(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
2018 年 5 月 24 日 (24.05.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/090642 A1

(51) 国际专利分类号:
G06F 9/445 (2006.01)

(21) 国际申请号: PCT/CN2017/091364

(22) 国际申请日: 2017 年 6 月 30 日 (30.06.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201611026893.2 2016年11月15日 (15.11.2016) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO.,LTD.) [CN/CN]; 中国广东省深圳福田区八卦岭八卦三路平安大厦吴东勤, Guangdong 518000 (CN)。

(72) 发明人: 秦伟强 (QIN, Weiqiang); 中国广东省深圳福田区八卦岭八卦三路平安大厦吴东勤, Guangdong 518000 (CN)。

(74) 代理人: 深圳市沃德知识产权代理事务所（普通合伙） (SHENZHEN WORLD INTELLECTUAL PROPERTY AGENCY (GENERAL PARTNERSHIP)); 中国广东省深圳福田区园岭街道八卦四路10号中浩大厦1528-1530室于志光, Guangdong 518000 (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,

(54) **Title:** APPLICATION PROGRAM UPGRADE METHOD, USER TERMINAL AND STORAGE MEDIUM

(54) 发明名称: 应用程序升级方法、用户终端及存储介质

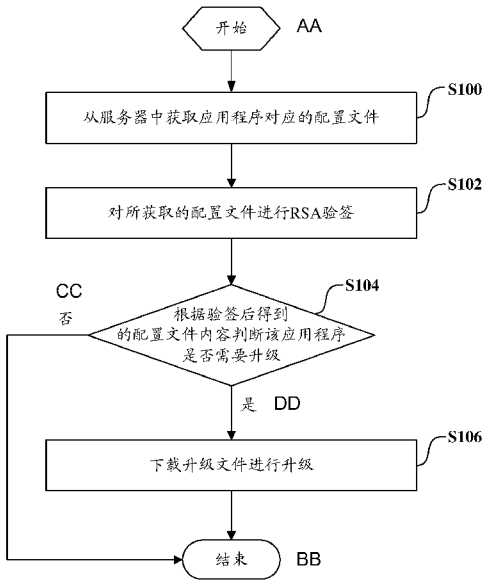

图 1

S100 Acquiring a configuration file corresponding to an application program from a server
S102 Performing RSA signature verification on the acquired configuration file
S104 Determining whether the application program needs to be upgraded according to the content of the configuration file acquired after signature verification
S106 Downloading an upgrade file for performing the upgrade
AA Start
BB End
CC No
DD Yes

(57) **Abstract:** An application program upgrade method, a user terminal and a computer-readable storage medium. The method comprises: acquiring a configuration file corresponding to an application program from a server (S100), the configuration file being encrypted by means of an RSA signature; performing RSA signature verification on the acquired configuration file (S102); determining whether the application program needs to be upgraded according to the content of the configuration file acquired after signature verification (S104); and when it is determined that same needs to be upgraded, downloading an upgrade file for performing the upgrade

WO 2018/090642 A1

[见续页]

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))。

(S106). Thus, the bypassing of a forced upgrade of the version can be effectively avoided.

(57) 摘要：一种应用程序升级方法，用户终端及计算机可读存储介质，该方法包括：从服务器中获取所述应用程序对应的配置文件（S100），所述配置文件通过RSA签名加密；对所获取的配置文件进行RSA验签（S102）；根据验签后得到的配置文件内容判断所述应用程序是否需要升级（S104）；当判断需要升级时，下载升级文件进行升级（S106）。由此可以有效地避免绕过版本的强制升级。

应用程序升级方法、用户终端及存储介质

优先权申明

本申请基于巴黎公约申明享有2016年11月15日递交的申请号为CN201611026893.2、名称为“应用程序升级方法及系统”的中国专利申请的优先权，该中国专利申请的整体内容以参考的方式结合在本申请中。

技术领域

本发明涉及程序升级技术领域，尤其涉及应用程序升级方法、用户终端及计算机可读存储介质。

背景技术

应用程序（APP）是指安装在手机等移动终端上的针对使用者的某种应用目的的客户端应用软件，例如某一家银行的手机银行 APP。所述应用程序包含Android 操作系统应用程序、iOS 操作系统应用程序等。

客户端的应用程序升级与服务器密切相关。现有的应用程序升级方案主要分为两种：一种是服务器简单地将最新版本号及下载地址、是否升级的开关下发给应用程序，由客户端来决定是否升级；另一种是客户端将现有应用程序版本号上传给服务器，由服务器强制应用程序进行升级。现有的这两种方案均容易绕过升级，而继续使用有缺陷的旧版本。

发明内容

有鉴于此，本发明的目的在于提供一种应用程序升级方法、用户终端及计算机可读存储介质，以解决如何有效防止绕过升级的问题。

为实现上述目的，本发明提供一种应用程序升级方法，该方法包括步骤：

从服务器中获取所述应用程序对应的配置文件，所述配置文件通过 RSA 公钥加密算法签名加密；

对所获取的配置文件进行 RSA 验签；

根据验签后得到的配置文件内容判断所述应用程序是否需要升级；及

当判断需要升级时，下载升级文件进行升级。

为实现上述目的，本发明还提出一种用户终端，该用户终端包括存储器及处理器，该存储器上存储有应用程序升级程序，该应用程序升级程序被该处理器执行，实现以下操作：

从服务器中获取所述应用程序对应的配置文件，所述配置文件通过 RSA 公钥加密算法签名加密；

对所获取的配置文件进行 RSA 验签；

根据验签后得到的配置文件内容判断所述应用程序是否需要升级；及

当判断需要升级时，下载升级文件进行升级。

为实现上述目的，本发明还提出一种计算机可读存储介质，该计算机可读存储介质上存储有应用程序升级程序，该以结果用程序升级程序可被至少一处理器执行，以实现以下操作:

从服务器中获取所述应用程序对应的配置文件，所述配置文件通过RSA公钥加密算法签名加密;

对所获取的配置文件进行RSA验签;

根据验签后得到的配置文件内容判断所述应用程序是否需要升级；及

当判断需要升级时，下载升级文件进行升级。

本发明的有益效果在于，本发明提出的应用程序升级方法、用户终端及计算机可读存储介质，通过对服务器中对应的配置文件通过RSA签名进行加密，从服务器获取该应用程序对应的配置文件时需要进行RSA验签，可以避免绕过版本的强制升级。并且，针对应用程序的某个版本升级，可以修改相应的JSON文件，升级方便。

