(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109768853 A
(43)申请公布日 2019.05.17

(21)申请号 201811654834.9

(22)申请日 2018.12.29

(71)申请人 百富计算机技术(深圳)有限公司
地址 518057 广东省深圳市南山区高新区科技中二路软件园3栋401、402

(72)发明人 董时舫

(74)专利代理机构 深圳中一联合知识产权代理有限公司 44414
代理人 李艳丽

(51)Int.Cl.
H04L 9/06(2006.01)
G06F 11/14(2006.01)

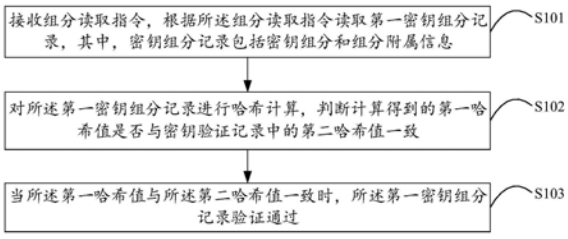
权利要求书2页 说明书10页 附图2页

(54)发明名称

一种密钥组分验证方法、装置及终端设备

(57)摘要

本申请适用于数据处理技术领域，提供了一种密钥组分验证方法、装置及终端设备，所述方法包括：接收组分读取指令，根据所述组分读取指令读取第一密钥组分记录，其中，密钥组分记录包括密钥组分和组分附属信息；对所述第一密钥组分记录进行哈希计算，判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致；当所述第一哈希值与所述第二哈希值一致时，所述第一密钥组分记录验证通过。可以解决现有的密钥组分验证算法通用性差，无法保证系统种子密钥实现安全备份存储与准确恢复的问题。



CN 109768853 A

1.一种密钥组分验证方法,其特征在于,包括:

接收组分读取指令,根据所述组分读取指令读取第一密钥组分记录,其中,密钥组分记录包括密钥组分和组分附属信息;

对所述第一密钥组分记录进行哈希计算,判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致;

当所述第一哈希值与所述第二哈希值一致时,所述第一密钥组分记录验证通过。

2.如权利要求1所述的密钥组分验证方法,其特征在于,所述方法还包括:

将各个第一密钥组分记录中的密钥组分以预设的合成公式进行合成,得到第一密钥原文;

以所述第一密钥原文和所述第一密钥原文对应的原文附属信息作为第一密钥原文记录;

对所述第一密钥原文记录进行哈希计算,判断计算得到的第三哈希值是否与所述密钥验证记录中的第四哈希值一致;

当所述第三哈希值与所述第四哈希值一致时,所述第一密钥原文记录验证通过。

3.如权利要求1所述的密钥组分验证方法,其特征在于,在所述对所述第一密钥组分记录进行哈希计算之前还包括:

接收密钥验证记录读取指令,根据所述密钥验证读取指令读取密钥验证记录,其中,所述密钥验证记录包括组分附属信息、第二哈希值和第四哈希值;

判断所述密钥验证记录是否符合预设格式要求;

对应地,所述对所述第一密钥组分记录进行哈希计算具体为:

当所述密钥验证记录符合所述预设格式要求时,对所述第一密钥组分记录进行哈希计算。

4.如权利要求3所述的密钥组分验证方法,其特征在于,所述当所述密钥验证记录符合所述预设格式要求时,对所述第一密钥组分记录进行哈希计算具体包括:

当所述密钥验证记录符合所述预设格式要求时,判断所述第一密钥组分记录中的组分附属信息是否与所述密钥验证记录中对应的组分附属信息一致;

当所述第一密钥组分记录中的组分附属信息与所述密钥验证记录中对应的组分附属信息一致时,对所述第一密钥组分记录进行哈希计算。

5.如权利要求1所述的密钥组分验证方法,其特征在于,所述第二哈希值的计算方法如下:

在密钥备份的过程中,以待备份的密钥组分和所述待备份的密钥组分对应的组分附属信息作为第二密钥组分记录;

对所述第二密钥组分记录进行哈希计算,得到所述第二哈希值。

6.如权利要求5所述的密钥组分验证方法,其特征在于,所述第四哈希值的计算方法如下:

在密钥备份的过程中,以待计算的密钥原文和所述待计算的密钥原文对应的原文附属信息作为第二密钥原文记录;

对所述第二密钥原文记录进行哈希计算,得到所述第四哈希值。

7.一种密钥组分验证装置,其特征在于,包括:

组分记录模块，用于接收组分读取指令，根据所述组分读取指令读取第一密钥组分记录，其中，密钥组分记录包括密钥组分和组分附属信息；

第一验证模块，用于对所述第一密钥组分记录进行哈希计算，判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致；

