(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
2023 年 3 月 30 日 (30.03.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/045249 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01)

(21) 国际申请号: PCT/CN2022/078323

(22) 国际申请日: 2022 年 2 月 28 日 (28.02.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202111116879.2 2021年9月23日 (23.09.2021) CN

(71) 申请人: 苏州浪潮智能科技有限公司 (INSPUR SUZHOU INTELLIGENT TECHNOLOGY CO., LTD.) [CN/CN]; 中国江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。

(72) 发明人: 范益 (FAN, Yi); 中国江苏省苏州市吴中区吴中经济开发区郭巷街道官浦路1号9幢, Jiangsu 215000 (CN)。

(74) 代理人: 北京市万慧达律师事务所 (BEIJING WANHUIDA LAW FIRM); 中国北京市海淀区中关村南大街1号友谊宾馆颐园写字楼2楼, Beijing 100873 (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, JM, 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,

(54) **Title:** OBFUSCATED CODE ENCRYPTION METHOD AND APPARATUS, AND DEVICE AND READABLE STORAGE

(54) **发明名称**: 一种代码混淆的加密方法、装置、设备及可读介质

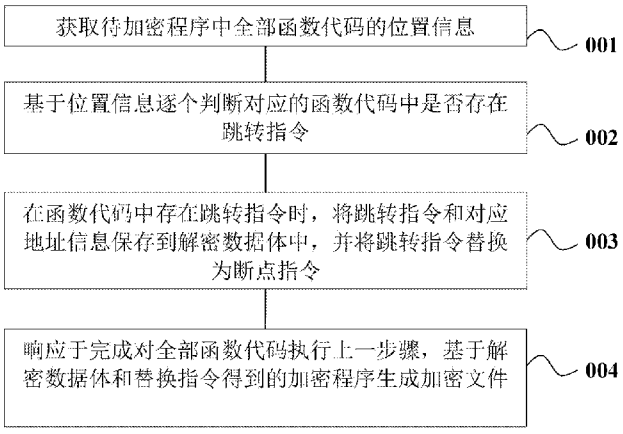

图 1

(57) **Abstract:** Disclosed in the present application are an obfuscated code encryption method and apparatus, and a device and a readable storage. The obfuscated code encryption method comprises: acquiring location information of all function codes in a program to be encrypted; on the basis of the location information, determining, one by one, whether jump instructions exist in corresponding function codes; when jump instructions exist in the function codes, storing the jump instructions and corresponding address information in a decrypted data volume, and replacing the jump instructions with breakpoint instructions; and in response to the completion of executing the previous step on all the function codes, generating an encrypted file on the basis of the decrypted data volume and an encrypted program that is obtained by means of instructions after replacement.

(57) **摘要**: 本申请公开了一种代码混淆的加密方法、装置、设备及可读介质。代码混淆的加密方法包括：获取待加密程序中全部函数代码的位置信息；基于位置信息逐个判断对应的函数代码中是否存在跳转指令；在函数代码中存在跳转指令时，将跳转指令和对应地址信息保存到解密数据体中，并将跳转指令替换为断点指令；以及响应于完成对全部函数代码执行上一步骤，基于解密数据体和替换指令得到的加密程序生成加密文件。

WO 2023/045249 A1

[见续页]

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))。

一种代码混淆的加密方法、装置、设备及可读介质

相关申请的交叉引用

本申请要求于 2021 年 9 月 23 日提交中国专利局，申请号为 CN202111116879.2，申请名称为“一种代码混淆的加密方法、装置、设备及可读介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及计算机与通信技术领域，尤其涉及一种代码混淆的加密方法、装置、设备及可读介质。

背景技术

随着互联网客户端技术的迅速发展，客户端的各种技术越来越丰富，功能也越来越复杂，但由于客户端代码是运行在用户终端上的，攻击者很容易阅读、分析和破解，给系统带来各种风险。

代码混淆（Obfuscated code）亦称为花指令，是将计算机程序的代码转换成一种功能上等价但是难于阅读和理解的形式的行为。代码混淆可以用于程序源代码，也可以用于程序编译而成的中间代码，也有对编译完成的二进制文件代码进行混淆加密的做法。执行代码混淆的程序被称作代码混淆器。

在市场上，各式各样的代码混淆工具常被用在保护软件产品不被反编译和破解，保护软件知识产权等方面，越来越受到人们的重视。现有存在许多功能各异的代码混淆器：将代码中的各种元素，如变量、函数、类的名字改成无意义的名字，比如改写成单个字母、或是简短的无意义字母组合、甚至改写成“_”这样的符号，使得阅读的人无法根据名字猜测其用途；重写代码中的逻辑部分，将其变成功能上等价，但是更难理解的形式，比如将 for 循环（编程语言中一种循环语句）改成 while 循环（编程语言中另一种循环语句）、将循环改写成递归、精简中间变量等；打乱代码的格式，比如删除空格、将多行代码挤到一行中、或者将一行代码断成多行等。

现有的代码混淆方案，可以通过一般的分析手段获得原始流程，从而被破解。

发明内容

在第一方面，本申请实施例提供了一种代码混淆的加密方法，包括以下步骤：获取待加密程序中全部函数代码的位置信息；基于位置信息逐个判断对应的函数代码中是否存在跳转指令；在函数代码中存在跳转指令时，将跳转指令和对应地址信息保存到解密数据体中，并将跳转指令替换为断点指令；以及响应于完成对全部函数代码执行上一步骤，基于解密数据体和替换指令得到的加密程序生成加密文件。

在一些实施方式中，代码混淆的加密方法还包括：通过加密文件获取加密程序，并执行加密程序；响应于执行断点指令，则基于解密数据体获取对应的跳转指令；以及基于跳转指令继续执行加密程序。

