

(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 3 日 (03.05.2018)



(10) 国际公布号
WO 2018/076894 A1

(51) 国际专利分类号:
H04L 27/18 (2006.01)

(21) 国际申请号: PCT/CN2017/097350

(22) 国际申请日: 2017 年 8 月 14 日 (14.08.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610927601.6 2016 年 10 月 31 日 (31.10.2016) CN

(71) 申请人: 深圳市中兴微电子有限公司
(SANECHIPS TECHNOLOGY CO., LTD.) [CN/CN];
中国广东省深圳市南山区西丽街道留仙大道
中兴工业园, Guangdong 518055 (CN)。

(72) 发明人: 韩健 (HAN, Jian); 中国广东省深圳市南山区西丽街道留仙大道中兴工业园, Guangdong 518055 (CN)。

(74) 代理人: 北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE); 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 2 层, Beijing 100080 (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,

(54) Title: METHOD AND DEVICE FOR OBTAINING PSEUDO-RANDOM SEQUENCE AND STORAGE MEDIUM

(54) 发明名称: 一种获取伪随机序列的方法和装置、存储介质

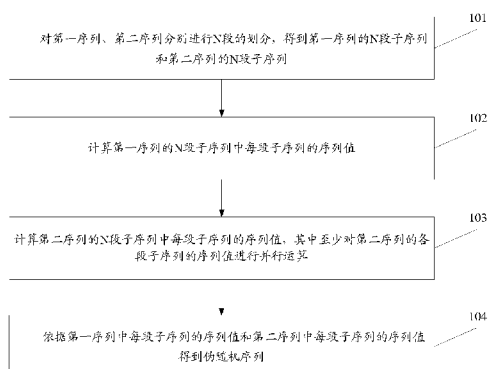


图 1

- 101 RESPECTIVELY DIVIDING A FIRST SEQUENCE AND A SECOND SEQUENCE INTO N SECTIONS, SO AS TO OBTAIN N SUBSEQUENCES OF THE FIRST SEQUENCE AND N SUBSEQUENCES OF THE SECOND SEQUENCE
- 102 CALCULATING A SEQUENCE VALUE FOR EACH SUBSEQUENCE IN THE N SUBSEQUENCES OF THE FIRST SEQUENCE
- 103 CALCULATING A SEQUENCE VALUE FOR EACH SUBSEQUENCE IN THE N SUBSEQUENCES OF THE SECOND SEQUENCE, WHEREIN PARALLEL CALCULATION IS PERFORMED AT LEAST ON THE SEQUENCE VALUE OF EACH SUBSEQUENCE OF THE SECOND SEQUENCE
- 104 OBTAINING A PSEUDO-RANDOM SEQUENCE ACCORDING TO THE SEQUENCE VALUE OF EACH SUBSEQUENCE IN THE FIRST SEQUENCE AND THE SEQUENCE VALUE OF EACH SUBSEQUENCE IN THE SECOND SEQUENCE

(57) Abstract: Disclosed in the embodiments of the present invention are a method and device for obtaining a pseudo-random sequence, and a storage medium, the method comprises: respectively dividing a first sequence and a second sequence into N sections, so as to obtain N subsequences of the first sequence and N subsequences of the second sequence; then calculating a sequence value for each subsequence in the N subsequences of the first sequence and the N subsequences of the second sequence; obtaining a pseudo-random sequence according to the sequence value of each subsequence in the first sequence and each subsequence in the sequence value of each

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))。

subsequence in the second sequence. Also disclosed is a device for obtaining a pseudo-random sequence. The present invention may achieve the quick calculation of a pseudo-random sequence, effectively reducing the amount of computation and saving storage space.

(57) 摘要: 本发明实施例公开了一种获取伪随机序列的方法和装置、存储介质, 所述方法包括: 对第一序列、第二序列分别进行N段的划分, 得到第一序列的N段子序列、第二序列的N段子序列, 再计算第一序列、第二序列的N段子序列中每段子序列的序列值, 依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值, 得到伪随机序列。还公开了一种获取伪随机序列的装置。可实现伪随机序列的快速计算, 可有效减少计算量和节约存储空间。

一种获取伪随机序列的方法和装置、存储介质

相关申请的交叉引用

本申请基于申请号为 201610927601.6、申请日为 2016 年 10 月 31 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的
5 全部内容在此引入本申请作为参考。

技术领域

本发明涉及伪随机序列生成技术，具体涉及一种获取伪随机序列的方法和装置、存储介质。

背景技术

10 伪随机序列既有随机信号所具备的优良的相关性，又具有随机信号不具备的规律性，使得它极易于从干扰信号中被识别和/或分离出来，且易于重复的产生和复制。由于具有这些特点，伪随机序列在扩频通信、多址通信、误码测试、信号同步等方面有着广泛的应用。

目前，在长期演进（LTE）系统中常用的伪随机序列（伪随机序列的序列值）产生方法有串行迭代公式法和基于状态转移矩阵乘法的产生方法。
15 其中，串行迭代公式法计算效率低，需要很长的迭代时间才能将伪随机序列计算出来。基于状态转移矩阵乘法的产生方法由于存在矩阵的乘法运算使得计算量大大增加且矩阵的大量计算增加了对存储空间的较大占用，不利于存储空间的节省。

20 发明内容

为解决现有存在的技术问题，本发明实施例提供一种获取伪随机序列

的方法和装置、存储介质，至少能够实现伪随机序列的快速计算，减少计算量和节约存储空间。

本发明实施例的技术方案是这样实现的：

本发明实施例提供一种获取伪随机序列的方法，所述方法包括：

5 对第一序列、第二序列分别进行N段的划分，得到第一序列的N段子序列、第二序列的N段子序列，N为正整数；

 计算第一序列的N段子序列中每段子序列的序列值；

 计算第二序列的N段子序列中每段子序列的序列值，其中至少对第二序列的各段子序列的序列值进行并行运算；

10 依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值，得到伪随机序列。

 上述方案中，所述计算第二序列的N段子序列中每段子序列的序列值，其中至少对第二序列的各段子序列的序列值进行并行运算，包括：

 确定第二序列的初值序列的序列值；

15 依据所述初值序列的序列值，得到第二序列中各段子序列的前L个值，L为正整数；

 依据各段子序列的前L个值，得到各段子序列中除前L个值之外的其它值；

20 将各段子序列的前L个值和对应段子序列中除前L个值之外的其它值进行集合，得到第二序列中各段子序列的序列值。

 上述方案中，在确定第二序列的初值序列的序列值之前，所述方法还包括：

 确定第二序列的初值序列；

 确定第二序列中各段子序列的前L位与所述初值序列的关系式；

25 相应的，所述依据所述初值序列的序列值，得到第二序列中各段子序

列的前 L 个值, 包括:

根据各段子序列的前 L 位与所述初值序列的关系式和所述初值序列的序列值, 计算第二序列中各段子序列的前 L 个值。

上述方案中, 所述依据各段子序列的前 L 个值, 得到各段子序列中除
5 前 L 个值之外的其它值, 包括:

针对各段子序列中任意一段子序列的前 L 个值;

将该段子序列的前 L 个值进行 M 次移位, 得到 M 个第一移位序列, M 为正整数;

将该段子序列的所述 M 个第一移位序列的前 L 个值进行 M 位的异或运
10 算, 得到第一目标序列;

将第一目标序列进行分割, 得到第一目标序列的第一部分子序列和第二部分子序列, 第一目标序列的第二部分子序列的长度长于第一目标序列的第一部分子序列的长度;

依据第一目标序列的第一部分子序列和第二部分子序列, 得到该段子
15 序列中除前 L 个值之外的其它值。

上述方案中, 所述依据第一目标序列的第一部分子序列和第二部分子序列, 得到该段子序列中除前 L 个值之外的其它值, 包括:

将第一目标序列的第二部分子序列进行 M 次移位, 得到 M 个第二移位序列;

20 将第一目标序列的第一部分子序列与所述 M 个第二移位序列进行最多 $M+1$ 位的异或运算, 得到第二目标序列;

将第二目标序列进行分割, 得到第二目标序列的第一部分子序列和第二部分子序列, 第二目标序列的第二部分子序列的长度大于第二目标序列的第一部分子序列的长度;