组分通过模块，用于当所述第一哈希值与所述第二哈希值一致时，所述第一密钥组分记录验证通过。

8.如权利要求7所述的密钥组分验证装置，其特征在于，所述装置还包括：

原文合成模块，用于将各个第一密钥组分记录中的密钥组分以预设的合成公式进行合成，得到第一密钥原文；

原文记录模块，用于以所述第一密钥原文和所述第一密钥原文对应的原文附属信息作为第一密钥原文记录；

第二验证模块，用于对所述第一密钥原文记录进行哈希计算，判断计算得到的第三哈希值是否与所述密钥验证记录中的第四哈希值一致；

原文通过模块，用于当所述第三哈希值与所述第四哈希值一致时，所述第一密钥原文记录验证通过。

9.一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述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计算机程序时实现如权利要求1至6任一项所述方法的步骤。

10.一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至6任一项所述方法的步骤。

一种密钥组分验证方法、装置及终端设备

技术领域

[0001] 本申请属于数据处理技术领域，尤其涉及一种密钥组分验证方法、装置及终端设备。

背景技术

[0002] 随着加密技术的发展，密钥逐渐被应用于加密各种需要加密的文件。在一个密钥系统中，可以通过系统种子密钥发散生成其他密钥，使得系统中的各终端设备既能满足密钥唯一性的要求，又能节省密钥存储空间。

[0003] 安全房内的密钥管理主机系统可能会遭受意外故障或断电以及自然灾害等外界因素的破坏，从而导致系统种子密钥损毁，因此，必须对系统种子密钥进行备份。在系统恢复过程中，可以从备份的媒介中恢复系统种子密钥。

[0004] 密钥组分是一种常见的密钥备份方式，一个密钥可以含有两个或两个以上的密钥组分，各个密钥组分长度可以相同，也可以不同，各个密钥组分按约定的合成公式生成密钥，因此，在备份过程中，可以将密钥组分交由不同的专职人员进行管理，当需要还原密钥时，获取各个密钥组分之后按约定的合成公式还原密钥。

[0005] 但是，密钥组分在理论上存在出错(例如个别密钥组分的数据出现误码)、误用(例如组分不匹配、版本不匹配、超过有效期等)、伪造、被恶意篡改或被秘密替换的可能，为了确保还原的密钥是正确的，需要对密钥组分进行验证。

[0006] 常规的密钥组分验证算法是采用验证密钥对受验证的密钥组分计算出一串验证码，但是，这种验证方式的通用性差，当受验证的密钥组分是系统种子密钥的密钥组分时，难以再创建一个验证密钥用于验证计算。

[0007] 综上，现有的密钥组分验证算法通用性差，无法保证系统种子密钥实现安全备份存储与准确恢复。

发明内容

[0008] 有鉴于此，本申请实施例提供了一种密钥组分验证方法、装置及终端设备，以解决现有的密钥组分验证算法通用性差，无法保证系统种子密钥实现安全备份存储与准确恢复的问题。

[0009] 本申请实施例的第一方面提供了一种密钥组分验证方法，包括：

[0010] 接收组分读取指令，根据所述组分读取指令读取第一密钥组分记录，其中，密钥组分记录包括密钥组分和组分附属信息；

[0011] 对所述第一密钥组分记录进行哈希计算，判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致；

[0012] 当所述第一哈希值与所述第二哈希值一致时，所述第一密钥组分记录验证通过。

[0013] 本申请实施例的第二方面提供了一种密钥组分验证装置，包括：

[0014] 组分记录模块，用于接收组分读取指令，根据所述组分读取指令读取第一密钥组

分记录，其中，密钥组分记录包括密钥组分和组分附属信息；

[0015] 第一验证模块，用于对所述第一密钥组分记录进行哈希计算，判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致；

[0016] 组分通过模块，用于当所述第一哈希值与所述第二哈希值一致时，所述第一密钥组分记录验证通过。

[0017] 本申请实施例的第三方面提供了一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现如上述方法的步骤。

[0018] 本申请实施例的第四方面提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现如上述方法的步骤。

[0019] 本申请实施例与现有技术相比存在的有益效果是：

[0020] 本申请的密钥组分验证方法中，对第一密钥组分记录进行哈希计算，判断哈希计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致，由于在哈希计算中，即使被计算的值发生微小变动，也会使哈希计算的结果产生极大的偏差，因此，当第一哈希值与第二哈希值一致时，可以确定第一密钥组分记录为可靠的记录，第一密钥组分记录验证通过，在密钥组分记录验证中，不需要额外生成验证密钥，可以对任何密钥的密钥组分进行验证，通用性高，解决了现有的密钥组分验证算法通用性差，无法保证系统种子密钥实现安全备份存储与准确恢复的问题。

