密钥。具体详细的实现方式，请参考上述图 5 所示的方法实施例中对应的详细描述。

在一种可实现的实施例中，密钥处理装置还包括第三加密模块 109；第三加密模块 109，用于在可信执行环境中获取个人识别密码的消息认证码；在可信执行环境中获取私有密钥；在可信执行环境中获取第二加密因子；在可信执行环境中利用私有密钥和第二加密因子对消息认证码进行加密得到第二派生密钥。具体详细的实现方式，请参考上述图 5 所示的方法实施例中对应的详细描述。结合图 1，第三加密模块 109 位于图 1 的密钥管理模块 21 中。

在一种可实现的实施例中，密钥处理装置还包括第四加密模块 110；第四加密模块 110，用于在可信执行环境中获取第二加密因子；在可信执行环境中获取私有密钥；在可信执行环境中利用私有密钥对第二加密因子进行加密得到第二派生密钥。具体详细的实现方式，请参考上述图 5 所示的方法实施例中对应的详细描述。结合图 1，第四加密模块 110 位于图 1 的密钥管理模块 21 中。

在一种可实现的实施例中，密钥处理装置还包括文件加密模块 111；文件加密模块 111，用于在普通运行环境中接收文件的处理指令；在普通运行环境中获取文件的密钥类型；在普通运行环境中获取密钥类型对应的密钥索引；在普通运行环境中获取初始向量；在普通运行环境中根据密钥索引和初始向量生成基于文件的处理请求；在普通运行环境中向存储控制器发送处理请求。具体详细的实现方式，请参考上述图 6 所示的方法实施例中步骤 S21 至步骤 S26 的详细描述，以及请参考上述图 7 所示的方

法实施例中步骤 S31 至步骤 S36 的详细描述。结合图 1，文件加密模块 111 等同于图 1 的文件加密模块 11 中。

在一种可实现的实施例中，文件加密模块 111，还用于在普通运行环境中利用元数据密钥对初始向量进行加密得到初始向量的密文；在普通运行环境中将初始向量的密文存储至存储器中。具体详细的实现方式，请参考上述图 6 或图 7 所示的方法实施例中对应的详细描述。

在一种可实现的实施例中，文件加密模块 111，具体用于在普通运行环境中获取存储器中初始向量的密文；在普通运行环境中获取元数据密钥；在普通运行环境中利用元数据密钥对初始向量的密文进行解密得到初始向量。具体详细的实现方式，请参考上述图 6 或图 7 所示的方法实施例中对应的详细描述。

需理解，在以上图 8 对应的实施例中，每个模块以软件形式实现，例如参考图 1，其中的文件加密模块 11、密钥管理模块 21、第三方应用软件 12 和口令鉴权模块 22 都是以软件模块的形式存在。但在实际应用中，其中的一个或多个模块可以由硬件实现。具体实施例中各个模块的功能时以软件还是硬件来实现可以是由设计人员自由选择的。

需要说明的是，当上述实施例中涉及软件实现的功能时，相关软件或软件中的模块可存储在计算机可读介质中或作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是计算机能够存取的任何可用介质。以此为例但不限于：计算机可读介质可以包括 RAM、ROM、EEPROM、CD-ROM 或其他光盘存储、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质。此外。任何连接可以适当的成为计算机可读介质。例如，如果软件是使用同轴电缆、光纤光缆、双绞线、数字用户线（DSL）或者诸如红外线、无线电和微波之类的无线技术从网站、服务器或者其他远程源传输的，那么同轴电缆、光纤光缆、双绞线、DSL 或者诸如红外线、无线和微波之类的无线技术包括在所属介质的定影中。如本申请所使用的，盘（Disk）和碟（disc）包括压缩光碟（CD）、激光碟、光碟、数字通用光碟（DVD）、软盘和蓝光光碟，其中盘通常磁性的复制数据，而碟则用激光来光学的复制数据。上面的组合也应当包括在计算机可读介质的保护范围之内。

需理解，相关软件或软件中的模块可以被图 1 所示的处理器 32 执行以实现之前实施例所对应的方法流程。此外，以上实施例仅用以说明本申请的技术方案而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，然而本领域的普通技术人员应当理解：其依然可对前述各实施例所记载的技术方案进行修改，或对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

权 利 要 求 书

1、一种密钥处理方法，其特征在于，所述方法包括：

在可信执行环境中接收普通运行环境中的文件加密模块发送的初始密钥；

在所述可信执行环境中对所述初始密钥进行解密处理得到文件密钥，所述文件密钥用于加密文件；

在所述可信执行环境中将所述文件密钥存储至存储控制器的密钥寄存器中，所述普通运行环境中的文件加密模块被禁止访问所述密钥寄存器；

在所述可信执行环境中获取所述密钥寄存器中所述文件密钥的密钥索引，所述密钥索引用于指示所述文件密钥在所述密钥寄存器中的存储位置；

在所述可信执行环境中将所述密钥索引发送给所述普通运行环境中的文件加密模块。

2、根据权利要求 1 所述的密钥处理方法，其特征在于，在所述可信执行环境中对初始密钥进行解密处理得到文件密钥包括：

在所述可信执行环境中利用第一派生密钥对所述初始密钥进行解密得到文件密钥。

3、根据权利要求 2 所述的密钥处理方法，其特征在于，在所述可信执行环境中利用第一派生密钥对所述初始密钥进行解密得到文件密钥之前，所述方法还包括：

在所述可信执行环境中获取个人识别密码的消息认证码；

在所述可信执行环境中获取私有密钥；

在所述可信执行环境中获取第一加密因子；

在所述可信执行环境中利用所述私有密钥和所述第一加密因子对所述消息认证码进行加密得到第一派生密钥。

4、根据权利要求 2 所述的密钥处理方法，其特征在于，在可信执行环境中利用第一派生密钥对初始密钥进行解密得到文件密钥之前，所述方法还包括：

在所述可信执行环境中获取第一加密因子；

在所述可信执行环境中获取私有密钥；

在所述可信执行环境中利用所述私有密钥对所述第一加密因子进行加密得到第一派生密钥。

5、根据权利要求 1 至 4 中任一项所述的密钥处理方法，其特征在于，在所述可信执行环境中将所述密钥索引发送给所述普通运行环境中的文件加密模块以后，所述方法还包括：

