

(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
2014 年 5 月 30 日 (30.05.2014)



(10) 国际公布号
WO 2014/079282 A1

- (51) 国际专利分类号:
G06F 21/00 (2013.01)
- (21) 国际申请号: PCT/CN2013/084865
- (22) 国际申请日: 2013 年 10 月 9 日 (09.10.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210482877.X 2012 年 11 月 23 日 (23.11.2012) CN
- (71) 申请人: 腾讯科技(深圳)有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。
- (72) 发明人: 周健 (ZHOU, Jian); 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 403 室, Guangdong 518000 (CN)。
- (74) 代理人: 北京德琦知识产权代理有限公司 (DEQI INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区知春路 1 号学院国际大厦 7 层, Beijing 100083 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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)。

根据细则 4.17 的声明:

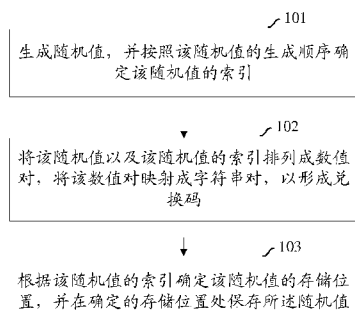
- 关于申请人有权要求在先申请的优先权(细则 4.17(iii))

本国际公布:

- 包括国际检索报告(条约第 21 条(3))。

(54) Title: METHOD AND APPARATUS FOR STORING AND VERIFYING REDEEM CODE

(54) 发明名称: 存储和验证兑换码的方法和装置



101 Generating a random value and determining an index of the random value according to the generation sequence of same

102 Arranging the random value and the index of random value into a value pair, mapping the value pair into a character string to form a redeem code

103 Determining storage location of the random value according to the index of the random value and storing the random value in the determined storage location

图 1 /FIG. 1

(57) Abstract: A method and an apparatus for storing and verifying a redeem code. The method comprises: generating a random value and determining an index for same according to the generation sequence thereof; generating a value pair according to the random value and the index of the random value, mapping the value pair into a character string, and generating a redeem code according to the character string; and determining storage location of the random value according to the index of the random value and storing the random value in the determined storage location.

(57) 摘要: 一种兑换码的存储、验证的方法和装置。方法包括: 生成随机值, 按照随机值的生成顺序确定随机值的索引; 根据随机值和随机值的索引生成数值对, 将数值对映射成字符串, 根据字符串生成兑换码; 根据随机值的索引确定随机值的存储位置, 并在所确定的存储位置保存随机值。

WO 2014/079282 A1

存储和验证兑换码的方法和装置

技术领域

本发明实施方式涉及信息处理技术领域，更具体地，涉及一种存储和验证兑换码的方法和装置。

5 发明背景

兑换码 (Redeem code)，又叫推广码 (promo code 或 promotion code)，一般是开发者用来推广实际产品或计算机程序产品的代码，其构成一般包括数字和字符等，例如：YWERE77RMJA9。用户可以使用兑换码获得计算机程序或者其他各种实体产品。在用户兑换完程序或者
10 者其他实体产品之后，兑换码一般就失效。

根据现有的兑换码生成和存储方式，采用随机算法生成若干个字符串，将该生成的字符串作为兑换码，并且将所有兑换码都完整地保存在存储空间，如数据库中。相应地，在验证兑换码时，通过字符串比较的方式来查找数据库，从而确定数据库中是否存在该验证码或确定
15 该验证码是否已经兑出。

然而，根据现有的兑换码的生成方式，在兑换码的数量非常巨大的情况下，随机生成的兑换码也可能重复，所以在生成兑换码的过程中或生成后还需要有去除重复生成的兑换码的步骤从而造成兑换码的生成效率低下。而且，由于全部兑换码完整地保存在数据库，大量的存
20 储空间被占用。如果单纯为了节约存储空间而降低兑换码的位数，则无法保证兑换码的破解成功率可控。进一步地，根据现有的兑换码的验证方式，需要采用全文对比的方式查找数据库、文件或其他存储介质，因此数据检索量大，验证效率低下。

发明内容

本发明实施方式提出一种存储和验证交换码的方法和装置，从而在保证交换码的破解成功率可控的情形下，节约数据存储空间，提高交换码的验证效率。

5 一种交换码的存储方法，包括：

生成随机值，并按照所述随机值的生成顺序确定所述随机值的索引；

根据所述随机值以及所述随机值的索引生成数值对，将所述数值对映射成字符串，根据所述字符串生成交换码；

10 根据所述随机值的索引确定所述随机值的存储位置，并在所确定的存储位置处保存所述随机值。

一种交换码的验证方法，包括：

接收交换码，其中所述交换码的生成方法包括：

生成随机值，并按照所述随机值的生成顺序确定所述随机值的索引；

15 根据所述随机值以及所述随机值的索引生成数值对，将所述数值对映射成字符串，根据所述字符串生成所述交换码；

根据交换码获取字符串，将所述字符串反映射为数值对，并按照所述数值对中的随机值的索引确定存储位置；

20 当判定所述存储位置处储存的随机值没有被交换时，进一步判断所述数值对中的所述随机值与在所述存储位置处储存的所述随机值是否一致，如果是，则判定交换码验证成功。

一种交换码的存储装置，该装置包括随机值生成单元、交换码生成单元和交换码存储单元，其中：

所述随机值生成单元，用于生成随机值，并按照所述随机值的生成顺序确定所述随机值的索引；

25 所述交换码生成单元，用于根据所述随机值以及所述随机值的索引

生成数值对，将所述数值对映射成字符串，根据所述字符串生成兑换码；

所述兑换码存储单元，用于根据所述随机值的索引确定所述随机值的存储位置，并在所确定的存储位置处保存所述随机值。

- 5 一种兑换码的验证装置，包括兑换码接收单元、存储位置确定单元和验证单元，其中：

所述兑换码接收单元，用于接收兑换码，其中该兑换码的生成方法包括：

- 生成随机值，并按照所述随机值的生成顺序确定所述随机值的索引；根据所述随机值以及所述随机值的索引生成数值对，将所述数值对映射成字符串，根据所述字符串生成所述兑换码；
- 10