25 将第二目标序列的第二部分子序列进行 M 次移位, 得到 M 个第三移位

序列；

将第二目标序列的第一部分子序列与所述 M 个第三移位序列进行最多 M+1 位的异或运算，得到第三目标序列；

以此类推，直至计算出最后一个目标序列；

- 5 确定第一目标序列的第二部分子序列至倒数第二个目标序列的第二部分子序列以及最后一个目标序列的集合为该段子序列中除前 L 个值之外的其它值。

本发明实施例还提供一种获取伪随机序列的装置，所述装置包括：

- 第一划分单元，配置为对第一序列、第二序列分别进行 N 段的划分，
10 得到第一序列的 N 段子序列、第二序列的 N 段子序列，N 为正整数；

 第一计算单元，配置为计算第一序列的 N 段子序列中每段子序列的序列值；

 第二计算单元，配置为计算第二序列的 N 段子序列中每段子序列的序列值，其中至少对第二序列的各段子序列的序列值进行并行运算；

- 15 第一获取单元，配置为依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值，得到伪随机序列。

 上述方案中，所述第二计算单元，配置为：

 确定第二序列的初值序列的序列值；

- 依据所述初值序列的序列值，得到第二序列中各段子序列的前 L 个值，
20 L 为正整数；

 依据各段子序列的前 L 个值，得到各段子序列中除前 L 个值之外的其它值；

 将各段子序列的前 L 个值和对应段子序列中除前 L 个值之外的其它值进行集合，得到第二序列中各段子序列的序列值。

- 25 上述方案中，所述第二计算单元，配置为：

确定第二序列的初值序列;

确定第二序列中各段子序列的前 L 位与所述初值序列的关系式;

根据各段子序列的前 L 位与所述初值序列的关系式和所述初值序列的序列值, 计算第二序列中各段子序列的前 L 个值。

5 上述方案中, 所述第二计算单元, 还配置为:

针对各段子序列中任意一段子序列的前 L 个值;

将该段子序列的前 L 个值进行 M 次移位, 得到 M 个第一移位序列;

将该段子序列的前 L 个值及所述 M 个第一移位序列进行 M 位的异或运算, 得到第一目标序列, M 为正整数;

10 将第一目标序列进行分割, 得到第一目标序列的第一部分子序列和第二部分子序列, 第一目标序列的第二部分子序列的长度长于第一目标序列的第一部分子序列的长度;

依据第一目标序列的第一部分子序列和第二部分子序列, 得到该段子序列中除前 L 个值之外的其它值。

15 上述方案中, 所述第二计算单元, 还配置为:

将第一目标序列的第二部分子序列进行 M 次移位, 得到 M 个第二移位序列;

将第一目标序列的第一部分子序列与所述 M 个第二移位序列进行最多 $M+1$ 位的异或运算, 得到第二目标序列;

20 将第二目标序列进行分割, 得到第二目标序列的第一部分子序列和第二部分子序列, 第二目标序列的第二部分子序列的长度大于第二目标序列的第一部分子序列的长度;

将第二目标序列的第二部分子序列进行 M 次移位, 得到 M 个第三移位序列;

25 将第二目标序列的第一部分子序列与所述 M 个第三移位序列进行最多

M+1 位的异或运算，得到第三目标序列；

以此类推，直至计算出最后一个目标序列；

确定第一目标序列的第二分子序列至倒数第二个目标序列的第二分子序列以及最后一个目标序列的集合为该段子序列中除前 L 个值之外的
5 其它值。

本发明实施例还提供一种获取伪随机序列的装置，包括：处理器和配置为存储能够在处理器上运行的计算机程序的存储器，其中，所述处理器配置为运行所述计算机程序时，执行以上所述方法的步骤。

本发明实施例还提供一种计算机可读存储介质，其上存储有计算机程序，其中，该计算机程序被处理器执行时实现以上所述方法的步骤。
10

本发明实施例提供的获取伪随机序列的方法和装置、存储介质，所述方法包括：对第一序列、第二序列分别进行 N 段的划分，得到第一序列的 N 段子序列、第二序列的 N 段子序列，再计算第一序列、第二序列的 N 段子序列中每段子序列的序列值，依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值，得到伪随机序列。本实施例在对第二序列进行 N 段子序列的划分后，对各段子序列的序列值进行并行运算。与相关技术相比，可实现伪随机序列的快速计算，可有效减少计算量和节约存储空间。
15

附图说明

20 图 1 为本发明提供的获取伪随机序列的第一实施例的实现流程示意图；
图 2 为本发明提供的获取伪随机序列的第二实施例的实现流程示意图；
图 3 为本发明提供的获取伪随机序列的第三实施例的实现流程示意图；
图 4 为本发明提供的获取第二序列的第 N_p 段子序列的序列值的示意图；
图；

25 图 5 为本发明提供的获取伪随机序列的装置的组成结构示意图。

具体实施方式

以下结合附图对本发明的优选实施例进行详细说明，应当理解，以下所说明的优选实施例仅用于说明和解释本发明，并不用于限定本发明。

本发明提供的获取伪随机序列的第一实施例，应用于通信系统中如码分多址系统、时分多址系统、频分多址系统及 LTE 系统中，优选为 LTE 系统。第三代合作伙伴计划 3GPP LTE 规范规定可采用一种 31-bit 戈尔德 (Gold) 序列经公式 (1) ~ (3) 的运算产生伪随机序列 $c(n)$ 。

$$c(n) = (x_1(n + N_c) + x_2(n + N_c) \bmod 2) \quad (1)$$

$$x_1(n + 31) = (x_1(n + 3) + x_1(n)) \bmod 2 \quad (2)$$

$$x_2(n + 31) = (x_2(n + 3) + x_2(n + 2) + x_2(n + 1) + x_2(n)) \bmod 2 \quad (3)$$

其中， $x_1(n)$ 、 $x_2(n)$ 为 Gold 序列； N_c 为预先设置的数值，可以根据实际情况而取值，如取值为 1600； $n = 0, 1, \dots, M_{PN} - 1$ ， M_{PN} 为伪随机序列 $c(n)$ 的长度。

图 1 为本发明提供的获取伪随机序列第一实施例的流程示意图；如图 1 所示，所述方法包括：

步骤 101：对第一序列、第二序列分别进行 N 段的划分，得到第一序列的 N 段子序列、第二序列的 N 段子序列，N 为正整数；

这里，执行步骤 101 的通信实体可以为终端和/或基站。所述终端包括但不限于传统手机、智能手机、掌上电脑 PAD、智能手表、智能手环等。

当伪随机序列 $c(n)$ 的长度是 M_{PN} 时， $x_1(n)$ 、 $x_2(n)$ 的序列长度均为 $M_{PN} + N_c$ 。

在公式 (1) 中，当 $n=0$ 时， $c(n) = c(0) = (x_1(0 + N_c) + x_2(0 + N_c) \bmod 2)$ 即伪随机序列 $c(n)$ 的第一个值 $c(0)$ 与 $x_1(N_c)$ 、 $x_2(N_c)$ 有关，伪随机序列 $c(n)$ 的第二个值 $c(1)$ 与 $x_1(1 + N_c)$ 、 $x_2(1 + N_c)$ 有关，由此可见，伪随机序列 $c(0)$ 、 $c(1) \dots c(M_{PN} - 1)$ 与

$x_1(0) \dots x_1(N_c-1)$ 和 $x_2(0) \dots x_2(N_c-1)$ 无关。基于此, 第一序列是 $x_1(N_c)$ 、 $x_1(1+N_c) \dots x_1(M_{PN}+N_c)$; 第二序列是 $x_2(N_c)$ 、 $x_2(1+N_c) \dots x_2(M_{PN}-1+N_c)$ 。对第一序列 $x_1(N_c)$ 、 $x_1(1+N_c) \dots x_1(M_{PN}-1+N_c)$, 第二序列是 $x_2(N_c)$ 、 $x_2(1+N_c) \dots x_2(M_{PN}-1+N_c)$ 进行 N 段的划分, 得到第一序列的第 1 段子序列~
 5 第 N 段子序列、第二序列的第 1 段子序列~第 N 段子序列, N 为正整数, 优选为 $N=2^x$, x 为自然数。在第一序列的各段子序列中具有的 bit 位相同, 在第二序列的各段子序列中具有的 bit 位相同。举个例子, 假定要获取的伪随机序列 $c(n)$ 的长度是 $M_{PN}=16000$, 那么第一序列和第二序列的长度也应该是 16000, 如果取 $N=16$ 段, 那么第一序列、第二序列中的每段子序列均具
 10 有 $c(n)/16=16000/16=1000$ 位。当 $N_c=1600$ 时, 第一序列的第 1 段子序列是 $x_1(1600)$ 、 $x_1(1601) \dots x_1(2599)$, 第 2 段子序列是 $x_1(2600)$ 、 $x_1(2601) \dots x_1(3599) \dots$ 以此类推。第二序列的第 1 段子序列是 $x_2(1600)$ 、 $x_2(1601) \dots x_2(2599)$, 第 2 段子序列是 $x_2(2600)$ 、 $x_2(2601) \dots x_2(3599) \dots$ 以此类推。