在所述普通运行环境中的所述文件加密模块接收所述文件的处理指令；

在所述普通运行环境中的所述文件加密模块响应于所述处理指令获取所述文件的密钥类型；

在所述普通运行环境中的所述文件加密模块获取所述密钥类型对应的所述密钥索引；

在所述普通运行环境中的所述文件加密模块获取初始向量，所述初始向量用于与所述文件密钥联合加密所述文件；

在所述普通运行环境中的所述文件加密模块根据所述密钥索引和所述初始向量生成基于所述文件的处理请求；

在所述普通运行环境中的所述文件加密模块向所述存储控制器发送所述处理请求。

6、根据权利要求 5 所述的密钥处理方法，其特征在于，在所述普通运行环境中的所述文件加密模块向所述存储控制器发送所述处理请求以后，所述方法还包括：

所述存储控制器接收所述普通运行环境中的文件加密模块发送的所述处理请求；

所述存储控制器响应于所述处理请求获取所述密钥寄存器中的所述密钥索引对应的文件密钥；

所述存储控制器利用所述文件密钥和所述初始向量对所述文件进行加密得到所述文件的密文，并将所述文件的密文存储到存储器中；

或者，所述存储控制器获取所述存储器中的所述文件的密文，利用所述文件密钥和所述初始向量对所述文件的密文进行解密得到所述文件。

7、根据权利要求 5 或 6 所述的密钥处理方法，其特征在于，在所述普通运行环境中的所述文件加密模块获取初始向量包括：

在所述普通运行环境中的所述文件加密模块获取存储器中初始向量的密文；

在所述普通运行环境中的所述文件加密模块获取元数据密钥；

在所述普通运行环境中的所述文件加密模块利用所述元数据密钥对所述初始向量的密文进行解密得到所述初始向量。

8、根据权利要求 5 或 6 所述的密钥处理方法，其特征在于，在所述普通运行环境中的所述文件加密模块获取初始向量后，所述方法还包括：

在所述普通运行环境中的所述文件加密模块获取元数据密钥；

在所述普通运行环境中的所述文件加密模块利用所述元数据密钥对所述初始向量进行加密得到所述初始向量的密文；

在所述普通运行环境中的所述文件加密模块将所述初始向量的密文存储至存储器中。

9、根据权利要求 7 或 8 所述的密钥处理方法，其特征在于，在所述普通运行环境中的所述文件加密模块获取元数据密钥前，所述方法还包括：

在所述可信执行环境中对所述初始密钥进行解密处理得到元数据密钥；

在所述可信执行环境中将所述元数据密钥发送给所述普通运行环境中的文件加密模块。

10、根据权利要求 9 所述的密钥处理方法，其特征在于，在所述可信执行环境中所述对初始密钥进行解密处理得到元数据密钥包括：

在所述可信执行环境中利用第二派生密钥对初始密钥进行解密得到元数据密钥。

11、根据权利要求 10 所述的密钥处理方法，其特征在于，在所述可信执行环境中利用第二派生密钥对初始密钥进行解密得到元数据密钥之前，所述方法还包括：

在所述可信执行环境中获取所述个人识别密码的消息认证码；

在所述可信执行环境中获取所述私有密钥；

在所述可信执行环境中获取第二加密因子；

在所述可信执行环境中利用所述私有密钥和所述第二加密因子对所述消息认证码进行加密得到第二派生密钥。

12、根据权利要求 10 所述的密钥处理方法，其特征在于，在所述可信执行环境中

利用第二派生密钥对初始密钥进行解密得到元数据密钥之前，所述方法还包括：

在所述可信执行环境中获取第二加密因子；

在所述可信执行环境中获取所述私有密钥；

在所述可信执行环境中利用所述私有密钥对所述第二加密因子进行加密得到第二派生密钥。

13、一种密钥处理方法，其特征在于，所述方法包括：

存储控制器接收普通运行环境中的文件加密模块发送的基于文件的处理请求，所述处理请求包括密钥索引，所述密钥索引用于指示文件密钥在存储控制器中的密钥寄存器中的存储位置；

所述存储控制器获取所述密钥寄存器中的所述密钥索引对应的文件密钥，所述普通运行环境中的文件加密模块被禁止访问所述密钥寄存器；

所述存储控制器利用所述文件密钥对所述文件进行加密得到所述文件的密文，并将所述文件的密文存储到存储器中；

或者，所述存储控制器获取存储器中的所述文件的密文，利用所述文件密钥对所述文件的密文进行解密得到所述文件。

14、根据权利要求 13 所述的密钥处理方法，其特征在于，所述处理请求还包括初始向量；

所述存储控制器利用所述文件密钥对所述文件进行加密得到所述文件的密文包括：

所述存储控制器利用所述文件密钥和所述初始向量对所述文件进行加密得到所述文件的密文。

15、根据权利要求 13 所述的密钥处理方法，其特征在于，所述处理请求还包括初始向量；

所述存储控制器利用所述文件密钥对所述文件的密文进行解密得到所述文件包括：

所述存储控制器利用所述文件密钥和所述初始向量对所述文件的密文进行解密得到所述文件。

16、一种密钥处理装置，其特征在于，所述装置包括处理器和接口，所述接口与存储控制器和所述处理器连接；

所述处理器，用于运行软件指令以产生可信执行环境和普通运行环境并在所述普通运行环境中实现文件加密模块的功能，并进一步执行以下操作：

在所述可信执行环境中接收所述普通运行环境中的文件加密模块发送的初始密钥；在所述可信执行环境中对所述初始密钥进行解密处理得到文件密钥，所述文件密钥用于加密文件；在所述可信执行环境中通过所述接口将所述文件密钥存储至存储控制器的密钥寄存器中，所述普通运行环境中的文件加密模块被禁止访问所述密钥寄存器；在所述可信执行环境中通过所述接口获取所述密钥寄存器中所述文件密钥的密钥索引，所述密钥索引用于指示所述文件密钥在所述密钥寄存器中的存储位置；在所述可信执行环境中将所述密钥索引发送给所述普通运行环境中的文件加密模块。

17、根据权利要求 16 所述的密钥处理装置，其特征在于：

所述处理器，具体用于在所述可信执行环境中利用第一派生密钥对所述初始密钥进行解密得到文件密钥。

18、根据权利要求 17 所述的密钥处理装置，其特征在于：

所述处理器，还用于在所述可信执行环境中获取个人识别密码的消息认证码；在所述可信执行环境中获取私有密钥；在所述可信执行环境中获取第一加密因子；在所述可信执行环境中利用所述私有密钥和所述第一加密因子对所述消息认证码进行加密得到第一派生密钥。

19、根据权利要求 17 所述的密钥处理装置，其特征在于：

所述处理器，还用于在所述可信执行环境中获取第一加密因子；在所述可信执行环境中获取私有密钥；在所述可信执行环境中利用所述私有密钥对所述第一加密因子进行加密得到第一派生密钥。

20、根据权利要求 16 至 19 中任一项所述的密钥处理装置，其特征在于：

所述处理器，还用于在所述普通运行环境中实现所述文件加密模块的如下功能：接收所述文件的处理指令；获取所述文件的密钥类型；获取所述密钥类型对应的密钥索引；获取初始向量，所述初始向量用于与所述文件密钥联合加密所述文件；根据所述密钥索引和所述初始向量生成基于所述文件的处理请求；向所述存储控制器发送所述处理请求。

21、根据权利要求 20 所述的密钥处理装置，其特征在于，所述装置还包括所述存储控制器，所述存储控制器包括加密装置和所述密钥寄存器；

所述存储控制器的加密装置，用于接收所述普通运行环境中的文件加密模块发送的所述处理请求；获取所述密钥寄存器中的所述密钥索引对应的文件密钥；利用所述文件密钥和所述初始向量对所述文件进行加密得到所述文件的密文，并将所述文件的密文存储到存储器中；或者，获取所述存储器中的所述文件的密文，利用所述文件密钥和所述初始向量对所述文件的密文进行解密得到所述文件。

22、根据权利要求 20 或 21 所述的密钥处理装置，其特征在于：

所述处理器，还用于在所述普通运行环境中实现所述文件加密模块的如下功能：获取存储器中初始向量的密文；获取元数据密钥；利用所述元数据密钥对所述初始向量的密文进行解密得到所述初始向量。

23、根据权利要求 20 或 21 所述的密钥处理装置，其特征在于：

所述处理器，还用于在所述普通运行环境中实现所述文件加密模块的如下功能：获取元数据密钥；利用所述元数据密钥对所述初始向量进行加密得到所述初始向量的密文；将所述初始向量的密文存储至存储器中。

24、根据权利要求 22 或 23 所述的密钥处理装置，其特征在于：

所述处理器，还用于在所述可信执行环境中对所述初始密钥进行解密处理得到元数据密钥；在所述可信执行环境中将所述元数据密钥发送给所述普通运行环境中的文件加密模块。

25、根据权利要求 24 所述的密钥处理装置，其特征在于：

所述处理器，具体用于在所述可信执行环境中利用第二派生密钥对初始密钥进行解密得到元数据密钥。

26、根据权利要求 25 所述的密钥处理装置，其特征在于：

所述处理器，还用于在所述可信执行环境中获取所述个人识别密码的消息认证码；

在所述可信执行环境中获取所述私有密钥；在所述可信执行环境中获取第二加密因子；在所述可信执行环境中利用所述私有密钥和所述第二加密因子对所述消息认证码进行加密得到第二派生密钥。

27、根据权利要求 25 所述的密钥处理装置，其特征在于：

所述处理器，还用于在所述可信执行环境中获取第二加密因子；在所述可信执行环境中获取所述私有密钥；在所述可信执行环境中利用所述私有密钥对所述第二加密因子进行加密得到第二派生密钥。

28、一种存储控制器，其特征在于，包括加密装置和密钥寄存器；

所述密钥寄存器用于存储文件密钥；

所述加密装置，用于接收普通运行环境中的文件加密模块发送的基于文件的处理请求，所述处理请求包括密钥索引，所述密钥索引用于指示文件密钥在所述密钥寄存器中的存储位置；获取所述密钥寄存器中的所述密钥索引对应的文件密钥，所述普通运行环境中的文件加密模块被禁止访问所述密钥寄存器；利用所述文件密钥对所述文件进行加密得到所述文件的密文，并将所述文件的密文存储到存储器中；或者，获取存储器中的所述文件的密文，利用所述文件密钥对所述文件的密文进行解密得到所述文件。