所述存储位置确定单元，用于根据所述兑换码获取字符串，将所述字符串反映射为数值对，并按照所述数值对中的随机值的索引确定存储位置；

- 15 所述验证单元，用于当判定所述存储位置处储存的随机值没有被兑换时，进一步判断所述数值对中的所述随机值与在所述存储位置处储存的随机值是否一致，如果是，则判定兑换码验证成功。

- 从上述技术方案可以看出，根据本发明实施方式，通过把兑换码设置成字符串与数值的映射规则，每个兑换码由一对数值构成，其中一个数值是随机值，另一个数值是与随机值生成顺序相关的索引，在生成兑换码环节把数值对映射成字符串对，而且在保存兑换码时只需要存储随机值，因此在保证兑换码的破解成功率可控的情形下，还可以节约数据存储空间。而且，在本发明实施方式中，在兑换环节把字符串对映射成数值对进行验证，从而提高兑换码的验证效率。另外，本发明实施方式可以应用到各种终端中，可以跨平台跨终端使用本发明
- 20
- 25

实施方式，适用范围非常广泛。

附图简要说明

图 1 为根据本发明实施方式的兑换码的存储方法流程图。

图 2 为根据本发明实施方式的兑换码的验证方法流程图。

5 图 3 为根据本发明实施方式的兑换码的生成过程示意图。

图 4 为根据本发明实施方式的兑换码的验证过程示意图。

图 5 为根据本发明实施方式的兑换码的存储装置结构图。

图 6 为根据本发明实施方式的兑换码的验证装置结构图。

实施本发明的方式

10 为使本发明的技术方案和优点更加清楚，下面结合附图对本发明作进一步的详细描述。

图 1 为根据本发明实施方式的兑换码的存储方法流程图。如图 1 所示，该方法包括如下步骤。

步骤 101：服务器生成随机值，并按照该随机值的生成顺序确定该
15 随机值的索引。

在本步骤中，可以利用各种随机数生成算法来生成随机值，而且可以按照该随机值的生成顺序确定该随机值的索引。

随机值的索引是由随机值的生成顺序所确定。在本发明的一个实施例中，该索引是连续递增的正整数。比如，应用随机数生成算法第一次生成了随机值 123，应用随机数生成算法第二次生成了随机值 478，
20 应用随机数生成算法第三次生成了随机值 567，则可以确定该随机值 123 的索引为 1、随机值 478 的索引为 2，随机值 567 的索引为 3。

步骤 102：服务器将该随机值以及该随机值的索引排列成数值对，

将该数值对映射成字符串，此时可以利用该字符串作为兑换码。

在本发明的一个实施例中，还可以进一步对映射出的字符串执行混淆操作，并将执行混淆操作后的字符串作为兑换码。

在本步骤中，首先将在步骤 101 中生成的随机值以及该随机值的索引排列成数值对，然后再将该数值对映射成字符串，并且混淆字符串对以形成兑换码。

本发明实施方式中，可以首先通过多种方式来将数值对映射成字符串对。其中一种实现方式是，利用数值到字符串函数（num2str），将该数值对中的每个数值转换为对应的 24 进制的字符串，从而将数值对映射为字符串对。之后根据索引值和随机值这两个数值对应的两个字符串组成一个新字符串，以这个新字符串作为验证码，进一步的可以对所述字符串（如所述 24 进制的字符串）进行混淆以加强安全性。混淆操作是一种可以用于对移动代码和软件知识产权进行保护的程序变换技术，本发明实施方式可以采用各种现有的混淆算法，或者采用将来可能出现的混淆算法。

在本发明的一个实施例中，在该数值对转化为字符串的过程中，可以分别将数值 0~23 映射为 24 个字符，比如：“0”、“1”、“2”、“3”、“4”、“5”、“6”、“7”、“8”、“9”、“A”、“B”、“C”、“D”、“E”、“F”、“G”、“H”、“I”、“J”、“K”、“L”、“M”、“N”。

假如在步骤 101 中第 50000 个随机值是 22078136，那么该数值对就是(50000,22078136)，该数据值对对应的 24 进制表示为（“3EJ8”，“2ID228”），此时映射出字符串为“3EJ82ID228”。

然后，可以利用各种混淆算法，对该映射出字符串进行混淆。比如，混淆为“3E2ID228J8”以作为等待存储的兑换码。

再比如，假设在步骤 101 中第 90000 个随机值是 33069592，那么该数值对就是(90000, 33069592)，该数据值对对应的 24 进制表示为 (“ 6C60 ” ， “ 43G4BG ”) ， 此时映射出字符串为 “6C6043G4BG” 。

5 然后，可以利用各种混淆算法，对该映射出字符串进行混淆。比如，混淆为 “6C43G4BG60” 以作为等待存储的兑换码。

再比如，假设在步骤 101 中第 100000 个随机值是 47892341，那么该数值对就是(100000, 47892341)，该数据值对对应的 24 进制表示为 (“ 75EG ” ， “ 608AA5 ”) ， 此时映射出字符串为
10 “75EG608AA5” 。