附图说明

[0021] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0022] 图1是本申请实施例提供的一种密钥组分验证方法的实现流程示意图；

[0023] 图2是本申请实施例提供的一种密钥组分验证装置的示意图；

[0024] 图3是本申请实施例提供的终端设备的示意图。

具体实施方式

[0025] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0026] 为了说明本申请所述的技术方案，下面通过具体实施例来进行说明。

[0027] 应当理解，当在本说明书和所附权利要求书中使用时，术语“包括”指示所描述特征、整体、步骤、操作、元素和/或组件的存在，但并不排除一个或多个其它特征、整体、步骤、操作、元素、组件和/或其集合的存在或添加。

[0028] 还应当理解，在此本申请说明书中所使用的术语仅仅是出于描述特定实施例的目的而并不意在限制本申请。如在本申请说明书和所附权利要求书中所使用的那样，除非上

下文清楚地指明其它情况，否则单数形式的“一”、“一个”及“该”意在包括复数形式。

[0029] 还应当进一步理解，在本申请说明书和所附权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合，并且包括这些组合。

[0030] 如在本说明书和所附权利要求书中所使用的那样，术语“如果”可以依据上下文被解释为“当...时”或“一旦”或“响应于确定”或“响应于检测到”。类似地，短语“如果确定”或“如果检测到[所描述条件或事件]”可以依据上下文被解释为意指“一旦确定”或“响应于确定”或“一旦检测到[所描述条件或事件]”或“响应于检测到[所描述条件或事件]”。

[0031] 另外，在本申请的描述中，术语“第一”、“第二”、“第三”等仅用于区分描述，而不能理解为指示或暗示相对重要性。

[0032] 实施例一：

[0033] 下面对本申请实施例一提供的一种密钥组分验证方法进行描述，请参阅附图1，本申请实施例一中的密钥组分验证方法包括：

[0034] 步骤S101、接收组分读取指令，根据所述组分读取指令读取第一密钥组分记录，其中，密钥组分记录包括密钥组分和组分附属信息；

[0035] 当需要进行密钥还原时，可以根据组分读取指令从安全存储介质读取待还原密钥的密钥组分，根据待还原密钥的密钥组分以预设的合成公式进行合成，可以得到待还原密钥的密钥原文。但是，由于密钥组分在存储过程中存在出错、误用、伪造、篡改和替换的可能，因此，为了保证还原的密钥原文的可靠性，需要对待还原密钥的密钥组分记录进行验证。

[0036] 此时，可以先根据所述组分读取指令读取第一密钥组分记录，密钥组分记录包括密钥组分和组分附属信息，其中，组分附属信息可以根据实际需要进行设置，组分附属信息可以设置为空，即密钥组分记录中只包含密钥组分，组分附属信息也可以不为空，根据需要记录的数据设置对应的组分附属信息，例如，组分附属信息可以包括密钥版本号、密钥生成时间、密钥有效期、密钥名称、密钥原文合成公式、组分编号、组分长度和填充的随机数。

[0037] 步骤S102、对所述第一密钥组分记录进行哈希计算，判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致；

[0038] 密钥验证记录所记录的内容可以根据实际需要进行设置，例如，密钥验证记录可以包括密钥版本号、密钥生成时间、密钥有效期、密钥名称、密钥原文合成公式、各密钥组分记录对应的组分长度、各密钥组分记录对应的第二哈希值、密钥原文记录对应的第四哈希值。

[0039] 第二哈希值为在生成密钥验证记录时，对第二密钥组分记录进行哈希计算得到的哈希值，第二哈希值可以在密钥还原的过程中对第一密钥组分记录进行验证。

[0040] 对第一密钥组分记录进行哈希计算，由于哈希计算过程中，即使被计算的值发生微小变动，也会使哈希计算的结果产生极大的偏差，因此，可以通过判断第一哈希值与第二哈希值是否一致来判断第一密钥组分记录是否可靠。

[0041] 哈希计算的算法可以根据实际情况进行设置，例如可以选用SHA256算法，SHA256算法是安全散列算法SHA(Secure Hash Algorithm)系列算法之一，其摘要长度为256bits，即32个字节，主要适用于数字签名，是数字签名标准里面定义的数字签名算法，该算法可以根据一段输入数据来生成另一固定长度的、小数据片段，原本很规整的输入数据，经过运算