29、根据权利要求 28 所述的密钥处理装置，其特征在于，所述处理请求还包括初始向量；

所述加密装置，具体用于利用所述文件密钥和所述初始向量对所述文件进行加密得到所述文件的密文。

30、根据权利要求 28 所述的密钥处理装置，其特征在于，所述处理请求还包括初始向量；

所述加密装置，具体用于利用所述文件密钥和所述初始向量对所述文件的密文进行解密得到所述文件。

31、一种密钥处理装置，其特征在于，包括：

接收模块，用于在可信执行环境中接收普通运行环境中的文件加密模块发送的初始密钥；

第一解密模块，用于在所述可信执行环境中对所述初始密钥进行解密处理得到文件密钥，所述文件密钥用于加密文件；

存储模块，用于在所述可信执行环境中将所述文件密钥存储至存储控制器的密钥寄存器中，所述普通运行环境中的文件加密模块被禁止访问所述密钥寄存器；

获取模块，用于在所述可信执行环境中获取所述密钥寄存器中所述文件密钥的密钥索引，所述密钥索引用于指示所述文件密钥在所述密钥寄存器中的存储位置；

发送模块，用于在所述可信执行环境中将所述密钥索引发送给所述普通运行环境中的文件加密模块。

32、根据权利要求 31 所述的密钥处理装置，其特征在于：

所述第一解密模块，具体用于在所述可信执行环境中利用第一派生密钥对所述初始密钥进行解密得到文件密钥。

33、根据权利要求 32 所述的密钥处理装置，其特征在于，所述装置还包括第一加

密模块；

所述第一加密模块，用于在所述可信执行环境中获取个人识别密码的消息认证码；在所述可信执行环境中获取私有密钥；在所述可信执行环境中获取第一加密因子；在所述可信执行环境中利用所述私有密钥和所述第一加密因子对所述消息认证码进行加密得到第一派生密钥。

34、根据权利要求 32 所述的密钥处理装置，其特征在于，所述装置还包括第二加密模块；

所述第二加密模块，用于在所述可信执行环境中获取第一加密因子；在所述可信执行环境中获取私有密钥；在所述可信执行环境中利用所述私有密钥对所述第一加密因子进行加密得到第一派生密钥。

35、根据权利要求 31 至 34 中任一项所述的密钥处理装置，其特征在于，所述装置还包括文件加密模块；

所述文件加密模块，用于在所述普通运行环境中接收文件的处理指令；在所述普通运行环境中获取所述文件的密钥类型；在所述普通运行环境中获取所述密钥类型对应的密钥索引；在所述普通运行环境中获取初始向量；在所述普通运行环境中根据所述密钥索引和所述初始向量生成基于所述文件的处理请求；在所述普通运行环境中向所述存储控制器发送所述处理请求。

36、根据权利要求 35 所述的密钥处理装置，其特征在于：

所述文件加密模块，具体用于在所述普通运行环境中获取存储器中初始向量的密文；在所述普通运行环境中获取元数据密钥；在所述普通运行环境中利用所述元数据密钥对所述初始向量的密文进行解密得到所述初始向量。

37、根据权利要求 35 所述的密钥处理装置，其特征在于：

所述文件加密模块，还用于在所述普通运行环境中获取元数据密钥；在所述普通运行环境中利用所述元数据密钥对所述初始向量进行加密得到所述初始向量的密文；在所述普通运行环境中将所述初始向量的密文存储至存储器中。

38、根据权利要求 35 所述的密钥处理装置，其特征在于，所述装置还包括第二解密模块：

所述第二解密模块，用于在所述可信执行环境中对所述初始密钥进行解密处理得到元数据密钥；

所述发送模块，还用于在所述可信执行环境中将所述元数据密钥发送给所述普通运行环境中的文件加密模块。

39、根据权利要求 38 所述的密钥处理装置，其特征在于：

所述第二解密模块，具体用于在所述可信执行环境中利用第二派生密钥对初始密钥进行解密得到元数据密钥。

40、根据权利要求 39 所述的密钥处理装置，其特征在于，所述装置还包括第三加密模块；

所述第三加密模块，用于在所述可信执行环境中获取所述个人识别密码的消息认证码；在所述可信执行环境中获取所述私有密钥；在所述可信执行环境中获取第二加密因子；在所述可信执行环境中利用所述私有密钥和所述第二加密因子对所述消息认

证码进行加密得到第二派生密钥。

41、根据权利要求 39 所述的密钥处理装置，其特征在于，所述装置还包括第四加密模块；

所述第四加密模块，用于在所述可信执行环境中获取第二加密因子；在所述可信执行环境中获取所述私有密钥；在所述可信执行环境中利用所述私有密钥对所述第二加密因子进行加密得到第二派生密钥。

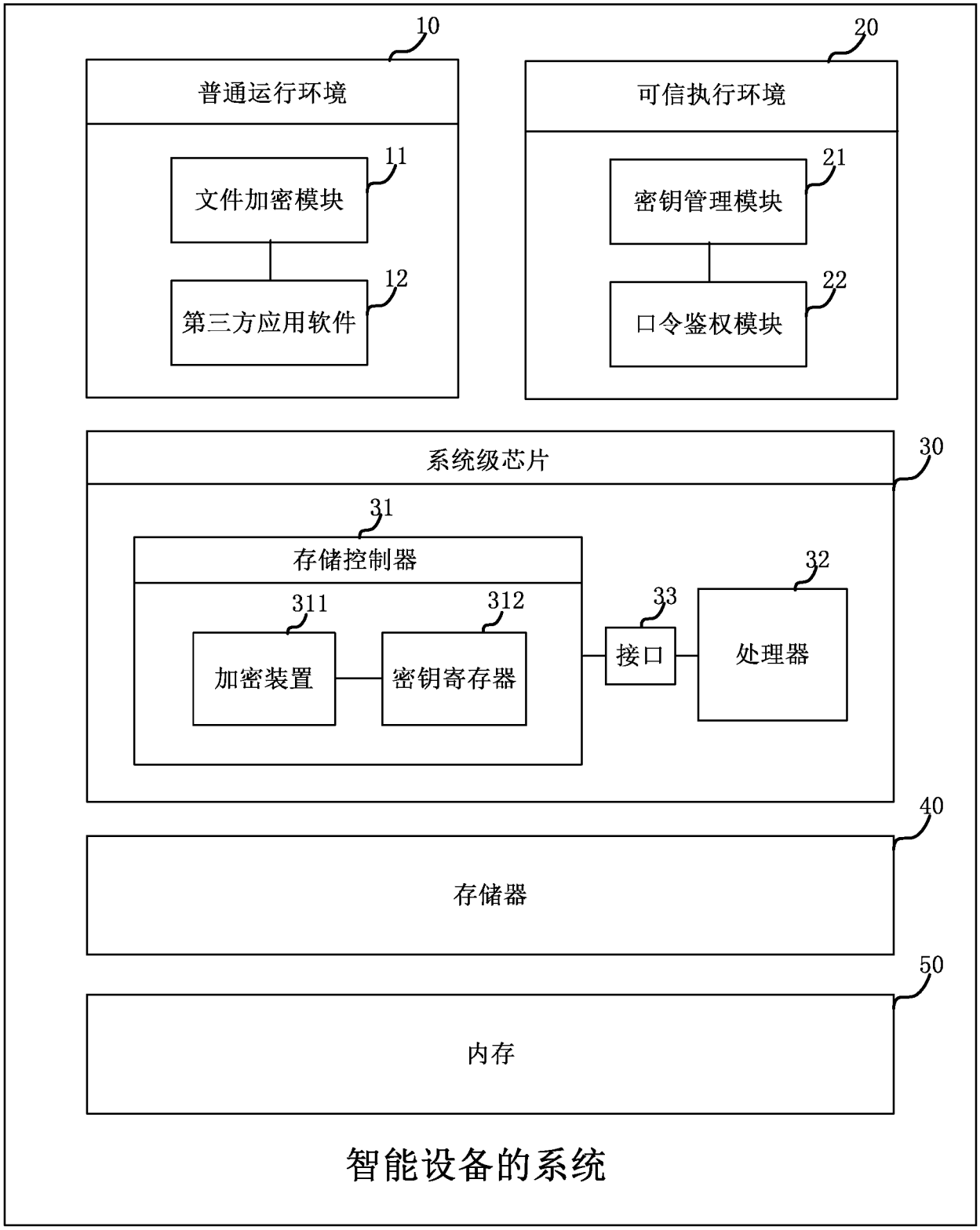

10
普通运行环境
11
文件加密模块
12
第三方应用软件
20
可信执行环境
21
密钥管理模块
22
口令鉴权模块
30
系统级芯片
31
存储控制器
311
加密装置
312
密钥寄存器
33
接口
32
处理器
40
存储器
50
内存
智能设备的系统