附图说明

图1为本发明第一实施例提出的一种应用程序升级方法的流程图;

图2为本发明中服务器对配置文件进行加密的过程的具体流程图;

图3为图1中步骤S102的具体流程图;

图4为图1中步骤S104的具体流程图;

图5为本发明第二实施例提出的一种用户终端的示意图;

图6为图5中应用程序升级程序的模块示意图。

本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

为了使本发明所要解决的技术问题、技术方案及有益效果更加清楚、明白，以下结合附图和实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

第一实施例

如图 1 所示，本发明第一实施例提出一种应用程序升级方法，应用于客户端中。该方法包括以下步骤:

S100，从服务器中获取应用程序对应的配置文件。

具体地，在服务器上为每个应用程序的版本创建对应的配置文件，并对该配置文件进行加密。在本实施例中，所述配置文件为JSON文件。

参阅图 2 所示，为服务器对所述配置文件进行加密的过程的具体流程图。该流程包括步骤:

S200，将该配置文件对应的多个预设字符串数据拼接在一起。

在本实施例中，所述多个预设字符串包括：当前版本号、需要升级到的版

本号、下载地址、是否需要强制升级的开关。所述配置文件中定义了所述多个预设字符串的内容。服务器将该应用程序对应的当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关这四个字符串的数据进行拼接，形成一个拼接后的字符串，记为第一拼接字符串。

S202，对拼接后的字符串进行哈希运算。

在本实施例中，服务器对所述第一拼接字符串进行哈希运算，得到的结果记为第一哈希数据。

S204，对哈希运算的结果通过RSA（公钥加密算法）签名加密。

在本实施例中，服务器对包含所述第一哈希数据的配置文件通过RSA签名进行加密。所述RSA签名的信息应该与客户端中预置在该应用程序中的RSA公钥信息一致。

回到图1，S102，对所获取的配置文件进行RSA验签。

具体地，参阅图3所示，为所述步骤S102的具体流程图。该流程包括步骤：

S300，读取预置在该应用程序中的RSA公钥。

具体地，所述RSA公钥预置在该应用程序的代码或配置文件中。

S302，比较该RSA公钥与所获取的配置文件的RSA签名是否一致。若一致，则执行步骤S304。若不一致，则执行步骤S312。

具体地，客户端根据该RSA公钥对所获取的配置文件进行RSA解密，若该RSA公钥与所获取的配置文件的RSA签名一致，则解密得到中间文件。所述中间文件中包括服务器对所述拼接后的字符串进行哈希运算后的结果，即第一哈希数据。

S304，接收服务器发送的所述多个预设字符串数据。

具体地，客户端接收与该应用程序对应的当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关这四个字符串的数据。

S306，根据接收到的所述多个预设字符串数据进行字符串拼接和哈希运算。

具体地，客户端对从服务器接收到的与该应用程序对应的当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关这四个字符串的数据也进行拼接，形成一个拼接后的字符串，记为第二拼接字符串。然后对该第二拼接字符串进行哈希运算，得到的结果记为第二哈希数据。

S308，比较本地得到的哈希运算结果和所获取的配置文件解密后的结果是否一致。若一致，则执行步骤S310。若不一致，则执行步骤S312。

在本实施例中，所述本地得到的哈希运算结果即为所述第二哈希数据，所获取的配置文件解密后的结果即为所述第一哈希数据。客户端比较所述第二哈希数据和所述第一哈希数据是否一致，从而判断验签是否成功。

S310，判断验签成功。

在本实施例中，当所述第二哈希数据和所述第一哈希数据一致时，客户端判断验签成功，可以读取所获取的配置文件中的内容。

S312，判断验签失败。

在本实施例中，当所述第二哈希数据和所述第一哈希数据不一致时，客户

端判断验签失败，无法读取所获取的配置文件中的内容。

回到图 1，S104，根据验签后得到的配置文件内容判断该应用程序是否需要升级。若需要升级，则执行步骤 S106。若不需要升级，则流程结束。

具体地，参阅图 4 所示，为所述步骤 S104 的具体流程图。该流程包括步骤：

S400，读取该应用程序自身存储的版本号。

S402，从验签后得到的配置文件中读取所记录的当前版本号。

S404，判断该应用程序的版本号是否等于或小于所述配置文件中的当前版本号。若是，则执行步骤 S406-S408。若否，则执行步骤 S412。

具体地，客户端比较该应用程序自身存储的版本号与所述配置文件中的当前版本号。若该应用程序自身存储的版本号等于所述配置文件中的当前版本号，表示客户端中该应用程序的版本与所述配置文件中记录的当前版本相同，因此需要升级。若该应用程序自身存储的版本号小于所述配置文件中的当前版本号，表示客户端中该应用程序的版本比所述配置文件中记录的当前版本更陈旧，因此需要升级。

S406，从验签后得到的配置文件中读取是否需要强制升级的开关。

S408，根据所述是否需要强制升级的开关判断该应用程序是否需要升级。若该开关为开，则执行步骤 S410，判断该应用程序需要升级。若该开关为关，则执行步骤 S412，判断该应用程序不需要升级。

回到图 1，S106，下载升级文件进行升级。

具体地，客户端从验签后得到的配置文件中读取该应用程序的升级文件的下载地址，从而下载对应的升级文件，完成对所述应用程序的该次升级。

本实施例提出的应用程序升级方法，对服务器中对应的配置文件通过 RSA 签名进行加密，客户端从服务器获取该配置文件时需要进行 RSA 验签，可以避免绕过版本的强制升级。并且，针对应用程序的某个版本升级，可以修改相应的 JSON 文件，升级方便。

第二实施例

如图 5 所示，本发明第二实施例提出一种用户终端。该用户终端包括，但不仅限于，存储器 11、处理器 12、通信总线 13 及网络接口 14。其中，通信总线 13 用于实现这些组件之间的连接通信。

其中，所述用户终端可以是智能手机、平板电脑、笔记本、桌上型计算机、电子书阅读器、MP3（Moving Picture Experts Group Audio Layer III，动态影像专家压缩标准音频层面 3）播放器、MP4（Moving Picture Experts Group Audio Layer IV，动态影像专家压缩标准音频层面 4）播放器等具有数据处理功能的终端设备。