后，得到的结果数据变得面目全非、散乱不堪，因此被称为散列算法。

[0042] 步骤S103、当所述第一哈希值与所述第二哈希值一致时，所述第一密钥组分记录验证通过。

[0043] 当第一哈希值与第二哈希值一致时，表示第一密钥组分记录并未出错或被篡改，该密钥组分记录是可靠的，第一密钥组分记录验证通过。

[0044] 当第一哈希值与第二哈希值不一致时，表示第一密钥组分记录存在出错的可能性，此时该密钥组分记录是不可靠的，第一密钥组分记录验证失败。

[0045] 进一步地，所述方法还包括：

[0046] A1、将各个第一密钥组分记录中的密钥组分以预设的合成公式进行合成，得到第一密钥原文；

[0047] 在对各个第一密钥组分记录进行验证之后，还可以将各个第一密钥组分记录的密钥组分以预设的合成进行合成，得到第一密钥原文，对第一密钥原文的可靠性进行验证。

[0048] A2、以所述第一密钥原文和所述第一密钥原文对应的原文附属信息作为第一密钥原文记录；

[0049] 第一密钥原文记录可以包括第一密钥原文和第一密钥原文对应的原文附属信息，其中，原文附属信息可以根据实际需要进行设置，原文附属信息可以设置为空，即密钥原文记录中只包含密钥原文，原文附属信息也可以不为空，根据需要记录的数据设置对应的原文附属信息，例如，原文附属信息可以包括密钥版本号、密钥生成时间、密钥有效期、密钥名称、密钥原文合成公式、组分编号数组和组分长度数组，其中，组分编号数组包括各个密钥组分的组分编号，组分长度数组包括各个密钥组分的组分长度。

[0050] A3、对所述第一密钥原文记录进行哈希计算，判断计算得到的第三哈希值是否与所述密钥验证记录中的第四哈希值一致；

[0051] 第四哈希值为生成密钥验证记录时，对第二密钥原文记录进行哈希计算得到的哈希值，第四哈希值可以在密钥还原的过程中对第一密钥原文记录进行验证。

[0052] A4、当所述第三哈希值与所述第四哈希值一致时，所述第一密钥原文记录验证通过。

[0053] 由于在密钥还原的过程中，保管员需要将各个第一密钥组分记录中密钥组分以预设的合成公式进行合成得到第一密钥原文，其中，有可能各个第一密钥组分记录均为可靠的密钥组分记录，但是可能出现保管员拿错了不同版本的密钥组分记录、拿到了重复的密钥组分记录或拿到了其他密钥的密钥组分记录等情况，导致虽然单个第一密钥组分记录验证均可通过，但是根据各个第一密钥组分记录合成的第一密钥原文为错误的密钥原文，例如，一个待还原的密钥由密钥组分记录1和密钥组分记录2合成，在还原密钥时，保管员A读取了密钥组分记录1，保管员B也读取了密钥组分记录1，虽然单个密钥组分记录1可以验证通过，但是两个密钥组分记录1无法合成正确的密钥原文，因此，需要对密钥原文记录的可靠性进行验证，确保密钥原文的正确性、完备性、有效性和合法性。

[0054] 当第三哈希值与第四哈希值一致时，表示第一密钥原文记录是可靠的，第一密钥原文记录中的第一密钥原文即是所需还原的密钥。

[0055] 当第三哈希值与第四哈希值不一致时，表示用于合成第一密钥原文的第一密钥组分记录存在偏差，需要查验合成第一密钥原文的第一密钥组分记录是否为正确的密钥组分

记录。

[0056] 进一步地，在所述对所述第一密钥组分记录进行哈希计算之前还包括：

[0057] B1、接收密钥验证记录读取指令，根据所述密钥验证读取指令读取密钥验证记录，其中，所述密钥验证记录包括组分附属信息、第二哈希值和第四哈希值；

[0058] B2、判断所述密钥验证记录是否符合预设格式要求；

[0059] 在对第一密钥组分记录进行哈希计算之前，可以先对密钥验证记录的格式进行检验，判断密钥验证记录是否符合预设格式要求。

[0060] 对应地，所述对所述第一密钥组分记录进行哈希计算具体为：

[0061] 当所述密钥验证记录符合所述预设格式要求时，对所述第一密钥组分记录进行哈希计算。

[0062] 当密钥验证记录符合预设格式要求时，则进行第一密钥组分记录的验证，对第一密钥组分记录进行哈希计算。当密钥验证记录中存在任意字段不符合预设格式要求，包含无效字符时，则中止对密钥组分记录的验证，报告“验证记录无效”给工作人员。