图 1

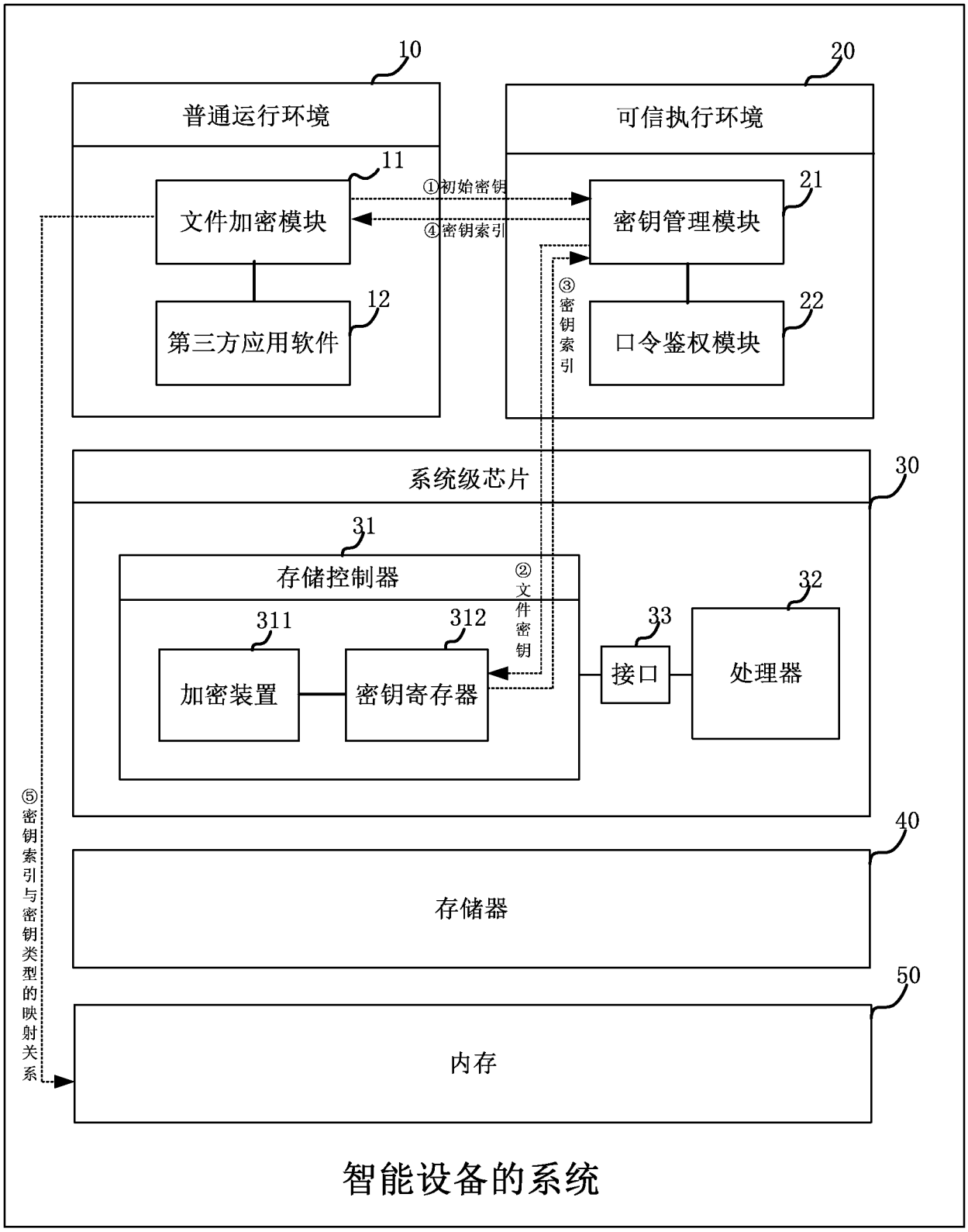

10
普通运行环境
11
文件加密模块
12
第三方应用软件
20
可信执行环境
21
密钥管理模块
22
口令鉴权模块
①初始密钥
④密钥索引
③密钥索引
系统级芯片
30
31
存储控制器
311
加密装置
312
密钥寄存器
②文件密钥
32
33
接口
处理器
⑤密钥索引与密钥类型的映射关系
40
存储器
50
内存
智能设备的系统