存储器 11 包括内存及至少一种类型的可读存储介质。内存为用户终端的运行提供缓存；可读存储介质可为如闪存、硬盘、多媒体卡、卡型存储器等的非易失性存储介质。在一些实施例中，所述可读存储介质可以是所述用户终端的内部存储单元，例如该用户终端的硬盘或内存。在另一些实施例中，所述可读存储介质也可以是所述用户终端的外部存储设备，例如所述用户终端上配备的

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。

本实施例中，所述存储器 11 的可读存储介质通常用于存储安装于所述用户终端的应用软件及各类数据，例如应用程序升级程序 500 等。所述存储器 11 还可以用于暂时地存储已经输出或者将要输出的数据。

处理器 12 在一些实施例中可以是一中央处理器（Central Processing Unit, CPU），微处理器或其他数据处理芯片，用于运行所述存储器 11 中存储的程序代码或处理数据。该处理器 12 执行应用程序升级程序 500，可实现上述应用程序升级方法的任一步骤。

网络接口 14 可以包括标准的有线接口、无线接口（如 WI-FI 接口）。

图 5 仅示出了具有组件 11-14 的用户终端，但是应理解的是，并不要求实施所有示出的组件，可以替代的实施更多或者更少的组件。

可选的，该用户终端还可以包括用户接口，用户接口可以包括标准的有线接口、无线接口。例如，输入单元比如键盘（Keyboard）、有线或无线头戴式耳机端口、外部电源(或电池充电器)端口、有线或无线数据端口、存储卡端口、用于连接具有识别模块的装置的端口、音频输入/输出(I/O)端口、视频 I/O 端口、耳机端口等等。该用户接口可以用于接收来自外部装置的输入(例如，数据信息、电力等等)并且将接收到的输入传输到终端的一个或多个元件。

可选地，该用户终端还可以包括显示器，显示器可以是 LED 显示器、液晶显示器、触控式液晶显示器以及 OLED（Organic Light-Emitting Diode，有机发光二极管）触摸器等。所述显示器用于显示在所述用户终端中处理的信息以及用于显示可视化的用户界面等。

在本实施例中，如图 6 所示，所述的应用程序升级程序 500 可以被分割成获取模块 502、验证模块 504、判断模块 506 及升级模块 508。当处理器 12 执行各模块的计算机程序指令段时，基于各个计算机程序指令段所能实现的操作和功能，可实现上述应用程序升级方法的任一步骤。以下描述将具体介绍所述获取模块 502、验证模块 504、判断模块 506 及升级模块 508 所实现的操作和功能。

所述获取模块 502，用于从服务器中获取应用程序对应的配置文件。

具体地，在服务器上为每个应用程序的版本创建对应的配置文件，并对该配置文件进行加密。在本实施例中，所述配置文件为 JSON 文件。

在本实施例中，服务器对该配置文件进行加密的过程具体包括:

服务器将该配置文件对应的多个预设字符串数据拼接在一起。在本实施例中，所述多个预设字符串包括：当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关。所述配置文件中定义了所述多个预设字符串的内容。服务器将该应用程序对应的当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关这四个字符串的数据进行拼接，形成一个拼接后的字符串，记为第一拼接字符串。

服务器对拼接后的字符串进行哈希运算。在本实施例中，服务器对所述第一拼接字符串进行哈希运算，得到的结果记为第一哈希数据。

服务器对哈希运算的结果通过RSA签名加密。在本实施例中，服务器对包含所述第一哈希数据的配置文件通过RSA签名进行加密。所述RSA签名的信息应该与客户端中预置在该应用程序中的RSA公钥信息一致。

所述验证模块504，用于对所获取的配置文件进行RSA验签。

在本实施例中，所述RSA验签的过程具体包括:

验证模块504读取预置在该应用程序中的RSA公钥。具体地，所述RSA公钥预置在该应用程序的代码或配置文件中。

验证模块504比较该RSA公钥与所获取的配置文件的RSA签名是否一致。若该RSA公钥与所获取的配置文件的RSA签名一致，则验证模块504根据该RSA公钥对所获取的配置文件进行RSA解密，得到中间文件。所述中间文件中包括服务器对所述拼接后的字符串进行哈希运算后的结果，即第一哈希数据。若该RSA公钥与所获取的配置文件的RSA签名不一致，则验证模块504判断验签失败。

验证模块504接收服务器发送的所述多个预设字符串数据。具体地，验证模块504接收与该应用程序对应的当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关这四个字符串的数据。

验证模块504根据接收到的所述多个预设字符串数据进行字符串拼接和哈希运算。具体地，验证模块504对从服务器接收到的与该应用程序对应的当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关这四个字符串的数据也进行拼接，形成一个拼接后的字符串，记为第二拼接字符串。然后对该第二拼接字符串进行哈希运算，得到的结果记为第二哈希数据。

验证模块504比较本地得到的哈希运算结果和所获取的配置文件解密后的结果是否一致。在本实施例中，所述本地得到的哈希运算结果即为所述第二哈希数据，所获取的配置文件解密后的结果即为所述第一哈希数据。客户端比较所述第二哈希数据和所述第一哈希数据是否一致。若一致，则验证模块504判断验签成功，可以读取所获取的配置文件中的内容。若不一致，则验证模块504判断验签失败，无法读取所获取的配置文件中的内容。

所述判断模块506，用于根据验签后得到的配置文件内容判断该应用程序是否需要升级。

在本实施例中，所述判断该应用程序是否需要升级的过程具体包括:

判断模块506读取该应用程序自身存储的版本号，并从验签后得到的配置文件中读取所记录的当前版本号。然后判断该应用程序的版本号是否等于或小于所述配置文件中的当前版本号。具体地，判断模块506比较该应用程序自身存储的版本号与所述配置文件中的当前版本号。若该应用程序自身存储的版本号等于所述配置文件中的当前版本号，表示客户端中该应用程序的版本与所述配置文件中记录的当前版本相同，因此需要升级。若该应用程序自身存储的版本号小于所述配置文件中的当前版本号，表示客户端中该应用程序的版本比所述配置文件中记录的当前版本更陈旧，因此需要升级。

当该应用程序的版本号等于或小于所述配置文件中的当前版本号时，判断

模块 506 继续从验签后得到的配置文件中读取是否需要强制升级的开关，然后根据所述是否需要强制升级的开关判断该应用程序是否需要升级。若该开关为开，则判断模块 506 判断该应用程序需要升级。若该开关为关，则判断模块 506 判断该应用程序不需要升级。