然后，可以利用各种混淆算法，对该映射出字符串进行混淆。比如，混淆为 “75608AA5EG 以作为等待存储的兑换码。

在本发明的一个实施例中，由于在 “0” 、 “1” 、 “2” 、 “3” 、 “4” 、 “5” 、 “6” 、 “7” 、 “8” 、 “9” 、 “A” 、 “B” 、
15 “C” 、 “D” 、 “E” 、 “F” 、 “G” 、 “H” 、 “I” 、 “J” 、 “K” 、 “L” 、 “M” 、 “N” 字符中，会有一些视觉类似的字符。因此，优选采用 “3” 、 “4” 、 “5” 、 “6” 、 “7” 、 “9” 、 “A” 、 “C” 、 “E” 、 “F” 、 “G” 、 “H” 、 “J” 、 “K” 、 “L” 、 “M” 、 “N” 、 “P” 、 “R” 、 “S” 、 “T” 、 “W” 、 “X” 、
20 “Y” 作为 24 进制转换中的 24 个字符。

以上虽然以 24 进制为实例对本发明实施方式进行了详细说明，本领域技术人员可以意识到，本发明实施方式并不局限于 24 进制，而是适用于任意的进制以及映射算法。

步骤 103: 服务器根据该随机值的索引确定该随机值的存储位置，
25 并在所确定的存储位置处保存该随机值。

在本发明的一个实施例中，将索引与存储位置的对应关系保存在交换索引表中。

在本步骤中，可以利用位图(bitmap)、哈希(hash)或数组(array)的方式，根据该随机值的索引确定该随机值在交换索引表中对应的存储位置，并在所确定的存储位置处保存该随机值。

在本发明的一个实施例中，进一步在交换索引表中保存与随机值对应的交换状态位，用于指示该随机值对应的交换码的交换状态，即该交换码是否已被交换。

比如：可以用 1 个比特(bit)作为交换状态位，这样存储容量为 1Mbyte 的内存就可以存储 800 万个交换码的交换状态。

当交换码较多的时候，还可以用多个比特来表示交换码的交换状况，本发明实施方式对此并无限定。

比如，第 50000 个随机值是 22078136，则可以在交换索引表中索引 50000 对应的存储位置存储该随机值 22078136；第 90000 个随机值是 33069592，则可以在交换索引表中索引 90000 对应的存储位置存储该随机值 33069592；第 100000 个随机值是 47892341，则可以在交换索引表中索引 10000 对应的存储位置存储该随机值 47892341。

在实际应用中，无需存储随机值的索引，只需要能够根据索引值确定随机值的存储位置即可。譬如到数组的 50000 位置存储 22078136 (array[5000]=22078136)。

在本发明的一个实施例中，还可以预先确定交换码的期望生成数目，并根据交换码的期望生成数目确定索引的位数；再确定交换码破解概率门限值，并根据所述交换码破解概率门限值确定随机值的位数。

此时，步骤 101 中的生成随机值并按照该随机值的生成顺序确定该

随机值的索引包括：按照该随机值的位数生成随机值，并且按照该随机值的生成顺序和索引的位数确定该随机值的索引。

以期望生成数量为 40 亿、破解成功概率小于 796 万分之 1 的兑换码为例进行说明。

- 5 由于 $24^7=4586471424$ ，其值域超过 45 亿，因此索引值可以占用 7 个字符。由于 $24^5=7962624$ ，其值域超过 796 万，因此随机值可以占用 5 个字符。因此，兑换码共 12 个字符（ $12=7+5$ ），则可以生成 45 亿个兑换码，而且破解的成功概率小于 796 万分之 1。

- 10 如果要进一步降低破解的成功率，可以增加随机值的字符个数。比如：当随机值有 6 位的话，破解成功率就小于 1 亿 9000 万分之 1，兑换码一共为 13 个字符。

- 15 在上述实施例提供的方法中，通过把索引值和随机值生成的字符串进行混淆，使得普通用户更难从中发现规律。而且索引值和随机值每个字符都可以表示一个 24 进制的值，因此可以将一个字符表示的含义拆开，其中一部分表示索引值，一部分表示随机值，比如第 1-20bit 表示随机值，第 21-24bit 表示索引值。而且，在验证兑换码的过程中，还可以采用位图（bitmap）、哈希（hash）或数组（array）的方式，将兑换索引表全部放在内存中加快查找的效率。

本发明实施方式还提出了一种兑换码的验证方法。

- 20 图 2 为根据本发明实施方式的兑换码的验证方法流程图。如图 2 所示，该方法包括如下步骤。

- 25 步骤 201：服务器接收兑换码，其中该兑换码的生成方法包括：生成随机值，并按照该随机值的生成顺序确定该随机值的索引；将该随机值以及该随机值的索引排列成数值对，将该数值对映射成字符串，并且混淆所述字符串对以形成兑换码。

在本步骤中，所接收的交换码可以是根据图 1 所示方法生成的交换码。

步骤 202：对该交换码执行反混淆操作，获取该交换码对应的字符串，进而确定交换码对应的字符串对，将所述字符串对反映射为数值对，并
5 对，并按照该数值对中的该随机值的索引确定存储位置。

首先，针对该交换码执行与交换码生成过程中的混淆操作相逆的反混淆操作，从而得到该交换码对应的原始字符串，将原始字符串拆解为字符串对，然后再将所述字符串对执行与交换码生成过程中的映射操作相逆的反映射操作，从而将该字符串对还原为数值对，该数值对
10 包括随机值以及随机值的索引，再按照该数值对中的该随机值的索引确定该交换码的存储位置。

步骤 203：当服务器判定所述存储位置处储存的该随机值没有被兑换时，进一步判断该数值对中的该随机值与在所述存储位置处储存的该随机值是否一致，如果是，则判定交换码验证成功。

