(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 2 月 21 日 (21.02.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/033751 A1

(51) 国际专利分类号:
H04L 29/08 (2006.01)

(21) 国际申请号: PCT/CN2018/079160

(22) 国际申请日: 2018 年 3 月 15 日 (15.03.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710693187.1 2017年8月14日 (14.08.2017) CN

(71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。

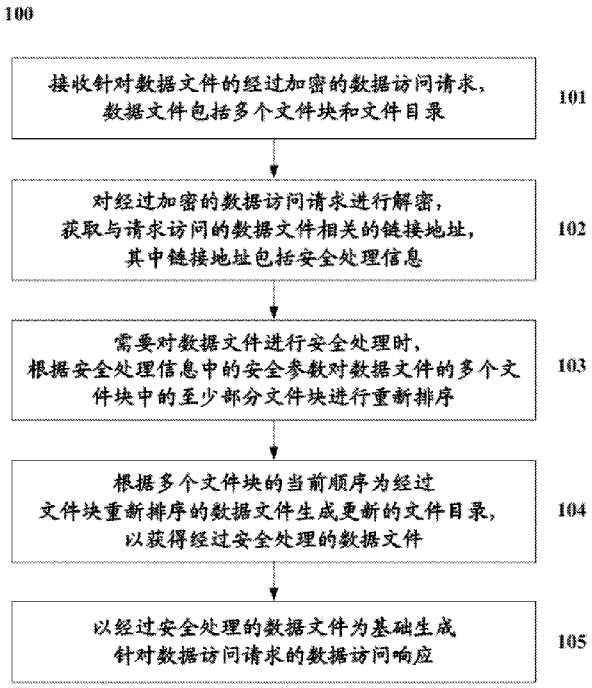
(72) 发明人: 尹俊 (YIN, Jun); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 李强 (LI, Qiang); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 刘贵荣 (LIU, Guirong); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 曾明 (ZENG, Ming); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 王兴刚 (WANG, Xinggang); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 田野 (TIAN, Ye); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 陈浩 (CHEN, Hao); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: 北京智汇东方知识产权代理事务所 (普通合伙) (WISEAST INTELLECTUAL PROPERTY

WO 2019/033751 A1

(54) **Title:** METHOD AND SYSTEM FOR PERFORMING SECURITY PROCESSING ON DATA FILE

(54) 发明名称: 一种用于对数据文件进行安全处理的方法及系统



101 RECEIVE AN ENCRYPTED DATA ACCESS REQUEST FOR A DATA FILE, THE DATA FILE COMPRISING A PLURALITY OF FILE BLOCKS AND A FILE DIRECTORY
102 DECRYPT THE ENCRYPTED DATA ACCESS REQUEST, AND OBTAIN A LINK ADDRESS RELATED TO THE REQUESTED DATA FILE, WHEREIN THE LINK ADDRESS COMPRISES SECURITY PROCESSING INFORMATION
103 IF THE DATA FILE REQUIRES SECURITY PROCESSING, RESORT, ACCORDING TO A SECURITY PARAMETER IN THE SECURITY PROCESSING INFORMATION, AT LEAST A PART OF THE FILE BLOCKS IN THE DATA FILE
104 GENERATE, ACCORDING TO A CURRENT ORDER OF THE FILE BLOCKS, AN UPDATED FILE DIRECTORY FOR THE DATA FILE IN WHICH THE FILE BLOCKS HAVE BEEN RESORTED, SO AS TO OBTAIN A DATA FILE HAVING UNDERGONE SECURITY PROCESSING
105 GENERATE A DATA ACCESS RESPONSE FOR THE DATA ACCESS REQUEST ON THE BASIS OF THE DATA FILE HAVING UNDERGONE SECURITY PROCESSING

图 1

(57) **Abstract:** The present invention discloses a method for performing security processing on a data file. The method comprises: receiving an encrypted data access request for a data file, the data file comprising a plurality of file blocks; decrypting the encrypted data access request, and obtaining a link address related to the requested data file, wherein the link address comprises security processing information; if a security identifier in the security processing information indicates that it is necessary to perform security processing on the data file before responding to the data access request, resorting, according to a security parameter in the security processing

[见续页]

LAW FIRM)；中国北京市海淀区花园路13号5幢320房间, Beijing 100088 (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。

(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))。

information, at least a part of the file blocks of the data file, so as to obtain the data file having undergone security processing; and generating a data access response for the data access request on the basis of the data file having undergone security processing.

(57) 摘要：本发明公开了一种用于对数据文件进行安全处理的方法，方法包括：接收针对数据文件的经过加密的数据访问请求，数据文件包括多个文件块；对经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中链接地址包括安全处理信息；当安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对数据文件进行安全处理时，根据安全处理信息中的安全参数对数据文件的多个文件块中的至少部分文件块进行重新排序，获得经过安全处理的数据文件；以及以经过安全处理的数据文件为基础生成针对数据访问请求的数据访问响应。

一种用于对数据文件进行安全处理的方法及系统

技术领域

本发明涉及信息技术领域，更具体地，涉及一种用于对数据文件进行安全处理的方法及系统。

背景技术

越来越多的用户通过网络进行数据文件的下载，在对热门应用的数据文件下载过程中，经常是由业务服务方提供下载链接渠道，服务方由于想向用户推送经过修改过的应用的数据，通常会对热门的应用数据的下载请求进行劫持，一般劫持方在识别到用户对应用的下载请求后，会将修改后的应用数据提供给用户，因此，用户会获得经过服务方修改后的应用。

例如，用户通过第三方浏览器请求下载应用的 APK 的数据文件，第三方浏览器利用 HPPT 分段下载的特征，第三方浏览器对用户请求下载的 APK 数据文件中的部分文件进行取样，并将取样的文件部分内容与浏览器方的 APK 数据文件进行匹配，在匹配成功后，将该应用 APK 数据文件的下载切换至浏览器方自己的服务平台，将用户的下载请求指向浏览器方的 APK 数据文件。用户从浏览器方下载 APK 数据文件后，由于 APK 数据文件已经经过了第三方浏览器的修改，并非为用户真正请求下载的 APK 文件。用户在下载被修改 APK 文件后，可能不能正常使用该 APK 数据文件，或修改后的 APK 文件，对用户的系统及数据安全造成威胁。

因此，需要一种技术，以实现对数据文件进行安全处理。

发明内容

本发明提供了一种用于对数据文件进行安全处理的方法及系统，以解决如何对数据文件进行安全处理的问题。

为了解决上述问题，本发明提供一种用于对数据文件进行安全处理的方法，所述方法包括：

接收针对数据文件的经过加密的数据访问请求，所述数据文件包括多个文件块；

对所述经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中所述链接地址包括安全处理信息；

当所述安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对所述数据文件进行安全处理时，根据所述安全处理信息中的安全参数对所述数据文件的多个文件块中的至少部分文件块进行重新排序；

获得经过安全处理的数据文件；以及

以所述经过安全处理的数据文件为基础生成针对所述数据访问请求的数据访问响应。

基于本发明的另一方面，提供一种用于对数据文件进行安全处理的方法，所述方法包括：

接收针对数据文件的经过加密的数据访问请求，所述数据文件包括多个文件块和文件目录；

对所述经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中所述链接地址包括安全处理信息；

当所述安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对所述数据文件进行安全处理时，在所述数据文件的多个随机位置增加多个随机文件块，根据所述安全处理信息中的安全参数对所述数据文件的当前文件块中的至少部分文件块进行重新排序；

根据所述当前文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，以获得经过安全处理的数据文件；以及

以所述经过安全处理的数据文件为基础生成针对所述数据访问请求的数据访问响应。

基于本发明的另一方面，提供一种用于对数据文件进行安全处理的系统，所述系统包括：

接收单元，接收针对数据文件的经过加密的数据访问请求，所述数据文件包括多个文件块；

解密单元，对所述经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中所述链接地址包括安全处理信息；

处理单元，当所述安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对所述数据文件进行安全处理时，根据所述安全处理信息中的安全参数对所述数据文件的多个文件块中的至少部分文件块进行重新排序；

更新单元，获得经过安全处理的数据文件；以及

发送单元，以所述经过安全处理的数据文件为基础生成针对所述数据访问请求的数据访问响应。

基于本发明的另一方面，提供一种移动终端，包括或用于执行上述中任意一项所述的系统。

基于本发明的另一方面，本发明提供一种用于对数据文件进行安全处理的系统，所述系统包括：

接收单元，接收针对数据文件的经过加密的数据访问请求，所述数据文件包括多个文件块和文件目录；

解密单元，对所述经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中所述链接地址包括安全处理信息；

处理单元，当所述安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对所述数据文件进行安全处理时，在所述数据文件的多个随机位置增加多

个随机文件块，根据所述安全处理信息中的安全参数对所述数据文件的当前文件块中的至少部分文件块进行重新排序；

更新单元，根据所述当前文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，以获得经过安全处理的数据文件；以及