图 2A

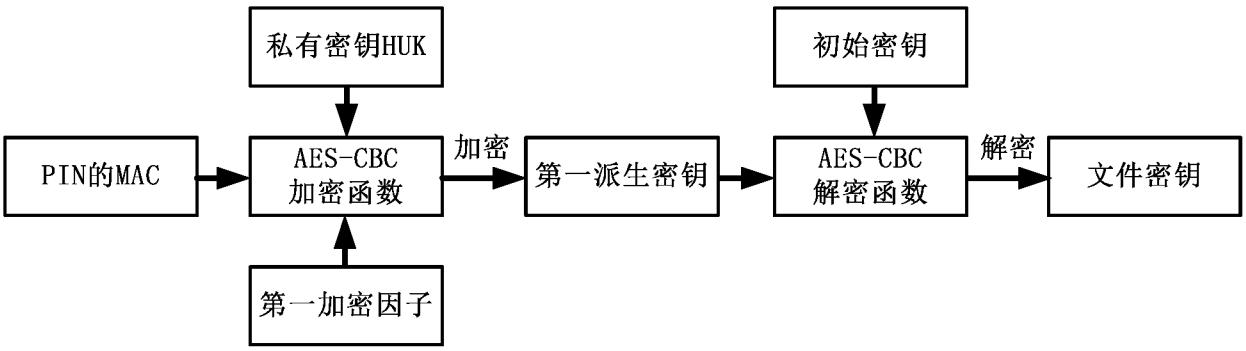


图 2B

图 2C

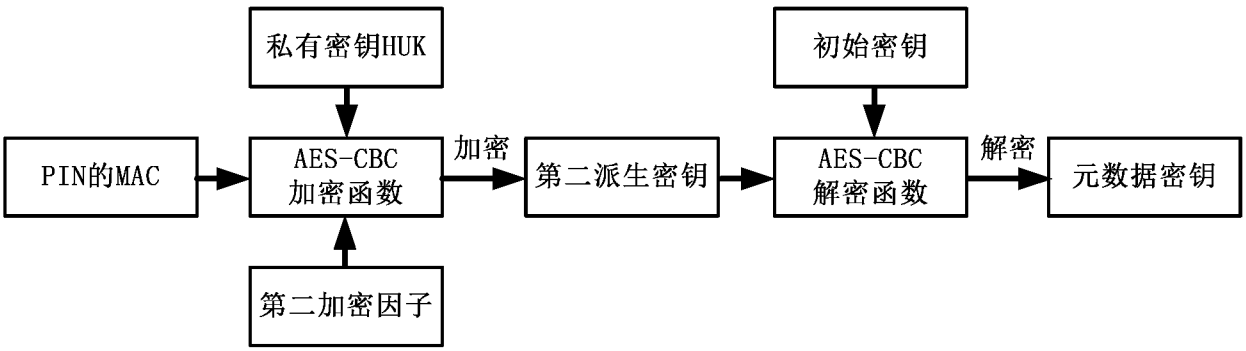


图 2D

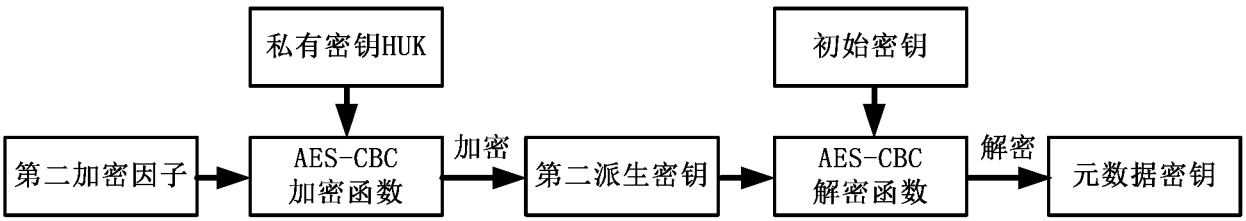


图 2E

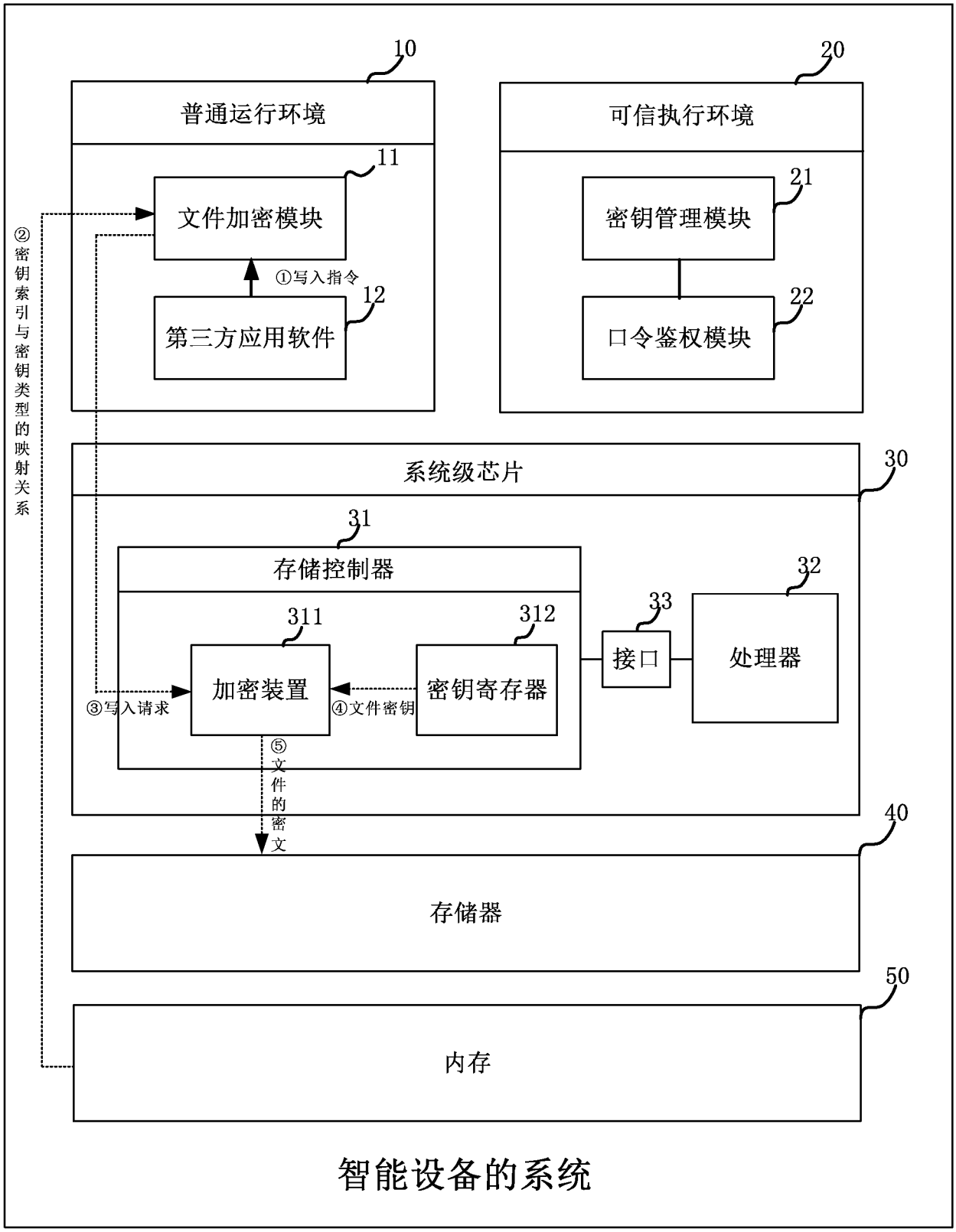

10
普通运行环境
11
文件加密模块
①写入指令
12
第三方应用软件
20
可信执行环境
21
密钥管理模块
22
口令鉴权模块
②密钥索引与密钥类型的映射关系
30
系统级芯片
31
存储控制器
311
加密装置
312
密钥寄存器
③写入请求
④文件密钥
⑤文件的密文
32
处理器
33
接口
40
存储器
50
内存
智能设备的系统