所述升级模块 508，用于当判断该应用程序需要升级时，下载升级文件进行升级。

具体地，升级模块 508 从验签后得到的配置文件中读取该应用程序的升级文件的下载地址，从而下载对应的升级文件，完成对所述应用程序的该次升级。

本实施例提出的用户终端，对服务器中对应的配置文件通过 RSA 签名进行加密，从服务器获取该配置文件时需要进行 RSA 验签，可以避免绕过版本的强制升级。并且，针对应用程序的某个版本升级，可以修改相应的 JSON 文件，升级方便。

第三实施例

本发明第三实施例还提出一种计算机可读存储介质，该计算机可读存储介质上存储有应用程序升级程序，该应用程序升级程序被该处理器执行时，可实现如下步骤:

从服务器中获取所述应用程序对应的配置文件，所述配置文件通过 RSA 公钥加密算法签名加密;

对所获取的配置文件进行 RSA 验签;

根据验签后得到的配置文件内容判断所述应用程序是否需要升级；及

当判断需要升级时，下载升级文件进行升级。

优选地，所述服务器对所述配置文件进行加密的过程具体包括:

将所述配置文件对应的多个预设字符串数据拼接在一起;

对拼接后的字符串进行哈希运算;

对哈希运算的结果通过 RSA 签名加密。

优选地，所述多个预设字符串包括：当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关。

优选地，所述配置文件为 JSON 文件，所述配置文件中定义了所述多个预设字符串的内容。

优选地，所述对所获取的配置文件进行 RSA 验签的步骤具体包括:

读取预置在所述应用程序中的 RSA 公钥;

比较所述 RSA 公钥与所获取的配置文件的 RSA 签名是否一致;

若所述 RSA 公钥与所述 RSA 签名一致，则接收服务器发送的所述多个预设字符串数据;

根据接收到的所述多个预设字符串数据进行字符串拼接和哈希运算;

比较本地得到的哈希运算结果和所获取的配置文件解密后的结果是否一致;

若结果一致，则判断验签成功;

若结果不一致或所述RSA公钥与所述RSA签名不一致，则判断验签失败。

优选地，所述根据验签后得到的配置文件内容判断所述应用程序是否需要升级的步骤具体包括:

读取所述应用程序自身存储的版本号;

从验签后得到的配置文件中读取所记录的当前版本号;

判断所述应用程序自身存储的版本号是否等于或小于所述当前版本号;

若是，则从验签后得到的配置文件中读取是否需要强制升级的开关;

根据所述是否需要强制升级的开关判断该应用程序是否需要升级。

本发明之计算机可读存储介质的具体实施方式与上述应用程序升级方法的实施例大致相同，故不再赘述。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件来实现，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可以是手机，计算机，服务器，空调器，或者网络设备等）执行本发明各个实施例所述的方法。

以上参照附图说明了本发明的优选实施例，并非因此局限本发明的权利范围。上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。另外，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

本领域技术人员不脱离本发明的范围和实质，可以有多种变型方案实现本发明，比如作为一个实施例的特征可用于另一实施例而得到又一实施例。凡在运用本发明的技术构思之内所作的任何修改、等同替换和改进，均应在本发明的权利范围之内。

权 利 要 求 书

1、一种应用程序升级方法，其特征在于，该方法包括步骤：

从服务器中获取所述应用程序对应的配置文件，所述配置文件通过RSA公钥加密算法签名加密；

对所获取的配置文件进行RSA验签；

根据验签后得到的配置文件内容判断所述应用程序是否需要升级；及

当判断需要升级时，下载升级文件进行升级。

2、根据权利要求1所述的应用程序升级方法，其特征在于，所述服务器对所述配置文件进行加密的过程具体包括：

将所述配置文件对应的多个预设字符串数据拼接在一起；

对拼接后的字符串进行哈希运算；

对哈希运算的结果通过RSA签名加密。

3、根据权利要求2所述的应用程序升级方法，其特征在于，所述多个预设字符串包括：当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关。

4、根据权利要求2所述的应用程序升级方法，其特征在于，所述配置文件为JSON文件，所述配置文件中定义了所述多个预设字符串的内容。

5、根据权利要求3所述的应用程序升级方法，其特征在于，所述配置文件为JSON文件，所述配置文件中定义了所述多个预设字符串的内容。

6、根据权利要求2所述的应用程序升级方法，其特征在于，所述对所获取的配置文件进行RSA验签的步骤具体包括：

读取预置在所述应用程序中的RSA公钥；

比较所述RSA公钥与所获取的配置文件的RSA签名是否一致；

若所述RSA公钥与所述RSA签名一致，则接收服务器发送的所述多个预设字符串数据；

根据接收到的所述多个预设字符串数据进行字符串拼接和哈希运算；

比较本地得到的哈希运算结果和所获取的配置文件解密后的结果是否一致；

若结果一致，则判断验签成功；

若结果不一致或所述RSA公钥与所述RSA签名不一致，则判断验签失败。

7、根据权利要求3所述的应用程序升级方法，其特征在于，所述根据验签后得到的配置文件内容判断所述应用程序是否需要升级的步骤具体包括：

读取所述应用程序自身存储的版本号；

从验签后得到的配置文件中读取所记录的当前版本号；

判断所述应用程序自身存储的版本号是否等于或小于所述当前版本号；

若是，则从验签后得到的配置文件中读取是否需要强制升级的开关；

根据所述是否需要强制升级的开关判断该应用程序是否需要升级。

8、一种用户终端，其特征在于，该用户终端包括：存储器及处理器，该存

储器存储有应用程序升级程序，该应用程序升级程序程序被所述处理器执行，实现以下操作：

从服务器中获取所述应用程序对应的配置文件，所述配置文件通过RSA公钥加密算法签名加密；

对所获取的配置文件进行RSA验签；

根据验签后得到的配置文件内容判断所述应用程序是否需要升级；及

当判断需要升级时，下载升级文件进行升级。

9、根据权利要求8所述的用户终端，其特征在于，所述服务器对所述配置文件进行加密的过程具体包括：

将所述配置文件对应的多个预设字符串数据拼接在一起；

对拼接后的字符串进行哈希运算；

对哈希运算的结果通过RSA签名加密。

10、根据权利要求9所述的用户终端，其特征在于，所述多个预设字符串包括：当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关。