步骤 102: 计算第一序列的 N 段子序列中每段子序列的序列值;

15 这里, 执行步骤 102 的通信实体可以为终端和/或基站。将第一序列 $x_1(N_c)$ 、 $x_1(1+N_c) \dots x_1(M_{PN}+N_c)$ 按段进行划分后, 计算每段子序列的序列值。在 LTE 系统中, 第一序列的初值序列是 $x_1(0) \dots x_1(30)$, 该初值序列的序列值 (即 $x_1(0)$ 的取值至 $x_1(30)$ 的取值) 是固定好的, 那么根据公式 (2) 第一序列中的各段子序列的序列值是可以计算出来的。根据公式 (2), 可以将第一
 20 序列中各个位的值进行依次计算 (串行运算), 也可以根据公式 (2) 及对第一序列的各段子序列的划分结果对各段子序列的序列值进行同时运算 (并行运算)。并行运算的好处在于节省计算时间。

步骤 103: 计算第二序列的 N 段子序列中每段子序列的序列值, 其中至少对第二序列的各段子序列的序列值进行并行运算;

这里, 执行步骤 103 的通信实体可以为终端和/或基站。在 LTE 系统中, 第二序列的初值序列 $x_2(0) \dots x_2(30)$ 通常是不固定的, 根据使用场景的不同而不同, 如此在对第二序列 $x_2(N_C)$ 、 $x_2(1+N_C) \dots x_2(M_{PN}-1+N_C)$ 进行 N 段子序列的划分后, 对各段子序列的序列值进行同时运算 (并行运算), 具体运算过程参见后续说明此处暂不详细描述。与相关计算技术中的串行迭代公式法相比, 并行运算的好处在于节省计算时间, 加速对伪随机序列 $c(n)$ 的运算。

需要说明的是, 由于第一序列和第二序列是两个独立的序列, 所以可以同时计算各自的子序列的序列值, 即步骤 102 和步骤 103 可以同时进行。

步骤 104: 依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值, 得到伪随机序列。

这里, 执行步骤 104 的通信实体可以为终端和/或基站。将第一序列中各段子序列的序列值和第二序列中对应子序列的序列值代入至公式 (1) 中, 得到伪随机序列的取值。以 $M_{PN}=16000$ 、 $N=16$ 段、 $N_C=1600$ 为例, 伪随机序列的第一个值 $c(0)=(x_1(1600)+x_2(1600)\bmod 2)$; 第二个值 $c(1)=(x_1(1601)+x_2(1601)\bmod 2) \dots$ 以此类推得到伪随机序列 $c(0)$ 、 $c(1) \dots c(M_{PN}-1)$ 的取值。

本发明实施例中, 对第一序列、第二序列分别进行 N 段的划分, 得到第一序列的 N 段子序列、第二序列的 N 段子序列, 再计算第一序列、第二序列的 N 段子序列中每段子序列的序列值, 依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值, 得到伪随机序列。其中, 考虑到在 LTE 系统中第二序列的初值序列通常为不固定, 本实施例在对第二序列 $x_2(N_C)$ 、 $x_2(1+N_C) \dots x_2(M_{PN}-1+N_C)$ 进行 N 段子序列的划分后, 对各段子序列的序列值进行并行运算。与相关技术相比, 对第二序列的各段子序列的序列值进行并行运算可实现伪随机序列的快速计算, 可有效减少计算量和节约存储空间。

本发明提供的获取伪随机序列的第二实施例，在前述第一实施例的基础上，如图 2 所示，步骤 102 进一步包括：

步骤 1021：确定第二序列的初值序列的序列值；

5 这里，执行步骤 1021 的通信实体可以为终端和/或基站。第二序列 $x_2(N_C)$ 、 $x_2(1+N_C) \dots x_2(M_{PN}-1+N_C)$ 的初值序列是 $x_2(0) \dots x_2(30)$ ，初值序列的这 31 个数值（初值序列的序列值）是可以通过对初值序列的初始化得到。

步骤 1022：依据所述初值序列的序列值，得到第二序列中各段子序列的前 L 个值，L 为正整数；

10 这里，执行步骤 1022 的通信实体可以为终端和/或基站。考虑到在 LTE 系统中采用 31-bit Gold 序列进行伪随机序列 $c(n)$ 的生成，此处 L 可取值为 31。当然，L 还可以取为其它值，根据实际使用情况而灵活取值。

步骤 1023：依据各段子序列的前 L 个值，得到各段子序列中除前 L 个值之外的其它值；

15 这里，执行步骤 1023 的通信实体可以为终端和/或基站。通过前面对第二序列的 N 段划分，各段子序列中具有相同数量的位值，本步骤中可通过各段子序列的前 L 个值，可得到各段子序列中除了前 L 个值之外的其它值。举个例子，针对第二序列的某段子序列，如果其具有 1000 位，可通过该段子序列的前 L 个值计算出该段子序列中剩余的 $(1000-L)$ 位值。

20 步骤 1024：将各段子序列的前 L 个值和对应段子序列中除前 L 个值之外的其它值进行集合，得到第二序列中各段子序列的序列值。

这里，执行步骤 1024 的通信实体可以为终端和/或基站。第二序列中某段子序列的序列值就是该段子序列的前 L 个值和剩余值的集合。

25 这里，因为已经将第二序列划分为 N 段子序列，本发明实施例中，不需要依次计算各段子序列的前 L 个值和对应段子序列的剩余值，需要对第 1

段子序列至第 N 段子序列的前 L 个值和对应段子序列的剩余值进行同时计算（并行计算），可缩短伪随机序列的计算时间。

在一个优选的实施例中，在确定第二序列的初值序列的序列值之前，所述方法还包括：

5 确定第二序列的初值序列；确定第二序列中各段子序列的前 L 位与所述初值序列的关系式；相应的，所述依据所述初值序列的序列值，得到第二序列中各段子序列的前 L 个值，包括：根据各段子序列的前 L 位与所述初值序列的关系式和所述初值序列的序列值，计算第二序列中各段子序列的前 L 个值。

10 考虑到在 LTE 系统中采用 31-bit Gold 序列进行伪随机序列 $c(n)$ 的生成，所以第二序列的初值序列是 $x_2(0) \dots x_2(30)$ 。确定第二序列中各段子序列的前 L 位与所述初值序列的关系式就是各段子序列的前 L 位用初值序列中的部分或全部元素来表达，得到各段子序列的前 L 位与第二序列的初值序列的关系（表达）式；再将初值序列的序列值代入至所得到的关系式，得到各
15 段子序列的前 L 个值。前述的关系式可通过预先设置而实现。

下面，举个例子，假定 $L=31$ 、 $N_c=31$ 为例，第二序列的初值序列是 $x_2(0) \dots x_2(30)$ ，第 1 段子序列中的前 31 位中的前 6 位用初值序列的部分元素来表达的关系式是：

$$\begin{aligned} x_2(31) &= (x_2(0) + x_2(1) + x_2(2) + x_2(3)) \bmod 2; \\ 20 \quad x_2(32) &= (x_2(1) + x_2(2) + x_2(3) + x_2(4)) \bmod 2; \\ x_2(33) &= (x_2(2) + x_2(3) + x_2(4) + x_2(5)) \bmod 2; \\ x_2(34) &= (x_2(3) + x_2(4) + x_2(5) + x_2(6)) \bmod 2; \\ x_2(35) &= (x_2(7) + x_2(4) + x_2(5) + x_2(6)) \bmod 2; \end{aligned}$$

将初值序列的序列值代入至上述的关系式，就可以得到第 1 段子序列
25 中的前 6 个值 $x_2(31) \sim x_2(35)$ 。

上述的关系式仅为具体举例而已，并不限于本发明实施例的所有表

现形式。当第二序列的初值序列确定后，只要找出第二序列中的各子序列的前 L 位与初值序列的部分或全部元素之间的关系，并用初值序列中的部分或全部元素对各段子序列的前 L 位进行关系式表达即可。