[0063] 进一步地，所述当所述密钥验证记录符合所述预设格式要求时，对所述第一密钥组分记录进行哈希计算具体包括：

[0064] C1、当所述密钥验证记录符合所述预设格式要求时，判断所述第一密钥组分记录中的组分附属信息是否与所述密钥验证记录中对应的组分附属信息一致；

[0065] 除了验证密钥验证记录的格式之外，还可以对第一密钥组分记录中的组分附属信息进行验证，判断第一密钥组分记录中的组分附属信息是否与密钥验证记录中对应的组分附属信息一致。

[0066] C2、当所述第一密钥组分记录中的组分附属信息与所述密钥验证记录中对应的组分附属信息一致时，对所述第一密钥组分记录进行哈希计算。

[0067] 当第一密钥组分记录中的组分附属信息与密钥验证记录中对应的组分附属信息一致时，可以继续进行第一密钥组分记录的验证，对第一密钥组分记录进行哈希计算。当第一密钥组分记录中的组分附属信息与密钥验证记录中对应的组分附属信息不一致时，则中止对第一密钥组分记录的验证，报告对应的验证出错信息给工作人员，例如，在读取第一密钥组分记录的组分附属信息时，可以将第一密钥组分记录中的密钥版本号、密钥生成时间、密钥有效期、密钥名称、密钥原文合成公式等字段与密钥验证记录中的同一字段逐一进行比较，若不一致，则报告“封装信息验证失败”并中止读取过程；然后核实组分编号字段，核实其是否属于密钥验证记录中组分编号数组中的一员，若不属于(例如第一密钥组分记录中的组分编号为2，密钥验证记录中的组分编号数组内记录的编号为一、二、三…)，则报告“组分编号验证失败”并中止读取过程；然后核实第一密钥组分记录中的组分长度是否与密钥验证记录中对应的组分长度一致，若不一致，则报告“组分长度验证失败”并中止读取过程。

[0068] 进一步地，所述第一哈希值的计算方法如下：

[0069] D1、在密钥备份的过程中，以待备份的密钥组分和所述待备份的密钥组分对应的组分附属信息作为第二密钥组分记录；

[0070] 在密钥备份的过程中，以待备份的密钥组分和待备份的密钥组分对应的组分附属信息作为第二密钥组分记录，第二密钥组分记录可以保存在不同的安全存储介质中，每一

个安全存储介质交给不同的密钥组分保管员进行保管，安全存储介质可以根据实际需要进行选择，例如可以选择IC卡、U盾等。

[0071] D2、对所述第二密钥组分记录进行哈希计算，得到所述第二哈希值。

[0072] 对第二密钥组分记录进行哈希计算，可以得到第二哈希值，第二哈希值可以保存在密钥验证记录中，用于在密钥还原的过程对第一密钥组分记录进行验证，密钥验证记录可以单独保存在另外的安全存储介质中，并将该安全存储介质交给密钥验证管理员进行保管。

[0073] 由于在密钥还原的过程中存在较多的出错原因，通过第二哈希值和第四哈希值虽然可以辨识密钥组分记录和密钥原文记录的准确性，但是无法得知具体错误原因，因此，可以在进行哈希计算之前对密钥验证记录的数据格式和第一密钥组分记录的组分附属信息的内容进行比对验证，从而及时发现错误原因，方便工作人员及时更改操作方法排除错误。

[0074] 进一步地，所述第二哈希值的计算方法如下：

[0075] E1、在密钥备份的过程中，以所述待计算的密钥原文和所述待计算的密钥原文对应的原文附属信息作为第二密钥原文记录；

[0076] E2、对所述第二密钥原文记录进行哈希计算，得到所述第四哈希值；

[0077] 对第二密钥原文记录进行哈希运算，可以得到第四哈希值，第四哈希值可以保存在密钥验证记录中，用于在密钥还原的过程对第一密钥原文记录进行验证。

[0078] 此外，还可以在第一密钥原文记录验证通过后，对密钥验证记录中的密钥有效期进行检查，判断密钥验证记录中的密钥有效期的值是否小于系统当前的时钟值，当密钥有效期的值大于或等于系统当前的时钟值时，密钥有效期验证通过，第一密钥原文为可靠的、可信任的密钥，当密钥有效期小于系统当前的时钟值时，表示第一密钥原文已超过有效期，不能再使用，报告“密钥已超过有效期”至工作人员，并中止读取过程。