发送单元，以所述经过安全处理的数据文件为基础生成针对所述数据访问请求的数据访问响应。

基于本发明的另一方面，提供一种移动终端，包括或用于执行上述中任意一项所述的系统。

根据本发明的又一个方面，提供了一种计算机可读介质，其中存储了计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行所述用于对数据文件进行安全处理的方法。

根据本发明的再一个方面，提供了一种计算设备，包括处理器；以及存储了计算机可读代码的存储器，所述计算机可读代码被所述处理器运行时，导致所述计算设备执行所述用于对数据文件进行安全处理的方法。

本申请的技术方案通过将用户请求下载的数据文件中文件块排序进行打乱，对于用户的每次下载请求，数据文件都会进行重新排序。本申请的技术方案避免了数据劫持者可以通过获取部分文件，以及通过提取部分文件的特征而获得对数据文件的匹配，为用户提供下载文件。

附图说明

通过参考下面的附图，可以更为完整地理解本发明的示例性实施方式：

图 1 为根据本发明优选实施方式的对数据文件进行安全处理的方法流程图；

图 2 为根据本发明优选实施方式的数据文件结构示意图；

图 3 为根据本发明优选实施方式的对数据文件中文件块进行重新排序示意图；

图 4 为根据本发明优选实施方式的对数据文件进行安全处理的方法流程图；

图 5 为根据本发明优选实施方式的对数据文件进行安全处理的方法流程图；图 6 为根据本发明优选实施方式的对数据文件进行安全处理的系统结构；

图 7 示出了用于执行根据本发明的用于对数据文件进行安全处理的方法的计算设备的框图；以及

图 8 示出了用于保持或者携带实现根据本发明的用于对数据文件进行安全处理的方法的程序代码的存储单元。

具体实施方式

现在参考附图介绍本发明的示例性实施方式，然而，本发明可以用许多不同的形式来实施，并且不局限于此处描述的实施例，提供这些实施例是为了详尽地且完全地公开本发明，并且向所属技术领域的技术人员充分传达本发明的范围。对于表

示在附图中的示例性实施方式中的术语并不是对本发明的限定。在附图中，相同的单元/元件使用相同的附图标记。

除非另有说明，此处使用的术语（包括科技术语）对所属技术领域的技术人员具有通常的理解含义。另外，可以理解的是，以通常使用的词典限定的术语，应当被理解为与其相关领域的语境具有一致的含义，而不应该被理解为理想化的或过于正式的意义。

图 1 为根据本发明优选实施方式的对数据文件进行安全处理的方法流程图。本申请的实施方式，通过服务方发起对数据文件的加密的数据访问请求，服务方可以为浏览器、APP、渠道、宽带服务商等，数据文件可以为 APK 数据文件等，本申请的实施方式以浏览器作为服务方进行举例说明，但本申请的实施方式中发起对数据文件请求的服务方不仅限于浏览器。通过浏览器方发起对数据文件的访问请求，数据文件存储在服务器端，数据文件包括多个文件块和文件目录，数据文件中文件块和文件目录能够匹配，即可认为是合法的文件，即数据文件中多个文件块的顺序可以调整，只需按文件块更新的顺序更新文件目录中文件块的位置等，使文件块和文件目录能够保持相互匹配，数据文件仍然是合法的文件。通过服务器对加密的数据访问请求进行解密后，获取与请求访问的数据文件相关的链接地址，其中链接地址包括安全处理信息。服务器方根据安全处理信息中的安全标识指示在对数据进行响应之前需要对数据文件进行安全处理时，根据安全处理信息中的安全参数对数据文件中的多个文件块中的至少部分文件块进行重新排序。根据多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，将数据文件转化为经过安全处理的数据文件，服务器方将经过安全处理的数据文件提供给数据文件的请求方。本申请的实施方式，对服务方发起的每次数据文件访问请求，都会根据安全处理信息中的安全参数对数据文件中的多个文件块中的至少部分文件块进行重新排序，防止劫持者提取到数据文件的特征，完成对数据文件的匹配。如图 1 所示，一种用于对数据文件进行安全处理的方法从步骤 101 开始：

优选地，在步骤 101：接收针对数据文件的经过加密的数据访问请求，数据文件包括多个文件块和文件目录。本发明的实施方式，用户通过浏览器方发起对服务器上数据文件的访问请求，访问请求为加密的请求，本发明实施方式访问请求采用对称的加密算法，服务方对访问请求进行加密处理，存储数据文件服务器方对访问请求进行解密处理。加密的数据文件访问请求包括需要下载的 APK 数据文件的原始地址、是否要进行安排处理的安全标识，安全参数，安装序列号等。

优选地，多个文件块中每个文件块均包括：文件头、文件数据和附加数据（图 1 未示出，详见图 2）。

优选地，其中文件目录包括多个文件块记录，每个文件块记录用于记载文件块的起始位置和文件块的结束位置。

优选地，其中数据文件还包括文件目录位置信息，用于标识文件目录的起始位

置和结束位置。

本发明的实施方式中，数据文件包括若干个文件块，每个文件块包括文件头、文件数据和附加数据，数据文件包括多个文件块、文件目录和文件目录记录，每个文件目录用于记录文件块的起始位置和文件块的结束位置，文件目录记录用于记录文件目录的起始位置和结束位置。数据文件中包括多个文件块，每个文件块的位置顺序可以调整，只需要相应更新保护文件目录和文件目录记录中的信息，即可实现文件块的顺序与文件目录和文件目录记录的匹配。

优选地，在步骤 102：对经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中链接地址包括安全处理信息。本发明的实施方式，服务器方在接收到数据访问请求后，对加密的请求进行解密，获取需要下载的 APK 数据文件的地址、是否要进行安排处理的安全标识，安全参数，安装序列号等。

优选地，在步骤 103：当安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对数据文件进行安全处理时，根据安全处理信息中的安全参数对数据文件的多个文件块中的至少部分文件块进行重新排序。本发明的实施方式，根据对数据文件访问请求解密后获取的安全标识的指示，来确定是否对数据文件进行安全处理。当安全标识指示服务器方对数据文件进行安全处理时，对数据文件进行重新排序处理。

优选地，其中当安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对数据文件进行安全处理时还包括：根据多个文件块的文件块数量 L 确定第一方阵的阶数 N，其中 L 小于 N^2 并且大于（N-1）^{2}。

优选地，还包括构建 N 阶的第一方阵，以行序为基础并且按照行内从左至右的次序，将多个文件块的序号按顺序填充至第一方阵，以及将 L+1 至 N^2 的元素填充为零。

本发明的实施方式中，例如文件块数量 L 为 95，为使 L 满足，L 小于 N^2 并且大于（N-1）^{2}，取 N 为 10，即第一方阵的除数为 N，第一方阵为 N*N 阶矩阵，在 N*N 阶矩阵中，从第一行开始，按照从左至右的次序，填写 5 个文件块的序号至第一方阵，将 N*N 阶矩阵中第 96 至第 100 的元素填充为零。

优选地，根据安全处理信息中的安全参数对数据文件的多个文件块中的至少部分文件块进行重新排序包括：构建 N 阶的第二方阵，确定安全参数对 N 进行取余运算的余数 K，从第一方阵的第 K 列开始以列序为基础至第 K-1 列为止，按照列内从上至下的次序将多个文件块的序号按顺序填充至第二方阵。

优选地，其中按顺序填充至第二方阵包括：以行序为基础并且按照行内从左至右的次序，将多个文件块的序号按顺序填充至第二方阵。

本发明的实施方式中，构建 N 阶的第二方阵，根据安全参数对 N 进行取余计算，获取余数 K。在对数据文件顺序进行重新排序时，选取第一方阵的第 K 列开始以列序为基础至第 K-1 列为止，按照列内从上至下的次序将多个文件块的序号按顺序填

充至第二方阵。在第二方阵中以行序为基础并且按照行内从左至右的次序，将多个文件块的序号按顺序填充至第二方阵。

优选地，在步骤 104：根据多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，以获得经过安全处理的数据文件。

优选地，根据多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录包括：根据第二方阵中记录的多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录。

本发明的实施方式（图 1 未示出，详见图 3），为使数据文件中的文件块的位置与文件目录和文件目录记录的信息相匹配，需要对文件目录和文件目录记录中的信息与文件块的位置信息进行实时更新，使数据文件为合法文件。

优选地，在步骤 105：以经过安全处理的数据文件为基础生成针对数据访问请求的数据访问响应。

优选地，以经过安全处理的数据文件为基础生成针对数据访问请求的数据访问响应包括：将数据访问请求所涉及的经过安全处理的数据文件或经过安全处理的数据文件的一部分作为数据访问响应。

本发明的实施方式，将经过安全处理，即重新排序后的数据文件或数据文件中的一部分作为数据访问响应，能够有效避免劫持方通过获取部分数据文件，使得劫持方能够提取到数据文件的特征。避免劫持方在确认用户需要下载的数据文件后，通过为用户推荐下载地址，使用户访问到经过恶意处理的数据文件，影响用户的数据使用安全。