本发明实施例中，对第一序列、第二序列分别进行 N 段的划分，得到
5 第一序列的 N 段子序列、第二序列的 N 段子序列，再计算第一序列的 N 段子序列中每段子序列的序列值；确定第二序列的初值序列的序列值，依据所述初值序列的序列值，得到第二序列中各段子序列的前 L 个值，依据各段子序列的前 L 个值，得到各段子序列中除前 L 个值之外的其它值，将各段子序列的前 L 个值和对应段子序列中除前 L 个值之外的其它值进行集合，
10 得到第二序列中各段子序列的序列值，依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值，得到伪随机序列。其中，考虑到在 LTE 系统中第二序列的初值序列通常为不固定，本实施例在对第二序列 $x_2(N_C)$ 、 $x_2(1+N_C)$... $x_2(M_{PN}-1+N_C)$ 进行 N 段子序列的划分后，依据初值序列的序列值，同时得到第二序列中各段子序列的前 L 个值，并依据各段子序列的前 L 个值，同时得到各段子序列中除前 L 个值之外的其它值，即对各段子序列的序列值进行并行运算。与相关技术相比，对第二序列的各段子序列的序列值进行并行运算可实现伪随机序列的快速计算，可有效减少计算量和节约存储空间。

20 本发明提供的获取伪随机序列的第三实施例，在前述第二实施例的基础上，如图 3 所示，所述依据各段子序列的前 L 个值，得到各段子序列中除前 L 个值之外的其它值（步骤 1023），包括：

步骤 1023A：针对各段子序列中任意一段子序列的前 L 个值，将该段子序列的前 L 个值进行 M 次移位，得到 M 个第一移位序列；

25 这里，执行步骤 1024A~1023D 的通信实体可以为终端和/或基站。因为

对第二序列进行了 N 段子序列的划分，各个子序列之间是相互独立的，可以同时对各段子序列进行自身序列值的计算，在计算完成后再将每段子序列的序列值按照段号进行依次集合即可得到第二序列的序列值。第二序列与第一序列按照前述公式 (1) 进行序列值的代入即可得到伪随机序列 $c(n)$ 。

5 由于第二序列的各段子序列的序列值是同时运算且运算方法相同，所以步骤 1023A~步骤 1023D 中描述的方法是针对第二序列的任意段子序列的序列值的计算方法。

在前述方案中，可以根据第二序列的初值公式与各段子序列的前 L 位的关系式，得到各段子序列的前 L 个值。在硬件实现上，对每段子序列的前 L 个值进行 M 次移位如 M 次左移或 M 次右移，每次可移动相同的位数如每次移动一位，当然也可以每次移动二位或三位，此处不做限定。每次移动得到一个第一移位序列。

步骤 1023B：将该段子序列的前 L 个值及所述 M 个第一移位序列进行 M 位的异或运算，得到第一目标序列， M 为正整数；

15 这里，针对 N 段子序列中的其中一段子序列，将该子序列中的前 L 个值及前 L 值经过 M 次移位而得到的 M 个第一移位序列进行 M 位的异或运算。通常选取 M 的位数大于 L 的位数，如 $L=31\text{bit}$ 时， M 可取 32bit ，当然 M 还可以取其它值。

步骤 1023C：将第一目标序列进行分割，得到第一目标序列的第一部分分子序列和第二部分分子序列，第一目标序列的第二部分分子序列的长度长于第一目标序列的第一部分分子序列的长度；

这里，对第一目标序列进行两部分的分割得到两部分分子序列即第一部分分子序列和第二部分分子序列，这两部分分子序列的 bit 长度需不同，通常分割的第二部分分子序列的长度大于第一部分分子序列的长度。

25 步骤 1023D：依据第一目标序列的第一部分分子序列和第二部分分子序列，

得到该段子序列中除前 L 个值之外的其它值。

这里，通过对第一目标序列分割而得到的两分子序列得到该段子序列中的除了 L 个值之外的其他值。

其中，所述依据第一目标序列的第一分子序列和第二分子序列，

5 得到该段子序列中除前 L 个值之外的其它值（步骤 1023D），进一步为：

将第一目标序列的第二分子序列进行 M 次移位，得到 M 个第二移位序列；将第一目标序列的第一分子序列与所述 M 个第二移位序列进行最多 M+1 位的异或运算，得到第二目标序列；将第二目标序列进行分割，得到第二目标序列的第一分子序列和第二分子序列，第二目标序列的第二分子序列的长度大于第二目标序列的第一分子序列的长度；将第二
10 目标序列的第二分子序列进行 M 次移位，得到 M 个第三移位序列；将第二目标序列的第一分子序列与所述 M 个第三移位序列进行最多 M+1 位的异或运算，得到第三目标序列；以此类推，直至计算出最后一个目标序列；确定第一目标序列的第二分子序列至倒数第二个目标序列的第二分子
15 序列以及最后一个目标序列的集合为该段子序列中除前 L 个值之外的其它值。

此处，在硬件实现上，第一目标序列的第二分子序列、第二目标序列的第二分子序列移位以及其它目标序列（第三目标序列、第四目标序列...最后一个目标序列）的第二分子序列的移位的次数需相同，每次移
20 动的方向及位数也需相同，优选为与对应段子序列的前 L 个值的移位次数与位数保持一致但移动方向相反。

在本发明实施例中，对第二序列中的各段子序列的序列值进行并行运算，具体的先通过各段子序列的前 L 位与第二序列的初值序列之间的关系式得到各段子序列的前 L 个值，针对各段子序列中任意一段子序列的前 L
25 个值，将该段子序列的前 L 个值进行 M 次移位，得到 M 个第一移位序列，

将第一目标序列进行分割，得到第一目标序列的第一部分子序列和第二部分子序列，第一目标序列的第二部分子序列的长度长于第一目标序列的第一部分子序列的长度，依据第一目标序列的第一部分子序列和第二部分子序列，得到该段子序列中除前 L 个值之外的其它值。在硬件上某段子序列中的某个值占用的比特位较少，优选为占用 1bit，与相关技术中基于状态转移矩阵乘法的伪随机序列的产生方法相比，可有效节省存储空间，且移位运算较矩阵乘法运算更为简单，有易于物理实现。另外，同时对各段子序列的序列值进行运算可实现伪随机序列的快速计算，节省计算时间。

下面结合图 4 对本发明实施例做进一步的说明，以加深对本实施例的理解。

在图 4 中假定 $L=31$ ，是第二序列的 N 段子序列中其中一段子序列如第 N_p ($N_p=1, 2 \dots N$) 段子序列的序列值的计算过程。同时， $M=32$ ，采用 32bit (图 4 中的每一行均具有 32 个小格) 的运算单元进行异或运算。

在第 N_p 段子序列中，根据第二序列的初值公式 $x_2(0) \dots x_2(30)$ 与第 N_p 段子序列的前 $L=31$ 位的关系式，得到第 N_p 段子序列的前 $L=31$ 个值，如图 4 中的第 1 行所示的数值 0~数值 30 所占用的小格。将第 N_p 段子序列的前 $L=31$ 个值进行一次右移，右移一位，得到第一个第一移位序列如图 4 中的第 2 行所示的数值 1~30 所占的小格。然后，将第一个第一移位序列再进行一次右移且右移一位，得到第二个第一移位序列如图 4 中的第 3 行所示的数值 2~30 所占的小格。再将第二个第一移位序列进行一次右移且右移一位，得到第三个第一移位序列如图 4 中的第 4 行所示的数值 3~30 所占的小格。将所述前 $L=31$ 个值、第一个~第三个第一移位序列进行 32 位的异或运算，得到第一目标序列，如图 4 中的第 5 行所示的数值 31~58 及 $H0 \sim H3$ 所占的小格。

将第一目标序列进行两部分的分割得到第一部分子序列（如图 4 中第 5 行所示的 H0~H3 所占的小格）和第二部分子序列（如图 4 中第 5 行所示的数值 31~58 所占的小格），将第一目标序列的第二部分子序列保留下来作为图 4 中第 6 行的数据。将所保留下来的第二部分子序列进行一次左移且左移一位，得到第一个第二移位序列如图 4 中第 7 行数值 31~58 所占的小格，再将第一个第二移位序列进行一次左移且左移一位，得到第二个第二移位序列如图 4 中第 8 行数值 31~58 所占的小格，再将第二个第二移位序列进行一次左移且左移一位，得到第三个第二移位序列如图 4 中第 9 行数值 31~58 所占的小格，将第一目标序列的第一部分子序列即第 5 行所示的 H0~H3 所占的小格保留下来并作为 32 位异或运算的低四位。接下来，将第一目标序列的第二部分子序列、第一个~第三个第二移位序列及第一目标序列的第一部分子序列进行 32 位的异或运算，得到第二目标序列如图 4 中的第 11 行数值 59~86 以及 H0~H3 所占的小格）。