在一些实施方式中，基于跳转指令继续执行加密程序，包括：将断点指令替换为对应的跳转指令并执行对应的跳转指令，以跳转到加密程序的对应区域；以及将对应的跳转指令替换为断点指令，并基于对应区域继续执行加密程序。

在一些实施方式中，代码混淆的加密方法还包括：获取待加密文件，并对待加密文件进行校验以判断待加密文件的文件头、程序头表和节头表是否有效；以及响应于待加密文件的文件头、程序头表和节头表有效，基于待加密文件获取待加密程序。

在一些实施方式中，获取待加密程序中全部函数代码的位置信息，包括：获取待加密程序的节头表中的符号列表，并遍历符号列表并基于符号类型判断对应的代码是否为函数；以及在对应的代码为函数代码时，记录函数代码的地址信息和大小信息。

在一些实施方式中，基于位置信息逐个判断对应的函数代码中是否存在跳转指令包括：基于位置信息逐个遍历对应的函数代码，以判断是否存在跳转指令；在不存在跳转指令时，进一步判断函数代码是否完成遍历；以及在函数代码未完成遍历时，继续判断函数代码中是否存在跳转指令。

在一些实施方式中，代码混淆的加密方法还包括：在函数代码完成遍历时，继续判断下一个函数代码中是否存在跳转指令。

在第二方面，本申请实施例提供了一种代码混淆的加密装置，包括：第一模块，用于获取待加密程序中全部函数代码的位置信息；第二模块，用于基于位置信息逐个判断对应的函数代码中是否存在跳转指令；第三模块，用于在函数代码中存在跳转指令时，将跳转指令和对应地址信息保存到解密数据体中，并将跳转指令替换为断点指令；以及第四模块，用于响应于完成对全部函数代码执行第三模块的步骤，基于解密数据体和替

换指令得到的加密程序生成加密文件。

在第三方面，本申请实施例提供了一种计算机设备，包括存储器及一个或多个处理器，存储器中储存有计算机可读指令，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行前述任一实施例中代码混淆的加密方法的步骤。

在第四方面，本申请实施例提供了一个或多个存储有计算机可读指令的非易失性计算机可读存储介质，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行前述任一实施例中代码混淆的加密方法的步骤。

附图说明

为了更清楚地说明本申请实施例或相关技术方案，下面将对实施例或相关描述中可能涉及的附图作简单地介绍，显而易见地，下面描述中的附图仅仅涉及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实施例。

图 1 为根据一个或多个实施例中，代码混淆的加密方法的实施例的示意图；

图 2 为根据一个或多个实施例中，代码混淆的加密方法的实施例的运行流程图；

图 3 为根据一个或多个实施例中，代码混淆的加密方法的实施例的运行流程图；

图 4 为根据一个或多个实施例中，代码混淆的加密装置的实施例的示意图；

图 5 为根据一个或多个实施例中，计算机设备的实施例的示意图；

图 6 为根据一个或多个实施例中，非易失性计算机可读存储介质的实施例的示意图。

具体实施方式

为使本申请的技术方案和优点更加清楚明白，以下结合具体实施例，并参照附图，对本申请实施例进一步详细说明。

需要说明的是，本申请实施例中所有使用“第一”和“第二”的表述均是为了区分两个相同名称非相同的实体或者非相同的参量，可见“第一”“第二”仅为了表述的方便，不应理解为对本申请实施例的限定，后续实施例对此不再一一说明。

在第一方面，本申请实施例提供了一种代码混淆的加密方法。图 1 示出的是本申请实施例提供的代码混淆的加密方法的示意图。如图 1 所示，本申请实施例的代码混淆的加密方法可以包括如下步骤：

001、获取待加密程序中全部函数代码的位置信息；

002、基于位置信息逐个判断对应的函数代码中是否存在跳转指令；

003、在函数代码中存在跳转指令时，将跳转指令和对应地址信息保存到解密数据体中，并将跳转指令替换为断点指令；

004、响应于完成对全部函数代码执行上一步骤，基于解密数据体和替换指令得到的加密程序生成加密文件。

在图 1 所示的实施例中，将动态调试技术和代码混淆技术相结合，利用动态调试技术实现代码的动态加密和解密。一方面，可以将原本的程序流程拆解，使得想要进行程序逆向就必须完整跟踪程序执行流程，或破解解密模块代码和数据体，进行手动的指令替换，这样可以大幅提高逆向难度，保护程序不被轻易破解；另一方面，已经附加了动态调试的程序是不能被附加第二个动态调试工具的，从这个层面上实现了一定反调试的效果。

图 1 所示的实施例涉及混淆工具本体和混淆加密后的解密模块部分。其中混淆工具本体包括代码混淆引擎模块，负责读取程序文件、提取关键信息、并对程序进行混淆加密。代码混淆引擎模块包括指令识别引擎和原始解密引擎：指令识别引擎负责对文件二进制代码进行识别，转换成汇编指令以进行分析和处理；原始解密引擎包括预先定义好的、包含完整解密流程，用于动态加密解密被混淆的程序。混淆加密后的解密模块部分包括解密引擎、解密数据体和被混淆的程序。