图 2 为根据本发明优选实施方式的数据文件结构示意图。如图 2 所示，数据文件包括若干个文件块，每个文件块包括文件头、文件数据和附加数据，数据文件包括多个文件块、文件目录和文件目录记录，每个文件目录用于记录文件块的起始位置和文件块的结束位置，文件目录记录用于记录文件目录的起始位置和结束位置。数据文件中包括多个文件块，每个文件块的位置顺序可以调整，只需要相应更新保护文件目录和文件目录记录中的信息，即可实现文件块的顺序与文件目录和文件目录记录的匹配。多个文件块中可以随意插入随机文件块，只需保证文件目录和文件目录记录更新与多个文件块中位置信息相匹配，数据文件仍然是合法的。

图 3 为根据本发明优选实施方式的对数据文件中文件块进行重新排序示意图。如图 3 所示，301 为原始顺序的数据文件，图 302 为进行安全处理排序后的数据文件，将数据文件中的文件块的排序进行乱序处理，同时保持文件目录和文件目录记录与文件块位置的更新。通过变更数据文件中文件块的位置。

图 4 为根据本发明优选实施方式的对数据文件进行安全处理的方法流程图。如图 4 所示，通过 360 用手发布 APK 文件，生成数据文件，将数据文件发布至 CDN 服务器。用户通过浏览器 Web 端获取下载 URL 地址，将包括下载 URL 地址的数据文件访问请求发送至 CDN 端服务器，CDN 服务器通过对数据文件访问请求进行解

密，获取需要下载的 APK 数据文件的解密后的 URL 地址、是否要进行安排处理的安全标识，安全参数，安装序列号等。当通过安全标识判断出需要对数据文件进行安全处理时，对数据文件进行重新排序处理，重新构造排序后的数据文件进行输出。本发明的实施方式，不对服务端的身份进行识别，是否对数据文件进行安全处理，由提供业务的服务端进行判断和确定。

图 5 为根据本发明优选实施方式的对数据文件进行安全处理的方法流程图。本申请的实施方式，通过服务方发起对数据文件的加密的数据访问请求，服务方可以为浏览器、APP、渠道、宽带服务商等，数据文件可以为 APK 数据文件等，本申请的实施方式以浏览器作为服务方进行举例说明，但本申请的实施方式中发起对数据文件请求的服务方不仅限于浏览器。通过浏览器方发起对数据文件的访问请求，数据文件存储在服务器端，数据文件包括多个文件块和文件目录，数据文件中文件块和文件目录能够匹配，即可认为是合法的文件，即数据文件中多个文件块的顺序可以调整，只需按文件块更新的顺序更新文件目录中文件块的位置等，使文件块和文件目录能够保持相互匹配，数据文件仍然是合法的文件。通过服务器对加密的数据访问请求进行解密后，获取与请求访问的数据文件相关的链接地址，其中链接地址包括安全处理信息。服务器方根据安全处理信息中的安全标识指示在对数据进行响应之前需要对数据文件进行安全处理时，可以在多个随机位置增加多个随机文件块，根据安全处理信息中的安全参数对数据文件中的多个文件块中的至少部分文件块进行重新排序。通过增加随机文件块，使原数据文件中的文件块数量和文件的排序进行较多的改变，增加劫持者在劫持部分数据文件并提取数据特征后对数据文件进行匹配的难度。根据多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，将数据文件转化为经过安全处理的数据文件，服务器方将经过安全处理的数据文件提供给数据文件的请求方。本申请的实施方式，对服务方发起的每次数据文件访问请求，都会根据安全处理信息中的安全参数对数据文件中的多个文件块中的至少部分文件块进行重新排序，以及在随机位置增加随机文件块，防止劫持者提取到数据文件的特征，完成对数据文件的匹配。如图 5 所示，一种用于对数据文件进行安全处理的方法从步骤 501 开始：

优选地，在步骤 501：接收针对数据文件的经过加密的数据访问请求，数据文件包括多个文件块和文件目录。本发明的实施方式，用户通过浏览器方发起对服务器上数据文件的访问请求，访问请求为加密的请求，本发明实施方式访问请求采用对称的加密算法，服务方对访问请求进行加密处理，存储数据文件服务器方对访问请求进行解密处理。加密的数据文件访问请求包括需要下载的 APK 数据文件的原始地址、是否要进行安排处理的安全标识，安全参数，安装序列号等。

优选地，多个文件块中每个文件块均包括：文件头、文件数据和附加数据（图 5 未示出，详见图 2）。

优选地，多个文件块中每个文件块均包括：文件头、文件数据和附加数据，以

及随机文件块，随机文件块包括文件头和随机数据，其中随机数据是与数据文件的内容无关的数据。随机文件块，主要用于在对数据文件进行安全处理时，增加了随机文件块的数据文件更难被提取出数据特征，保证数据文件访问的安全性。

优选地，其中文件目录包括多个文件块记录，每个文件块记录用于记载文件块的起始位置和文件块的结束位置。

优选地，其中数据文件还包括文件目录位置信息，用于标识文件目录的起始位置和结束位置。

本发明的实施方式中，数据文件包括若干个文件块，每个文件块包括文件头、文件数据和附加数据，数据文件包括多个文件块、文件目录和文件目录记录，每个文件目录用于记录文件块的起始位置和文件块的结束位置，文件目录记录用于记录文件目录的起始位置和结束位置。数据文件中包括多个文件块，每个文件块的位置顺序可以调整，只需要相应更新保护文件目录和文件目录记录中的信息，即可实现文件块的顺序与文件目录和文件目录记录的匹配。

优选地，在步骤 502：对经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中链接地址包括安全处理信息。本发明的实施方式，服务器方在接收到数据访问请求后，对加密的请求进行解密，获取需要下载的 APK 数据文件的地址、是否要进行安排处理的安全标识，安全参数，安装序列号等。

优选地，在步骤 503：当安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对数据文件进行安全处理时，在数据文件的多个随机位置增加多个随机文件块，根据安全处理信息中的安全参数对数据文件的多个文件块中的至少部分文件块进行重新排序。本发明的实施方式，根据对数据文件访问请求解密后获取的安全标识的指示，来确定是否对数据文件进行安全处理。当安全标识指示服务器方对数据文件进行安全处理时，对数据文件进行重新排序处理，并且通过在随机位置增加随机文件块，增加文件块乱序的程度，使劫持者难以提取出数据文件的特征，增加数据文件的安全性。

优选地，其中当安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对数据文件进行安全处理时还包括：根据多个文件块的文件块数量 L 确定第一方阵的阶数 N，其中 L 小于 N^2 并且大于（N-1）^{2}。

优选地，还包括构建 N 阶的第一方阵，以行序为基础并且按照行内从左至右的次序，将多个文件块的序号按顺序填充至第一方阵，以及将 L+1 至 N^2 的元素填充为零。

本发明的实施方式中，例如文件块数量 L 为 95，为使 L 满足，L 小于 N^2 并且大于（N-1）^{2}，取 N 为 10，即第一方阵的除数为 N，第一方阵为 N*N 阶矩阵，在 N*N 阶矩阵中，从第一行开始，按照从左至右的次序，填写 5 个文件块的序号至第一方阵，将 N*N 阶矩阵中第 96 至第 100 的元素填充为零。

优选地，根据安全处理信息中的安全参数对数据文件的多个文件块中的至少部

分文件块进行重新排序包括：构建 N 阶的第二方阵，确定安全参数对 N 进行取余运算的余数 K，从第一方阵的第 K 列开始以列序为基础至第 K-1 列为止，按照列内从上至下的次序将多个文件块的序号按顺序填充至第二方阵。

优选地，其中按顺序填充至第二方阵包括：以行序为基础并且按照行内从左至右的次序，将多个文件块的序号按顺序填充至第二方阵。

本发明的实施方式中，构建 N 阶的第二方阵，根据安全参数对 N 进行取余计算，获取余数 K。在对数据文件顺序进行重新排序时，选取第一方阵的第 K 列开始以列序为基础至第 K-1 列为止，按照列内从上至下的次序将多个文件块的序号按顺序填充至第二方阵。在第二方阵中以行序为基础并且按照行内从左至右的次序，将多个文件块的序号按顺序填充至第二方阵。

优选地，在步骤 504：根据多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，以获得经过安全处理的数据文件。

优选地，根据多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录包括：根据第二方阵中记录的多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录。

本发明的实施方式（图 5 未示出，详见图 3），为使数据文件中的文件块的位置与文件目录和文件目录记录的信息相匹配，需要对文件目录和文件目录记录中的信息与文件块的位置信息进行实时更新，使数据文件为合法文件。

优选地，在步骤 505：以经过安全处理的数据文件为基础生成针对数据访问请求的数据访问响应。

优选地，以经过安全处理的数据文件为基础生成针对数据访问请求的数据访问响应包括：将数据访问请求所涉及的经过安全处理的数据文件或经过安全处理的数据文件的一部分作为数据访问响应。