11、根据权利要求9所述的用户终端，其特征在于，所述配置文件为JSON文件，所述配置文件中定义了所述多个预设字符串的内容。

12、根据权利要求10所述的用户终端，其特征在于，所述配置文件为JSON文件，所述配置文件中定义了所述多个预设字符串的内容。

13、根据权利要求9所述的用户终端，其特征在于，所述对所获取的配置文件进行RSA验签的步骤具体包括：

读取预置在所述应用程序中的RSA公钥；

比较所述RSA公钥与所获取的配置文件的RSA签名是否一致；

若所述RSA公钥与所述RSA签名一致，则接收服务器发送的所述多个预设字符串数据；

根据接收到的所述多个预设字符串数据进行字符串拼接和哈希运算；

比较本地得到的哈希运算结果和所获取的配置文件解密后的结果是否一致；

若结果一致，则判断验签成功；

若结果不一致或所述RSA公钥与所述RSA签名不一致，则判断验签失败。

14、根据权利要求10所述的用户终端，其特征在于，所述根据验签后得到的配置文件内容判断所述应用程序是否需要升级的步骤具体包括：

读取所述应用程序自身存储的版本号；

从验签后得到的配置文件中读取所记录的当前版本号；

判断所述应用程序自身存储的版本号是否等于或小于所述当前版本号；

若是，则从验签后得到的配置文件中读取是否需要强制升级的开关；

根据所述是否需要强制升级的开关判断该应用程序是否需要升级。

15、一种计算机可读存储介质，其特征在于，该计算机可读存储介质上存储有应用程序升级程序，该应用程序升级程序可被至少一处理器执行，以实现

以下操作:

从服务器中获取所述应用程序对应的配置文件，所述配置文件通过RSA公钥加密算法签名加密;

对所获取的配置文件进行RSA验签;

根据验签后得到的配置文件内容判断所述应用程序是否需要升级；及

当判断需要升级时，下载升级文件进行升级。

16、根据权利要求15所述的计算机可读存储介质，其特征在于，所述服务器对所述配置文件进行加密的过程具体包括:

将所述配置文件对应的多个预设字符串数据拼接在一起;

对拼接后的字符串进行哈希运算;

对哈希运算的结果通过RSA签名加密。

17、根据权利要求16所述的计算机可读存储介质，其特征在于，所述多个预设字符串包括：当前版本号、需要升级到的版本号、下载地址、是否需要强制升级的开关。

18、根据权利要求16所述的计算机可读存储介质，其特征在于，所述配置文件为JSON文件，所述配置文件中定义了所述多个预设字符串的内容。

19、根据权利要求16所述的计算机可读存储介质，其特征在于，所述对所获取的配置文件进行RSA验签的步骤具体包括:

读取预置在所述应用程序中的RSA公钥;

比较所述RSA公钥与所获取的配置文件的RSA签名是否一致;

若所述RSA公钥与所述RSA签名一致,则接收服务器发送的所述多个预设字符串数据;

根据接收到的所述多个预设字符串数据进行字符串拼接和哈希运算;

比较本地得到的哈希运算结果和所获取的配置文件解密后的结果是否一致;

若结果一致，则判断验签成功;

若结果不一致或所述RSA公钥与所述RSA签名不一致，则判断验签失败。

20、根据权利要求17所述的计算机可读存储介质，其特征在于，所述根据验签后得到的配置文件内容判断所述应用程序是否需要升级的步骤具体包括:

读取所述应用程序自身存储的版本号;

从验签后得到的配置文件中读取所记录的当前版本号;

判断所述应用程序自身存储的版本号是否等于或小于所述当前版本号;

若是，则从验签后得到的配置文件中读取是否需要强制升级的开关;

根据所述是否需要强制升级的开关判断该应用程序是否需要升级。

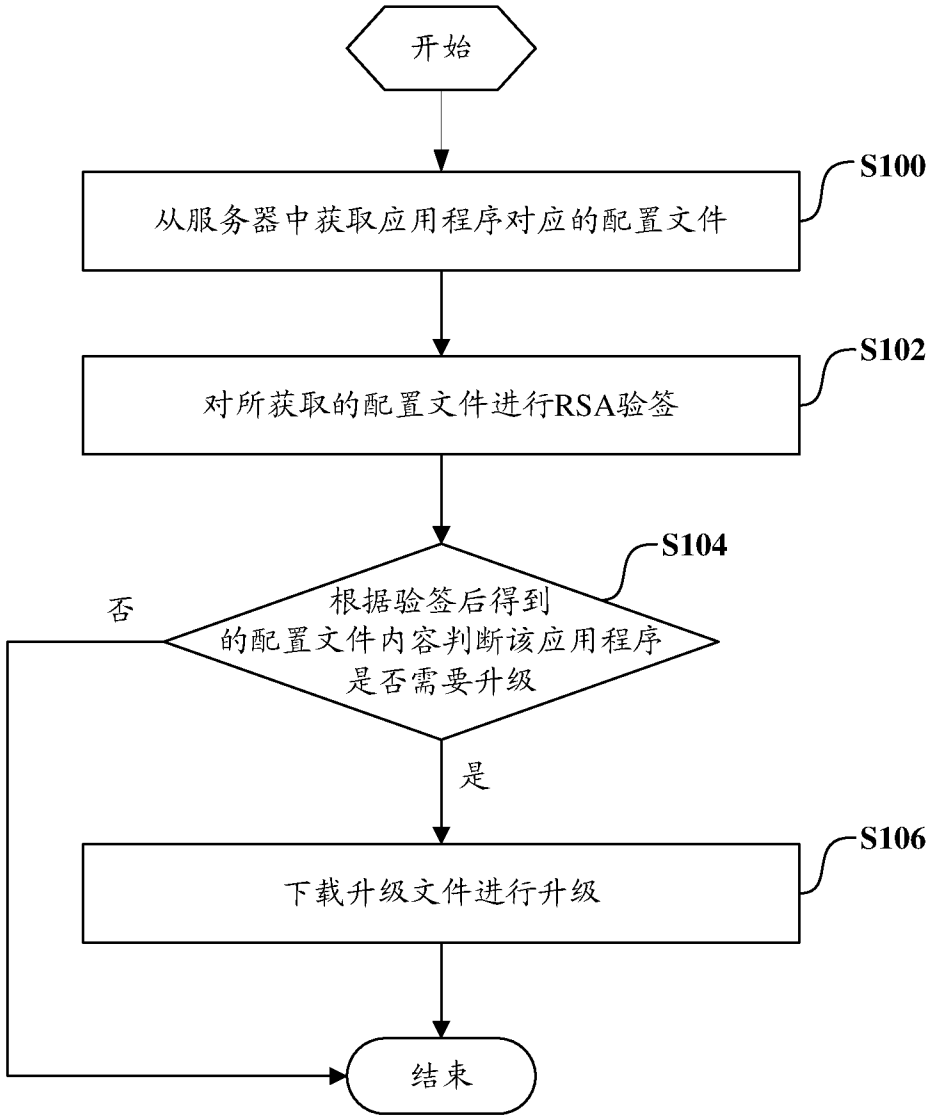
开始
S100
从服务器中获取应用程序对应的配置文件
S102
对所获取的配置文件进行RSA验签
S104
根据验签后得到
的配置文件内容判断该应用程序
是否需要升级
否
是
S106
下载升级文件进行升级
结束