在一些实施例中，图 1 中的步骤 003，具体包括：响应于函数代码中存在跳转指令，将跳转指令和对应地址信息保存到解密数据体中，并将跳转指令替换为断点指令。

图 2 示出的是本申请实施例提供的代码混淆的加密方法的一种运行流程图。如图 2 所示，在本实施例中，运行流程包括：

步骤 101，读取待加密程序文件。待加密程序文件可以由用户指定。

步骤 102，校验文件。校验文件指校验待加密程序文件。步骤 102 主要包括校验文件结构和头结构。头结构包括文件头、程序头表和节头表。其中文件头和节头表是最主要使用的两个部分。对于节头表，仅需校验其是否有效即可，因为部分程序在编译时指定了参数，会消除程序中的节头表，导致无法通过节头表去获知和遍历程序中的函数及其代码，因而是无法进行混淆的，因此需要进行严格的校验。

步骤 103，根据表信息遍历函数。在校验并读取节头表信息（也可称为表信息）后，便在节头表信息中进行查找和检索，主要是在节头表中查找和检索符号表.symtab 节，从而获取文件符号（一般指向的是函数或全局变量等）列表。然后通过遍历文件符号列

表，并校验符号类型判断是否为函数，如果是函数则获取其地址和大小的信息，这样就获取到了具体的函数的代码在文件中的位置。

步骤 104，判断是否遍历结束。步骤 104 用于和步骤 103 协作。判断是否遍历结束，可以理解为判断文件符号列表的遍历是否完成。

如果遍历结束，即文件符号列表的遍历完成，则执行步骤 107，如遍历未结束，即文件符号列表的遍历未完成，则继续进行遍历混淆的流程，开始执行步骤 105。

步骤 105，遍历函数代码。在步骤 103 获取了函数代码在文件中的位置后，便跳转到对应的位置上，使用一个循环遍历该函数的代码，结束条件为遍历到函数结尾，即获取到该函数的地址和大小信息。步骤 105 与图 2 中“调用指令识别引擎，识别指令”的流程是相互协作的。在跳转到函数开头后，需要将指针传递给识别引擎，由识别引擎判断决定需要读入几个字节的数据，以及判断这是一个什么指令，因为指令不定长，短的指令只有 1 个字节，长的则可能包含地址操作数等。当读取并判断出一条完整的指令后，指针将会移动到下一个指令开头的位置。可以判断识别出的指令判断是否为跳转指令 JMP 或 CALL 指令，可以根据判断结果执行步骤 106 或其他。

步骤 106，保存指令及地址到解密数据体中，将指令替换为 INT3。当识别出的指令为跳转指令 JMP 或 CALL 时，执行步骤 106。步骤 106 将会将原指令的信息，如地址、指令类型、原指令内容等保存到一个数据体（即解密数据体）中，然后将原指令替换为 INT3，INT3 为一种断点指令。断点指令将会在执行时被系统拦截，然后将控制权移交给动态调试工具，在本方案中是解密模块，由解密模块进行解密后再执行，并在执行过后重新加密。

步骤 107，将解密数据体与解密引擎绑定。当遍历混淆完成后，便会将预先定义好的解密模块与保存了完整混淆信息的数据体，即解密数据体相绑定，然后与混淆加密保护后的程序文件一同写入到一个文件中，这个文件就是保护后的程序。由此，完成解密数据体与解密引擎绑定。之后，根据需要，可以提示混淆成功，并推出流程。

在本申请的一些实施例中，代码混淆的加密方法还包括：通过加密文件获取加密程序，并执行加密程序；响应于执行断点指令，基于解密数据体获取对应的跳转指令；基于跳转指令继续执行加密程序。

在本实施例中，待加密程序在执行时，会通过动态调试技术进行动态的解密和加密，在程序正常执行的同时保证安全性。图 3 示出的是本申请实施例提供的一种代码混淆的加密方法的运行流程图。如图 3 所示，运行流程包括：

步骤 201，待加密程序启动解密模块注册加载。在程序启动时，解密模块会优先于待

加密程序启动，完成环境初始化，设置动态调试环境等工作，然后创建一个子进程并启动待加密程序，解密模块以父进程的形式对待加密程序的子进程进行动态调试。

步骤 202，待加密程序正常执行。待加密程序大部分的原始代码未做更改，可正常执行。

步骤 203，执行 INT3 指令。因为程序中的跳转指令 JMP/CALL 指令均被替换，所以在执行到该指令时，会被替换后的断点指令 INT3 所拦截，然后系统会将执行权转移给动态调试工具，本方案中是父进程的解密模块。

步骤 204，解密模块接受拦截信息。在系统将控制权移交给解密模块时，会将断点指令的信息一并传递给模块，因此解密模块可以获得该指令的相关信息，如地址等。

步骤 205，根据信息查找解密数据体。随后解密模块将依据此信息（主要是地址偏移等），进入解密数据体中进行查找，找到该地址所对应的原始指令信息，然后使用原始指令替换该 INT3 指令，实现动态解密。替换后，使用单步步过的函数执行该指令，使待加密程序正常执行到下一区域，并且保持解密模块的控制权。

步骤 206，重新替换为 INT3 指令。在执行后，解密模块会将原指令再次替换回 INT3 断点指令，实现动态加密。然后解密模块会将控制权转移回待加密程序，其已经执行到跳转指令 JMP/CALL 指令所指向的新区域，待加密程序在获取到控制权后可以正常执行，直到下一次遇到 INT3 跳转指令再次执行本流程。

在本申请的一些实施例中，基于跳转指令继续执行加密程序，包括：将断点指令替换为对应的跳转指令并执行对应的跳转指令，以跳转到加密程序的对应区域；将对应的跳转指令替换为断点指令，并基于对应区域继续执行加密程序。

在本申请的一些实施例中，代码混淆的加密方法还包括：获取待加密文件，并对待加密文件进行校验以判断待加密文件的文件头、程序头表和节头表是否有效；响应于待加密文件的文件头、程序头表和节头表有效，基于待加密文件获取待加密程序。