图 3A

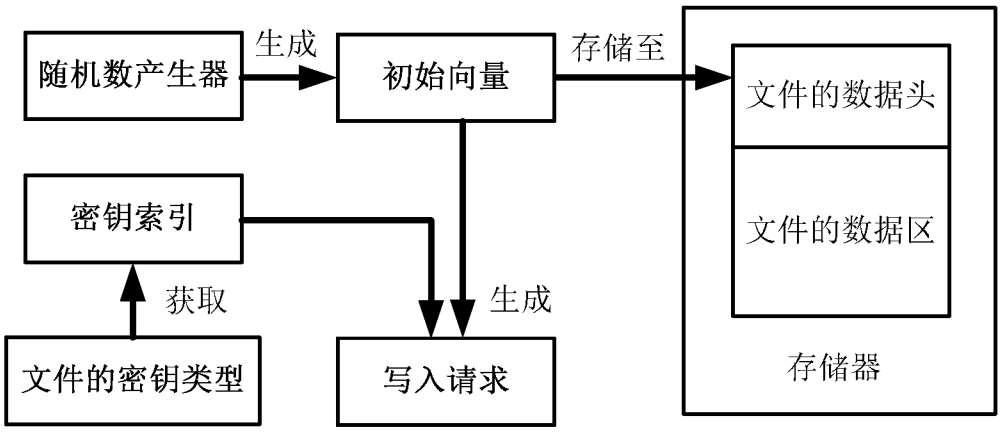

随机数产生器
生成
初始向量
存储至
文件的数据头
文件的数据区
存储器
密钥索引
获取
文件的密钥类型
生成
写入请求

图 3B

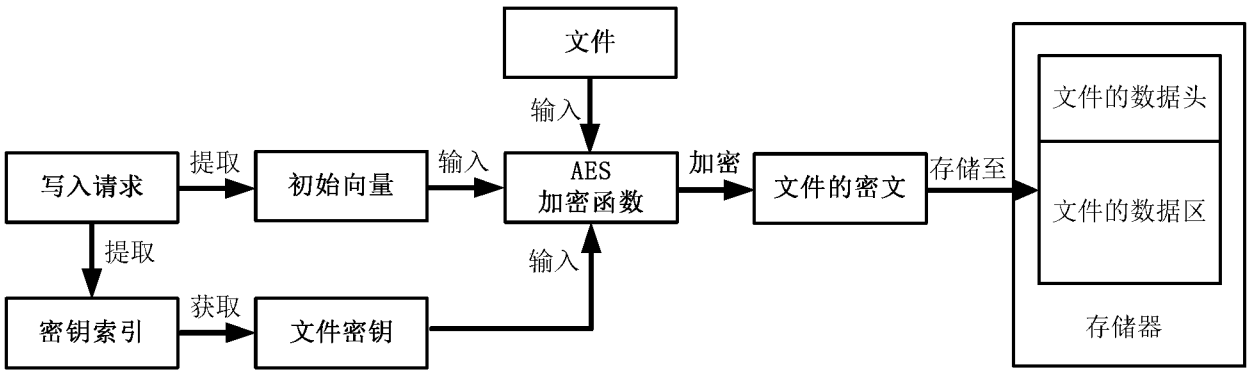

文件
输入
写入请求
提取
初始向量
输入
AES
加密函数
加密
文件的密文
存储至
文件的数据头
文件的数据区
存储器
提取
输入
密钥索引
获取
文件密钥

图 3C

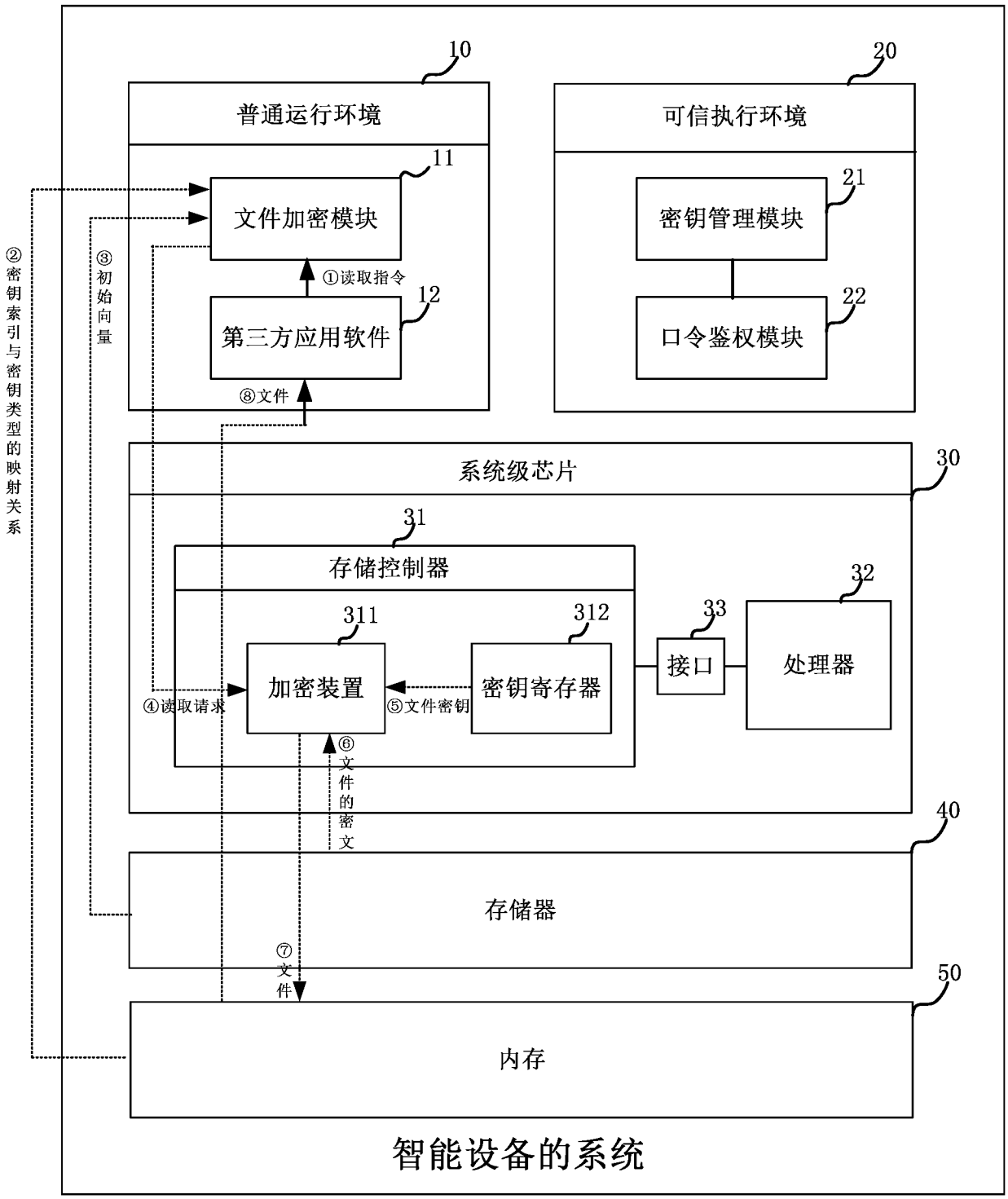

10
普通运行环境
20
可信执行环境
11
文件加密模块
21
密钥管理模块
①读取指令
12
第三方应用软件
22
口令鉴权模块
⑧文件
②密钥索引与密钥类型的映射关系
③初始向量
系统级芯片
30
31
存储控制器
32
311
312
33
加密装置
密钥寄存器
接口
处理器
④读取请求
⑤文件密钥
⑥文件的密文
40
存储器
⑦文件
50
内存
智能设备的系统

图 4A

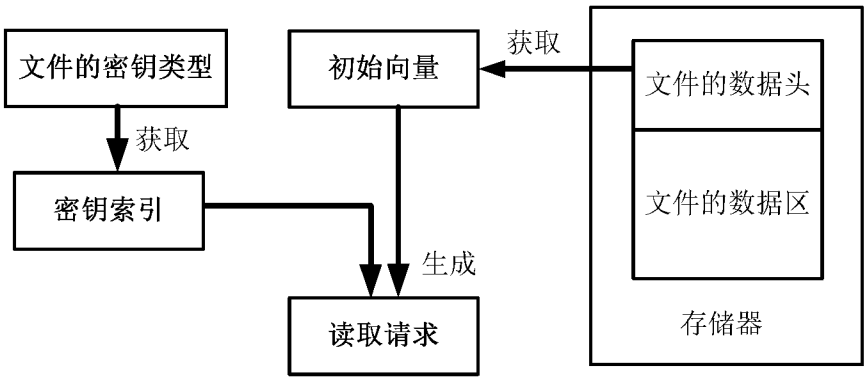

文件的密钥类型
获取
密钥索引
初始向量
获取
生成
读取请求
文件的数据头
文件的数据区
存储器

图 4B

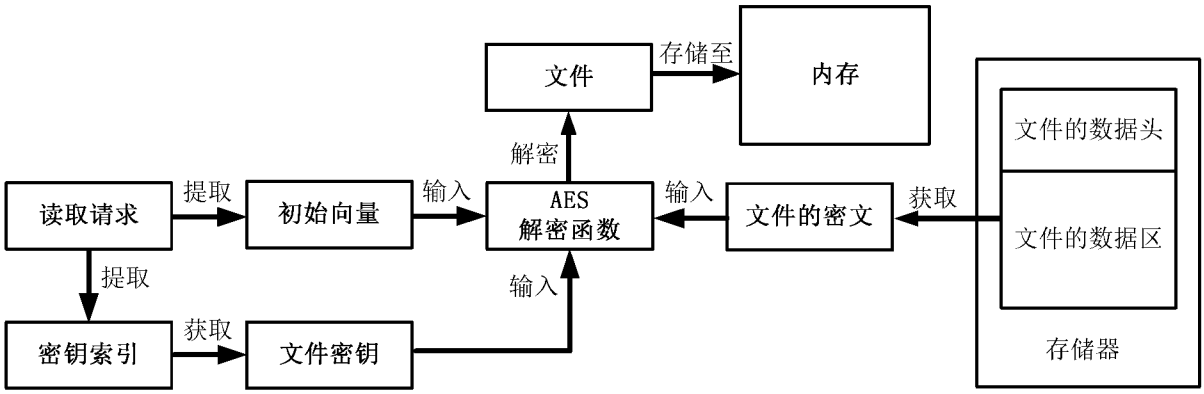

文件
存储至
内存
解密
读取请求
提取
初始向量
输入
AES
解密函数
输入
文件的密文
获取
文件的数据头
文件的数据区
存储器
提取
输入
密钥索引
获取
文件密钥