在本发明的一个实施例中，可以首先判断所述存储位置处储存的该随机值是否已经兑换，如果所述存储位置处储存的该随机值已经被兑换，则判定交换码验证失败；如果所述存储位置处储存的该随机值未被兑换，则进一步判断该数值对中的该随机值与在所述存储位置处储存的该随机值是否一致，如果该数值对中的该随机值与在所述存储位置处储存的该随机值一致，则判定交换码验证成功，如果该数值对中的该随机值与在所述存储位置处储存的该随机值不一致，则判定交换码验证失败。
15
20

在本步骤中，可以根据交换索引表中的交换状态位来判定存储位置处储存的该随机值是否已经兑换。当判断所述存储位置处储存的该随机值已经兑换时，则判定交换码之前已经兑现过，因此验证失败。
25

当判断所述存储位置处储存的该随机值没有交换时，则判定交换码之前没有兑现过，进一步查询交换索引表，判断步骤 202 中获得的随机值是否与交换索引表中存储位置处储存的随机值是否一致，如果步骤 202 中获得的随机值与交换索引表中存储位置处储存的随机值一致，判定交换码验证成功，如果步骤 202 中获得的随机值是否与交换索引表中存储位置处储存的随机值不一致，则判定交换码验证失败。

在本发明的一个实施例中，在该方法中，进一步当判定交换码验证成功时，更新交换索引表中该随机值对应的交换状态位为已交换。

通过应用本发明实施方式，提高了交换码的生成效率和验证效率，并且交换码的存储和验证过程完全摆脱数据库，根据索引存储和查询交换码，而且交换码破解的成功率是可控的。

图 3 为根据本发明实施方式的交换码的生成过程示意图。图 4 为根据本发明实施方式的交换码的验证过程示意图。

根据本发明的一个实施例，以生成 40 亿个交换码为例进行说明。

在交换码的生成和存储过程中，首先顺序生成 40 亿个值域为[0, 7962624)的随机值。并保留一份索引与随机值的对照关系在交换索引表中以备后续交换阶段使用。然后把索引值（input_idx）和随机值（input_random）通过数值到字符串（string）的函数 num2str 转化为 40 亿个字符串，再把这 40 亿个字符串通过一定的混淆算法，譬如调换次序组合成 40 亿个交换码，并提供给客户进行使用。同时将随机值存储在索引对应的存储位置。

在验证交换码的过程中，首先把交换码通过反混淆操作还原为一对字符串，再把这对字符串通过字符串到数值的函数 str2num 转化为数值对，其中索引值是 input_idx，随机值是 input_random，再根据 input_idx 查找交换索引表，该交换索引表可以是 bitmap 也可以是 hash 或者数据

库的表，确定该交换码是否已经交换过了，如果该交换码没有交换过，则找到在交换索引表中与 input_idx 对应的随机值，比较找到的随机值和 input_random，如果找到的随机值和 input_random 相同，则确定交换码验证成功，并且在交换索引表中更新该交换码对应的交换状态位；如果找到的随机值和 input_random 不相同，则确定交换码验证失败。

本发明实施方式提供的方法可以在各种形式的服务器中实施。

本发明实施方式还提出了一种交换码的存储装置。

图 5 为根据本发明实施方式的交换码的存储装置结构图。如图 5 所示，该装置包括随机值生成单元 501、交换码生成单元 502 和交换码存储单元 503。

随机值生成单元 501 用于生成随机值，并按照该随机值的生成顺序确定该随机值的索引。

交换码生成单元 502 用于将该随机值以及该随机值的索引排列成数值对，将该数值对映射成字符串，以形成交换码。

交换码存储单元 503 用于根据该随机值的索引确定该随机值的存储位置，并在所确定的存储位置处保存所述随机值。

在一个实施方式中，该装置进一步包括位数确定单元 504。

位数确定单元 504 用于确定交换码的数目，并根据交换码的数目确定索引的位数；确定交换码破解概率门限值，并根据所述交换码破解概率门限值确定随机值的位数。

随机值生成单元 501 用于按照该随机值的位数生成随机值，并且按照该随机值的生成顺序和索引的位数确定该随机值的索引。

根据本发明一个实施例，交换码存储单元 502 用于以位图（bitmap）、哈希（hash）或数组（array）的方式，根据该随机值的索

引确定该随机值在交换索引表中的存储位置，并在所确定的交换索引表中的存储位置处保存该随机值，而且在交换索引表中保存表明该随机值是否已交换的交换状态位；并进一步用于当判定交换码验证成功时，更新交换索引表中该存储位置处随机值的交换状态位状态为已交换。

本发明实施方式还提出了一种交换码的验证装置。

图 6 为根据本发明实施方式的交换码的验证装置结构图。如图 6 所示，该装置包括交换码接收单元 601、存储位置确定单元 602 和验证单元 603。

10 交换码接收单元 601，用于接收交换码，其中该交换码的生成方法包括：生成随机值，并按照该随机值的生成顺序确定该随机值的索引；将该随机值以及该随机值的索引排列成数值对，将该数值对映射成字符串对，并且混淆所述字符串对以形成交换码。

15 存储位置确定单元 602，用于对所述交换码执行反混淆操作，获取该交换码对应的字符串，并将所述字符串反映射为数值对，并按照该数值对中的该随机值的索引确定存储位置。

验证单元 603，用于当判定所述存储位置处储存的该随机值没有被交换时，进一步判断该数值对中的该随机值与在所述存储位置处储存的该随机值是否一致，如果是，则判定交换码验证成功。

20 在本发明的一个实施例中，验证单元 603，判断所述存储位置处储存的该随机值是否已经交换，如果所述存储位置处储存的该随机值已经被交换，则判定交换码验证失败；如果所述存储位置处储存的该随机值未被交换，则进一步判断该数值对中的该随机值与在所述存储位置处储存的该随机值是否一致，如果该数值对中的该随机值与在所述
25 存储位置处储存的该随机值一致，则判定交换码验证成功，如果该数