图 1

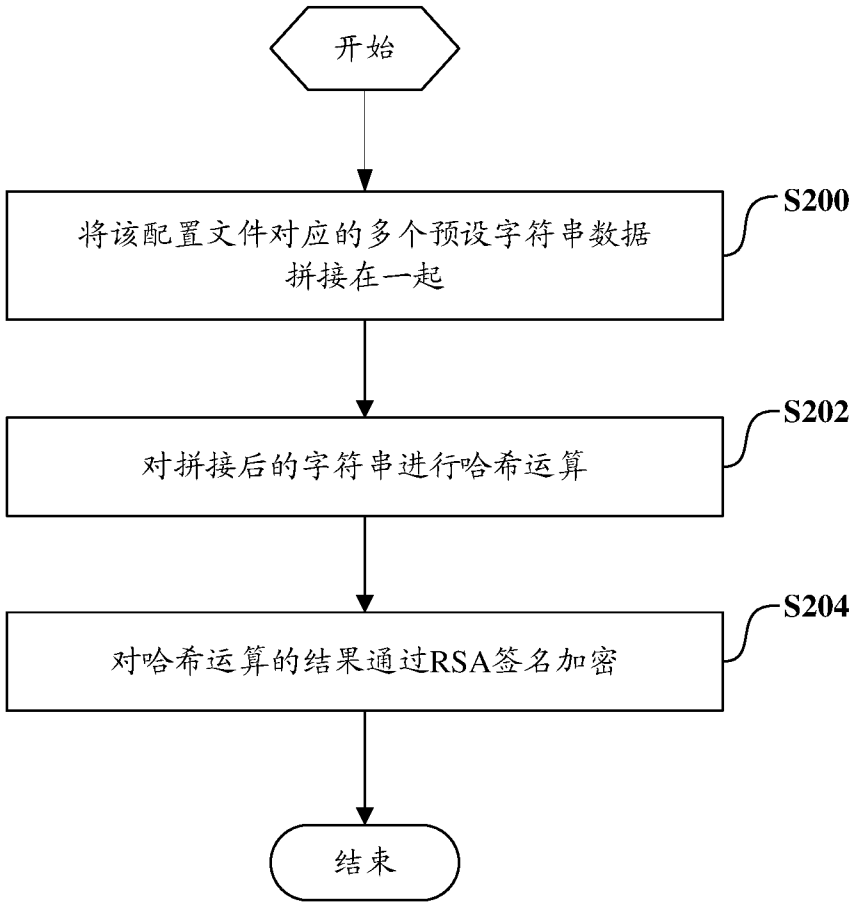
开始
将该配置文件对应的多个预设字符串数据拼接在一起
S200
对拼接后的字符串进行哈希运算
S202
对哈希运算的结果通过RSA签名加密
S204
结束

图 2

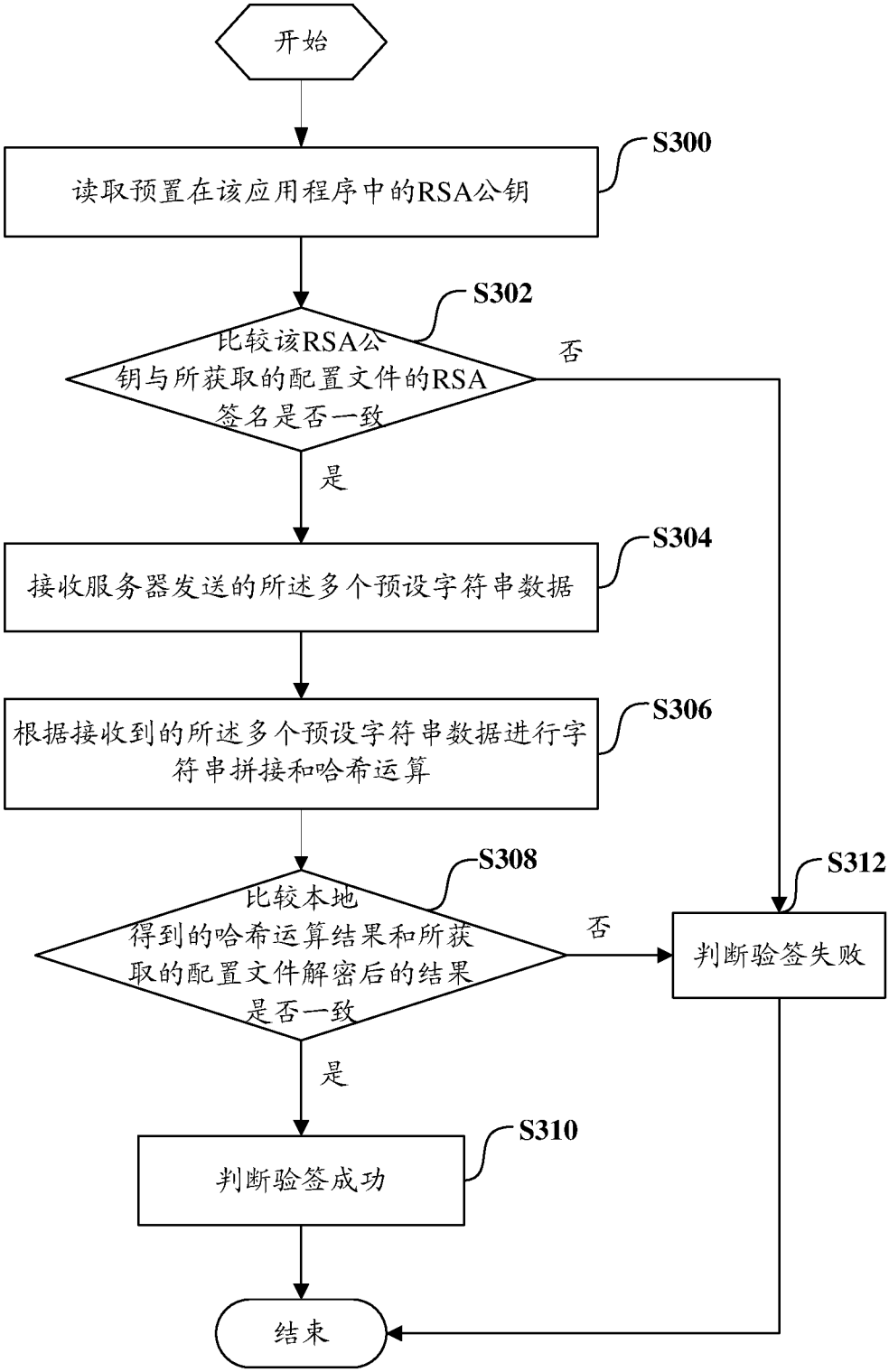
开始
S300
读取预置在该应用程序中的RSA公钥
S302
比较该RSA公钥与所获取的配置文件的RSA签名是否一致
否
是
S304
接收服务器发送的所述多个预设字符串数据
S306
根据接收到的所述多个预设字符串数据进行字符串拼接和哈希运算
S308
比较本地得到的哈希运算结果和所获取的配置文件解密后的结果是否一致
否
S312
判断验签失败
是
S310
判断验签成功
结束

