(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 12 月 8 日 (08.12.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/252449 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01) *G06F 21/62* (2013.01)

(21) 国际申请号: PCT/CN2021/120591

(22) 国际申请日: 2021 年 9 月 26 日 (26.09.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110604096.2 2021年5月31日 (31.05.2021) CN

(71) 申请人: 统信软件技术有限公司 (**UNIONTECH SOFTWARE TECHNOLOGY CO., LTD.**) [CN/CN]; 中国北京市北京经济技术开发区科谷一街10号院12号楼18层, Beijing 100176 (CN)。

(72) 发明人: 卢桢 (**LU, Zhen**); 中国北京市北京经济技术开发区科谷一街10号院12号楼18层, Beijing 100176 (CN)。

(74) 代理人: 北京瀚方律师事务所 (**BEIJING HANFANG LAW FIRM**); 中国北京市东城区朝阳门内大街银河SOHOB座21702周红力, Beijing 100010 (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, IT, 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,

WO 2022/252449 A1

(54) **Title:** FILE ACCESS CONTROL METHOD, FILE ENCRYPTION METHOD, AND COMPUTING DEVICE

(54) 发明名称: 文件访问控制方法、文件加密方法及计算设备

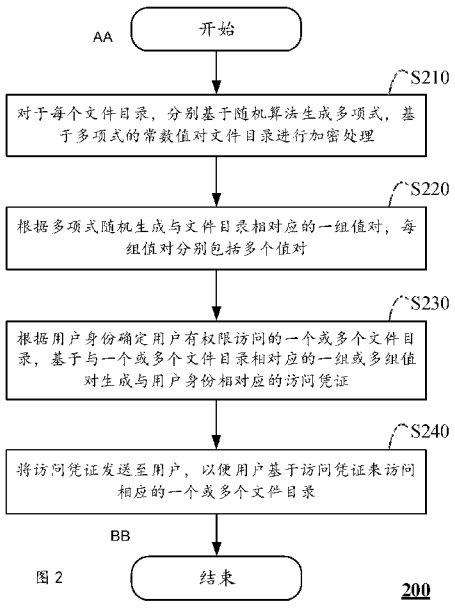

图 2

S210 For each file directory, generate a polynomial on the basis of a random algorithm, respectively, and encrypt the file directory on the basis of a constant value of the polynomial

S220 Randomly generate, according to the polynomial, a group of value pairs corresponding to the file directory, each group of value pairs respectively comprising a plurality of value pairs

S230 Determine, according to the identity of a user, one or more file directories that a user has permission to access, and generate, on the basis of one or more groups of value pairs corresponding to the one or more file directories, an access credential corresponding to the identity of the user

S240 Send the access credential to the user, such that the user can access the corresponding one or more file directories on the basis of the access credential

AA Start

BB End

(57) **Abstract:** Disclosed is a file access control method, implemented in a computing device and comprising the steps: receiving an access request for a file sent by a user on the basis of an access credential; obtaining one or more groups of value pairs on the basis of the access credential, each group of value pairs comprising a plurality of value pairs, and each group of value pairs respectively corresponding to one file directory; decrypting the corresponding file directory according to each group of value pairs, respectively, to obtain one or more decrypted file directories corresponding to the access credential of the user; and combining and mounting the one

[见续页]

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, 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))。

or more decrypted file directories to a predetermined directory, such that the user can access the one or more decrypted file directories under the predetermined directory. A corresponding file encryption method and the computing device are further disclosed. According to the solution of the present invention, access permissions of users of different identities to a file directory can be controlled, and user experience is better.

(57) 摘要：本发明公开了一种文件访问控制方法，在计算设备中执行，包括步骤：接收用户基于访问凭证发送的对文件的访问请求；基于所述访问凭证获取一组或多组值对，每组值对包括多个值对，且每组值对分别对应一个文件目录；分别根据每组值对对相应的文件目录进行解密处理，以得到与用户的访问凭证相对应的一个或多个解密文件目录；以及将所述一个或多个解密文件目录合并挂载到预定目录，以便用户在所述预定目录下访问所述一个或多个解密文件目录。本发明还一并公开了相应的文件加密方法和计算设备。根据本发明的方案，能实现控制不同身份的用户对文件目录的访问权限，且用户体验感更好。

文件访问控制方法、文件加密方法及计算设备

技术领域

本发明涉及计算机及互联网技术领域，特别涉及一种文件访问控制方法、文件加密方法及计算设备。

背景技术

目前，在日常工作中存在不同身份用户访问不同机密等级文件的情况，而现有的加密技术，只要用户持有文件的解密密钥就可以打开并修改里面的全部内容，这种修改是不受用户身份限制的，很容易造成对数据的滥操作。

现有技术中，为了实现在一台机器上不同用户访问的文件夹不同，需要为用户分别创建不同的加密文件夹，使每个用户只能访问自己的加密文件夹。这种文件加密方案，由于加密文件夹分散在不同路径，无法实现对文件的统一管理，而且，对于相同的文件，每个用户都需要保存一份，造成对存储空间的浪费。另外，这种方案无法限制不同身份的用户的访问权限。

还有一种方案，通过创建一个加密目录和若干子目录，用户持有加密目录的密钥和证明用户身份的令牌。当用户需要查看相应权限的文件时，首先进行解锁操作，再将令牌传给加密系统，系统确定用户身份后显示相应权限的目录。该方案虽然可以实现不同身份用户的访问权限，但由于不是对各个目录单独加密，导致只要是进入根目录的用户通过技术手段都可以查看并操作所有的文件。可见，这种方案即使设置了权限限制，也无法实现不同身份的用户之间的数据隔离，导致数据安全性得不到保障。

为此，需要一种文件访问控制方法来解决上述技术方案中存在的问题。

发明内容

为此，本发明提供一种文件访问控制方法和文件加密方法，以力图解决或者至少缓解上面存在的问题。

根据本发明的一个方面，提供了一种文件访问控制方法，在计算设备中执行，包括步骤：接收用户基于访问凭证发送的对文件的访问请求；基于所述访问凭证获取一组或多组值对，每组值对包括多个值对，且每组值对分别对应一个文件目录；分别根据每组值对对相应的文件目录进行解密处理，以得到与用户的访问凭证相对应的一个或多个解密文件目录；以及将所述一个或多个解密文件目录合并挂载到预定目录，以便用户在所述预定目录下访问所述一个或多个解密文件目录。