将第二目标序列进行两部分的分割得到第一部分子序列（如图 4 中第 11 行所示的 H0~H3 所占的小格）和第二部分子序列（如图 4 中第 11 行所示的数值 59~86 所占的小格），将第二目标序列的第二部分子序列保留下来作为图 4 中第 12 行的数据。将所保留下来的第二部分子序列进行一次左移且左移一位，得到第一个第二移位序列如图 4 中第 13 行数值 59~86 所占的小格，再将第一个第二移位序列进行一次左移且左移一位，得到第二个第二移位序列如图 4 中第 14 行数值 59~86 所占的小格，再将第二个第二移位序列进行一次左移且左移一位，得到第三个第二移位序列如图 4 中第 15 行数值 59~86 所占的小格，将第二目标序列的第一部分子序列即第 16 行所示的 H0~H3 所占的小格保留下来并作为 32 位异或运算的低四位。接下来，将第二目标序列的第二部分子序列、第一个~第三个第三移位序列及第二目标序列的第一部分子序列进行 32 位的异或运算，得到第三目标序列如图 4

中的第 17 行数值 87~114 以及 H0~H3 所占的小格)。

以此类推,直至计算出第 N_p 段子序列中的最后一个目标序列。第一目标序列的第二分子序列至倒数第二个目标序列的第二分子序列以及最后一个目标序列的集合为第 N_p 段子序列中除前 L 个值之外的其它值。

- 5 需要说明的是第一目标序列、第二目标序列、第三目标序列及其他目标序列的一部分子序列之所以占用 4 个小格,是因为前述公式 (3) 中 $x_2(n+31)$ 与 $x_2(n+3), x_2(n+2), x_2(n+1), x_2(n)$ 这 4 个值有关。

这里,因为第一序列 $x_1(N_C)$ 、 $x_1(1+N_C)$... $x_1(M_{PN}+N_C)$ 的初值序列 $x_1(0)$... $x_1(30)$ 是已知的,根据前述公式 (2) 可得出第一序列的 N 段子序列
10 中的各个元素的值即第一序列的 N 段子序列的序列值是已知的。考虑到第二序列中的 N 段子序列的序列值是并行运算的,当第二序列中的 N 段子序列中的第 N_p 段子序列的序列值计算出时立即读取第一序列的第 N_p 段子序列的序列值,并根据前述公式 (1) 得出伪随机序列的部分序列值。

在上述实施例中,采用 32bit 的运算单元进行异或运算即图 4 中的一个
15 小格仅占用 1 个比特位,与相关技术中基于状态转移矩阵乘法的伪随机序列的产生方法相比,可有效节省存储空间,且移位运算较矩阵乘法运算更为简单,有易于物理实现。另外,同时对各段子序列的序列值进行运算可实现伪随机序列的快速计算,节省计算时间。

- 20 本发明提供的获取伪随机序列的装置,应用于通信系统中如码分多址系统、时分多址系统、频分多址系统及 LTE 系统中,优选为 LTE 系统。如图 5 所示,

所述装置包括:第一划分单元 501、第一计算单元 502、第二计算单元 503、第一获取单元 504; 其中,

- 25 第一划分单元 501,配置为对第一序列、第二序列分别进行 N 段的划

分, 得到第一序列的 N 段子序列、第二序列的 N 段子序列, N 为正整数;

第一计算单元 502, 配置为计算第一序列的 N 段子序列中每段子序列的序列值;

第二计算单元 503, 配置为计算第二序列的 N 段子序列中每段子序列的序列值, 其中至少对第二序列的各段子序列的序列值进行并行运算;

第一获取单元 504, 配置为依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值, 得到伪随机序列。

其中, 所述第二计算单元 502, 进一步配置为:

确定第二序列的初值序列的序列值;

依据所述初值序列的序列值, 得到第二序列中各段子序列的前 L 个值, L 为正整数;

依据各段子序列的前 L 个值, 得到各段子序列中除前 L 个值之外的其它值;

将各段子序列的前 L 个值和对应段子序列中除前 L 个值之外的其它值进行集合, 得到第二序列中各段子序列的序列值。

所述第二计算单元 502, 配置为: 在确定第二序列的初值序列的序列值之前, 确定第二序列的初值序列;

确定第二序列中各段子序列的前 L 位与所述初值序列的关系式;

根据各段子序列的前 L 位与所述初值序列的关系式和所述初值序列的序列值, 计算第二序列中各段子序列的前 L 个值。

上述方案中, 所述第二计算单元 502, 还配置为:

针对各段子序列中任意一段子序列的前 L 个值,

将该段子序列的前 L 个值进行 M 次移位, 得到 M 个第一移位序列;

将该段子序列的前 L 个值及所述 M 个第一移位序列进行 M 位的异或运算, 得到第一目标序列, M 为正整数;

将第一目标序列进行分割，得到第一目标序列的第一部分子序列和第二部分子序列，第一目标序列的第二部分子序列的长度长于第一目标序列的第一部分子序列的长度；

依据第一目标序列的第一部分子序列和第二部分子序列，得到该段子
5 序列中除前 L 个值之外的其它值。

所述第二计算单元 502，还配置为：

将第一目标序列的第二部分子序列进行 M 次移位，得到 M 个第二移位
序列；

将第一目标序列的第一部分子序列与所述 M 个第二移位序列进行最多
10 $M+1$ 位的异或运算，得到第二目标序列；

将第二目标序列进行分割，得到第二目标序列的第一部分子序列和第二部分子序列，第二目标序列的第二部分子序列的长度大于第二目标序列的第一部分子序列的长度；

将第二目标序列的第二部分子序列进行 M 次移位，得到 M 个第三移位
15 序列；

将第二目标序列的第一部分子序列与所述 M 个第三移位序列进行最多
 $M+1$ 位的异或运算，得到第三目标序列；

以此类推，直至计算出最后一个目标序列；

确定第一目标序列的第二部分子序列至倒数第二个目标序列的第二部
20 分子序列以及最后一个目标序列的集合为该段子序列中除前 L 个值之外的
其它值。

本发明实施例中，对第一序列、第二序列分别进行 N 段的划分，得到
第一序列的 N 段子序列、第二序列的 N 段子序列，再计算第一序列、第二
序列的 N 段子序列中每段子序列的序列值，依据第一序列中每段子序列的
25 序列值和第二序列中每段子序列的序列值，得到伪随机序列。其中，考虑

到在 LTE 系统中第二序列的初值序列通常为不固定，本实施例在对第二序列 $x_2(N_C)$ 、 $x_2(1+N_C) \dots x_2(M_{PN}-1+N_C)$ 进行 N 段子序列的划分后，对各段子序列的序列值进行并行运算。与相关技术相比，对第二序列的各段子序列的序列值进行并行运算可实现伪随机序列的快速计算，可有效减少计算量和节约存储空间。

需要说明的是，本发明实施例的获取伪随机序列的装置，由于该装置解决问题的原理与前述的获取伪随机序列的方法相似，因此，装置的实施过程及实施原理均可以参见前述获取伪随机序列的方法的实施过程及实施原理描述，重复之处不再赘述。

在实际应用中，所述第一划分单元 501、第一计算单元 502、第二计算单元 503 及第一获取单元 504 均可由中央处理单元 (CPU, Central Processing Unit)、或数字信号处理 (DSP, Digital Signal Processor)、或微处理器 (MPU, Micro Processor Unit)、或现场可编程门阵列 (FPGA, Field Programmable Gate Array) 等来实现。

本发明还提供了一种获取伪随机序列的装置，包括：处理器和配置为存储能够在处理器上运行的计算机程序的存储器，其中，所述处理器配置为运行所述计算机程序时，执行以下步骤：

对第一序列、第二序列分别进行 N 段的划分，得到第一序列的 N 段子序列、第二序列的 N 段子序列，N 为正整数；

计算第一序列的 N 段子序列中每段子序列的序列值；

计算第二序列的 N 段子序列中每段子序列的序列值，其中至少对第二序列的各段子序列的序列值进行并行运算；

依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值，得到伪随机序列。

在一具体实施例中，还执行：

确定第二序列的初值序列的序列值;