本发明的实施方式，将经过安全处理，即重新排序后的数据文件或数据文件中的一部分作为数据访问响应，能够有效避免劫持方通过获取部分数据文件，使得劫持方能够提取到数据文件的特征。避免劫持方在确认用户需要下载的数据文件后，通过为用户推荐下载地址，使用户访问到经过恶意处理的数据文件，影响用户的数据使用安全。

图 6 为根据本发明优选实施方式的对数据文件进行安全处理的系统结构。本申请的实施方式，通过服务方发起对数据文件的加密的数据访问请求，服务方可以为浏览器、APP、渠道、宽带服务商等，数据文件可以为 APK 数据文件等，本申请的实施方式以浏览器作为服务方进行举例说明，但本申请的实施方式中发起对数据文件请求的服务方不仅限于浏览器。通过浏览器方发起对数据文件的访问请求，数据文件存储在服务器端，数据文件包括多个文件块和文件目录，数据文件中文件块和文件目录能够匹配，即可认为是合法的文件，即数据文件中多个文件块的顺序可以调整，只需按文件块更新的顺序更新文件目录中文件块的位置等，使文件块和文件

目录能够保持相互匹配，数据文件仍然是合法的文件。通过服务器对加密的数据访问请求进行解密后，获取与请求访问的数据文件相关的链接地址，其中链接地址包括安全处理信息。服务器方根据安全处理信息中的安全标识指示在对数据进行响应之前需要对数据文件进行安全处理时，根据安全处理信息中的安全参数对数据文件中的多个文件块中的至少部分文件块进行重新排序。根据多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，将数据文件转化为经过安全处理的数据文件，服务器方将经过安全处理的数据文件提供给数据文件的请求方。本申请的实施方式，对服务方发起的每次数据文件访问请求，都会根据安全处理信息中的安全参数对数据文件中的多个文件块中的至少部分文件块进行重新排序，防止劫持者提取到数据文件的特征，完成对数据文件的匹配。如图 6 所示，一种用于对数据文件进行安全处理的系统 600 包括：

接收单元 601，接收针对数据文件的经过加密的数据访问请求，数据文件包括多个文件块和文件目录。本发明的实施方式，接收单元 601 用于接收用户通过浏览器方发起对服务器上数据文件的访问请求，访问请求为加密的请求，本发明实施方式访问请求采用对称的加密算法，服务方对访问请求进行加密处理，存储数据文件服务器方对访问请求进行解密处理。加密的数据文件访问请求包括需要下载的 APK 数据文件的原始地址、是否要进行安排处理的安全标识，安全参数，安装序列号等。

优选地，多个文件块中每个文件块均包括：文件头、文件数据和附加数据（图 6 未示出，详见图 2）。

优选地，多个文件块中每个文件块均包括：文件头、文件数据和附加数据，以及随机文件块，随机文件块包括文件头和随机数据，其中随机数据是与数据文件的内容无关的数据。随机文件块，主要用于在对数据文件进行安全处理时，增加了随机文件块的数据文件更难被提取出数据特征，保证数据文件访问的安全性。

优选地，其中文件目录包括多个文件块记录，每个文件块记录用于记载文件块的起始位置和文件块的结束位置。

优选地，其中数据文件还包括文件目录位置信息，用于标识文件目录的起始位置和结束位置。

本发明的实施方式中，数据文件包括若干个文件块，每个文件块包括文件头、文件数据和附加数据，数据文件包括多个文件块、文件目录和文件目录记录，每个文件目录用于记录文件块的起始位置和文件块的结束位置，文件目录记录用于记录文件目录的起始位置和结束位置。数据文件中包括多个文件块，每个文件块的位置顺序可以调整，只需要相应更新保护文件目录和文件目录记录中的信息，即可实现文件块的顺序与文件目录和文件目录记录的匹配。

解密单元 602，对经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中链接地址包括安全处理信息。

本发明的实施方式，解密单元 602 用于服务器方在接收到数据访问请求后，对

加密的请求进行解密，获取需要下载的 APK 数据文件的地址、是否要进行安排处理的安全标识，安全参数，安装序列号等。

处理单元 603，当安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对数据文件进行安全处理时，根据安全处理信息中的安全参数对数据文件的多个文件块中的至少部分文件块进行重新排序。本发明的实施方式，处理单元 603 用于根据对数据文件访问请求解密后获取的安全标识的指示，来确定是否对数据文件进行安全处理。当安全标识指示服务器方对数据文件进行安全处理时，对数据文件进行重新排序处理。

可替换地，处理单元 603：当安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对数据文件进行安全处理时，在数据文件的多个随机位置增加多个随机文件块，根据安全处理信息中的安全参数对数据文件的多个文件块中的至少部分文件块进行重新排序。本发明的实施方式，处理单元 603 根据对数据文件访问请求解密后获取的安全标识的指示，来确定是否对数据文件进行安全处理。当安全标识指示服务器方对数据文件进行安全处理时，对数据文件进行重新排序处理，并且通过在随机位置增加随机文件块，增加文件块乱序的程度，使劫持者难以提取出数据文件的特征，增加数据文件的安全性。

优选地，其中当安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对数据文件进行安全处理时还包括：根据多个文件块的文件块数量 L 确定第一方阵的阶数 N，其中 L 小于 N^2 并且大于（N-1）^{2}。

优选地，还包括构建 N 阶的第一方阵，以行序为基础并且按照行内从左至右的次序，将多个文件块的序号按顺序填充至第一方阵，以及将 L+1 至 N^2 的元素填充为零。

本发明的实施方式中，例如文件块数量 L 为 95，为使 L 满足，L 小于 N^2 并且大于（N-1）^{2}，取 N 为 10，即第一方阵的除数为 N，第一方阵为 N*N 阶矩阵，在 N*N 阶矩阵中，从第一行开始，按照从左至右的次序，填写 5 个文件块的序号至第一方阵，将 N*N 阶矩阵中第 96 至第 100 的元素填充为零。

优选地，根据安全处理信息中的安全参数对数据文件的多个文件块中的至少部分文件块进行重新排序包括：构建 N 阶的第二方阵，确定安全参数对 N 进行取余运算的余数 K，从第一方阵的第 K 列开始以列序为基础至第 K-1 列为止，按照列内从上至下的次序将多个文件块的序号按顺序填充至第二方阵。

优选地，其中按顺序填充至第二方阵包括：以行序为基础并且按照行内从左至右的次序，将多个文件块的序号按顺序填充至第二方阵。

本发明的实施方式中，构建 N 阶的第二方阵，根据安全参数对 N 进行取余计算，获取余数 K。在对数据文件顺序进行重新排序时，选取第一方阵的第 K 列开始以列序为基础至第 K-1 列为止，按照列内从上至下的次序将多个文件块的序号按顺序填充至第二方阵。在第二方阵中以行序为基础并且按照行内从左至右的次序，将多个

文件块的序号按顺序填充至第二方阵。

更新单元 604，根据多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，以获得经过安全处理的数据文件。

优选地，根据多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录包括：根据第二方阵中记录的多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录。

本发明的实施方式（图 6 未示出，详见图 3），更新单元 604 为使数据文件中的文件块的位置与文件目录和文件目录记录的信息相匹配，需要对文件目录和文件目录记录中的信息与文件块的位置信息进行实时更新，使数据文件为合法文件。

发送单元 605，以经过安全处理的数据文件为基础生成针对数据访问请求的数据访问响应。优选地，以经过安全处理的数据文件为基础生成针对数据访问请求的数据访问响应包括：发送单元 605 将数据访问请求所涉及的经过安全处理的数据文件或经过安全处理的数据文件的一部分作为数据访问响应。优选地，根据本发明的优选实施方式，如上所述的系统 600 可以被包括在移动终端中，或由移动终端来执行。

本发明的实施方式，将经过安全处理，即重新排序后的数据文件或数据文件中的一部分作为数据访问响应，能够有效避免劫持方通过获取部分数据文件，使得劫持方能够提取到数据文件的特征。避免劫持方在确认用户需要下载的数据文件后，通过为用户推荐下载地址，使用户访问到经过恶意处理的数据文件，影响用户的数据使用安全。

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的特征。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。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的用于对数据文件进行安全处理系统中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 7 示出了可以实现根据本发明的用于对数据文件进行安全处理的计算设备的框图。该计算设备传统上包括处理器 710 和以存储器 720 形式的计算机程序产品或者计算机可读介质。存储器 720 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 720 具有存储用于执行上述方法中的任何方法步骤的程序代码 731 的存储空间 730。例如，存储程序代码的存储空间 730 可以存储分别用于实现上面的方法中的各种步骤的各个程序代码 731。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如图 8 所示的便携式或者固定存储单元。该存储单元可以具有与图 7 的计算设备中的存储器 720 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括存储有用于执行根据本发明的方法步骤的计算机可读程序代码 731’，即可以由例如诸如 710 之类的处理器读取的程序代码，当这些程序代码由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