[0079] 本实施例一提供的密钥组分验证方法中，对第一密钥组分记录进行哈希计算，判断哈希计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致，由于在哈希计算中，即使被计算的值发生微小变动，也会使哈希计算的结果产生极大的偏差，因此，当第一哈希值与第二哈希值一致时，可以确定第一密钥组分记录为可靠的记录，第一密钥组分记录验证通过，在密钥组分记录验证中，不需要额外生成验证密钥，可以对任何密钥的密钥组分进行验证，通用性高，解决了现有的密钥组分验证算法通用性差，无法保证系统种子密钥实现安全备份存储与准确恢复的问题。

[0080] 验证了第一密钥组分记录之后，还可以通过第四哈希值验证第一密钥原文记录，从而保证第一密钥原文的正确性、完备性、有效性和合法性。

[0081] 在使用第一哈希值进行验证之前，还可以对密钥验证记录的格式和第一密钥组分记录中的组分附属信息的内容进行验证，从而使工作人员及时发现错误和改正操作方法，方便工作人员的使用。

[0082] 第二哈希值和第四哈希值为密钥备份的过程中，对第二密钥组分记录和第二密钥原文计算进行哈希运算得到，可以在密钥还原的过程中对第一密钥组分记录和第一密钥原文记录进行验证。

[0083] 在第一密钥原文验证之后，还可以验证密钥验证记录中的密钥有效期是否小于系统当前的时钟值；若密钥有效期小于系统当前的时钟值时，则表示第一密钥原文已超过有

效期，不能再使用，报告“密钥已超过有效期”至工作人员，并中止读取过程；若密钥有效期的值大于或等于系统当前的时钟值时，密钥有效期验证通过，则证实并报告所合成的第一密钥原文是可靠的、可信任的密钥。

[0084] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

[0085] 实施例二：

[0086] 本申请实施例二提供了一种密钥组分验证装置，为便于说明，仅示出与本申请相关的部分，如图2所示，密钥组分验证装置包括，

[0087] 组分记录模块201，用于接收组分读取指令，根据所述组分读取指令读取第一密钥组分记录，其中，密钥组分记录包括密钥组分和组分附属信息；

[0088] 第一验证模块202，用于对所述第一密钥组分记录进行哈希计算，判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致；

[0089] 组分通过模块203，用于当所述第一哈希值与所述第二哈希值一致时，所述第一密钥组分记录验证通过。

[0090] 进一步地，所述装置还包括：

[0091] 原文合成模块，用于将各个第一密钥组分记录中的密钥组分以预设的合成公式进行合成，得到第一密钥原文；

[0092] 原文记录模块，用于以所述第一密钥原文和所述第一密钥原文对应的原文附属信息作为第一密钥原文记录；

[0093] 第二验证模块，用于对所述第一密钥原文记录进行哈希计算，判断计算得到的第三哈希值是否与所述密钥验证记录中的第四哈希值一致；

[0094] 原文通过模块，用于当所述第三哈希值与所述第四哈希值一致时，所述第一密钥原文记录验证通过。

[0095] 进一步地，所述装置还包括：

[0096] 验证读取模块，用于接收密钥验证记录读取指令，根据所述密钥验证读取指令读取密钥验证记录，其中，所述密钥验证记录包括组分附属信息、第二哈希值和第四哈希值；

[0097] 格式检测模块，用于判断所述密钥验证记录是否符合预设格式要求；

[0098] 对应地，所述组分通过模块203，具体用于当所述密钥验证记录符合所述预设格式要求时，对所述第一密钥组分记录进行哈希计算，判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致。

[0099] 进一步地，所述组分通过模块203，具体包括：

[0100] 信息判断子模块，用于当所述密钥验证记录符合所述预设格式要求时，判断所述第一密钥组分记录中的组分附属信息是否与所述密钥验证记录中对应的组分附属信息一致；

[0101] 哈希判断子模块，用于当所述第一密钥组分记录中的组分附属信息与所述密钥验证记录中对应的组分附属信息一致时，对所述第一密钥组分记录进行哈希计算，判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致。

[0102] 进一步地，所述装置还包括：

[0103] 组分备份模块，用于在密钥备份的过程中，以待备份的密钥组分和所述待备份的密钥组分对应的组分附属信息作为第二密钥组分记录；

[0104] 第二哈希模块，用于对所述第二密钥组分记录进行哈希计算，得到所述第二哈希值。

[0105] 进一步地，所述装置还包括：

[0106] 第二原文模块，用于在密钥备份的过程中，以所述待计算的密钥原文和所述待计算的密钥原文对应的原文附属信息作为第二密钥原文记录；

[0107] 第四哈希模块，用于对所述第二密钥原文记录进行哈希计算，得到所述第四哈希值。

[0108] 需要说明的是，上述装置/单元之间的信息交互、执行过程等内容，由于与本申请方法实施例基于同一构思，其具体功能及带来的技术效果，具体可参见方法实施例部分，此处不再赘述。