依据所述初值序列的序列值,得到第二序列中各段子序列的前 L 个值,
 L 为正整数;

依据各段子序列的前 L 个值,得到各段子序列中除前 L 个值之外的其
5 它值;

将各段子序列的前 L 个值和对应段子序列中除前 L 个值之外的其它值
进行集合,得到第二序列中各段子序列的序列值。

在一具体实施例中,还执行:

确定第二序列的初值序列;

10 确定第二序列中各段子序列的前 L 位与所述初值序列的关系式;

相应的,所述依据所述初值序列的序列值,得到第二序列中各段子序
列的前 L 个值,包括:

根据各段子序列的前 L 位与所述初值序列的关系式和所述初值序列的
序列值,计算第二序列中各段子序列的前 L 个值。

15 在一具体实施例中,还执行:

针对各段子序列中任意一段子序列的前 L 个值,

将该段子序列的前 L 个值进行 M 次移位,得到 M 个第一移位序列;

将该段子序列的前 L 个值及所述 M 个第一移位序列进行 M 位的异或运
算,得到第一目标序列, M 为正整数;

20 将第一目标序列进行分割,得到第一目标序列的第一分子序列和第
二分子序列,第一目标序列的第二分子序列的长度长于第一目标序列
的第一分子序列的长度;

依据第一目标序列的第一分子序列和第二分子序列,得到该段子
序列中除前 L 个值之外的其它值。

25 在一具体实施例中,还执行:

将第一目标序列的第二分子子序列进行 M 次移位, 得到 M 个第二移位序列;

将第一目标序列的第一分子子序列与所述 M 个第二移位序列进行最多 $M+1$ 位的异或运算, 得到第二目标序列;

- 5 将第二目标序列进行分割, 得到第二目标序列的第一分子子序列和第二分子子序列, 第二目标序列的第二分子子序列的长度大于第二目标序列的第一分子子序列的长度;

将第二目标序列的第二分子子序列进行 M 次移位, 得到 M 个第三移位序列;

- 10 将第二目标序列的第一分子子序列与所述 M 个第三移位序列进行最多 $M+1$ 位的异或运算, 得到第三目标序列;

以此类推, 直至计算出最后一个目标序列;

- 15 确定第一目标序列的第二分子子序列至倒数第二个目标序列的第二分子子序列以及最后一个目标序列的集合为该段子序列中除前 L 个值之外的其它值。

- 这里, 所述处理器可能是一种集成电路芯片, 具有信号的处理能力。在实现过程中, 上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、DSP, 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。处理器可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本发明实施例所公开的方法的步骤, 可以直接体现为硬件译码处理器执行完成, 或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中, 该存储介质位于存储器, 处理器读取存储器中的信息, 结合其硬件
- 20 完成前述方法的步骤。
- 25

本发明的实施例还提供了一种计算机可读存储介质，例如包括计算机程序的存储器，上述计算机程序可由获取伪随机序列的装置的处理器的处理器执行，以完成前述方法所述步骤。计算机可读存储介质可以是磁性随机存取存储器（FRAM, ferromagnetic random access memory）、ROM、可编程只读存储器（PROM, Programmable Read-Only Memory）、可擦除可编程只读存储器（EPROM, Erasable Programmable Read-Only Memory）、电可擦除可编程只读存储器（EEPROM, Electrically Erasable Programmable Read-Only Memory）、快闪存储器（Flash Memory）、磁表面存储器、光盘、或只读光盘（CD-ROM, Compact Disc Read-Only Memory）等存储器；也可以是包括上述存储器之一或任意组合的各种设备。

进一步地，所述计算机可读存储介质上存储有计算机程序，其中，该计算机程序被处理器执行时实现以下步骤：

对第一序列、第二序列分别进行N段的划分，得到第一序列的N段子序列、第二序列的N段子序列，N为正整数；

15 计算第一序列的N段子序列中每段子序列的序列值；

计算第二序列的N段子序列中每段子序列的序列值，其中至少对第二序列的各段子序列的序列值进行并行运算；

依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值，得到伪随机序列。

20 在一具体实施例中，还执行：

确定第二序列的初值序列的序列值；

依据所述初值序列的序列值，得到第二序列中各段子序列的前L个值，L为正整数；

25 依据各段子序列的前L个值，得到各段子序列中除前L个值之外的其它值；

将各段子序列的前 L 个值和对应段子序列中除前 L 个值之外的其它值进行集合，得到第二序列中各段子序列的序列值。

在一具体实施例中，还执行：

确定第二序列的初值序列；

5 确定第二序列中各段子序列的前 L 位与所述初值序列的关系式；

相应的，所述依据所述初值序列的序列值，得到第二序列中各段子序列的前 L 个值，包括：

根据各段子序列的前 L 位与所述初值序列的关系式和所述初值序列的序列值，计算第二序列中各段子序列的前 L 个值。

10 在一具体实施例中，还执行：

针对各段子序列中任意一段子序列的前 L 个值，

将该段子序列的前 L 个值进行 M 次移位，得到 M 个第一移位序列；

将该段子序列的前 L 个值及所述 M 个第一移位序列进行 M 位的异或运算，得到第一目标序列， M 为正整数；

15 将第一目标序列进行分割，得到第一目标序列的第一部分子序列和第二部分子序列，第一目标序列的第二部分子序列的长度长于第一目标序列的第一部分子序列的长度；

依据第一目标序列的第一部分子序列和第二部分子序列，得到该段子序列中除前 L 个值之外的其它值。

20 在一具体实施例中，还执行：

将第一目标序列的第二部分子序列进行 M 次移位，得到 M 个第二移位序列；

将第一目标序列的第一部分子序列与所述 M 个第二移位序列进行最多 $M+1$ 位的异或运算，得到第二目标序列；

25 将第二目标序列进行分割，得到第二目标序列的第一部分子序列和第

二部分子序列，第二目标序列的第二部分子序列的长度大于第二目标序列的第一部分子序列的长度；

将第二目标序列的第二部分子序列进行 M 次移位，得到 M 个第三移位序列；

5 将第二目标序列的第一部分子序列与所述 M 个第三移位序列进行最多 $M+1$ 位的异或运算，得到第三目标序列；

以此类推，直至计算出最后一个目标序列；

确定第一目标序列的第二部分子序列至倒数第二个目标序列的第二部分子序列以及最后一个目标序列的集合为该段子序列中除前 L 个值之外的
10 其它值。

这里，本领域技术人员应当理解，本发明实施例所述的获取伪随机序列的装置中的各处理单元的实现功能可参照前述获取伪随机序列方法的相关描述而理解。本领域技术人员应当理解，图 5 所示的获取伪随机序列的装置中各处理单元的功能可通过运行于处理器上的程序而实现，也可通过
15 具体的逻辑电路而实现。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用硬件实施例、软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘
20 存储器和光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、
25 嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得

通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

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保护范围。

工业实用性

本发明实施例在对第二序列进行 N 段子序列的划分后，能够对各段子序列的序列值进行并行运算，所以，与相关技术相比，可实现伪随机序列的快速计算，可有效减少计算量和节约存储空间。

权利要求书

1、一种获取伪随机序列的方法，所述方法包括：

对第一序列、第二序列分别进行N段的划分，得到第一序列的N段子序列、第二序列的N段子序列，N为正整数；

5 计算第一序列的N段子序列中每段子序列的序列值；

计算第二序列的N段子序列中每段子序列的序列值，其中至少对第二序列的各段子序列的序列值进行并行运算；

依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值，得到伪随机序列。

10 2、根据权利要求1所述的方法，其中，所述计算第二序列的N段子序列中每段子序列的序列值，其中至少对第二序列的各段子序列的序列值进行并行运算，包括：

确定第二序列的初值序列的序列值；

依据所述初值序列的序列值，得到第二序列中各段子序列的前L个值，

15 L为正整数；

依据各段子序列的前L个值，得到各段子序列中除前L个值之外的其它值；

将各段子序列的前L个值和对应段子序列中除前L个值之外的其它值进行集合，得到第二序列中各段子序列的序列值。

20 3、根据权利要求2所述的方法，其中，在确定第二序列的初值序列的序列值之前，所述方法还包括：

确定第二序列的初值序列；

确定第二序列中各段子序列的前L位与所述初值序列的关系式；

相应的，所述依据所述初值序列的序列值，得到第二序列中各段子序

列的前 L 个值, 包括:

根据各段子序列的前 L 位与所述初值序列的关系式和所述初值序列的序列值, 计算第二序列中各段子序列的前 L 个值。

- 4、根据权利要求 2 或 3 所述的方法, 其中, 所述依据各段子序列的前 L 个值, 得到各段子序列中除前 L 个值之外的其它值, 包括:

针对各段子序列中任意一段子序列的前 L 个值;

将该段子序列的前 L 个值进行 M 次移位, 得到 M 个第一移位序列;

将该段子序列的前 L 个值及所述 M 个第一移位序列进行 M 位的异或运算, 得到第一目标序列, M 为正整数;

- 10 将第一目标序列进行分割, 得到第一目标序列的第一部分子序列和第二部分子序列, 第一目标序列的第二部分子序列的长度长于第一目标序列的第一部分子序列的长度;

依据第一目标序列的第一部分子序列和第二部分子序列, 得到该段子序列中除前 L 个值之外的其它值。

- 15 5、根据权利要求 4 所述的方法, 其中, 所述依据第一目标序列的第一部分子序列和第二部分子序列, 得到该段子序列中除前 L 个值之外的其它值, 包括:

将第一目标序列的第二部分子序列进行 M 次移位, 得到 M 个第二移位序列;

- 20 将第一目标序列的第一部分子序列与所述 M 个第二移位序列进行最多 M+1 位的异或运算, 得到第二目标序列;

将第二目标序列进行分割, 得到第二目标序列的第一部分子序列和第二部分子序列, 第二目标序列的第二部分子序列的长度大于第二目标序列的第一部分子序列的长度;

- 25 将第二目标序列的第二部分子序列进行 M 次移位, 得到 M 个第三移位

序列;

将第二目标序列的第一部分子序列与所述 M 个第三移位序列进行最多 M+1 位的异或运算, 得到第三目标序列;

以此类推, 直至计算出最后一个目标序列;

- 5 确定第一目标序列的第二部分子序列至倒数第二个目标序列的第二部分子序列以及最后一个目标序列的集合为该段子序列中除前 L 个值之外的其它值。

6、一种获取伪随机序列的装置, 所述装置包括:

- 第一划分单元, 配置为对第一序列、第二序列分别进行 N 段的划分,
10 得到第一序列的 N 段子序列、第二序列的 N 段子序列, N 为正整数;

 第一计算单元, 配置为计算第一序列的 N 段子序列中每段子序列的序列值;

 第二计算单元, 配置为计算第二序列的 N 段子序列中每段子序列的序列值, 其中至少对第二序列的各段子序列的序列值进行并行运算;

- 15 第一获取单元, 配置为依据第一序列中每段子序列的序列值和第二序列中每段子序列的序列值, 得到伪随机序列。

7、根据权利要求 6 所述的装置, 其中, 所述第二计算单元, 配置为:

 确定第二序列的初值序列的序列值;

- 依据所述初值序列的序列值, 得到第二序列中各段子序列的前 L 个值,
20 L 为正整数;

 依据各段子序列的前 L 个值, 得到各段子序列中除前 L 个值之外的其它值;

 将各段子序列的前 L 个值和对应段子序列中除前 L 个值之外的其它值进行集合, 得到第二序列中各段子序列的序列值。

- 25 8、根据权利要求 7 所述的装置, 其中, 所述第二计算单元, 配置为:

确定第二序列的初值序列;

确定第二序列中各段子序列的前 L 位与所述初值序列的关系式;

根据各段子序列的前 L 位与所述初值序列的关系式和所述初值序列的序列值, 计算第二序列中各段子序列的前 L 个值。

5 9、根据权利要求 7 或 8 所述的装置, 其中, 所述第二计算单元, 还配置为:

针对各段子序列中任意一段子序列的前 L 个值;

将该段子序列的前 L 个值进行 M 次移位, 得到 M 个第一移位序列;

10 将该段子序列的前 L 个值及所述 M 个第一移位序列进行 M 位的异或运算, 得到第一目标序列, M 为正整数;

将第一目标序列进行分割, 得到第一目标序列的第一部分子序列和第二部分子序列, 第一目标序列的第二部分子序列的长度长于第一目标序列的第一部分子序列的长度;

15 依据第一目标序列的第一部分子序列和第二部分子序列, 得到该段子序列中除前 L 个值之外的其它值。

10、根据权利要求 9 所述的装置, 其中, 所述第二计算单元, 还配置为:

将第一目标序列的第二部分子序列进行 M 次移位, 得到 M 个第二移位序列;

20 将第一目标序列的第一部分子序列与所述 M 个第二移位序列进行最多 M+1 位的异或运算, 得到第二目标序列;

将第二目标序列进行分割, 得到第二目标序列的第一部分子序列和第二部分子序列, 第二目标序列的第二部分子序列的长度大于第二目标序列的第一部分子序列的长度;