在一些实施例中，获取待加密程序中全部函数代码的位置信息，包括：获取待加密程序的节头表中的符号列表，并遍历符号列表并基于符号类型判断对应的代码是否为函数；若是对应的代码为函数代码，则记录函数代码的地址信息和大小信息。

在一些实施例中，获取待加密程序中全部函数代码的位置信息，包括：获取待加密程序的节头表中的符号列表，并遍历符号列表并基于符号类型判断对应的代码是否为函数；在对应的代码为函数代码时，记录函数代码的地址信息和大小信息。具体地，在对应的代码为函数代码时，记录函数代码的地址信息和大小信息，包括：响应于对应的代码为函数代码，记录函数代码的地址信息和大小信息。

在一些实施例中，基于位置信息逐个判断对应的函数代码中是否存在跳转指令，包括：基于位置信息逐个遍历对应的函数代码，以判断是否存在跳转指令；若是不存在跳转指令，则进一步判断函数代码是否完成遍历；若是函数代码未完成遍历，则继续判断函数代码中是否存在跳转指令。

在一些实施例中，基于位置信息逐个判断对应的函数代码中是否存在跳转指令，包括：基于位置信息逐个遍历对应的函数代码，以判断是否存在跳转指令；在不存在跳转指令时，进一步判断函数代码是否完成遍历；在函数代码未完成遍历时，继续判断函数代码中是否存在跳转指令。

具体地，在不存在跳转指令时，进一步判断函数代码是否完成遍历，包括：响应于不存在跳转指令，进一步判断函数代码是否完成遍历。在函数代码未完成遍历时，继续判断函数代码中是否存在跳转指令，包括：响应于函数代码未完成遍历，继续判断函数代码中是否存在跳转指令。

在本申请的一些实施例中，方法还包括：若是函数代码完成遍历，则继续判断下一个函数代码中是否存在跳转指令。

代码混淆的加密方法中，将动态调试技术融入到代码混淆中，通过指令替换将原本的程序流程进行拆解，并允许被加密保护的程序在运行中动态地还原和拆解代码，能有效避免出现破解者将完整的程序代码保存下来导致程序被破解的问题。本申请实施例所提供的方法不能通过一般的分析手段获得原始流程，并在运行中通过动态调试技术实时恢复和再混淆，因而必须完整地跟踪每一步程序执行流程才有发现原始流程的可能。这样，大幅提高了加密保护强度，提高了破解成本，从而提高了程序的安全性。

需要特别指出的是，在合理的前提下，上述各个实施例中代码混淆的加密方法的一些步骤可以相互交叉、替换、增加或删减，因此，这些合理的排列组合变换之于代码混淆的加密方法也应当属于本申请的保护范围，并且不应将本申请的保护范围局限在实施例之上。

在第二方面，本申请实施例提供了一种代码混淆的加密装置。图 4 是本申请实施例提供的一种代码混淆的加密装置的示意图。如图 4 所示，本申请实施例的代码混淆的加密装置包括如下模块：第一模块 011，用于获取待加密程序中全部函数代码的位置信息；第二模块 012，用于基于位置信息逐个判断对应的函数代码中是否存在跳转指令；第三模块 013，用于在函数代码中存在跳转指令时，将跳转指令和对应地址信息保存到解密数据体中，并将跳转指令替换为断点指令；以及第四模块 014，用于响应于完成对全部函数代码执行第三模块的步骤，基于解密数据体和替换指令得到的加密程序生成加密文件。

在第三方面，本申请实施例的提供了一种计算机设备。图 5 是本申请实施例提供的计算机设备的示意图。如图 5 所示，本申请实施例的计算机设备包括一个或多个处理器 021 以及存储器 022。存储器 022 存储有计算机可读指令 023，计算机可读指令 023 被一个或多个处理器 021 执行时，使得一个或多个处理器 021 执行前述任一实施例中代码混淆的加密方法的步骤。

在第四方面，本申请实施例提供了一个或多个存储有计算机可读指令的非易失性计算机可读存储介质。图 6 示出的是非易失性计算机可读存储介质的示意图。如图 6 所示，非易失性计算机可读存储介质 031 存储有计算机程可读指令 032，计算机可读指令 032 被一个或多个处理器执行时，使得一个或多个处理器执行前述任一实施例中代码混淆的加密方法的步骤。

最后需要说明的是，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，可以通过计算机可读指令来指令相关硬件来完成，代码混淆的加密方法的计算机可读指令可存储于一计算机可读存储介质中，计算机可读指令被执行时，可实现前述任一实施例中代码混淆的加密方法的步骤。其中，计算机可读存储介质可为磁碟、光盘、只读存储记忆体（ROM）或随机存储记忆体（RAM）等。上述计算机可读指令的实施例，可以达到与之对应的前述任一代码混淆的加密方法实施例相同或者相类似的效果。

此外，代码混淆的加密方法中的步骤以及系统单元也可以利用控制器以及用于存储使得控制器实现上述步骤或单元功能的计算机可读指令的计算机可读存储介质实现。

本领域技术人员还将明白的是，结合这里的公开所描述的各种示例性逻辑块、模块、电路和算法步骤可以被实现为电子硬件、计算机软件或两者的组合。为了清楚地说明硬件和软件的这种可互换性，已经就各种示意性组件、方块、模块、电路和步骤的功能对其进行了一般性的描述。这种功能是被实现为软件还是被实现为硬件取决于具体应用以及施加给整个系统的设计约束。本领域技术人员可以针对每种具体应用以各种方式来实现的功能，但是这种实现决定不应被解释为导致脱离本申请实施例公开的范围。