可选地，在根据本发明的文件访问控制方法中，将所述一个或多个解密文件目录合并挂载到预定目录的步骤包括：在预定目录挂载堆叠文件系统，以便基于堆叠文件系统将一个或多个解密文件目录合并挂载到预定目录。

可选地，在根据本发明的文件访问控制方法中，分别根据每组值对对相应的文件目录进行解密处理的步骤包括：根据拉格朗日插值算法对每组值对分别进行计算，以得到与每组值对相对应的常数值；基于每组值对对应的常数值对相应的文件目录进行解密处理，以得到与每组值对相对应的解密文件目录。

可选地，在根据本发明的文件访问控制方法中，在根据每组值对对相应的文件目录进行解密处理之前，包括步骤：对每组值对进行验证。

可选地，在根据本发明的文件访问控制方法中，所述每个值对分别对应一个用户属性；所述用户属性包括部门、职位和职级。

根据本发明的一个方面，提供了一种文件加密方法，在计算设备中执行，包括步骤：对于每个文件目录，分别基于随机算法生成多项式，基于多项式的常数值对所述文件目录进行加密处理；根据所述多项式随机生成与所述文件目录相对应的一组值对，每组值对分别包括多个值对；根据用户身份确定用户有权限访问的一个或多个文件目录，基于与一个或多个文件目录相对应的一组或多组值对生成与用户身份相对应的访问凭证；以及将所述访问凭证发送至用户，以便用户基于所述访问凭证来访问相应的一个或多个文件目录。

可选地，在根据本发明的文件加密方法中，根据所述多项式随机生成与文件目录相对应的一组值对的步骤包括：随机生成多个随机数；基于每个随机数分别与所述多项式计算得到相应的值对，以得到与多个随机数相对应的

多个值对。

可选地，在根据本发明的文件加密方法中，生成与用户身份相对应的访问凭证的步骤包括：将与一个或多个文件目录相对应的一组或多组值对基于预定格式进行组合，生成相应的数据值，将所述数据值作为访问凭证。

可选地，在根据本发明的文件加密方法中，基于多项式的常数值对文件目录进行加密处理包括：计算所述多项式的常数值，并基于对常数值进行哈希计算后得到的哈希值对文件目录进行加密处理。

可选地，在根据本发明的文件加密方法中，所述每个值对分别对应一个用户属性；所述用户属性包括部门、职位和职级。

根据本发明的一个方面，提供了一种计算设备，包括：至少一个处理器；以及存储器，存储有程序指令，其中，所述程序指令被配置为适于由所述至少一个处理器执行，所述程序指令包括用于执行如上所述的文件访问控制方法的指令。

根据本发明的一个方面，提供了一种存储有程序指令的可读存储介质，当所述程序指令被计算设备读取并执行时，使得所述计算设备执行如上所述方法。

根据本发明的技术方案，提供了一种文件加密方法和文件访问控制方法，其中，根据文件加密方法分别对每个文件目录进行加密处理，并分别为每个文件目录生成相应的一组值对，值对与用户属性相关。根据用户有权限访问的一个或多个文件目录，来为用户分发相应权限的访问凭证，访问凭证中包括与用户有权限访问的一个或多个文件目录相对应的一组或多组值对。这样，通过执行文件访问控制方法，使用户可以基于相应的访问凭证解密一个或多个文件目录，从而能访问与用户身份相匹配的一个或多个文件目录。可见，根据本发明的技术方案，能实现控制不同身份的用户对文件目录的访问权限，并且，实现了不同身份的用户之间的数据隔离。

此外，通过将用户有权限访问的一个或多个文件目录合并挂载到同一个预定目录下，使用户可以在同一个目录下查看与其身份相对应的所有文件目录下的文件、对文件进行修改操作，而不用切换到不同的目录查看不同文件目录下的文件。这样，实现了针对不同身份的用户来整理有权限访问的所有

文件目录的效果，有利于提高用户对文件的查看和操作效率，用户体验感更好。

附图说明

为了实现上述以及相关目的，本文结合下面的描述和附图来描述某些说明性方面，这些方面指示了可以实践本文所公开的原理的各种方式，并且所有方面及其等效方面旨在落入所要求保护的主题的范围内。通过结合附图阅读下面的详细描述，本公开的上述以及其它目的、特征和优势将变得更加明显。遍及本公开，相同的附图标记通常指代相同的部件或元素。

图 1 示出了根据本发明一个实施例的计算设备 100 的示意图；

图 2 示出了根据本发明一个实施例的文件加密方法 200 的流程图；

图 3 示出了根据本发明一个实施例的文件访问控制方法 300 的流程图；以及

图 4、图 5 分别示出了根据本发明一个实施例的访问凭证的数据格式示意图。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

根据本发明的技术方案，根据文件加密方法来对每个文件目录进行加密处理，并根据用户身份为用户分发相应的访问凭证。进而，通过执行文件访问控制方法，使用户可以基于相应的访问凭证来解密一个或多个文件目录，以便访问与用户身份相匹配的一个或多个文件目录。

图 1 是示例计算设备 100 的示意框图。

如图 1 所示，在基本的配置 102 中，计算设备 100 典型地包括系统存储器 106 和一个或者多个处理器 104。存储器总线 108 可以用于在处理器 104 和系统存储器 106 之间的通信。

取决于期望的配置，处理器 104 可以是任何类型的处理，包括但不限于：微处理器（UP）、微控制器（UC）、数字信息处理器（DSP）或者它们的任何组合。处理器 104 可以包括诸如一级高速缓存 110 和二级高速缓存 112 之类的一个或者多个级别的高速缓存、处理器核心 114 和寄存器 116。示例的处理器核心 114 可以包括运算逻辑单元（ALU）、浮点数单元（FPU）、数字信号处理核心（DSP 核心）或者它们的任何组合。示例的存储器控制器 118 可以与处理器 104 一起使用，或者在一些实现中，存储器控制器 118 可以是处理器 104 的一个内部部分。

取决于期望的配置，系统存储器 106 可以是任意类型的存储器，包括但不限于：易失性存储器（诸如 RAM）、非易失性存储器（诸如 ROM、闪存等）或者它们的任何组合。系统存储器 106 可以包括操作系统 120、一个或者多个应用 122 以及程序数据 124。在一些实施方式中，应用 122 可以布置为在操作系统上由一个或多个处理器 104 利用程序数据 124 执行指令。