已经通过参考少量实施方式描述了本发明。然而，本领域技术人员所公知的，正如附带的专利权利要求所限定的，除了本发明以上公开的其他的实施例等同地落在本发明的范围内。

通常地，在权利要求中使用的所有术语都根据他们在技术领域的通常含义被解释，除非在其中被另外明确地定义。所有的参考“一个/所述/该[装置、组件等]”都被开放地解释为所述装置、组件等中的至少一个实例，除非另外明确地说明。这里公开的任何方法的步骤都没必要以公开的准确的顺序运行，除非明确地说明。

此外，还应当注意，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

1、一种用于对数据文件进行安全处理的方法，所述方法包括：接收针对数据文件的经过加密的数据访问请求，所述数据文件包括多个文件块；对所述经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中所述链接地址包括安全处理信息；当所述安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对所述数据文件进行安全处理时，根据所述安全处理信息中的安全参数对所述数据文件的多个文件块中的至少部分文件块进行重新排序，获得经过安全处理的数据文件；以及以所述经过安全处理的数据文件为基础生成针对所述数据访问请求的数据访问响应。

2、根据权利要求 1 所述的方法，其中所述数据文件还包括文件目录，所述获得经过安全处理的数据文件之前还包括：根据所述多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录。

3、根据权利要求 2 所述的方法，所述多个文件块中每个文件块均包括：文件头、文件数据和附加数据。

4、根据权利要求 3 所述的方法，其中所述文件目录包括多个文件块记录，每个文件块记录用于记载文件块的起始位置和文件块的结束位置。

5、根据权利要求 4 所述的方法，其中所述数据文件还包括文件目录位置信息，用于标识所述文件目录的起始位置和结束位置。

6、根据权利要求 2 所述的方法，其中所述当所述安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对所述数据文件进行安全处理时还包括：根据所述多个文件块的文件块数量 L 确定第一方阵的阶数 N，其中 L 小于 N^2 并且大于 $(N-1)^2$。

7、根据权利要求 6 所述的方法，还包括构建 N 阶的第一方阵，以行序为基础并且按照行内从左至右的次序，将所述多个文件块的序号按顺序填充至所述第一方阵，以及将 L+1 至 N^2 的元素填充为零。

8、根据权利要求 7 所述的方法，所述根据所述安全处理信息中的安全参数对所述数据文件的多个文件块中的至少部分文件块进行重新排序包括：构建 N 阶的第二方阵，确定安全参数对 N 进行取余运算的余数 K，从所述第一方阵的第 K 列开始以列序为基础至第 K-1 列为止，按照列内从上至下的次序将所述多个文件块的序号按顺序填充至所述第二方阵。

9、根据权利要求 8 所述的方法，其中所述按顺序填充至所述第二方阵包括：以行序为基础并且按照行内从左至右的次序，将所述多个文件块的序号按顺序填充至所述第二方阵。

10、根据权利要求 9 所述的方法，所述根据所述多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录包括：根据所述第二方阵中记录的

所述多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录。

11、根据权利要求 2 所述的方法，所述以所述经过安全处理的数据文件为基础生成针对所述数据访问请求的数据访问响应包括：将所述数据访问请求所涉及的经过安全处理的数据文件或经过安全处理的数据文件的一部分作为数据访问响应。

12、一种用于对数据文件进行安全处理的方法，所述方法包括：

接收针对数据文件的经过加密的数据访问请求，所述数据文件包括多个文件块和文件目录；

对所述经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中所述链接地址包括安全处理信息；

当所述安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对所述数据文件进行安全处理时，在所述数据文件的多个随机位置增加多个随机文件块，根据所述安全处理信息中的安全参数对所述数据文件的当前文件块中的至少部分文件块进行重新排序；

根据所述当前文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，以获得经过安全处理的数据文件；以及

以所述经过安全处理的数据文件为基础生成针对所述数据访问请求的数据访问响应。

13、根据权利要求 12 所述的方法，其中每个文件块包括：文件头、文件数据和附加数据，并且所述多个随机文件块中每个随机文件块包括：文件头和随机数据，其中所述随机数据是与所述数据文件的内容无关的数据。

14、根据权利要求 13 所述的方法，其中所述文件目录包括多个文件块记录，每个文件块记录用于记载文件块的起始位置和文件块的结束位置，其中所述数据文件还包括文件目录位置信息，用于标识所述文件目录的起始位置和结束位置。

15、根据权利要求 14 所述的方法，所述多个随机位置中的每个随机位置是所述数据文件的多个文件块中两个相邻文件块之间的位置。

16、根据权利要求 12 所述的方法，其中所述当所述安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对所述数据文件进行安全处理时还包括：根据所述当前文件块的文件块数量 L 确定第一方阵的阶数 N，其中 L 小于 N^2 并且大于（N-1）^{2}。

17、根据权利要求 16 所述的方法，还包括构建 N 阶的第一方阵，以行序为基础并且按照行内从左至右的次序，将所述当前文件块的序号按顺序填充至所述第一方阵，以及将 L+1 至 N^2 的元素填充为零。

18、根据权利要求 17 所述的方法，所述根据所述安全处理信息中的安全参数对所述数据文件的当前文件块中的至少部分文件块进行重新排序包括：构建 N 阶的第二方阵，确定安全参数对 N 进行取余运算的余数 K，从所述第一方阵的第 K 列开始

以列序为基础至第 K-1 列为止，按照列内从上至下的次序将所述当前文件块的序号按顺序填充至所述第二方阵。

19、根据权利要求 18 所述的方法，其中所述按顺序填充至所述第二方阵包括：以行序为基础并且按照行内从左至右的次序，将所述当前文件块的序号按顺序填充至所述第二方阵。

20、根据权利要求 19 所述的方法，所述根据所述当前文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录包括：根据所述第二方阵中记录的所述当前文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录。

21、根据权利要求 12 所述的方法，所述以所述经过安全处理的数据文件为基础生成针对所述数据访问请求的数据访问响应包括：将所述数据访问请求所涉及的经过安全处理的数据文件或经过安全处理的数据文件的一部分作为数据访问响应。

22、一种用于对数据文件进行安全处理的系统，所述系统包括：

接收单元，接收针对数据文件的经过加密的数据访问请求，所述数据文件包括多个文件块；

解密单元，对所述经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中所述链接地址包括安全处理信息；

处理单元，当所述安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对所述数据文件进行安全处理时，根据所述安全处理信息中的安全参数对所述数据文件的多个文件块中的至少部分文件块进行重新排序；

更新单元，获得经过安全处理的数据文件；以及

发送单元，以所述经过安全处理的数据文件为基础生成针对所述数据访问请求的数据访问响应。

23.根据权利要求 22 所述的系统，其中所述数据文件还包括文件目录，所述更新单元具体用于：根据所述多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，以获得经过安全处理的数据文件。

24、根据权利要求 23 所述的系统，所述多个文件块中每个文件块均包括：文件头、文件数据和附加数据。

25、根据权利要求 24 所述的系统，其中，所述文件目录包括多个文件块记录，每个文件块记录用于记载文件块的起始位置和文件块的结束位置。

26、根据权利要求 25 所述的系统，其中，所述数据文件还包括文件目录位置信息，用于标识所述文件目录的起始位置和结束位置。

27、根据权利要求 23 所述的系统，其中，所述处理单元根据所述多个文件块的文件块数量 L 确定第一方阵的阶数 N，其中 L 小于 N^2 并且大于（N-1）^{2}。

28、根据权利要求 27 所述的系统，所述处理单元构建 N 阶的第一方阵，以行序为基础并且按照行内从左至右的次序，将所述多个文件块的序号按顺序填充至所述

第一方阵，以及将 L+1 至 N^2 的元素填充为零。

29、根据权利要求 28 所述的系统，所述处理单元构建 N 阶的第二方阵，确定安全参数对 N 进行取余运算的余数 K，从所述第一方阵的第 K 列开始以列序为基础至第 K-1 列为止，按照列内从上至下的次序将所述多个文件块的序号按顺序填充至所述第二方阵。

30、根据权利要求 29 所述的系统，所述处理单元：以行序为基础并且按照行内从左至右的次序，将所述多个文件块的序号按顺序填充至所述第二方阵。

31、根据权利要求 30 所述的系统，所述更新单元根据所述第二方阵中记录的所述多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录。

32、根据权利要求 23 所述的系统，所述发送单元将所述数据访问请求所涉及的经过安全处理的数据文件或经过安全处理的数据文件的一部分作为数据访问响应。

33、一种移动终端，包括或用于执行如权利要求 22-32 中任意一项所述的系统。

34、一种用于对数据文件进行安全处理的系统，所述系统包括：

接收单元，接收针对数据文件的经过加密的数据访问请求，所述数据文件包括多个文件块和文件目录；

解密单元，对所述经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中所述链接地址包括安全处理信息；

处理单元，当所述安全处理信息中的安全标识指示在对数据访问请求进行响应之前需要对所述数据文件进行安全处理时，在所述数据文件的多个随机位置增加多个随机文件块，根据所述安全处理信息中的安全参数对所述数据文件的当前文件块中的至少部分文件块进行重新排序；