图 3

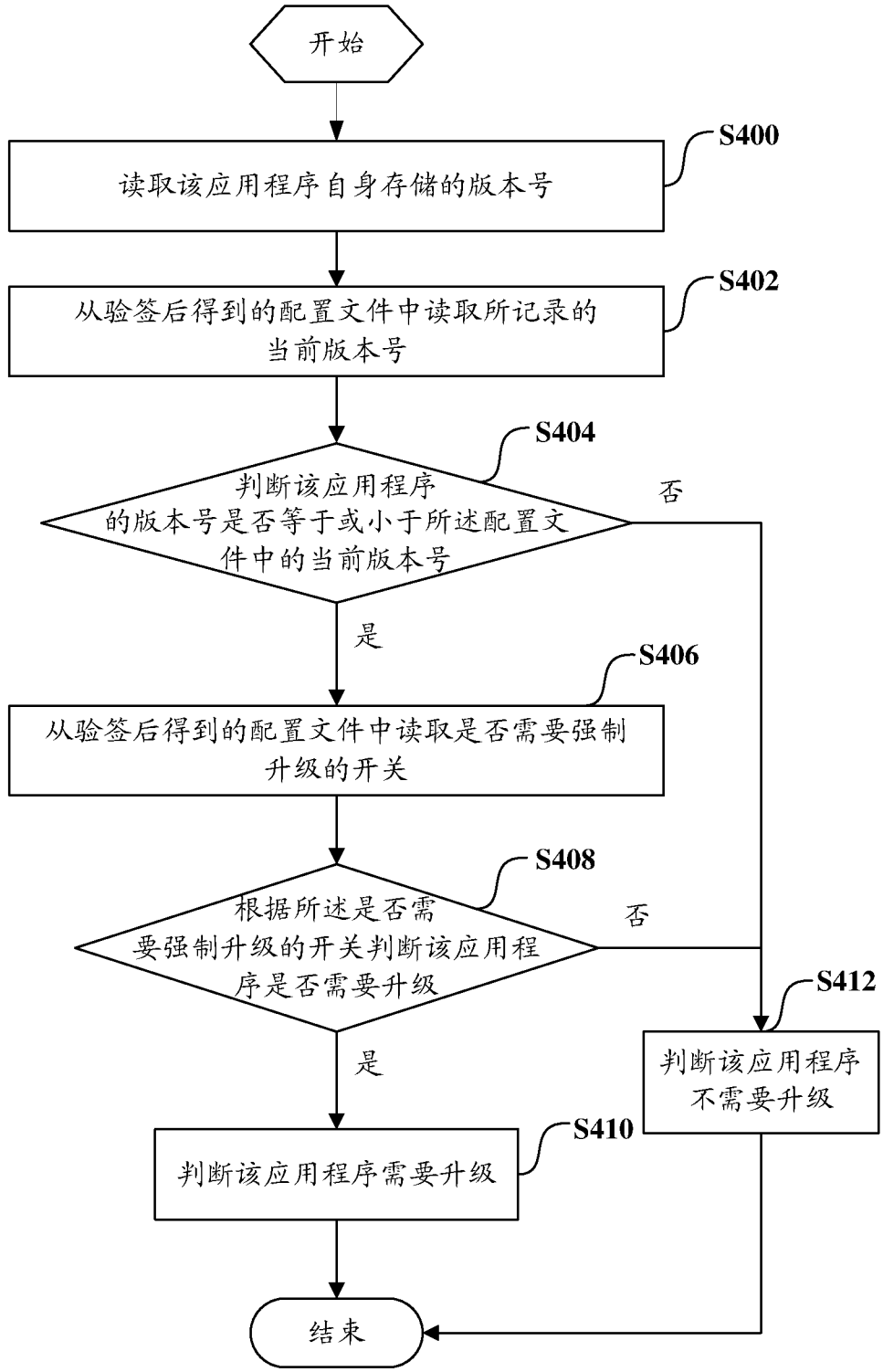
开始
S400
读取该应用程序自身存储的版本号
S402
从验签后得到的配置文件中读取所记录的当前版本号
S404
判断该应用程序的版本号是否等于或小于所述配置文件中的当前版本号
否
是
S406
从验签后得到的配置文件中读取是否需要强制升级的开关
S408
根据所述是否需要强制升级的开关判断该应用程序是否需要升级
否
是
S412
判断该应用程序不需要升级
S410
判断该应用程序需要升级
结束