计算设备 100 还包括储存设备 132，储存设备 132 包括可移除储存器 136 和不可移除储存器 138。

计算设备 100 还可以包括储存接口总线 134。储存接口总线 134 实现了从储存设备 132（例如，可移除储存器 136 和不可移除储存器 138）经由总线/接口控制器 130 到基本配置 102 的通信。操作系统 120、应用 122 以及数据 124 的至少一部分可以存储在可移除储存器 136 和/或不可移除储存器 138 上，并且在计算设备 100 上电或者要执行应用 122 时，经由储存接口总线 134 而加载到系统存储器 106 中，并由一个或者多个处理器 104 来执行。

计算设备 100 还可以包括有助于从各种接口设备（例如，输出设备 142、外设接口 144 和通信设备 146）到基本配置 102 经由总线/接口控制器 130 的通信的接口总线 140。示例的输出设备 142 包括图形处理单元 148 和音频处理单元 150。它们可以被配置为有助于经由一个或者多个 A/V 端口 152 与诸如显示器或者扬声器之类的各种外部设备进行通信。示例外设接口 144 可以包括串行接口控制器 154 和并行接口控制器 156，它们可以被配置为有助于经由一个或者多个 I/O 端口 158 和诸如输入设备（例如，键盘、鼠标、笔、语音输入设备、触摸输入设备）或者其他外设（例如打印机、扫描仪等）之类的外部设备进行通信。示例的通信设备 146 可以包括网络控制器 160，其可以被布

置为便于经由一个或者多个通信端口 164 与一个或者多个其他计算设备 162 通过网络通信链路的通信。

网络通信链路可以是通信介质的一个示例。通信介质通常可以体现为在诸如载波或者其他传输机制之类的调制数据信号中的计算机可读指令、数据结构、程序模块，并且可以包括任何信息递送介质。“调制数据信号”可以是这样的信号，它的数据集中的一个或者多个或者它的改变可以在信号中以编码信息的方式进行。作为非限制性的示例，通信介质可以包括诸如有线网络或者专线网络之类的有线介质，以及诸如声音、射频（RF）、微波、红外（IR）或者其它无线介质在内的各种无线介质。这里使用的术语计算机可读介质可以包括存储介质和通信介质二者。

计算设备 100 可以实现为包括桌面计算机和笔记本计算机配置的个人计算机。当然，计算设备 100 也可以实现为小尺寸便携（或者移动）电子设备的一部分，这些电子设备可以是诸如蜂窝电话、数码照相机、个人数字助理（PDA）、个人媒体播放器设备、无线网络浏览设备、个人头戴设备、应用专用设备、或者可以包括上面任何功能的混合设备。甚至可以被实现为服务器，如文件服务器、数据库服务器、应用程序服务器和 WEB 服务器等。本发明的实施例对此均不做限制。

在根据本发明的实施例中，计算设备 100 被配置为执行根据本发明的文件文件加密方法 200 和/或文件访问控制方法 300。其中，计算设备 100 的应用 122 中包含用于执行本发明的文件加密方法 200 和/或文件访问控制方法 300 的多条程序指令，这些程序指令可以被计算设备 100 读取并执行，以便计算设备 100 执行根据本发明的文件加密方法 200、文件访问控制方法 300。

图 2 示出了根据本发明一个实施例的文件加密方法 200 的流程图。方法 200 适于在计算设备（例如前述计算设备 200）中执行。应当指出，根据本发明的技术方案，基于文件加密方法 200 对每个文件目录分别进行加密处理。

如图 2 所示，方法 200 始于步骤 S210。

在步骤 S210 中，对于每个文件目录，在对文件目录进行加密时，分别基于随机算法生成一个多项式，基于多项式的常数值对该文件目录进行加密处理。

这里，多项式可以表示为 f(x)，其中$f(x) = ax^{(n-1)} + bx^{(n-2)} \ldots + c$。多项式的常数值是 x=0 时的多项式的值，即常数值 f(0)。在一个实施例中，在随机生成多项式，并计算出随机多项式的常数值 f(0)后，可以基于哈希函数对该常数值 f(0)进行哈希计算得到哈希值，并基于常数值 f(0)对应的哈希值作为文件目录的加密密钥来对文件目录进行加密处理。

随后，在步骤 S220 中，根据多项式随机生成与文件目录相对应的一组值对，每组值对分别包括多个值对。应当指出，每个文件目录分别对应一组值对，也即是，每个文件目录分别对应多个值对。不同的文件目录对应不同的值对组，以便基于相应的一组值对来对文件目录进行加密处理。这里，本发明对每组值对所包括的值对的数量不做限制。

在一个实施例中，通过随机生成多个随机数，基于每个随机数分别与多项式进行计算得到相应的值对。具体地说，通过将每个随机数带入多项式来计算多项式 f(x)的值，并将随机数与相应的多项式的值来组合得到与随机数相对应的值对。例如，其中一个随机数为 a，则随机数 a 对应的值对可以表示为{a, f(a)}。这样，最终可以计算得到与多个随机数相对应的多个值对，其中每个随机数分别对应一个值对。

随后，在步骤 S230 中，根据用户身份确定用户有权限访问的一个或多个文件目录。通过确定每个文件目录对应的一组值对，基于与用户有权限访问的一个或多个文件目录相对应的一组或多组值对，来生成与用户身份相对应的访问凭证。

应当指出，根据本发明的技术方案，每个用户对应的访问凭证（一组或多组值对）是根据用户身份来确定的，访问凭证也决定了根据用户身份有权限访问的一个或多个文件目录。因此，用户的访问凭证中的一组或多组值对与用户身份相关，能够证明用户身份。

在一个实施例中，每个值对分别对应一个用户属性，用户属性也即是能与用户身份相关的属性。应当指出，根据本发明的技术方案，用户身份可以由一个或多个用户属性来确定，或者说，用户身份与一个或多个用户属性相关。例如，与用户身份相关的用户属性可以包括用户所在的部门、职位、职级等，但不限于此。

应当理解，当用于确定用户身份的属性包括用户所在的部门、职位和职级时，用户身份便与部门、职位和职级这三个用户属性相关。而在生成与用户身份相对应的访问凭证时，每个用户属性是由相应的值对来表示，基于与多个用户属性对应的多个值对来生成访问凭证，其中每个值对分别代表了一个用户属性。这样，基于多个值对生成的访问凭证也即是与用户身份相关的访问凭证。