更新单元，根据所述当前文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，以获得经过安全处理的数据文件；以及

发送单元，以所述经过安全处理的数据文件为基础生成针对所述数据访问请求的数据访问响应。

35、根据权利要求 34 所述的系统，其中每个文件块包括：文件头、文件数据和附加数据，并且所述多个随机文件块中每个随机文件块包括：文件头和随机数据，其中所述随机数据是与所述数据文件的内容无关的数据。

36、根据权利要求 35 所述的系统，其中所述文件目录包括多个文件块记录，每个文件块记录用于记载文件块的起始位置和文件块的结束位置，其中所述数据文件还包括文件目录位置信息，用于标识所述文件目录的起始位置和结束位置。

37、根据权利要求 36 所述的系统，所述多个随机位置中的每个随机位置是所述数据文件的多个文件块中两个相邻文件块之间的位置。

38、根据权利要求 34 所述的系统，其中，所述处理单元根据所述当前文件块的文件块数量 L 确定第一方阵的阶数 N，其中 L 小于 N^2 并且大于（N-1）^{2}。

39、根据权利要求 38 所述的系统，所述处理单元构建 N 阶的第一方阵，以行序

为基础并且按照行内从左至右的次序，将所述当前文件块的序号按顺序填充至所述第一方阵，以及将 L+1 至 N^2 的元素填充为零。

40、根据权利要求 39 所述的系统，所述处理单元构建 N 阶的第二方阵，确定安全参数对 N 进行取余运算的余数 K，从所述第一方阵的第 K 列开始以列序为基础至第 K-1 列为止，按照列内从上至下的次序将所述当前文件块的序号按顺序填充至所述第二方阵。

41、根据权利要求 40 所述的系统，所述处理单元以行序为基础并且按照行内从左至右的次序，将所述当前文件块的序号按顺序填充至所述第二方阵。

42、根据权利要求 41 所述的系统，所述更新单元根据所述第二方阵中记录的所述当前文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录。

43、根据权利要求 34 所述的系统，所述发送单元将所述数据访问请求所涉及的经过安全处理的数据文件或经过安全处理的数据文件的一部分作为数据访问响应。

44、一种移动终端，包括或用于执行如权利要求 34-43 中任意一项所述的系统。

45、一种计算机可读介质，其中存储了计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1-21 任一个所述的用于对数据文件进行安全处理的方法。

46、一种计算设备，包括：

处理器；以及

存储了计算机可读代码的存储器，所述计算机可读代码被所述处理器运行时，导致所述计算设备执行根据权利要求 1-21 任一个所述的用于对数据文件进行安全处理的方法。

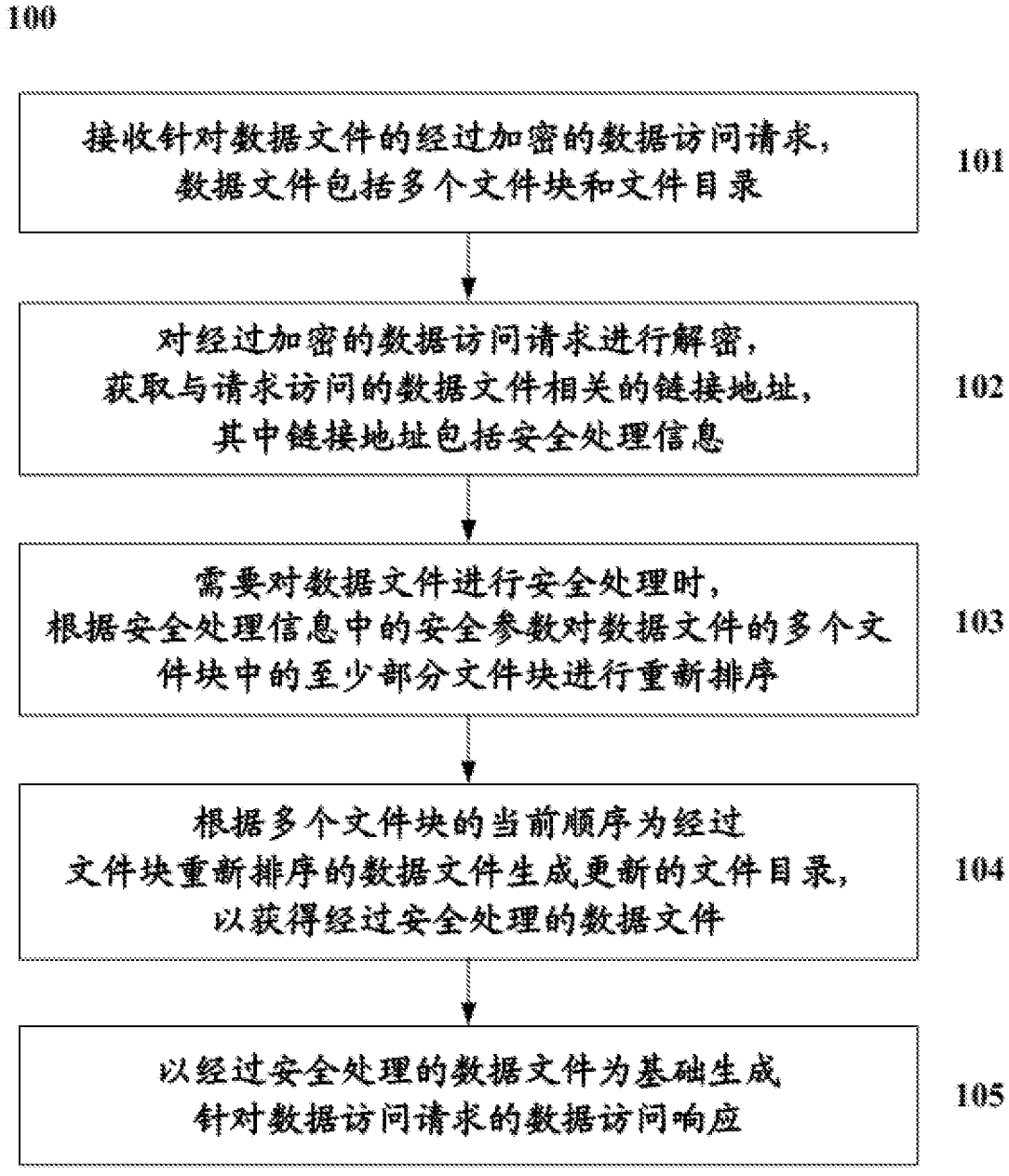

100
接收针对数据文件的经过加密的数据访问请求，
数据文件包括多个文件块和文件目录
101
对经过加密的数据访问请求进行解密，
获取与请求访问的数据文件相关的链接地址，
其中链接地址包括安全处理信息
102
需要对数据文件进行安全处理时，
根据安全处理信息中的安全参数对数据文件的多个文
件块中的至少部分文件块进行重新排序
103
根据多个文件块的当前顺序为经过
文件块重新排序的数据文件生成更新的文件目录，
以获得经过安全处理的数据文件
104
以经过安全处理的数据文件为基础生成
针对数据访问请求的数据访问响应
105

图 1


200
文件头
文件数据和附加数据
文件头
文件数据和附加数据
文件头
文件数据和附加数据
文件头
文件数据和附加数据
文件目录
文件目录记录

图 2

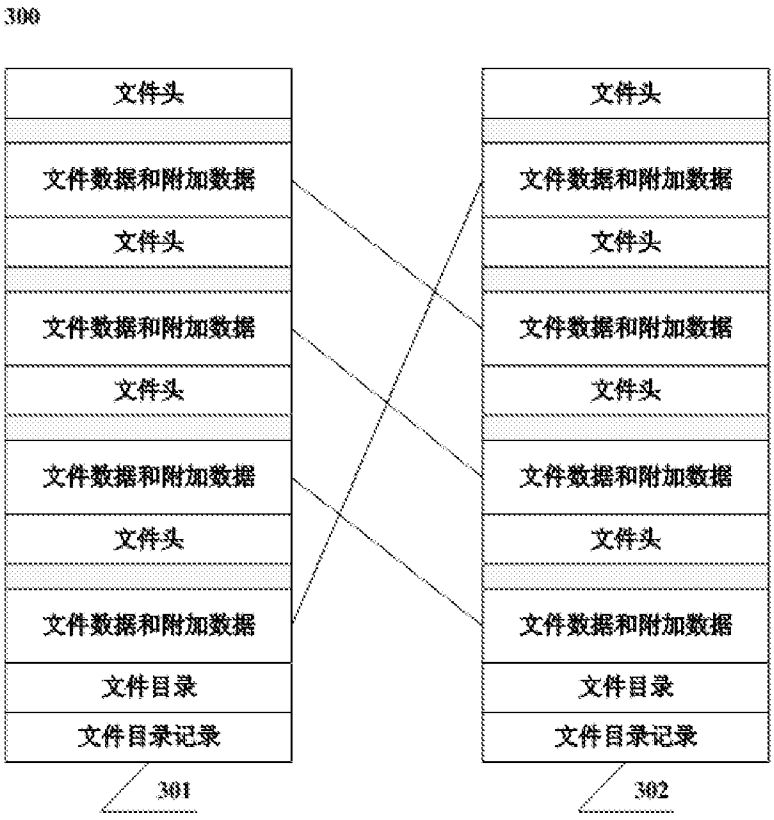

300
文件头
文件数据和附加数据
文件头
文件数据和附加数据
文件头
文件数据和附加数据
文件头
文件数据和附加数据
文件目录
文件目录记录
301
文件头
文件数据和附加数据
文件头
文件数据和附加数据
文件头
文件数据和附加数据
文件头
文件数据和附加数据
文件目录
文件目录记录
302