值对中的该随机值与在所述存储位置处储存的该随机值不一致，则判定兑换码验证失败。

在一个实施方式中，验证单元 603 用于根据兑换索引表中的兑换状态位来判定存储位置处储存的该随机值是否已经兑换，并当判定兑换码验证成功时，更新兑换索引表中该存储位置处随机值的兑换状态位为已兑换。

图 1、图 2 所示方法流程和图 5、图 6 所示装置结构可以集成到各种形式的作为服务器的硬件实体当中。比如，可以集成到：功能手机、智能手机、掌上电脑、个人电脑（PC）、平板电脑或个人数字助理（PDA），等等设备之中。

本发明实施例提供的方法和装置可以由硬件、或计算机可读指令、或者硬件和计算机可读指令的结合来实现。本实施例中使用的计算机可读指令由多个处理器存储在可读存储介质中，例如硬盘、CD-ROM、DVD、光盘、软盘、磁带、RAM、ROM 或其它合适的存储设备。或者，至少部分计算机可读指令可以由具体硬件替换，例如，定制集成线路、门阵列、FPGA、PLD 和具体功能的计算机等等。

本发明实施例提供了计算机可读存储介质，用于存储指令使得计算机执行本文所述的方法。具体地，本实施例提供的系统或设备都具有存储介质，其中存储了计算机可读程序代码，用于实现上述任意实施例的功能，并且这些系统或设备（或 CPU 或 MPU）能够读取并且执行存储在存储介质中的程序代码。

在这种情况下，从存储介质中读取的程序代码可以实现上述任一实施例，因此该程序代码和存储该程序代码的存储介质是技术方案的一部分。

用于提供程序代码的存储介质包括软盘、硬盘、磁光盘、光盘（例

如 CD-ROM、CD-R、CD-RW、DVD-ROM、DVD-RAM、DVD-RW、DVD+RW)、磁盘、闪存卡、ROM 等等。可选地，程序代码也可以通过通信网络从服务器电脑上下载。

5 应该注意的是，对于由计算机执行的程序代码，至少部分由程序代码实现的操作可以由运行在计算机上的操作系统实现，从而实现上述任一实施例的技术方案，其中该计算机基于程序代码执行指令。

另外，存储介质中的程序代码被写入存储器，其中，该存储器位于插入在计算机中的扩展板中，或者位于连接到计算机的扩展单元中。在本实施例中，扩展板或扩展单元中的 CPU 根据指令，基于程序代码执行至少部分操作，从而实现上述任一实施例的技术方案。

实际上，可以通过多种方式来具体实施本发明实施方式所提出的兑换码的存储和/或验证方法。比如，可以遵循一定规范的应用程序接口，将计算机文件运行装置编写为安装到计算机系统上的插件程序，也可以将其封装为应用程序以供用户自行下载使用。当编写为插件程序时，可以将其实施为 ocx、dll、cab 等多种插件形式。也可以通过 Flash 插件、RealPlayer 插件、MMS 插件、MIDI 五线谱插件、ActiveX 插件等具体技术来实施本发明实施方式所提出的兑换码的存储和/或验证装置。

综上所述，在本发明实施方式中，通过把兑换码设置成字符串与数值的映射规则，每个兑换码由一对数值构成，其中一个数值是随机值，另一个数值是与随机值生成顺序相关的索引。在生成兑换码环节把数值对映射成字符串，而且在保存兑换码时只需要存储随机值，从而在保证兑换码的破解成功率可控的情形下，还可以节约数据存储空间。

25 而且，在本发明实施方式中，在兑换环节把字符串映射成数值对进

行验证，从而提高兑换码的验证效率。

另外，可以将本发明实施方式可以应用到各种终端中，可以跨平台跨终端使用本发明实施方式，适用范围非常广泛。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的
5 保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求书

1、一种兑换码的存储方法，其特征在于，该方法包括：

生成随机值，并按照所述随机值的生成顺序确定所述随机值的索引；

根据所述随机值以及所述随机值的索引生成数值对，将所述数值对
5 映射成字符串，根据所述字符串生成兑换码；

根据所述随机值的索引确定所述随机值的存储位置，并在所确定的
存储位置处保存所述随机值。

2、根据权利要求1所述的兑换码的存储方法，其特征在于，该方法
进一步包括：

10 确定兑换码期望生成数目，并根据所述兑换码期望生成数目确定所
述索引的位数；确定兑换码破解概率门限值，并根据所述兑换码破解概
率门限值确定所述随机值的位数，

所述生成随机值，并按照所述随机值的生成顺序确定所述随机值的
索引包括：按照所述随机值的位数生成所述随机值，并且按照所述随机
15 值的生成顺序和所述索引的位数确定所述随机值的索引。

3、根据权利要求1所述的兑换码的存储方法，其特征在于，所述根
据所述随机值的索引确定所述随机值的存储位置，并保存所述随机值包
括：

以位图（bitmap）、哈希（hash）或数组（array）的方式，根据所述
20 随机值的索引确定所述随机值在兑换索引表中的存储位置，并在所述存
储位置处保存所述随机值，并且在兑换索引表中保存表明所述随机值是
否已兑换的兑换状态位。

4、根据权利要求1所述的兑换码的存储方法，其特征在于，所述将
所述数值对映射成字符串为：

利用数值到字符串函数 (num2str) 将所述数值对中的每个数值转换为对应的 24 进制的字符串表示, 并根据每个数值的字符串表示组成字符串。

- 5、根据权利要求 1 所述的交换码的存储方法, 其特征在于, 所述将
- 5 根据所述字符串生成交换码包括:

对所述字符串执行混淆处理, 生成所述交换码。

- 6、一种交换码的验证方法, 其特征在于, 该方法包括:

接收交换码, 其中所述交换码的生成方法包括:

生成随机值, 并按照所述随机值的生成顺序确定所述随机值的索引;

- 10 根据所述随机值以及所述随机值的索引生成数值对, 将所述数值对映射成字符串, 根据所述字符串生成所述交换码;

根据交换码获取字符串, 将所述字符串反映射为数值对, 并按照所述数值对中的随机值的索引确定存储位置;

- 当判定所述存储位置处储存的随机值没有被交换时, 进一步判断所
- 15 述数值对中的所述随机值与在所述存储位置处储存的所述随机值是否一致, 如果是, 则判定交换码验证成功。

- 7、根据权利要求 6 所述的交换码的验证方法, 其特征在于,

当生成所述交换码时对所述字符串进行了混淆处理时, 根据交换码获取字符串包括:

- 20 对所述交换码执行反混淆操作以获取所述字符串。

- 8、根据权利要求 6 所述的交换码的验证方法, 其特征在于,

所述将所述数值对映射成字符串包括: 利用数值到字符串函数 (num2str) 将所述数值对中的每个数值转换为对应的 24 进制的字符串, 并根据每个数值的字符串组成字符串;

- 25 所述将所述字符串反映射为数值对为: 利用字符串到数值函数

(str2num) 将所述字符串中的每个 24 进制的字符串表示转换为对应的数值，并根据每个数值组成数值对。

9、根据权利要求 6 所述的交换码的验证方法，其特征在于，所述按照所述数值对中的所述随机值的索引确定存储位置为：按照所述数值对
5 中的所述随机值的索引确定交换索引表中的存储位置；

所述当判定所述存储位置处储存的该随机值没有被交换包括：根据交换索引表中表明随机值是否已交换的交换状态位来判定存储位置处储存的该随机值是否已经交换；该方法进一步包括：

当判定交换码验证成功时，更新交换索引表中所述存储位置处随机
10 值的交换状态位为已交换。

10、一种交换码的存储装置，其特征在于，该装置包括随机值生成单元、交换码生成单元和交换码存储单元，其中：

所述随机值生成单元，用于生成随机值，并按照所述随机值的生成顺序确定所述随机值的索引；

15 所述交换码生成单元，用于根据所述随机值以及所述随机值的索引生成数值对，将所述数值对映射成字符串，根据所述字符串生成交换码；

所述交换码存储单元，用于根据所述随机值的索引确定所述随机值的存储位置，并在所确定的存储位置处保存所述随机值。

11、根据权利要求 10 所述的交换码的存储装置，其特征在于，进一
20 步包括位数确定单元，其中：

所述位数确定单元，用于确定交换码期望生成数目，并根据所述交换码期望生成数目确定所述索引的位数；确定交换码破解概率门限值，并根据所述交换码破解概率门限值确定所述随机值的位数；

所述随机值生成单元，用于按照所述随机值的位数生成所述随机值，
25 并且按照所述随机值的生成顺序和所述索引的位数确定所述随机值的

索引。

12、根据权利要求 10 所述的交换码的存储装置，其特征在于，

所述交换码存储单元，用于以位图（bitmap）、哈希（hash）或数组（array）的方式，根据所述随机值的索引确定所述随机值在交换索引表中的存储位置，并在所述存储位置处保存所述随机值，而且在交换索引表中保存表明所述随机值是否已交换的交换状态位；并进一步用于当判定交换码验证成功时，更新交换索引表中该存储位置处随机值的交换状态位状态为已交换。

13、根据权利要求 10 所述的交换码的存储装置，其特征在于，

所述交换码生成单元，用于对所述字符串执行混淆处理，生成所述交换码。

14、一种交换码的验证装置，其特征在于，包括交换码接收单元、存储位置确定单元和验证单元，其中：

所述交换码接收单元，用于接收交换码，其中该交换码的生成方法包括：

生成随机值，并按照所述随机值的生成顺序确定所述随机值的索引；根据所述随机值以及所述随机值的索引生成数值对，将所述数值对映射成字符串，根据所述字符串生成所述交换码；

所述存储位置确定单元，用于根据所述交换码获取字符串，将所述字符串映射为数值对，并按照所述数值对中的随机值的索引确定存储位置；

所述验证单元，用于当判定所述存储位置处储存的随机值没有被交换时，进一步判断所述数值对中的所述随机值与在所述存储位置处储存的随机值是否一致，如果是，则判定交换码验证成功。

15、根据权利要求 14 所述的交换码的验证装置，所述存储位置确定

单元进一步用于，当生成所述交换码时对所述字符串进行了混淆处理时，对所述交换码执行反混淆操作以获取所述字符串。

16、根据权利要求 12 所述的交换码的验证装置，其特征在于，

- 所述验证单元，用于根据交换索引表中表明随机值是否已交换的交换状态位来判断存储位置处储存的该随机值是否已经交换，并当判定交换码验证成功时，进一步用于更新交换索引表中所述存储位置处随机值的交换状态位为已交换。
- 5