可以理解，每组值对所包括的值对的数量与用户身份相关的用户属性的种数相等。例如，用户身份与部门、职位和职级这三个用户属性相关时，每个文件目录对应的一组值对是由三个值对组成。

根据一个实施例，在基于一组或多组值对生成与用户相对应的访问凭证时，可以将与一个或多个文件目录相对应的一组或多组值对基于预定格式进行拼装组合，来生成相应的数据值，并将该数据值作为访问凭证。这里，本发明对访问凭证对应的数据值的具体数据格式不做限定，其可以由本领域技术人员根据实际需求自行设置。

图 4、图 5 分别示出了根据本发明一个实施例的访问凭证的数据格式示意图。

在一个实施例中，基于一组或多组值对生成访问凭证可以根据以下方法执行：

如图 4 所示，数据起始的 4 个字节用于存放随机数 x 的长度，后面紧接着存放随机数 x 的值，x 后面紧接着存放对应的多项式 f(x)值的长度，在 f(x)值的长度后面存放多项式 f(x)值。以此规律来处理每个值对，以便对每个值对进行组合，直到把一个多项式对应的所有值对（也即是与一个文件目录相对应的一组值对）处理完毕，并将最后的值置为 0。在一个多项式对应的所有对值对处理完成后，对 0 值前面的数据进行哈希计算，得到一个哈希值，并将该哈希值（Hash）存放于 0 值后面，用于密钥值对的正确性校验和防暴力破解。

如图 5 所示，对于多组值对的组合生成访问凭证，由于 Hash 值的长度是固定的，因此，在处理完成一组值对时，只需偏移固定长度的位置即可确定下一组值对的起始位置，并按照上述方法对每组值对进行拼装组合，直到所

有值对组都处理完成，最终，便基于多组值对拼装组合得到预定数据格式的访问凭证。

最后，在步骤 S240 中，将访问凭证发送至用户，以便用户基于访问凭证来访问相应的一个或多个文件目录。这里，基于访问凭证能够访问的一个或多个文件目录即是与用户身份相匹配的用户有权限访问的一个或多个文件目录。

图 3 示出了根据本发明一个实施例的文件访问控制方法 300 的流程图。方法 300 可以在计算设备 100 中执行。

应当指出，通过执行文件访问控制方法 300，使得用户可以基于在前述方法 200 中获取的访问凭证有权限访问与用户身份相对应的一个或多个文件目录。这样，能实现控制不同身份的用户对文件目录的访问权限。

如图 3 所示，方法 300 始于步骤 S310。

在步骤 S310 中，接收用户基于访问凭证发送的对文件的访问请求。这里，访问凭证即是基于前述方法 200 为用户分发的与用户身份相对应的访问凭证，访问凭证是由一组或多组值对进行组合得到的数据值。

在步骤 S320 中，基于访问凭证获取一组或多组值对。如前文所述，每组值对包括多个值对，且每组值对分别对应一个用户有权限访问的文件目录。

根据一个实施例，与前文所述的基于多个值对生成的访问凭证的方法和数据格式相对应，在基于访问凭证获取一组或多组值对时，根据访问凭证对应的数据值的预定格式，从访问凭证对应的数据值的起始位置开始，首先获取预定字节作为 x 的长度值，进而可以获取在长度值之后存放的 x 值，随后，可以获取到在 x 值之后存放的 f(x)值，这样，便获取到第一组值对。进而，获取位于第一组值对之后的第二组值对。以此类推，最终可以从访问凭证对应的数据值中获取到多组值对分别包括的多个值对。

随后，在步骤 S330 中，分别根据每组值对对相应的文件目录进行解密处理，以得到与用户的访问凭证相对应的一个或多个解密文件目录。应当理解，解密文件目录即是用户有权限访问的文件目录。

根据一个实施例，在获取到一组或多组值对后、在根据每组值对对相应的文件目录进行解密处理之前，还对每组值对进行验证处理，以便判断每组

值对的有效性。具体地，根据前文所述的基于多个值对生成的访问凭证的方法和数据格式，在对访问凭证进行验证时，基于哈希函数对 0 值以及 0 值前面的数据（一组值对中的多个值对）进行哈希计算得到 H 值，进而，将这里计算得到的 H 值与访问凭证数据值中的哈希值进行比对，如果两者相等，则验证通过，根据该值对组中的多个值对对相应的文件目录进行解密处理。

根据一个实施例，在根据每组值对对相应的文件目录进行解密处理时，首先根据拉格朗日插值算法对每组值对分别进行计算，来得到与每组值对相对应的常数值 f(0)。进而，基于每组值对对应的常数值 f(0)对相应的文件目录进行解密处理，从而得到与每组值对相对应的解密文件目录。这样，使得用户可以基于访问凭证来访问解密后的一个或多个文件目录。

还应当指出，与前文所述的对文件目录进行加密的方法相对应，在步骤 S330 中，在基于每组值对对应的常数值 f(0)对相应的文件目录进行解密处理时，实际上，可以基于哈希函数对常数值 f(0)进行哈希计算得到哈希值，进而，基于常数值 f(0)对应的哈希值来对文件目录进行解密处理。

最后，在步骤 S340 中，将一个或多个解密文件目录合并挂载到预定目录，以便用户在预定目录下访问一个或多个解密文件目录。应当指出，本发明对合并挂载的预定目录不做限制，只要是便于用户查看的文件目录即可，例如，预定目录可以实现为用户目录。

在一个实施例中，通过在预定目录挂载堆叠文件系统，基于堆叠文件系统可以将一个或多个解密文件目录合并挂载到预定目录。这里，堆叠文件系统例如可以实现为 AUFS。但，本发明对堆叠文件系统的具体种类不做限制，现有技术中所有能实现将多个文件目录合并挂载到同一个目录的堆叠文件系统均在本发明的保护范围之内。

需要说明的是，通过将用户有权限访问的一个或多个文件目录合并挂载到同一个预定目录下，使用户可以在同一个目录下查看与其身份相对应的所有文件目录下的文件、对文件进行修改操作，而不用切换到不同的目录查看不同文件目录下的文件。这样，实现了针对不同身份的用户来整理有权限访问的所有文件目录的效果，有利于提高用户对文件的查看和操作效率，用户体验感更好。