图 3

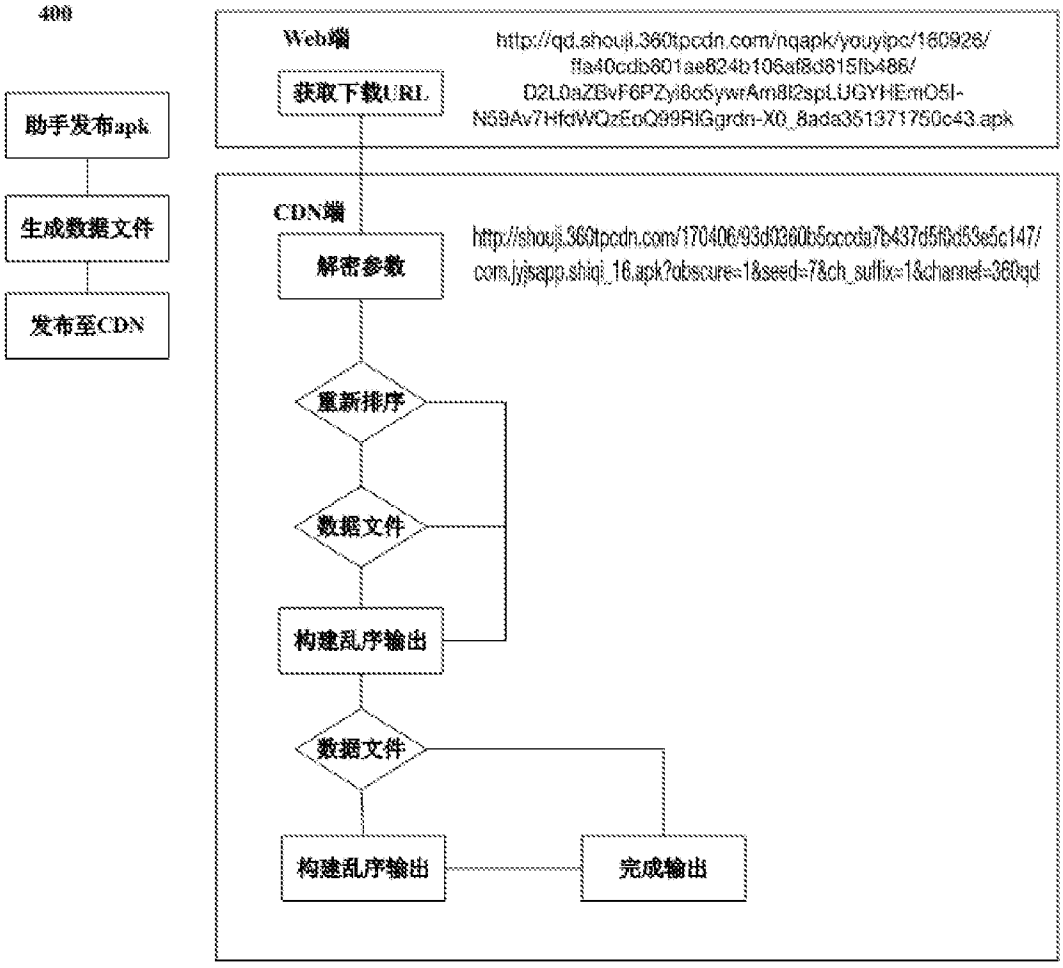

400
助手发布apk
生成数据文件
发布至CDN
Web端
获取下载URL
http://qd.shouji.360tpcdn.com/nqapk/youyipc/160926/ffa40cdb601ae824b106af8d815fb485/D2L0aZBvF6PZyi6o5ywrAm8I2spLUGYHEmO5I-N59Av7HfdWOzEoQ99RIGgrdn-X0_8ada351371750c43.apk
CDN端
解密参数
http://shouji.360tpcdn.com/170406/93d02b0b5cccda7b437d5fbd53e5c147/com.jysapp.shiqi_16.apk?obscure=1&seed=7&ch_suffix=1&channel=360qd
重新排序
数据文件
构建乱序输出
数据文件
构建乱序输出
完成输出

图 4

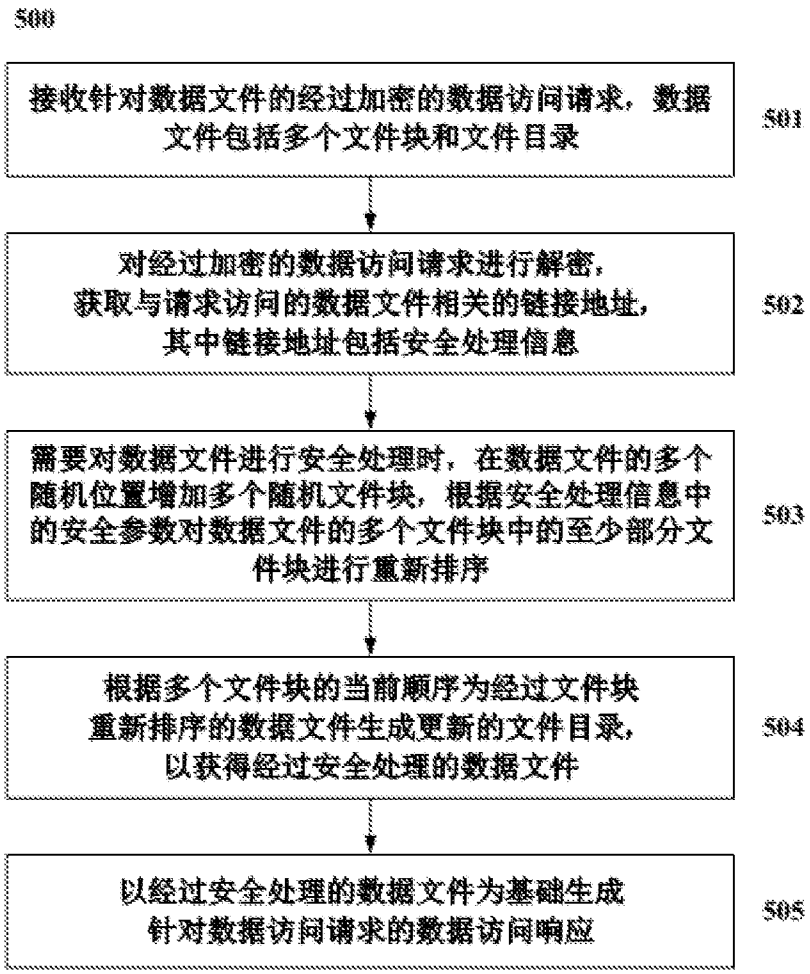

500
接收针对数据文件的经过加密的数据访问请求，数据文件包括多个文件块和文件目录
501
对经过加密的数据访问请求进行解密，获取与请求访问的数据文件相关的链接地址，其中链接地址包括安全处理信息
502
需要对数据文件进行安全处理时，在数据文件的多个随机位置增加多个随机文件块，根据安全处理信息中的安全参数对数据文件的多个文件块中的至少部分文件块进行重新排序
503
根据多个文件块的当前顺序为经过文件块重新排序的数据文件生成更新的文件目录，以获得经过安全处理的数据文件
504
以经过安全处理的数据文件为基础生成针对数据访问请求的数据访问响应
505