[0109] 实施例三：

[0110] 图3是本申请实施例三提供的终端设备的示意图。如图3所示，该实施例的终端设备3包括：处理器30、存储器31以及存储在所述存储器31中并可在所述处理器30上运行的计算机程序32。所述处理器30执行所述计算机程序32时实现上述密钥组分验证方法实施例中的步骤，例如图1所示的步骤S101至S103。或者，所述处理器30执行所述计算机程序32时实现上述各装置实施例中各模块/单元的功能，例如图2所示模块201至203的功能。

[0111] 示例性的，所述计算机程序32可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器31中，并由所述处理器30执行，以完成本申请。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述所述计算机程序32在所述终端设备3中的执行过程。例如，所述计算机程序32可以被分割成组分记录模块、第一验证模块以及组分通过模块，各模块具体功能如下：

[0112] 组分记录模块，用于接收组分读取指令，根据所述组分读取指令读取第一密钥组分记录，其中，密钥组分记录包括密钥组分和组分附属信息；

[0113] 第一验证模块，用于对所述第一密钥组分记录进行哈希计算，判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致；

[0114] 组分通过模块，用于当所述第一哈希值与所述第二哈希值一致时，所述第一密钥组分记录验证通过。

[0115] 所述终端设备3可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。所述终端设备可包括，但不仅限于，处理器30、存储器31。本领域技术人员可以理解，图3仅仅是终端设备3的示例，并不构成对终端设备3的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述终端设备还可以包括输入输出设备、网络接入设备、总线等。

[0116] 所称处理器30可以是中央处理单元(Central Processing Unit,CPU)，还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现成可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器

等。

[0117] 所述存储器31可以是所述终端设备3的内部存储单元，例如终端设备3的硬盘或内存。所述存储器31也可以是所述终端设备3的外部存储设备，例如所述终端设备3上配备的插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)等。进一步地，所述存储器31还可以既包括所述终端设备3的内部存储单元也包括外部存储设备。所述存储器31用于存储所述计算机程序以及所述终端设备所需的其他程序和数据。所述存储器31还可以用于暂时地存储已经输出或者将要输出的数据。

[0118] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、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单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块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。另外，各功能单元、模块的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0119] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述或记载的部分，可以参见其它实施例的相关描述。

[0120] 本领域普通技术人员可以意识到，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，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

[0121] 在本申请所提供的实施例中，应该理解到，所揭露的装置/终端设备和方法，可以通过其它的方式实现。例如，以上所描述的装置/终端设备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讯连接可以是通过一些接口，装置或单元的间接耦合或通讯连接，可以是电性，机械或其它的形式。

[0122] 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。

[0123] 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。

[0124] 所述集成的模块/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，本申请实现上述实施例方法中的全部或部分流程，也可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一计算机可读存储介质中，该计算机程序在被处理器执行时，可实现上

述各个方法实施例的步骤。其中，所述计算机程序包括计算机程序代码，所述计算机程序代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括：能够携带所述计算机程序代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、电载波信号、电信信号以及软件分发介质等。需要说明的是，所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括电载波信号和电信信号。

[0125] 以上所述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，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者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，均应包含在本申请的保护范围之内。