图 4

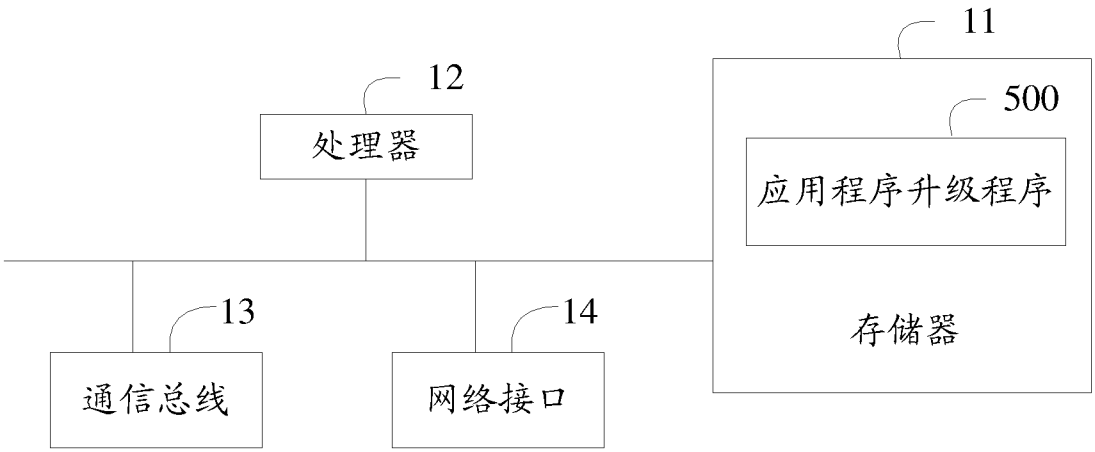
11
12
处理器
500
应用程序升级程序
存储器
13
通信总线
14
网络接口

图 5

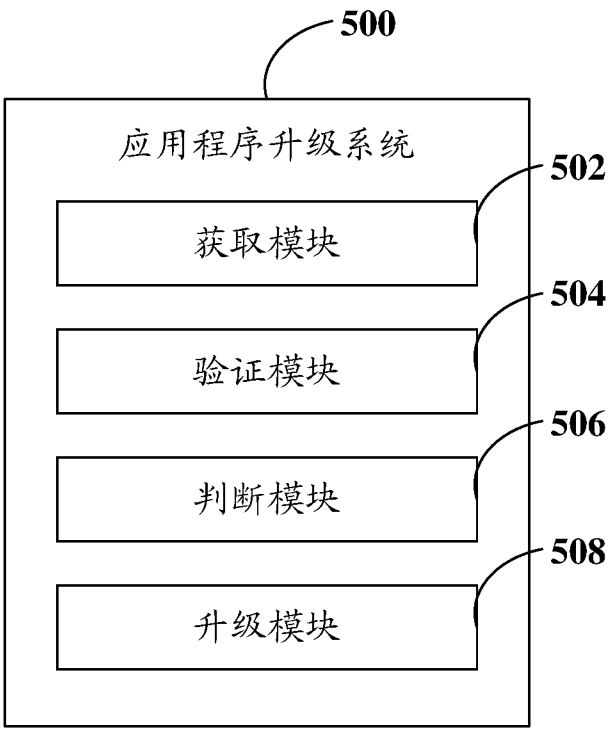
500
应用程序升级系统
502
获取模块
504
验证模块
506
判断模块
508
升级模块

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/091364

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/445 (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)

G06F; H04L

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, WPI, EPODOC, CNKI, IEEE, GOOGLE: 应用, 程序, 软件, 升级, 加密, 非对称, application, software, update, encode, RSA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101163044 A (BEIJING SHENSI LUOKE DATA PROTECTION CENTER) 16 April 2008 (16.04.2008), description, pages 5-8	1-20
A	CN 103873440 A (BEIJING WATERTEK INFORMATION TECHNOLOGY CO., LTD.) 18 June 2014 (18.06.2014), entire document	1-20
A	CN 101090452 A (CHINA NETWORK COMMUNICATION GROUP CORP.) 19 December 2007 (19.12.2007), entire document	1-20
A	US 2012039462 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 16 February 2012 (16.02.2012), entire document	1-20
A	US 2005128520 A1 (GLICKMAN, JEFF) 16 June 2005 (16.06.2005), entire document	1-20

☐ 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
29 August 2017	11 October 2017
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 KONG, Xin Telephone No. (86-10) 62413668

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/091364

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101163044 A	16 April 2008	WO 2009067879 A1	04 June 2009
CN 103873440 A	18 June 2014	None	
CN 101090452 A	19 December 2007	None	
US 2012039462 A1	16 February 2012	KR 20120015590 A	22 February 2012
US 2005128520 A1	16 June 2005	JP 2007517289 A	28 June 2007
		EP 1695519 A1	30 August 2006
		WO 2005122530 A1	22 December 2005
		CN 1914873 A	14 February 2007

国际检索报告

国际申请号 PCT/CN2017/091364

A. 主题的分类

G06F 9/445(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)

G06F; H04L

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, WPI, EPODOC, CNKI, IEEE, GOOGLE：应用，程序，软件，升级，加密，非对称，application，software，update，encode，RSA

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
X	CN 101163044 A (北京深思洛克数据保护中心) 2008年 4月 16日 (2008-04-16) 说明书第5页-第8页	1-20
A	CN 103873440 A (北京旋极信息技术股份有限公司) 2014年 6月 18日 (2014-06-18) 全文	1-20
A	CN 101090452 A (中国网络通信集团公司) 2007年 12月 19日 (2007-12-19) 全文	1-20
A	US 2012039462 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 2012年 2月 16日 (2012-02-16) 全文	1-20
A	US 2005128520 A1 (GLICKMAN, JEFF) 2005年 6月 16日 (2005-06-16) 全文	1-20

☐ 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
2017年 8月 29日	2017年 10月 11日

ISA/CN的名称和邮寄地址	受权官员
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	孔昕
传真号 (86-10)62019451	电话号码 (86-10)62413668

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/091364

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	101163044	A	2008年 4月 16日	WO	2009067879	A1	2009年 6月 4日
CN	103873440	A	2014年 6月 18日		无		
CN	101090452	A	2007年 12月 19日		无		
US	2012039462	A1	2012年 2月 16日	KR	20120015590	A	2012年 2月 22日
US	2005128520	A1	2005年 6月 16日	JP	2007517289	A	2007年 6月 28日
				EP	1695519	A1	2006年 8月 30日
				WO	2005122530	A1	2005年 12月 22日
				CN	1914873	A	2007年 2月 14日