图 5

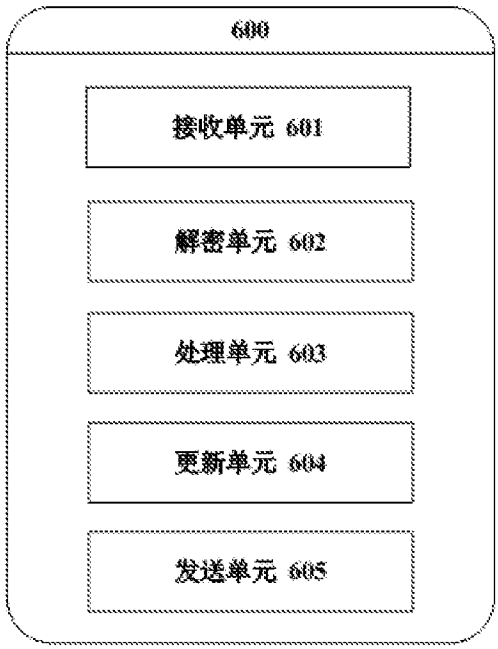

600
接收单元 601
解密单元 602
处理单元 603
更新单元 604
发送单元 605

图 6

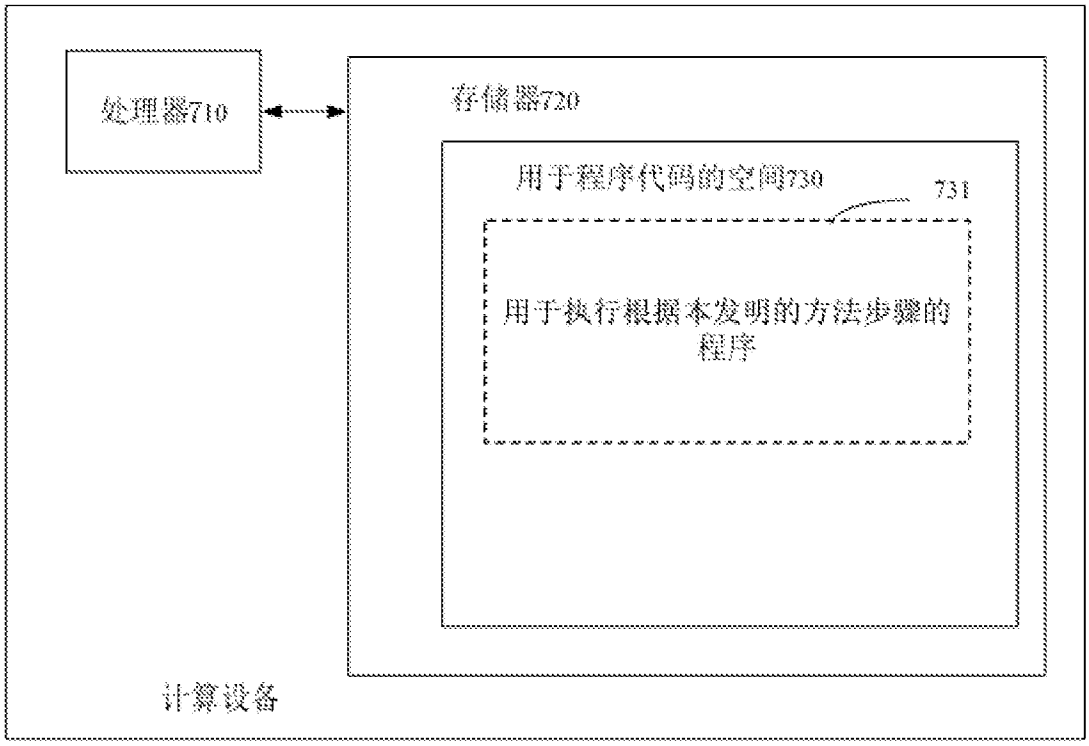

处理器710
存储器720
用于程序代码的空间730
731
用于执行根据本发明的方法步骤的程序
计算设备

图 7

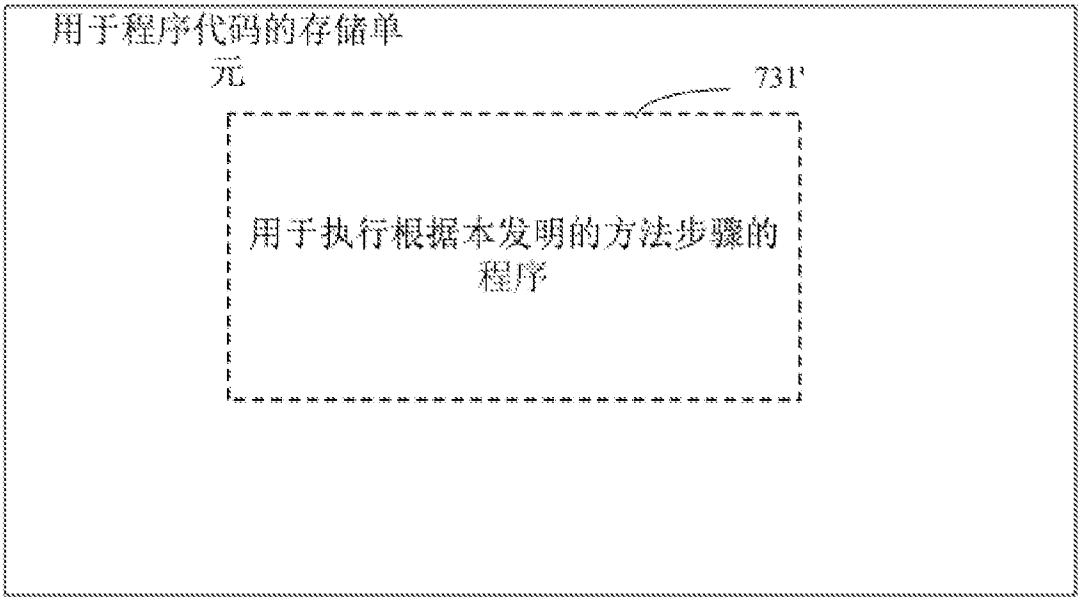

用于程序代码的存储单元
731'
用于执行根据本发明的方法步骤的程序

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/079160

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08 (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)

H04L; H04W; H04Q; 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)

CNPAT, CNKI, EPODOC, WPI: 数据, 文件, 安装包, 访问, 下载, 请求, 加密, 解密, 安全, 排序, 重排, 乱序, 劫持, 拦截, 截获, data, file, APR, Android, package, download, request, encrypt+, secur+, sort, order, sequence, hijack

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107395616 A (BEIJING QIHOO TECHNOLOGY CO., LTD.), 24 November 2017 (24.11.2017), description, paragraphs 0079-0145, and figures 1-6	1-46
A	CN 105718276 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 29 June 2016 (29.06.2016), description, paragraphs 0037-0070, and figures 1-5	1-46
A	CN 105227673 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 06 January 2016 (06.01.2016), entire document	1-46
A	CN 104156225 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 19 November 2014 (19.11.2014), entire document	1-46
A	CN 104135503 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 05 November 2014 (05.11.2014), entire document	1-46
A	CN 104657629 A (CHINA MOBILE COMMUNICATIONS CORPORATION), 27 May 2015 (27.05.2015), entire document	1-46
A	US 6134584 A (INTERNATIONAL BUSINESS MACHINES CORPORATION), 17 October 2000 (17.10.2000), entire document	1-46

☐ 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
19 May 2018	31 May 2018
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LIU, Hanyan Telephone No. 86-010-53961659

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/079160

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 107395616 A	24 November 2017	None	
CN 105718276 A	29 June 2016	None	
CN 105227673 A	06 January 2016	None	
CN 104156225 A	19 November 2014	WO 2014183447 A1	20 November 2014
CN 104135503 A	05 November 2014	WO 2015003570 A1	15 January 2015
CN 104657629 A	27 May 2015	None	
US 6134584 A	17 October 2000	None	

国际检索报告

国际申请号
PCT/CN2018/079160

A. 主题的分类

H04L 29/08(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)

H04L; H04W; H04Q; 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））

CNPAT, CNKI, EPODOC, WPI: 数据，文件，安装包，访问，下载，请求，加密，解密，安全，排序，重排，乱序，劫持，拦截，截获，data, file, APK, Android, package, download, request, encrypt+, secur+, sort, order, sequence, hijack

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 107395616 A (北京奇虎科技有限公司) 2017年 11月 24日 (2017-11-24) 说明书第0079-0145段，图1-6	1-46
A	CN 105718276 A (北京奇虎科技有限公司等) 2016年 6月 29日 (2016-06-29) 说明书第0037-0070段，图1-5	1-46
A	CN 105227673 A (北京奇虎科技有限公司等) 2016年 1月 6日 (2016-01-06) 全文	1-46
A	CN 104156225 A (腾讯科技深圳有限公司) 2014年 11月 19日 (2014-11-19) 全文	1-46
A	CN 104135503 A (腾讯科技深圳有限公司) 2014年 11月 5日 (2014-11-05) 全文	1-46
A	CN 104657629 A (中国移动通信集团公司) 2015年 5月 27日 (2015-05-27) 全文	1-46
A	US 6134584 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2000年 10月 17日 (2000-10-17) 全文	1-46

☐ 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
2018年 5月 19日	2018年 5月 31日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(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 刘寒艳 电话号码 86-010-53961659

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/079160

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 107395616 A	2017年 11月 24日	无	
CN 105718276 A	2016年 6月 29日	无	
CN 105227673 A	2016年 1月 6日	无	
CN 104156225 A	2014年 11月 19日	WO 2014183447 A1	2014年 11月 20日
CN 104135503 A	2014年 11月 5日	WO 2015003570 A1	2015年 1月 15日
CN 104657629 A	2015年 5月 27日	无	
US 6134584 A	2000年 10月 17日	无	