综上，根据本发明的文件加密方法 200 分别对每个文件目录进行加密处理，并分别为每个文件目录生成相应的一组值对，值对与用户属性相关。根据用户有权限访问的一个或多个文件目录，来为用户分发相应权限的访问凭证，访问凭证中包括与用户有权限访问的一个或多个文件目录相对应的一组或多组值对。这样，通过执行本发明的文件访问控制方法 300，使用户可以基于相应的访问凭证解密一个或多个文件目录，从而能访问与用户身份相匹配的一个或多个文件目录。可见，根据本发明的技术方案，能实现控制不同身份的用户对文件目录的访问权限，并且，实现了不同身份的用户之间的数据隔离。

这里描述的各种技术可结合硬件或软件，或者它们的组合一起实现。从而，本发明的方法和设备，或者本发明的方法和设备的某些方面或部分可采取嵌入有形媒介，例如可移动硬盘、U 盘、软盘、CD-ROM 或者其它任意机器可读的存储介质中的程序代码(即指令)的形式，其中当程序被载入诸如计算机之类的机器，并被所述机器执行时，所述机器变成实践本发明的设备。

在程序代码在可编程计算机上执行的情况下，计算设备一般包括处理器、处理器可读的存储介质(包括易失性和非易失性存储器和/或存储元件)，至少一个输入装置，和至少一个输出装置。其中，存储器被配置用于存储程序代码；处理器被配置用于根据该存储器中存储的所述程序代码中的指令，执行本发明的多语言垃圾文本的识别方法。

以示例而非限制的方式，可读介质包括可读存储介质和通信介质。可读存储介质存储诸如计算机可读指令、数据结构、程序模块或其它数据等信息。通信介质一般以诸如载波或其它传输机制等已调制数据信号来体现计算机可读指令、数据结构、程序模块或其它数据，并且包括任何信息传递介质。以上的任一种的组合也包括在可读介质的范围之内。

在此处所提供的说明书中，算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与本发明的示例一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳

实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下被实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员应当理解在本文所公开的示例中的设备的模块或单元或组件可以布置在如该实施例中所描述的设备中，或者可替换地可以定位在与该示例中的设备不同的一个或多个设备中。前述示例中的模块可以组合为一个模块或者此外可以分成多个子模块。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使

用。

此外，所述实施例中的一些在此被描述成可以由计算机系统的处理器或者由执行所述功能的其它装置实施的方法或方法元素的组合。因此，具有用于实施所述方法或方法元素的必要指令的处理器形成用于实施该方法或方法元素的装置。此外，装置实施例的在此所述的元素是如下装置的例子：该装置用于实施由为了实施该发明的目的的元素所执行的功能。

如在此所使用的那样，除非另行规定，使用序数词“第一”、“第二”、“第三”等等来描述普通对象仅仅表示涉及类似对象的不同实例，并且并不意图暗示这样被描述的对象必须具有时间上、空间上、排序方面或者以任意其它方式的给定顺序。

尽管根据有限数量的实施例描述了本发明，但是受益于上面的描述，本技术领域内的技术人员明白，在由此描述的本发明的范围内，可以设想其它实施例。此外，应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求 书

1、一种文件访问控制方法，在计算设备中执行，包括步骤：

接收用户基于访问凭证对文件的访问请求；

基于所述访问凭证获取一组或多组值对，每组值对包括多个值对，且每组值对分别对应一个文件目录；

分别根据每组值对对相应的文件目录进行解密处理，以得到与用户的访问凭证相对应的一个或多个解密文件目录；以及

将所述一个或多个解密文件目录合并挂载到预定目录，以便用户在所述预定目录下访问所述一个或多个解密文件目录。

2、如权利要求 1 所述的方法，其中，将所述一个或多个解密文件目录合并挂载到预定目录的步骤包括：

在预定目录挂载堆叠文件系统，以便基于堆叠文件系统将一个或多个解密文件目录合并挂载到预定目录。

3、如权利要求 1 所述的方法，其中，分别根据每组值对对相应的文件目录进行解密处理的步骤包括：

根据拉格朗日插值算法对每组值对分别进行计算，以得到与每组值对相对应的常数值；

基于每组值对对应的常数值对相应的文件目录进行解密处理，以得到与每组值对相对应的解密文件目录。

4、如权利要求 1-3 中任一项所述的方法，其中，在根据每组值对对相应的文件目录进行解密处理之前，包括步骤：

对每组值对进行验证。

5、如权利要求 1-3 中任一项所述的方法，其中，

所述每个值对分别对应一个用户属性；

所述用户属性包括部门、职位、职级中的一种或多种。

6、一种文件加密方法，在计算设备中执行，包括步骤：

对于每个文件目录，分别基于随机算法生成多项式，基于多项式的常数值对所述文件目录进行加密处理；

根据所述多项式随机生成与所述文件目录相对应的一组值对，每组值对分别包括多个值对；

根据用户身份确定用户有权限访问的一个或多个文件目录，基于与一个或多个文件目录相对应的一组或多组值对生成与用户身份相对应的访问凭证；以及

将所述访问凭证发送至用户，以便用户基于所述访问凭证来访问相应的一个或多个文件目录。

7、如权利要求 6 所述的方法，其中，根据所述多项式随机生成与文件目录相对应的一组值对的步骤包括：

随机生成多个随机数；

基于每个随机数分别与所述多项式计算得到相应的值对，以得到与多个随机数相对应的多个值对。

8、如权利要求 6 所述的方法，其中，生成与用户身份相对应的访问凭证的步骤包括：

将与一个或多个文件目录相对应的一组或多组值对基于预定格式进行组合，生成相应的数据值，将所述数据值作为访问凭证。

9、如权利要求 6-8 中任一项所述的方法，其中，基于多项式的常数值对文件目录进行加密处理包括：

计算所述多项式的常数值，并基于对常数值进行哈希计算后得到的哈希值对文件目录进行加密处理。

10、如权利要求 6-8 中任一项所述的方法，其中，

所述每个值对分别对应一个用户属性；

所述用户属性包括部门、职位、职级中的一种或多种。

11、一种计算设备，包括：

至少一个处理器；以及

存储器，存储有程序指令，其中，所述程序指令被配置为适于由所述至少一个处理器执行，所述程序指令包括用于执行如权利要求 1-5 和/或 6-10 中任一项所述的方法的指令。