1/3

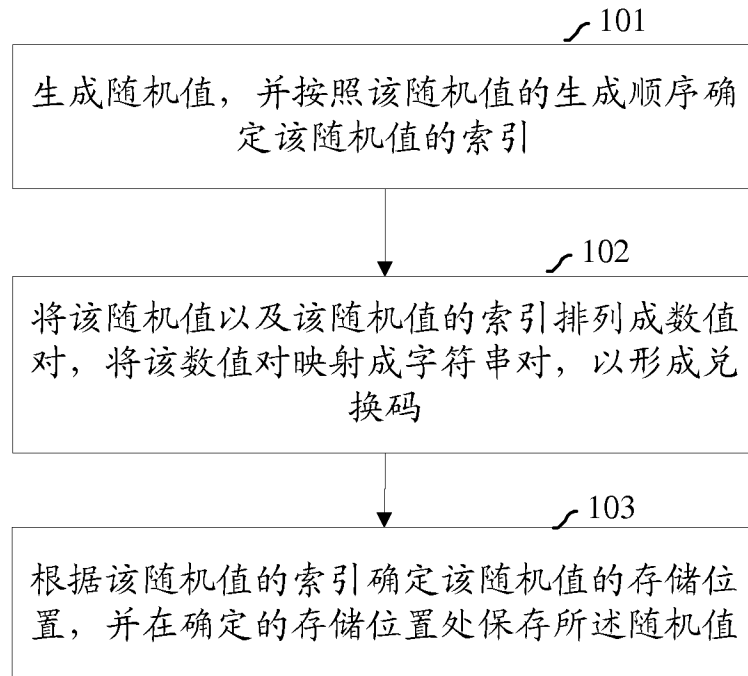


图 1

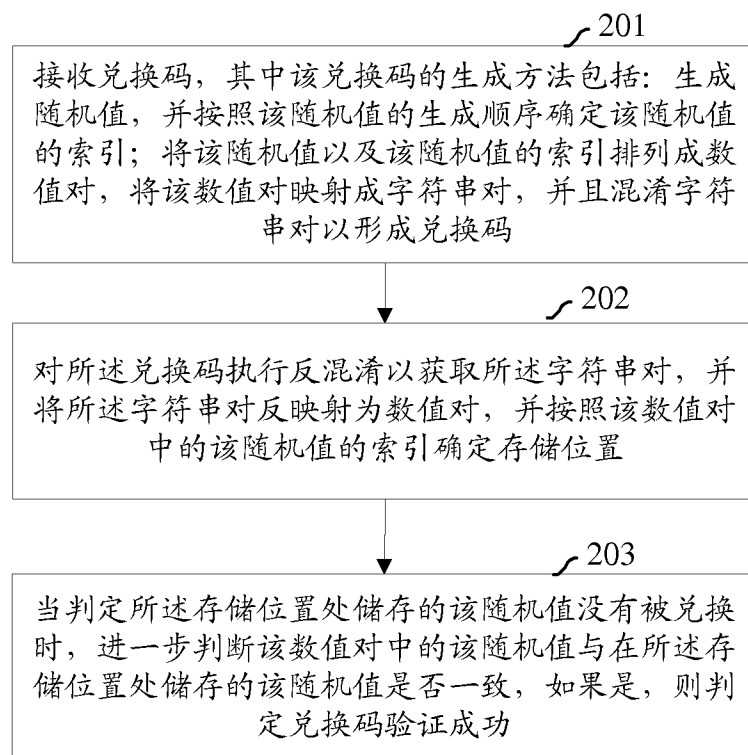


图 2

2/3

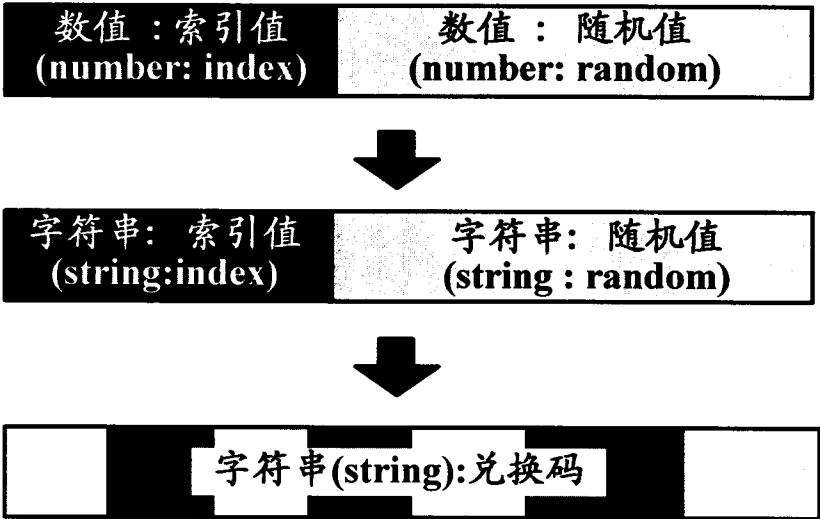


图 3

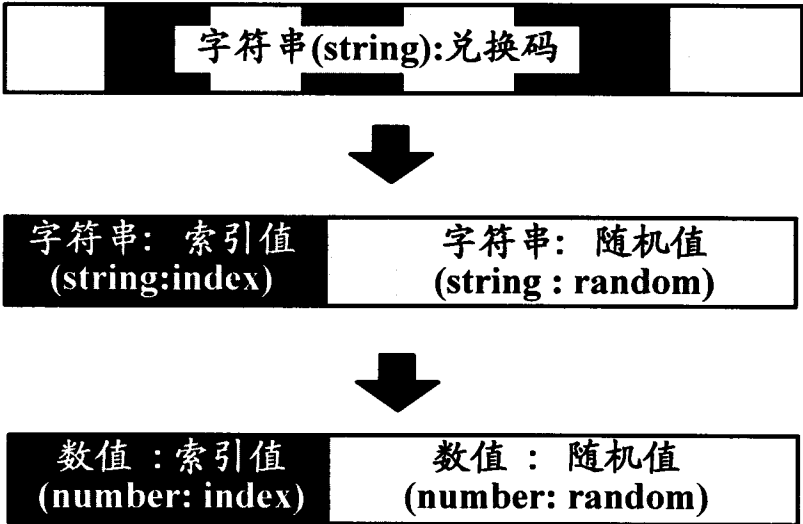


图 4

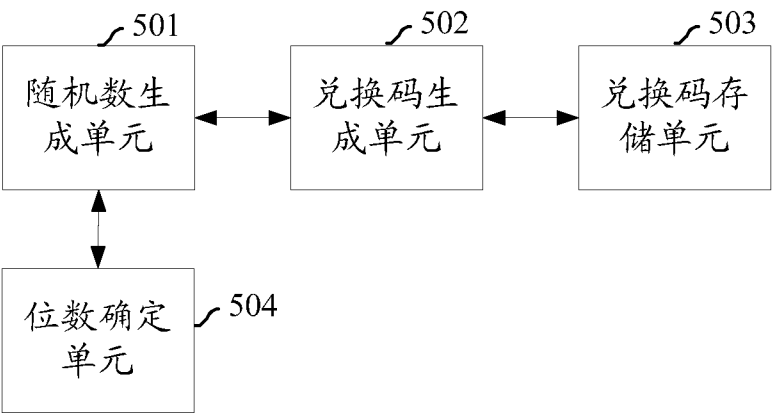


图 5



图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/084865

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00 (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)

IPC: 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)

WPI; EPODOC; CNTXT; WOTXT; CJFD: promo, promotion, redeem, code, key, random, index, identification, mapping, switch, character, number, stor+, address, sequence, bitmap, hash, array, retrieve, use, system, verification, confusion

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102752115 A (BEIJING TIANLONG RONGHE SOFTWARE CO LTD) 24 October 2012 (24.10.2012) description, paragraph [0052]	1, 10
Y	CN 102332030 A (CHINESE ACAD SCI COMPUTER TECHNOLOGY INS) 25 January 2012 (25.01.2012) description, paragraph [0071]	1, 10
A	WO 2012014231 A1 (JUTHANI N) 02 February 2012 (02.02.2012) the whole document	1-16
A	CN 101076807 A (VERISIGN INC.) 21 November 2007 (21.11.2007) the whole document	1-16

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 06 January 2014 (06.01.2014)	Date of mailing of the international search report 16 January 2014 (16.01.2014)
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 ZHAO, Weihua Telephone No. (86-10) 62411830

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/084865

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102752115 A	24.10.2012	None	
CN 102332030 A	25.01.2012	None	
WO 2012014231 A1	02.02.2012	EP 2598984 A1	05.06.2013
		IN 201002166 I3	11.01.2013
		US 2013124292 A1	16.05.2013
		WO 2012014231 A4	07.06.2012
CN 101076807 A	21.11.2007	WO 2006044717 A2	27.04.2006
		KR 20070050504 A	15.05.2007
		JP 4938673 B2	23.05.2012
		AU 2005295579 B2	04.08.2011
		US 8434138 B2	30.04.2013