在一个或多个示例性设计中，功能可以在硬件、软件、固件或其任意组合中实现。如果在软件中实现，则可以将功能作为一个或多个指令或代码存储在计算机可读介质上或通过计算机可读介质来传送。计算机可读介质包括计算机存储介质和通信介质，该通信介质包括有助于将计算机程序从一个位置传送到另一个位置的任何介质。存储介质可以是能够被通用或专用计算机访问的任何可用介质。作为例子而非限制性的，该计算机可读介质可以包括 RAM、ROM、EEPROM、CD-ROM 或其它光盘存储设备、磁盘存储

设备或其它磁性存储设备，或者是可以用于携带或存储形式为指令或数据结构的所需程序代码并且能够被通用或专用计算机或者通用或专用处理器访问的任何其它介质。此外，任何连接都可以适当地称为计算机可读介质。例如，如果使用同轴线缆、光纤线缆、双绞线、数字用户线路（DSL）或诸如红外线、无线电和微波的无线技术来从网站、服务器或其它远程源发送软件，则上述同轴线缆、光纤线缆、双绞线、DSL 或诸如红外线、无线电和微波的无线技术均包括在介质的定义。如这里所使用的，磁盘和光盘包括压缩盘（CD）、激光盘、光盘、数字多功能盘（DVD）、软盘、蓝光盘，其中磁盘通常磁性地再现数据，而光盘利用激光光学地再现数据。上述内容的组合也应当包括在计算机可读介质的范围内。

以上是本申请公开的示例性实施例，但是应当注意，在不背离权利要求限定的本申请实施例公开的范围的前提下，可以进行多种改变和修改。根据这里描述的公开实施例的方法权利要求的功能、步骤和/或动作不需以任何特定顺序执行。此外，尽管本申请实施例公开的元素可以以个体形式描述或要求，但除非明确限制为单数，也可以理解为多个。

应当理解的是，在本文中使用的，除非上下文清楚地支持例外情况，单数形式“一个”旨在也包括复数形式。还应当理解的是，在本文中使用的“和/或”是指包括一个或者一个以上相关联地列出的项目的任意和所有可能组合。

本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过计算机可读指令来指令相关的硬件完成，计算机可读指令可以存储于一种计算机可读存储介质中，计算机可读存储介质可以是只读存储器，磁盘或光盘等。

所属领域的普通技术人员应当理解：以上任何实施例的讨论仅为示例性的，并非旨在暗示本申请实施例公开的范围（包括权利要求）被限于这些例子；在本申请实施例的思路下，以上实施例或者不同实施例中的技术特征之间也可以进行组合，并存在如上的本申请实施例的不同方面的许多其它变化，为了简明它们没有在细节中提供。因此，凡在本申请实施例的精神和原则之内，所做的任何省略、修改、等同替换、改进等，均应包含在本申请实施例的保护范围之内。

权 利 要 求 书

1. 一种代码混淆的加密方法，其特征在于，包括：

获取待加密程序中全部函数代码的位置信息；

基于所述位置信息逐个判断对应的所述函数代码中是否存在跳转指令；

在所述函数代码中存在跳转指令时，将所述跳转指令和对应地址信息保存到解密数据体中，并将所述跳转指令替换为断点指令；以及

响应于完成对所述全部函数代码执行上一步骤，基于所述解密数据体和替换指令得到的加密程序生成加密文件。

2. 根据权利要求 1 所述的代码混淆的加密方法，其特征在于，还包括：

通过所述加密文件获取所述加密程序，并执行所述加密程序；

响应于执行断点指令，基于所述解密数据体获取对应的跳转指令；以及

基于所述跳转指令继续执行所述加密程序。

3. 根据权利要求 2 所述的代码混淆的加密方法，其特征在于，所述基于所述跳转指令继续执行所述加密程序，包括：

将所述断点指令替换为所述对应的跳转指令并执行所述对应的跳转指令，以跳转到所述加密程序的对应区域；以及

将所述对应的跳转指令替换为所述断点指令，并基于所述对应区域继续执行所述加密程序。

4. 根据权利要求 1 至 3 任一所述的代码混淆的加密方法，其特征在于，还包括：

获取待加密文件，并对所述待加密文件进行校验以判断所述待加密文件的文件头、程序头表和节头表是否有效；以及

响应于所述待加密文件的文件头、程序头表和节头表有效，基于所述待加密文件获取待加密程序。

5. 根据权利要求 1 至 3 任一所述的代码混淆的加密方法，其特征在于，所述获取待加密程序中全部函数代码的位置信息，包括：

获取待加密程序的节头表中的符号列表，并遍历所述符号列表并基于符号类型判断对应的代码是否为函数；以及

在对应的代码为函数代码时，记录所述函数代码的地址信息和大小信息。

6. 根据权利要求 1 至 3 任一所述的代码混淆的加密方法，其特征在于，所述基于所述位置信息逐个判断对应的所述函数代码中是否存在跳转指令，包括：

基于所述位置信息逐个遍历对应的所述函数代码，以判断是否存在跳转指令；

在不存在跳转指令时，进一步判断所述函数代码是否完成遍历；以及

在所述函数代码未完成遍历时，继续判断所述函数代码中是否存在跳转指令。

7. 根据权利要求 6 所述的代码混淆的加密方法，其特征在于，还包括：

在所述函数代码完成遍历时，继续判断下一个所述函数代码中是否存在跳转指令。

8. 一种代码混淆的加密装置，其特征在于，包括：

第一模块，用于获取待加密程序中全部函数代码的位置信息；

第二模块，用于基于所述位置信息逐个判断对应的所述函数代码中是否存在跳转指令；

第三模块，用于在所述函数代码中存在跳转指令时，将所述跳转指令和对应地址信息保存到解密数据体中，并将所述跳转指令替换为断点指令；以及

第四模块，用于响应于完成对所述全部函数代码执行所述第三模块的步骤，基于所述解密数据体和替换指令得到的加密程序生成加密文件。

9. 一种计算机设备，其特征在于，包括存储器及一个或多个处理器，所述存储器中储存有计算机可读指令，所述计算机可读指令被所述一个或多个处理器执行时，使得所述一个或多个处理器执行如权利要求 1-7 任一项所述方法的步骤。