12、一种存储有程序指令的可读存储介质，当所述程序指令被计算设备读取并执行时，使得所述计算设备执行如权利要求 1-5 和/或 6-10 中任一项所述方法。

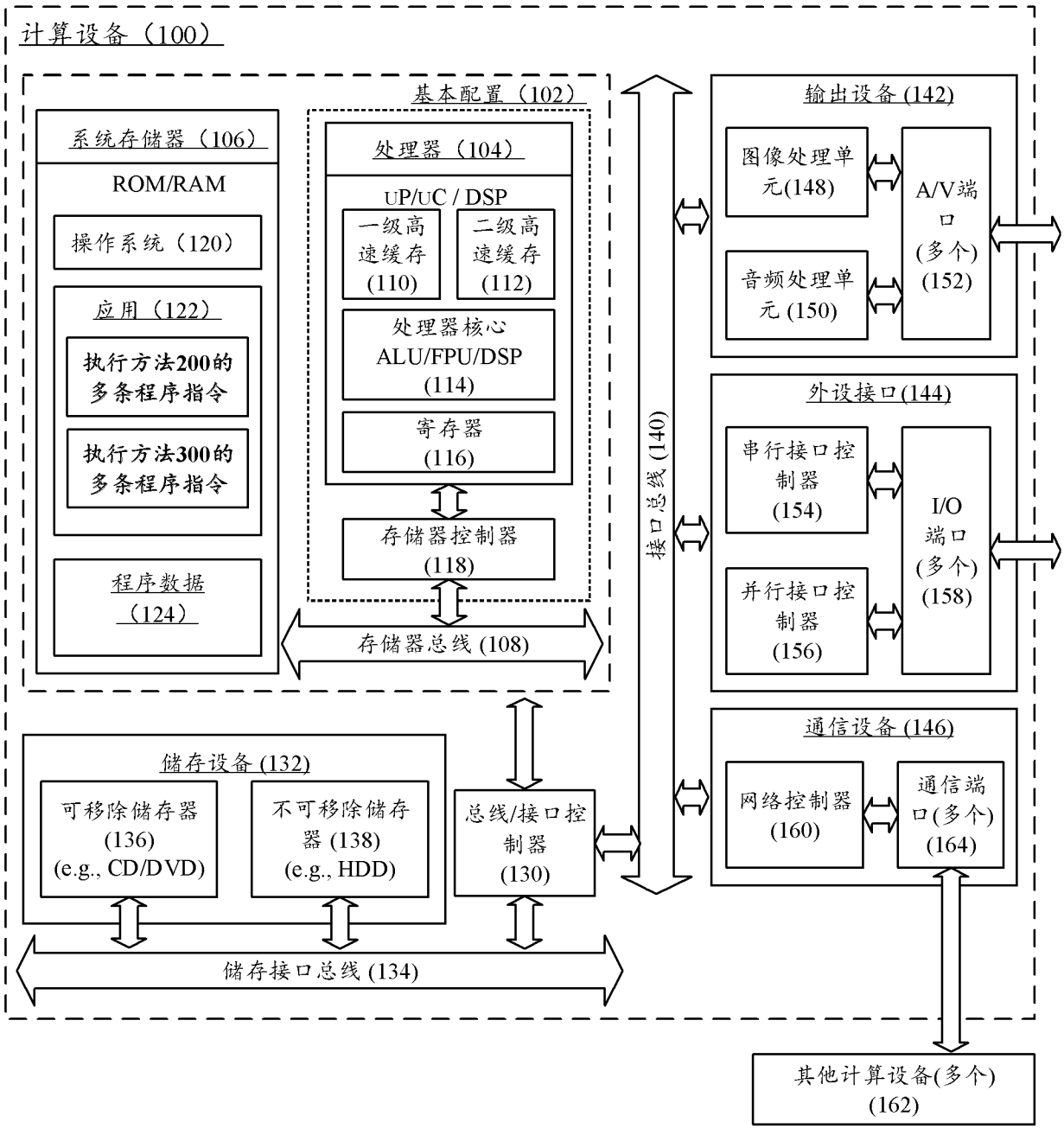
计算设备（100）
基本配置（102）
系统存储器（106）
ROM/RAM
操作系统（120）
应用（122）
执行方法200的多条程序指令
执行方法300的多条程序指令
程序数据（124）
处理器（104）
UP/UC / DSP
一级高速缓存(110)
二级高速缓存(112)
处理器核心ALU/FPU/DSP(114)
寄存器(116)
存储器控制器(118)
存储器总线 (108)
接口总线 (140)
输出设备 (142)
图像处理单元(148)
音频处理单元 (150)
A/V端口(多个)(152)
外设接口(144)
串行接口控制器(154)
并行接口控制器(156)
I/O端口(多个)(158)
通信设备 (146)
网络控制器(160)
通信端口(多个)(164)
储存设备 (132)
可移除储存器(136)(e.g., CD/DVD)
不可移除储存器 (138)(e.g., HDD)
总线/接口控制器(130)
储存接口总线 (134)
其他计算设备(多个)(162)