		EP 1828946 A2	05.09.2007
		JP 2008517384 A	22.05.2008
		SG 156643 A1	26.11.2009
		US 8087074 B2	27.12.2011
		WO 2006044717 A3	28.09.2006
		AU 2005295579 A1	27.04.2006
		US 2009313687 A1	17.12.2009
		US 2012096535 A1	19.04.2012

A. 主题的分类

G06F 21/00 (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)

IPC: 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))

WPI; EPODOC; CNTXT; WOTXT; CJFD: 兑换码, 推广码, 一次性密码, 密钥, 随机值, 索引, 目录, 标识, 标志, 摘要, 映射, 转换, 字符串, 数字, 字母, 存储, 保存, 位置, 地址, 顺序, 先后, 次序, 混淆, 反混淆, 位图, 哈希, 数组, 进制, 验证, 使用, 兑换, 检索, promo, promotion, redeem, code, key, random, index, identification, mapping, switch, character, number, stor+, address, sequence, bitmap, hash, array, retrieve

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
Y	CN 102752115 A (北京天龙融合软件有限公司) 24.10 月 2012 (24.10.2012) 说明书第 52 段	1, 10
Y	CN 102332030 A (中国科学院计算技术研究所) 25.1 月 2012 (25.01.2012) 说明书第 71 段	1, 10
A	WO 2012014231 A1 (JUTHANI N) 02.2 月 2012 (02.02.2012) 全文	1-16
A	CN 101076807 A (弗里塞恩公司) 21.11 月 2007 (21.11.2007) 全文	1-16

☐ 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
06.1 月 2014 (06.01.2014)

国际检索报告邮寄日期
16.1 月 2014 (16.01.2014)

ISA/CN 的名称和邮寄地址:
中华人民共和国国家知识产权局
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

赵伟华

电话号码: (86-10) 62411830

国际检索报告

关于同族专利的信息

国际申请号

PCT/CN2013/084865

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN 102752115 A	24.10.2012	无	
CN 102332030 A	25.01.2012	无	
WO 2012014231 A1	02.02.2012	EP 2598984 A1	05.06.2013
		IN 201002166 I3	11.01.2013
		US 2013124292 A1	16.05.2013
		WO 2012014231 A4	07.06.2012
CN 101076807 A	21.11.2007	WO 2006044717 A2	27.04.2006
		KR 20070050504 A	15.05.2007
		JP 4938673 B2	23.05.2012
		AU 2005295579 B2	04.08.2011
		US 8434138 B2	30.04.2013
		EP 1828946 A2	05.09.2007
		JP 2008517384 A	22.05.2008
		SG 156643 A1	26.11.2009
		US 8087074 B2	27.12.2011
		WO 2006044717 A3	28.09.2006
		AU 2005295579 A1	27.04.2006
		US 2009313687 A1	17.12.2009
		US 2012096535 A1	19.04.2012