图 4C

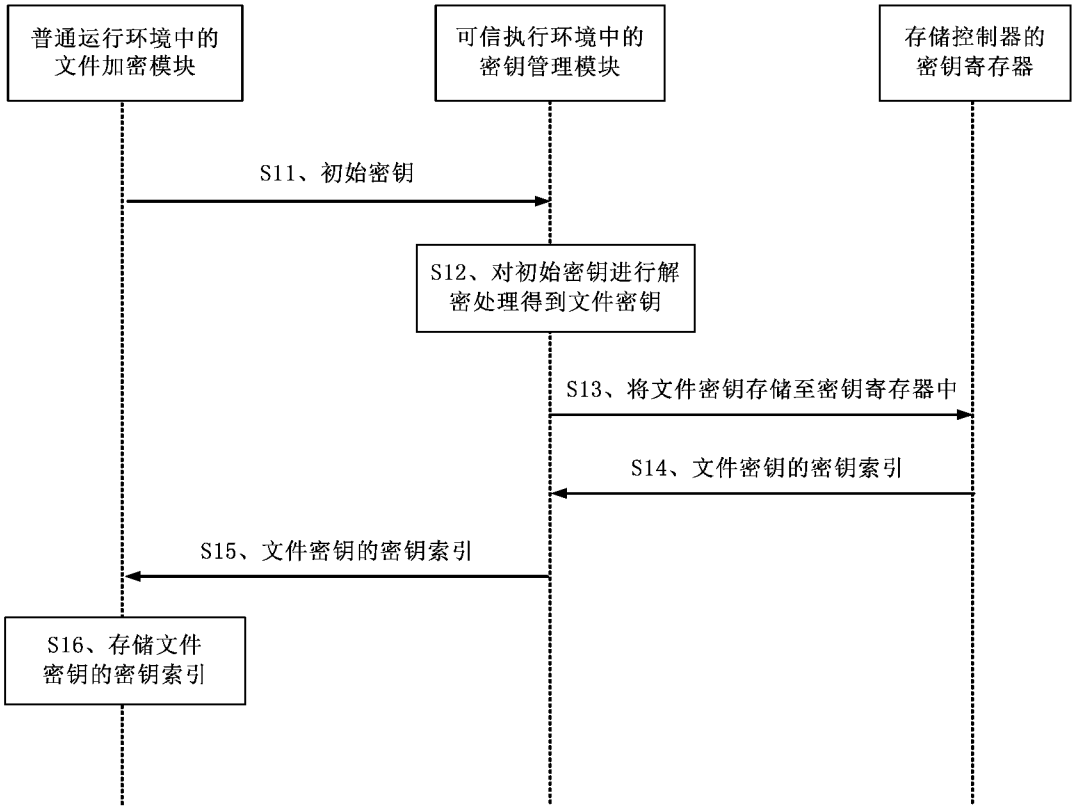

普通运行环境中的
文件加密模块
可信执行环境中的
密钥管理模块
存储控制器的
密钥寄存器
S11、初始密钥
S12、对初始密钥进行解
密处理得到文件密钥
S13、将文件密钥存储至密钥寄存器中
S14、文件密钥的密钥索引
S15、文件密钥的密钥索引
S16、存储文件
密钥的密钥索引

图 5

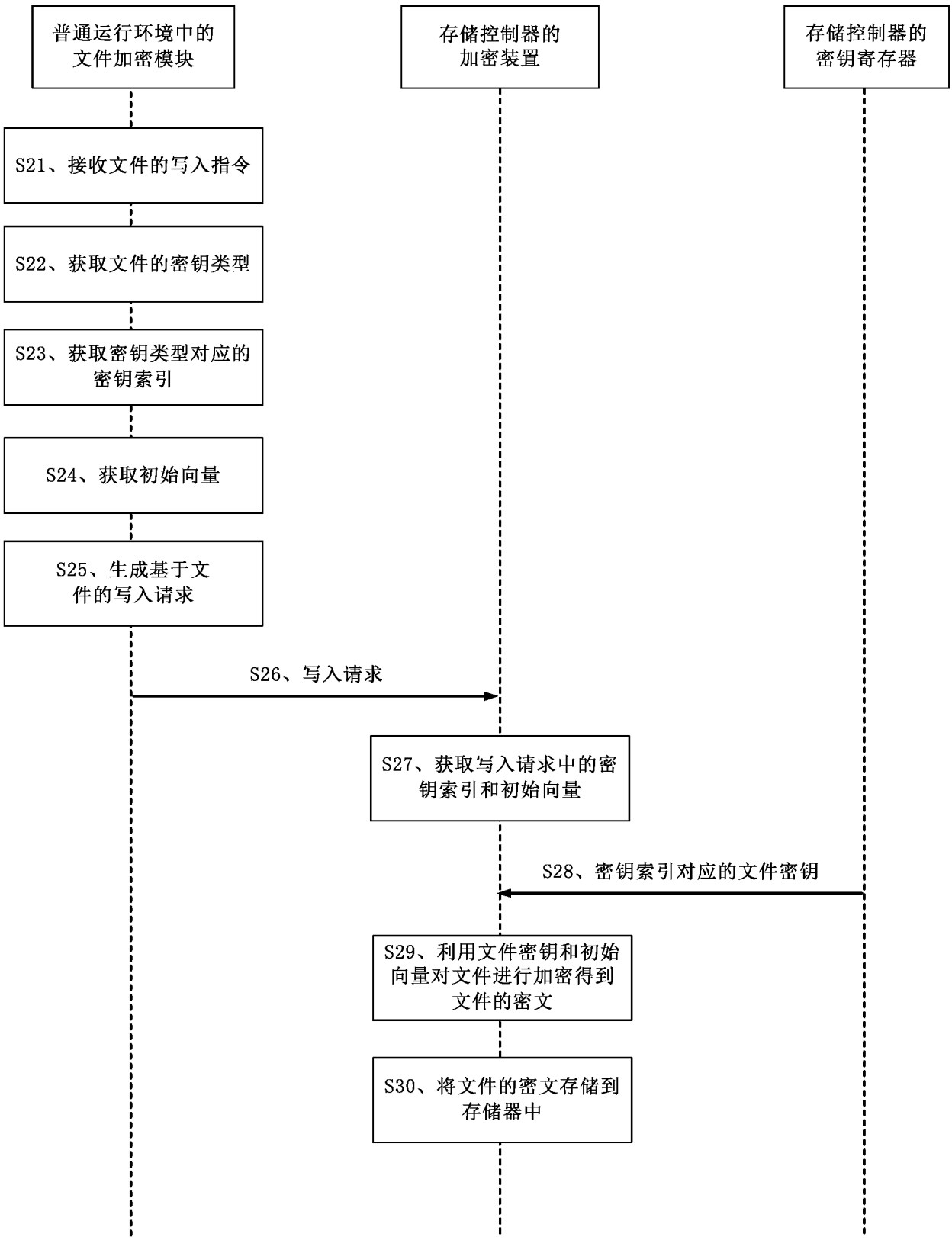

普通运行环境中的文件加密模块
存储控制器的加密装置
存储控制器的密钥寄存器
S21、接收文件的写入指令
S22、获取文件的密钥类型
S23、获取密钥类型对应的密钥索引
S24、获取初始向量
S25、生成基于文件的写入请求
S26、写入请求
S27、获取写入请求中的密钥索引和初始向量
S28、密钥索引对应的文件密钥
S29、利用文件密钥和初始向量对文件进行加密得到文件的密文
S30、将文件的密文存储到存储器中