10. 一个或多个存储有计算机可读指令的非易失性计算机可读存储介质，其特征在于，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行如权利要 1-7 任一项所述方法的步骤。

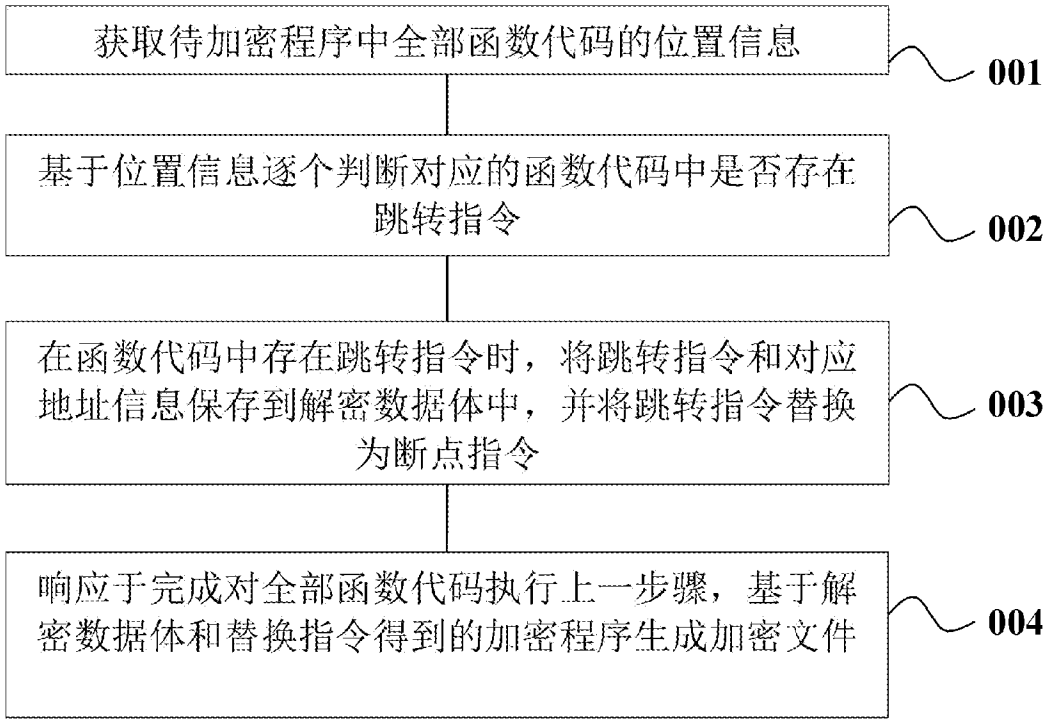
获取待加密程序中全部函数代码的位置信息
001
基于位置信息逐个判断对应的函数代码中是否存在跳转指令
002
在函数代码中存在跳转指令时，将跳转指令和对应地址信息保存到解密数据体中，并将跳转指令替换为断点指令
003
响应于完成对全部函数代码执行上一步骤，基于解密数据体和替换指令得到的加密程序生成加密文件
004