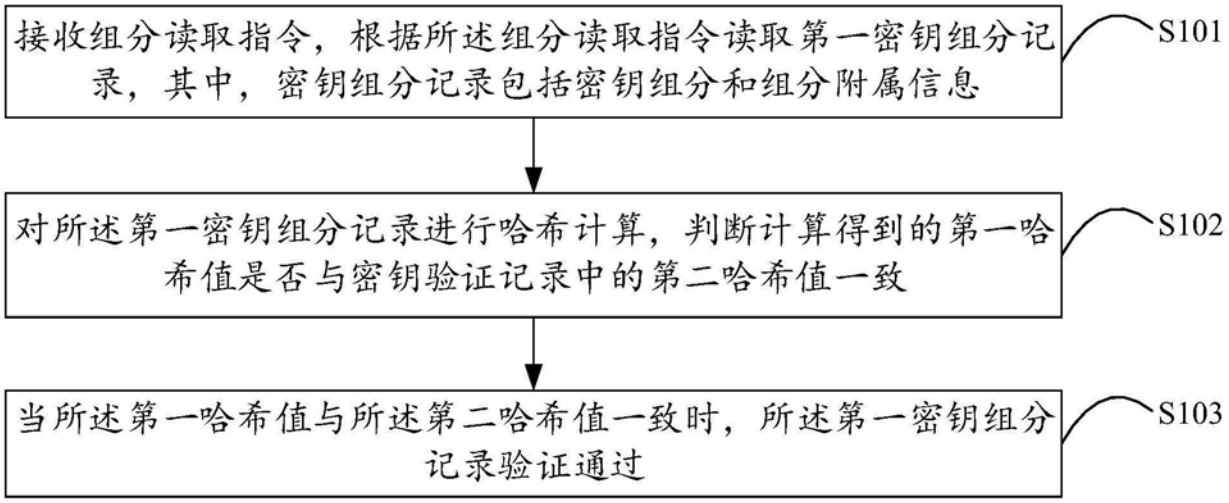

接收组分读取指令，根据所述组分读取指令读取第一密钥组分记录，其中，密钥组分记录包括密钥组分和组分附属信息
S101
对所述第一密钥组分记录进行哈希计算，判断计算得到的第一哈希值是否与密钥验证记录中的第二哈希值一致
S102
当所述第一哈希值与所述第二哈希值一致时，所述第一密钥组分记录验证通过
S103

图1

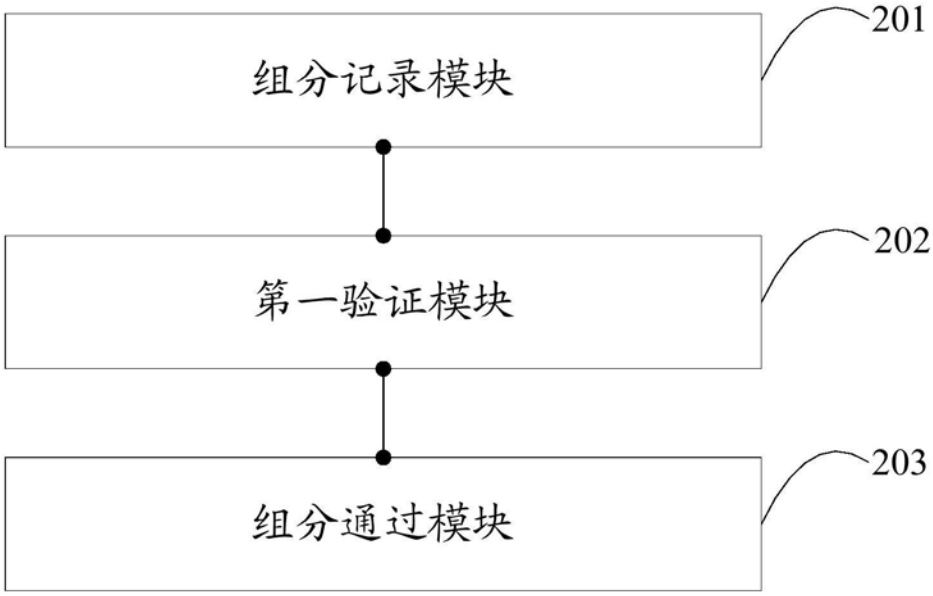

组分记录模块
201
第一验证模块
202
组分通过模块
203

图2

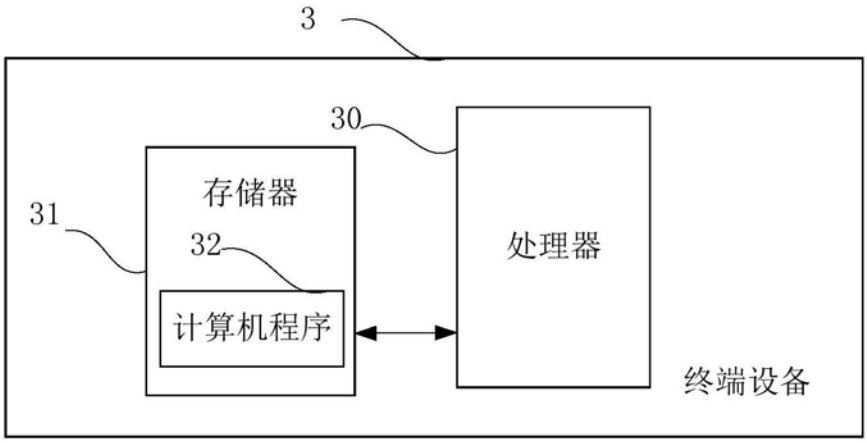


图3