图 6

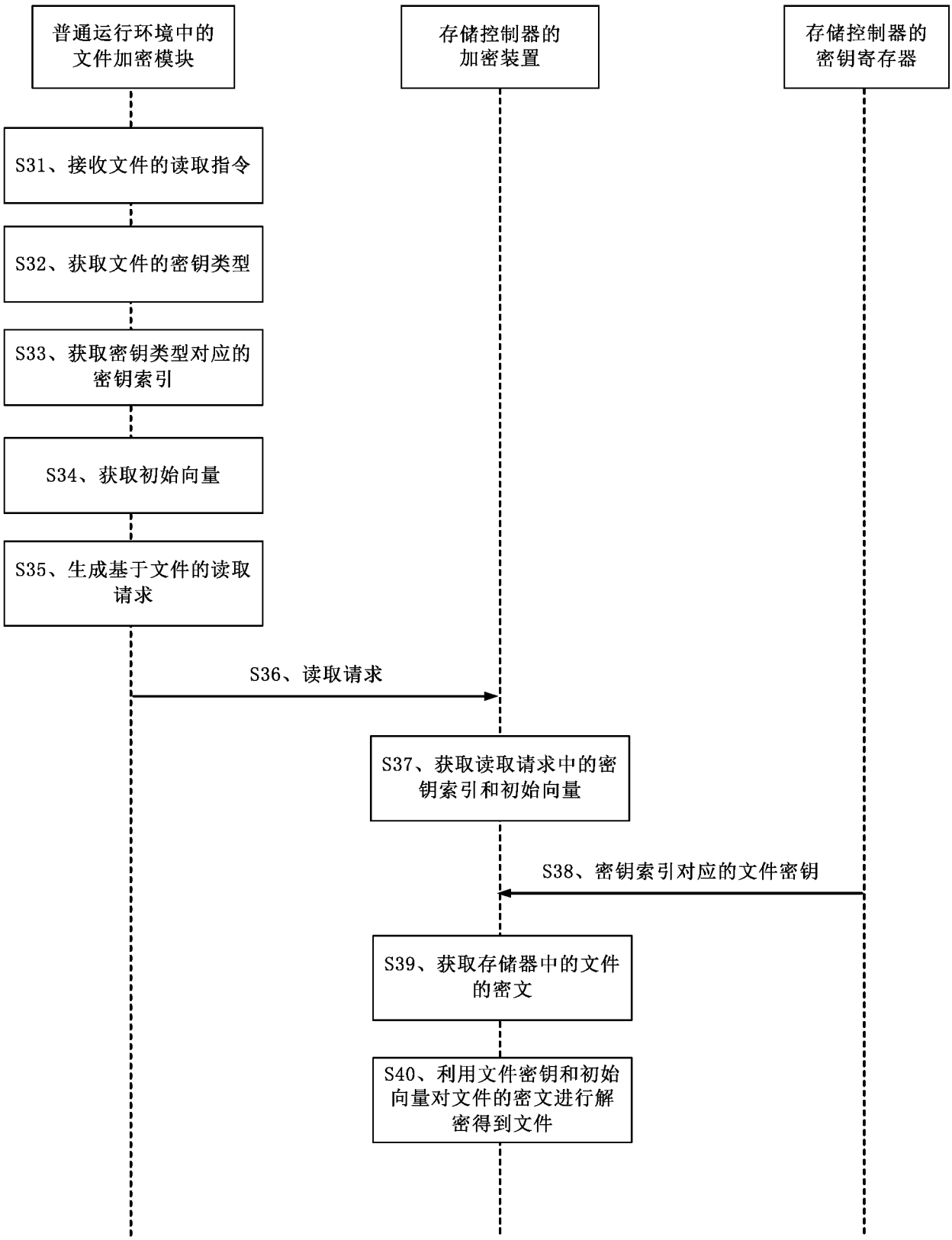

普通运行环境中的文件加密模块
存储控制器的加密装置
存储控制器的密钥寄存器
S31、接收文件的读取指令
S32、获取文件的密钥类型
S33、获取密钥类型对应的密钥索引
S34、获取初始向量
S35、生成基于文件的读取请求
S36、读取请求
S37、获取读取请求中的密钥索引和初始向量
S38、密钥索引对应的文件密钥
S39、获取存储器中的文件的密文
S40、利用文件密钥和初始向量对文件的密文进行解密得到文件

图 7

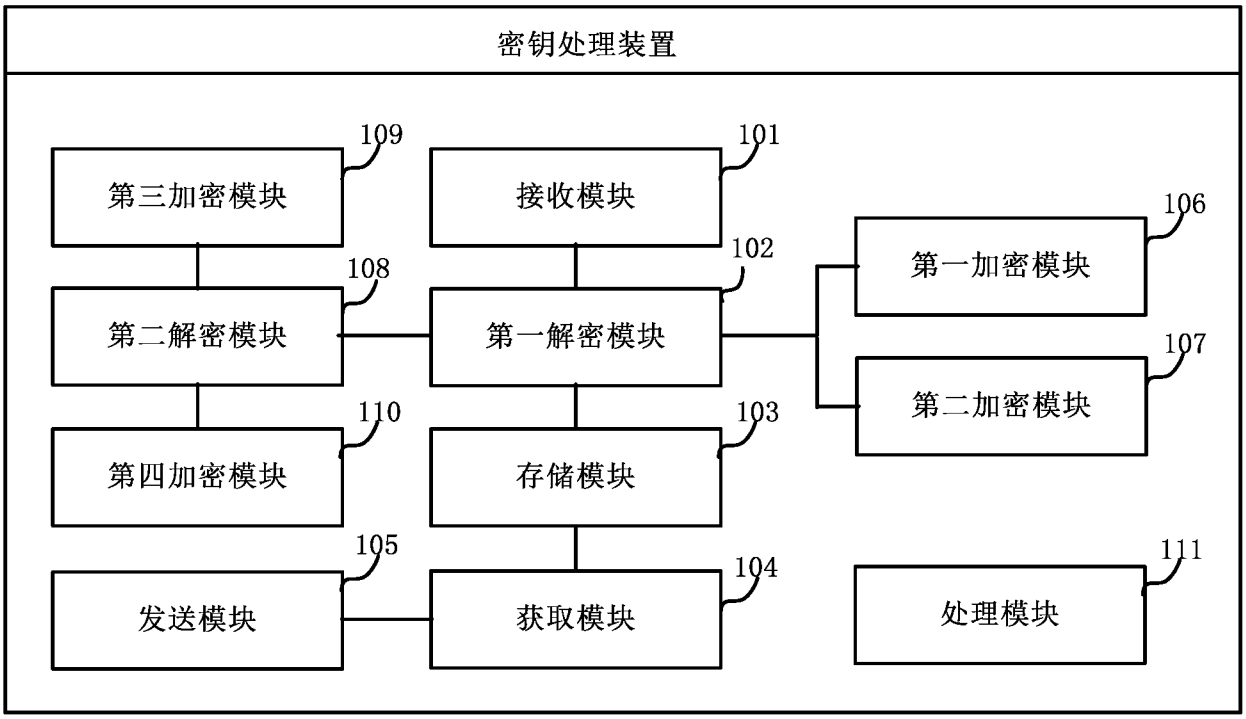

密钥处理装置
109
第三加密模块
101
接收模块
106
第一加密模块
108
第二解密模块
102
第一解密模块
107
第二加密模块
110
第四加密模块
103
存储模块
105
发送模块
104
获取模块
111
处理模块

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/091282

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC: 密钥, 可信执行环境, 加密, 解密, 禁止, 隔离, 索引, 密文, 密码, 保护, TEE, REE, Trust Execution Environment, Secure Storage, key, cryptographic, encryption, protect+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 108155986 A (AMLOGIC (SHANGHAI), INC.) 12 June 2018 (2018-06-12) description, paragraphs 0036-0064	1-41
Y	CN 105812332 A (BEIJING WATCHDATA TECHNOLOGIES CO., LTD.) 27 July 2016 (2016-07-27) description, paragraphs 0046-0055	1-41
A	CN 107851161 A (INTEL CORPORATION) 27 March 2018 (2018-03-27) entire document	1-41
A	US 2017005790 A1 (ACTIVEVIDEO NETWORKS INC.) 05 January 2017 (2017-01-05) entire document	1-41
A	US 2017331628 A1 (BLACKBERRY LIMITED) 16 November 2017 (2017-11-16) entire document	1-41

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 January 2019	**31 January 2019**

Name and mailing address of the ISA/CN	Authorized officer
National Intellectual Property Administration, PRC (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/091282

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	108155986	A	12 June 2018	None			
CN	105812332	A	27 July 2016	None			
CN	107851161	A	27 March 2018	EP	3326102	A1	30 May 2018
				WO	2017014885	A1	26 January 2017
				US	2017026171	A1	26 January 2017
US	2017005790	A1	05 January 2017	WO	2017004447	A1	05 January 2017
US	2017331628	A1	16 November 2017	None			

国际检索报告

国际申请号
PCT/CN2018/091282

A. 主题的分类

H04L 9/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W H04L H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNKI，CNPAT，WPI，EPODOC：密钥，可信执行环境，加密，解密，禁止，隔离，索引，密文，密码，保护，TEE，REE，Trust Execution Environment，Secure Storage，key，cryptographic，encryption，protect+

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
Y	CN 108155986 A (晶晨半导体上海股份有限公司) 2018年 6月 12日 (2018-06-12) 说明书0036-0064段	1-41
Y	CN 105812332 A (北京握奇智能科技有限公司) 2016年 7月 27日 (2016-07-27) 说明书0046-0055段	1-41
A	CN 107851161 A (英特尔公司) 2018年 3月 27日 (2018-03-27) 全文	1-41
A	US 2017005790 A1 (ACTIVEVIDEO NETWORKS INC.) 2017年 1月 5日 (2017-01-05) 全文	1-41
A	US 2017331628 A1 (BLACKBERRY LIMITED) 2017年 11月 16日 (2017-11-16) 全文	1-41

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 1月 6日	2019年 1月 31日

ISA/CN的名称和邮寄地址	受权官员
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	柴华
传真号 (86-10)62019451	电话号码 86-(10)-53961630

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/091282

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	108155986	A	2018年 6月 12日	无			
CN	105812332	A	2016年 7月 27日	无			
CN	107851161	A	2018年 3月 27日	EP	3326102	A1	2018年 5月 30日
				WO	2017014885	A1	2017年 1月 26日
				US	2017026171	A1	2017年 1月 26日
US	2017005790	A1	2017年 1月 5日	WO	2017004447	A1	2017年 1月 5日
US	2017331628	A1	2017年 11月 16日	无			