图 1

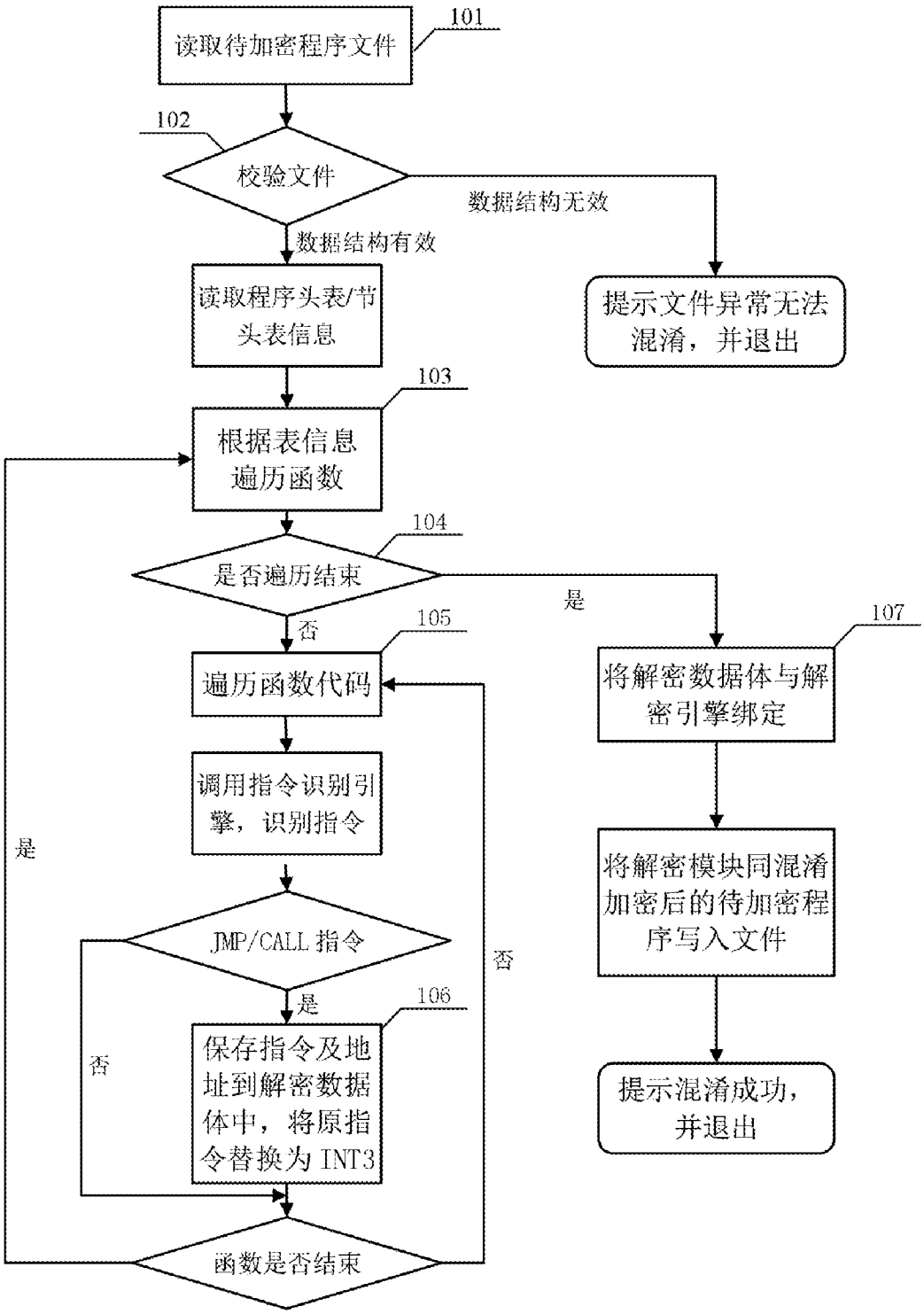
读取待加密程序文件
101
102
校验文件
数据结构无效
数据结构有效
提示文件异常无法混淆，并退出
读取程序头表/节头表信息
103
根据表信息遍历函数
104
是否遍历结束
是
否
105
遍历函数代码
调用指令识别引擎，识别指令
JMP/CALL 指令
是
否
106
保存指令及地址到解密数据体中，将原指令替换为 INT3
否
函数是否结束
是
107
将解密数据体与解密引擎绑定
将解密模块同混淆加密后的待加密程序写入文件
提示混淆成功，并退出

图 2

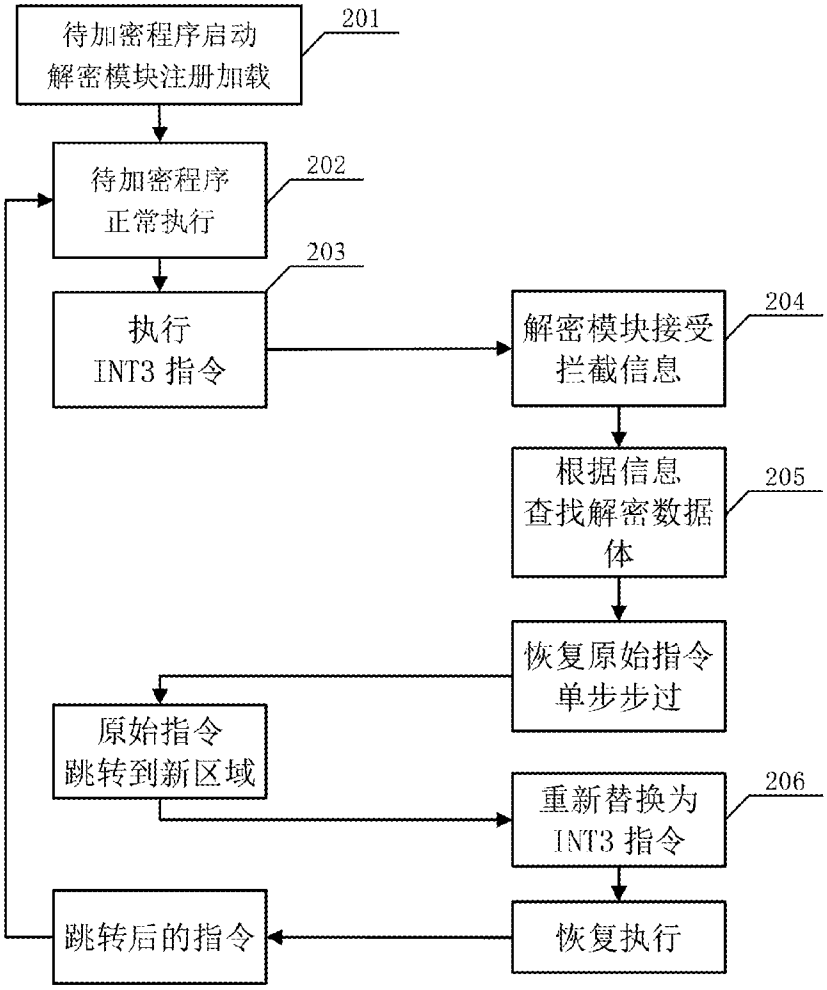
待加密程序启动
解密模块注册加载
201
待加密程序
正常执行
202
执行
INT3 指令
203
解密模块接受
拦截信息
204
根据信息
查找解密数据
体
205
恢复原始指令
单步步过
原始指令
跳转到新区域
重新替换为
INT3 指令
206
跳转后的指令
恢复执行