图 1

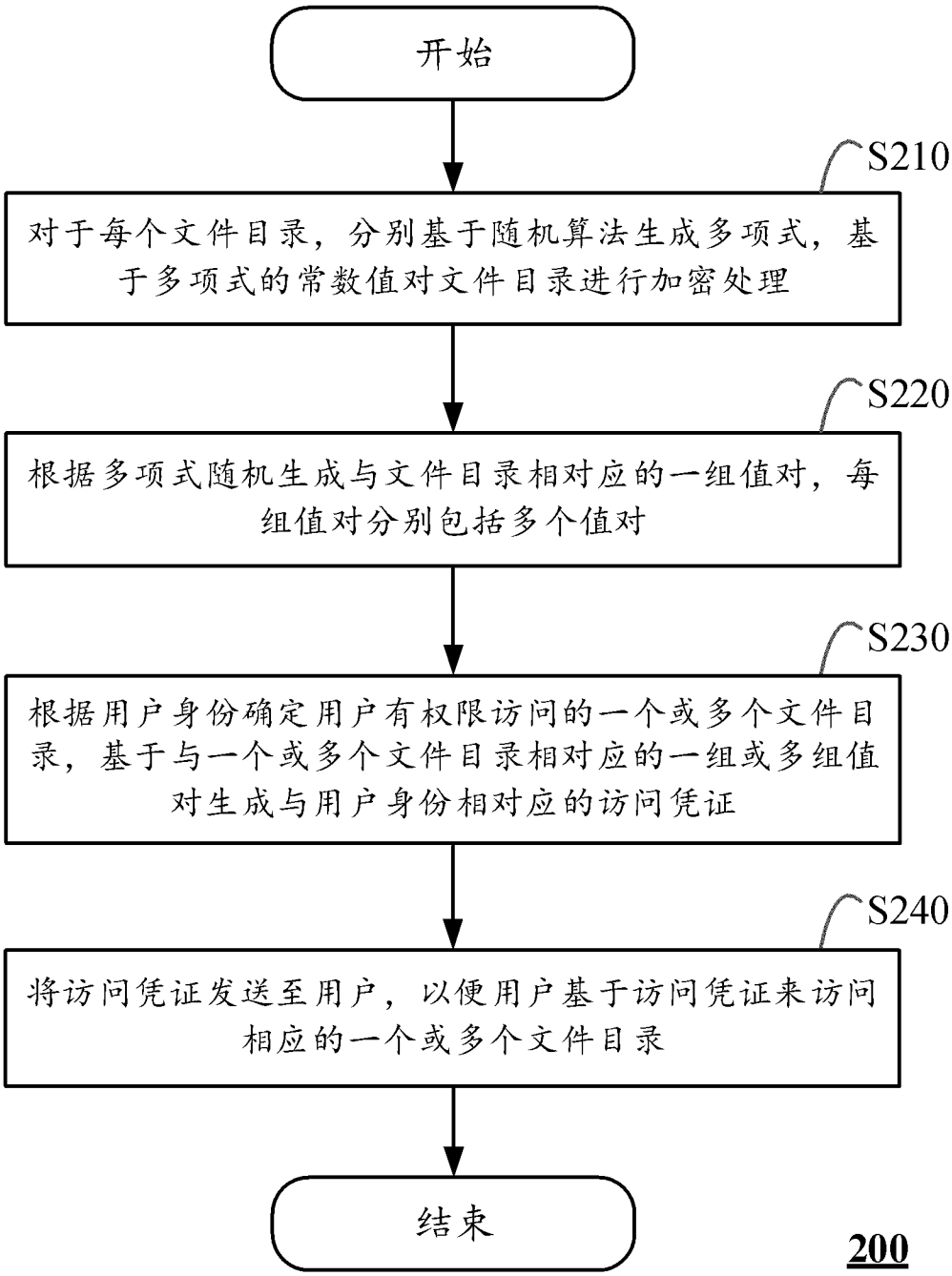
开始
S210
对于每个文件目录，分别基于随机算法生成多项式，基于多项式的常数值对文件目录进行加密处理
S220
根据多项式随机生成与文件目录相对应的一组值对，每组值对分别包括多个值对
S230
根据用户身份确定用户有权限访问的一个或多个文件目录，基于与一个或多个文件目录相对应的一组或多组值对生成与用户身份相对应的访问凭证
S240
将访问凭证发送至用户，以便用户基于访问凭证来访问相应的一个或多个文件目录
结束
200

图 2

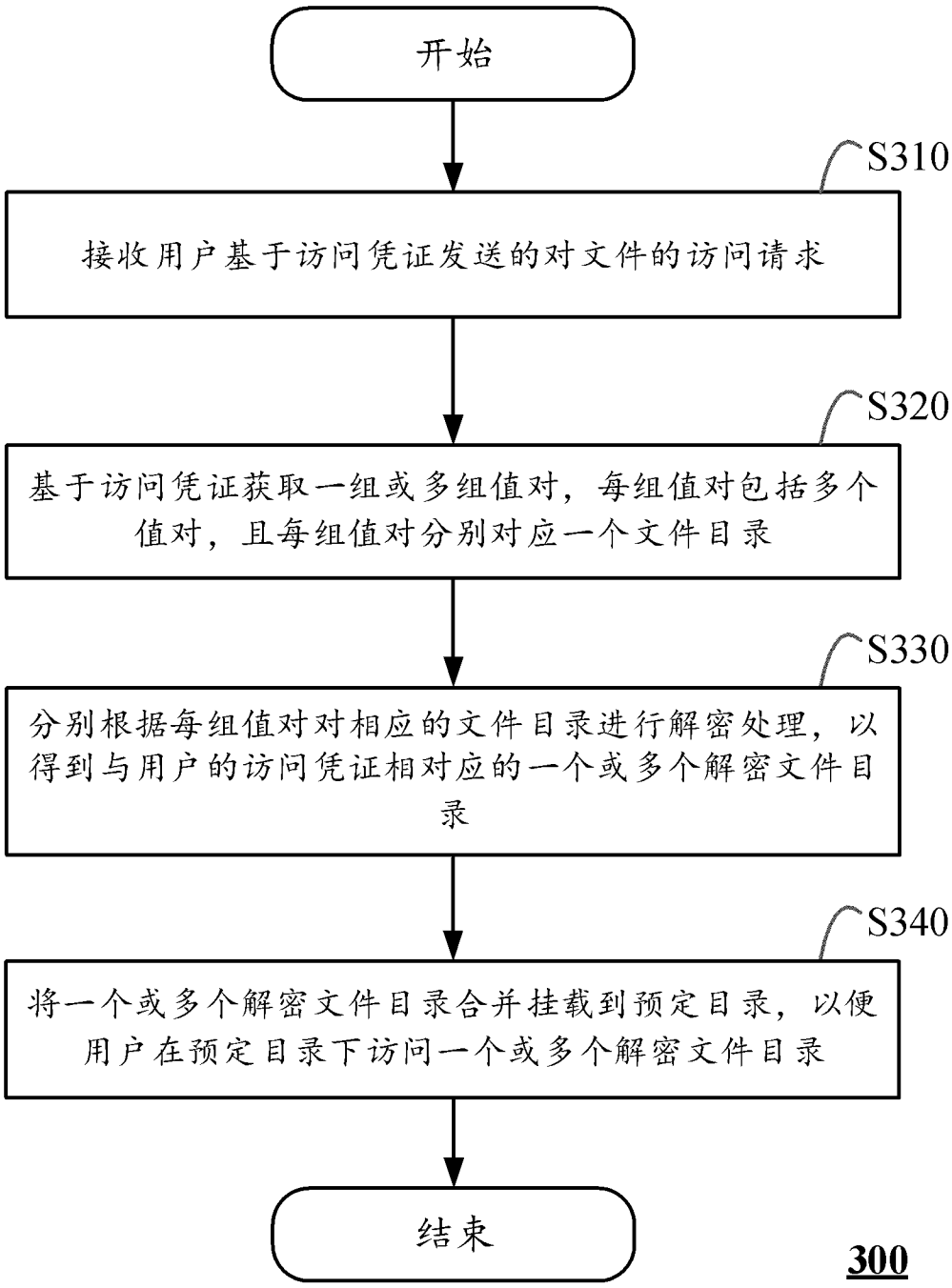
开始
S310
接收用户基于访问凭证发送的对文件的访问请求
S320
基于访问凭证获取一组或多组值对，每组值对包括多个值对，且每组值对分别对应一个文件目录
S330
分别根据每组值对对相应的文件目录进行解密处理，以得到与用户的访问凭证相对应的一个或多个解密文件目录
S340
将一个或多个解密文件目录合并挂载到预定目录，以便用户在预定目录下访问一个或多个解密文件目录
结束
300

图 3

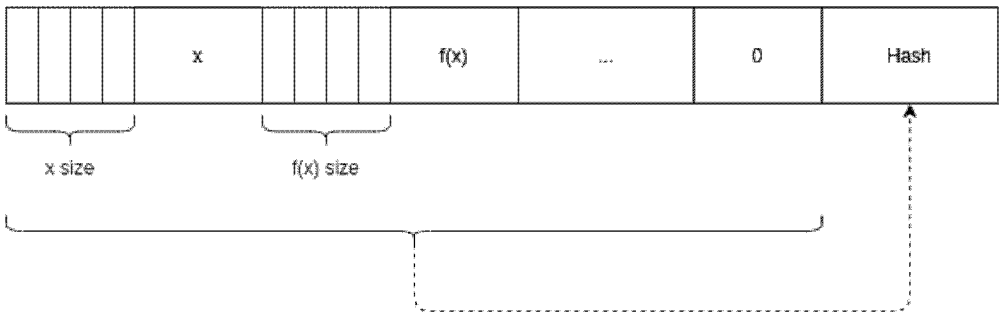

图 4

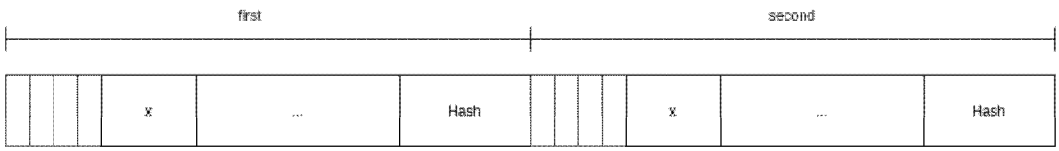

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/120591

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i; G06F 21/62(2013.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

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

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

CNABS; CNTXT; CNKI; SIPOABS; DWPI; USTXT; WOTXT; EPTXT: 文件, 目录, 路径, 加密, 解密, 访问, 多项式, 常数项, 常数值, 密钥, 插值, 堆叠, 挂载, 函数, file, contents, path, encrypt, decrypt, access, polynomial, constant, key, interpolation, function

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 113051598 A (UNIONTECH SOFTWARE TECHNOLOGY CO., LTD.) 29 June 2021 (2021-06-29) claims 1-10, and description, paragraphs [0007]-[0074]	1-12
Y	CN 103473490 A (PACIFIC BAOLONG TECHNOLOGY (HUNAN) CO., LTD.) 25 December 2013 (2013-12-25) description, paragraphs [0035]-[0072]	1-12
Y	CN 108632237 A (HUNAN UNIVERSITY OF SCIENCE AND TECHNOLOGY) 09 October 2018 (2018-10-09) description, paragraphs [0018]-[0026]	1-12
Y	CN 104866391 A (SAMSUNG ELECTRONICS (CHINA) R&D CENTER et al.) 26 August 2015 (2015-08-26) description, paragraph [0056]	1-5
A	CN 102136911 A (XIJING UNIVERSITY) 27 July 2011 (2011-07-27) entire document	1-12
A	CN 107241191 A (SOUTHWEST JIAOTONG UNIVERSITY) 10 October 2017 (2017-10-10) entire document	1-12

☐ 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 2022	**26 January 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/120591

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	113051598	A	29 June 2021	CN	113051598	B	15 October 2021
CN	103473490	A	25 December 2013	CN	103473490	B	12 October 2016
CN	108632237	A	09 October 2018		None		
CN	104866391	A	26 August 2015	CN	104866391	B	02 August 2019
CN	102136911	A	27 July 2011		None		
CN	107241191	A	10 October 2017		None		

国际检索报告

国际申请号
PCT/CN2021/120591

A. 主题的分类

G06F 21/60(2013.01)i; G06F 21/62(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNABS;CNTXT;CNKI;SIPOABS;DWPI;USTXT;WOTXT;EPTXT：文件，目录，路径，加密，解密，访问，多项式，常数项，常数值，密钥，插值，堆叠，挂载，函数，file，contents，path，encrypt，decrypt，access，polynomial，constant，key，interpolation，function

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
PX	CN 113051598 A (统信软件技术有限公司) 2021年6月29日 (2021 - 06 - 29) 权利要求第1-10项，说明书第[0007]-[0074]段	1-12
Y	CN 103473490 A (亚太宝龙科技湖南有限公司) 2013年12月25日 (2013 - 12 - 25) 说明书第[0035]-[0072]段	1-12
Y	CN 108632237 A (湖南科技大学) 2018年10月9日 (2018 - 10 - 09) 说明书第[0018]-[0026]段	1-12
Y	CN 104866391 A (三星电子中国研发中心 等) 2015年8月26日 (2015 - 08 - 26) 说明书第[0056]段	1-5
A	CN 102136911 A (西京学院) 2011年7月27日 (2011 - 07 - 27) 全文	1-12
A	CN 107241191 A (西南交通大学) 2017年10月10日 (2017 - 10 - 10) 全文	1-12

☐ 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
2022年1月6日	2022年1月26日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 潘秋羽 电话号码 （86-512）88995784

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/120591

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	113051598	A	2021年6月29日	CN	113051598	B	2021年10月15日
CN	103473490	A	2013年12月25日	CN	103473490	B	2016年10月12日
CN	108632237	A	2018年10月9日		无		
CN	104866391	A	2015年8月26日	CN	104866391	B	2019年8月2日
CN	102136911	A	2011年7月27日		无		
CN	107241191	A	2017年10月10日		无		