图 3

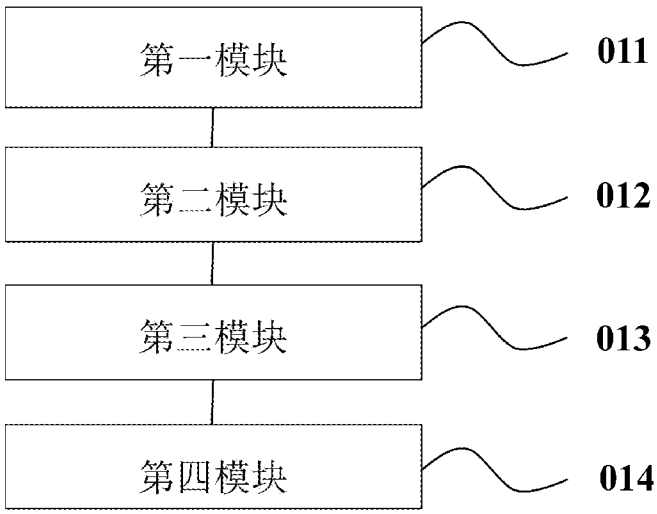
第一模块
011
第二模块
012
第三模块
013
第四模块
014

图 4

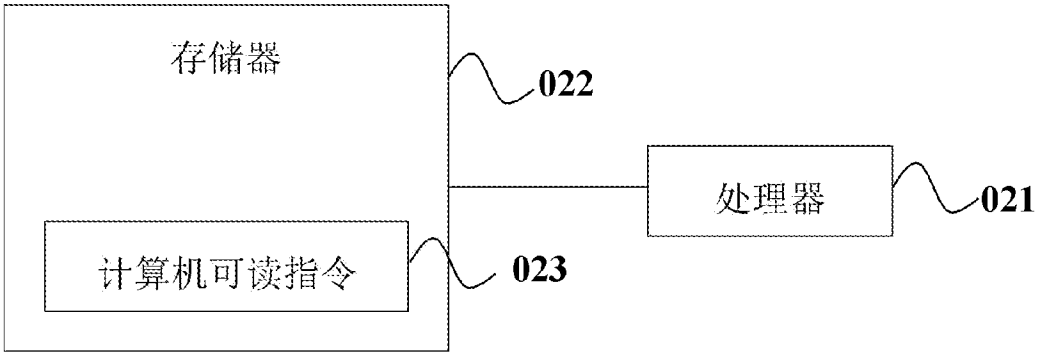

图 5

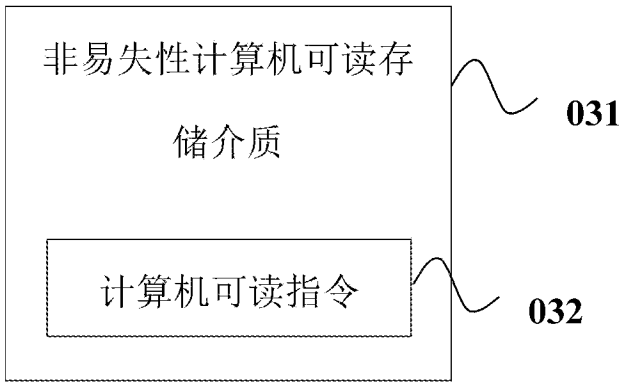

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/078323

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(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)

WPI, EPODOC, CNPAT, IEEE, CNKI, 百度, BAIDU: 代码, 混淆, 加密, 解密, 跳转, 函数, 断点, 替换, 位置, 地址, 校验, 遍历, code, obfuscate, encrypt, decrypt, jump, function, breakpoint, replace, location, address, verify, traversal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 113569269 A (SUZHOU INSPUR INTELLIGENT TECHNOLOGY CO., LTD.) 29 October 2021 (2021-10-29) claims 1-10	1-10
X	CN 110502874 A (XI'AN UNIVERSITY OF TECHNOLOGY) 26 November 2019 (2019-11-26) description, paragraphs [0026]-[0055], and figures 1-3	1-10
A	CN 112115427 A (MIGU CULTURE TECHNOLOGY CO., LTD. et al.) 22 December 2020 (2020-12-22) entire document	1-10
A	CN 112052461 A (BEIJING ZHIYOU WANG'AN TECHNOLOGY CO., LTD.) 08 December 2020 (2020-12-08) entire document	1-10

☐ 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
01 June 2022	**21 June 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/CN2022/078323

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 113569269 A	29 October 2021	None	
CN 110502874 A	26 November 2019	CN 110502874 B	25 May 2021
CN 112115427 A	22 December 2020	None	
CN 112052461 A	08 December 2020	None	

国际检索报告

国际申请号
PCT/CN2022/078323

A. 主题的分类

G06F 21/60(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））

WPI,EPODOC,CNPAT,IEEE,CNKI,百度:代码，混淆，加密，解密，跳转，函数，断点，替换，位置，地址，校验，遍历，code，obfuscate，encrypt，decrypt，jump，function，breakpoint，replace，location，address，verify，traversal

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 113569269 A (苏州浪潮智能科技有限公司) 2021年10月29日 (2021-10-29) 权利要求1-10	1-10
X	CN 110502874 A (西安理工大学) 2019年11月26日 (2019-11-26) 说明书第[0026]-[0055]段，附图1-3	1-10
A	CN 112115427 A (咪咕文化科技有限公司 等) 2020年12月22日 (2020-12-22) 全文	1-10
A	CN 112052461 A (北京智游网安科技有限公司) 2020年12月8日 (2020-12-08) 全文	1-10

☐ 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6月1日	2022年6月21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 李易玮 电话号码 86-(10)-53961395

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/078323

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 113569269 A	2021年10月29日	无	
CN 110502874 A	2019年11月26日	CN 110502874 B	2021年5月25日
CN 112115427 A	2020年12月22日	无	
CN 112052461 A	2020年12月8日	无	