25 将第二目标序列的第二部分子序列进行 M 次移位, 得到 M 个第三移位

序列；

将第二目标序列的第一部分子序列与所述 M 个第三移位序列进行最多 M+1 位的异或运算，得到第三目标序列；

以此类推，直至计算出最后一个目标序列；

- 5 确定第一目标序列的第二部分子序列至倒数第二个目标序列的第二部分子序列以及最后一个目标序列的集合为该段子序列中除前 L 个值之外的其它值。

11 一种获取伪随机序列的装置，包括：处理器和配置为存储能够在处理器上运行的计算机程序的存储器，

- 10 其中，所述处理器配置为运行所述计算机程序时，执行权利要求 1 至 5 所述方法的步骤。

12、一种计算机可读存储介质，其上存储有计算机程序，其中，该计算机程序被处理器执行时实现权利要求 1 至 5 所述方法的步骤。

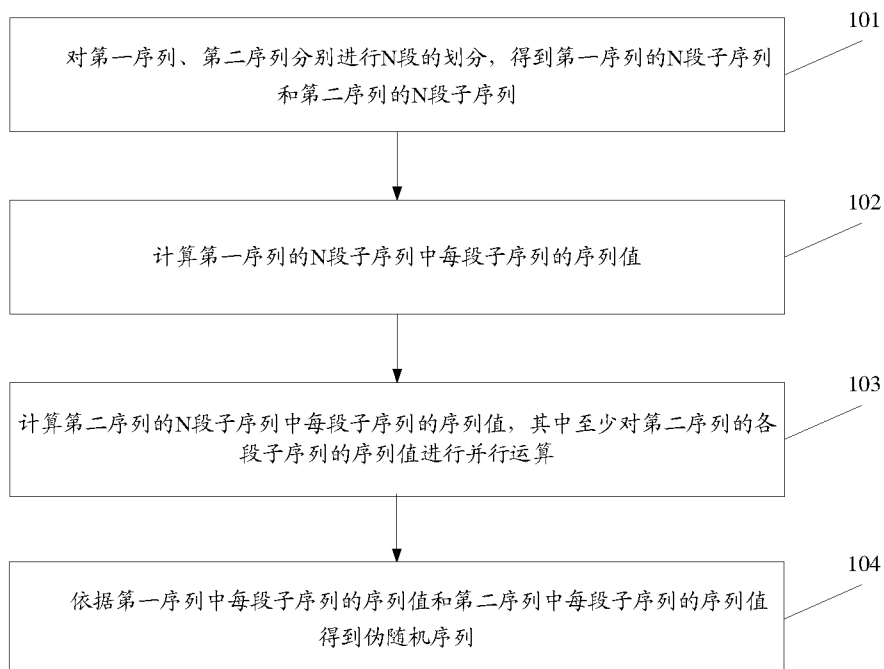


图 1

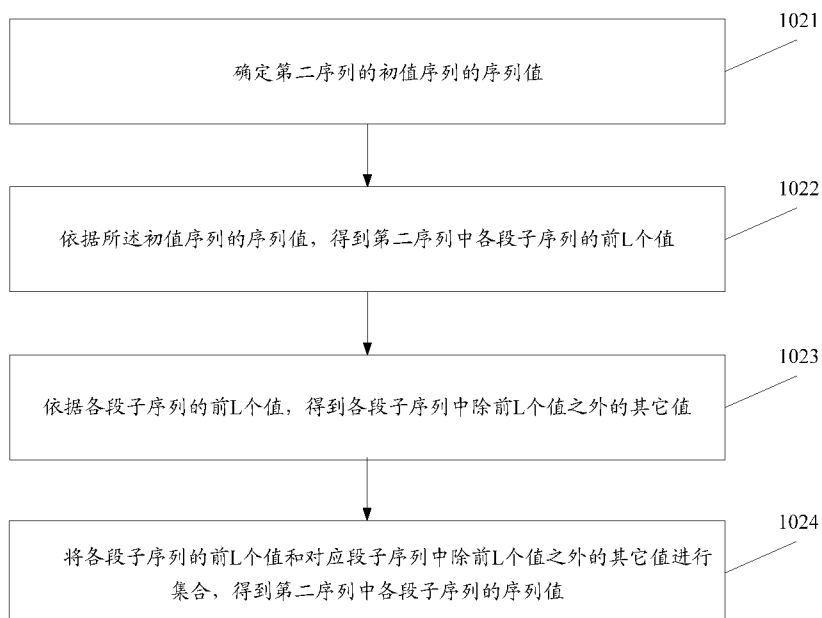


图 2

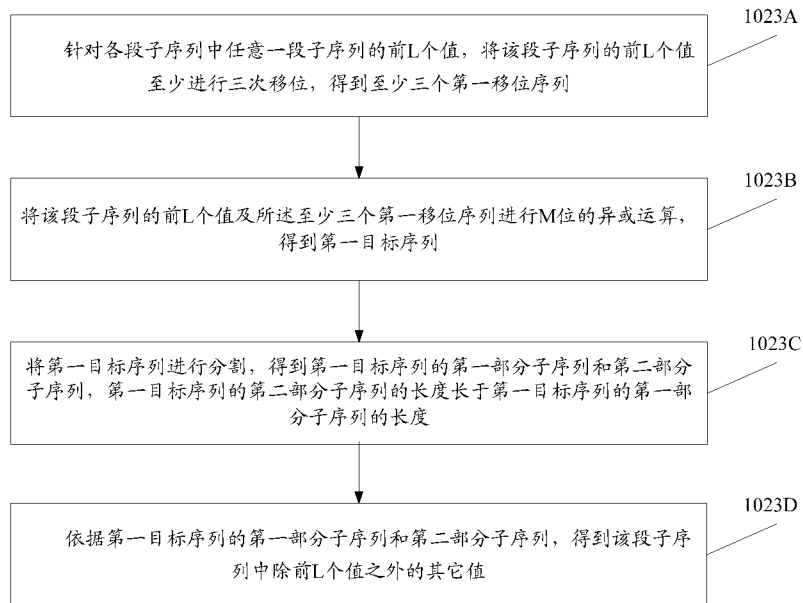


图 3

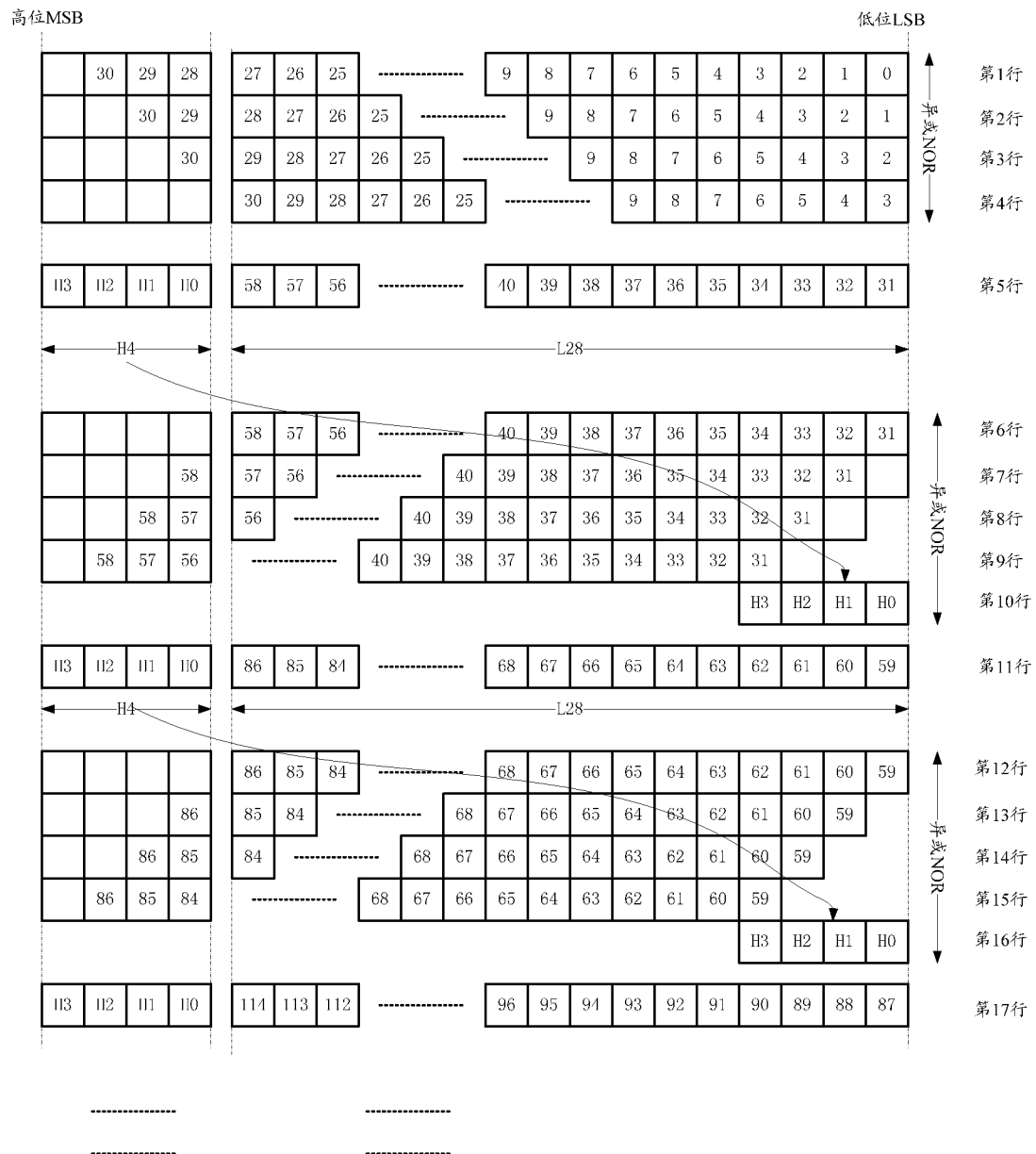


图 4



图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/097350

A. CLASSIFICATION OF SUBJECT MATTER

H04L 27/18 (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

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

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

CNABS, CNTXT, CNKI: 伪随机序列, M 序列, 生成, 子序列, 初始值, 并行, 计算

USTXT, VEN: pseudo-random, M sequence, generate, initial value, parallel, compute

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 105227259 A (INSTITUTE OF COMPUTING TECHNOLOGY, CHINESE ACADEMY OF SCIENCES), 06 January 2016 (06.01.2016), entire document	1-12
A	CN 101132383 A (ZTE CORP.), 27 February 2008 (27.02.2008), entire document	1-12
A	CN 101394266 A (HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY), 25 March 2009 (25.03.2009), entire document	1-12
A	US 2007273401 A1 (KIRYU, N.), 29 November 2007 (29.11.2007), entire document	1-12
A	US 2007294508 A1 (SUSSMAN, M.A. et al.), 20 December 2007 (20.12.2007), entire document	1-12

☐ 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 16 October 2017	Date of mailing of the international search report 27 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 FAN, Xiaohan Telephone No. (86-10) 62089546

International application No.
PCT/CN2017/097350

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2017/097350

A. 主题的分类

H04L 27/18(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

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNABS, CNTXT, CNKI: 伪随机序列, M序列, 生成, 子序列, 初始值, 并行, 计算; USTXT, VEN: pseudo-random, M sequence, generate, initial value, parallel, compute

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
A	CN 105227259 A (中国科学院计算技术研究所) 2016年 1月 6日 (2016 - 01 - 06) 全文	1-12
A	CN 101132383 A (中兴通讯股份有限公司) 2008年 2月 27日 (2008 - 02 - 27) 全文	1-12
A	CN 101394266 A (华中科技大学) 2009年 3月 25日 (2009 - 03 - 25) 全文	1-12
A	US 2007273401 A1 (KIRYU NAOKI) 2007年 11月 29日 (2007 - 11 - 29) 全文	1-12
A	US 2007294508 A1 (SUSSMAN MYLES A等) 2007年 12月 20日 (2007 - 12 - 20) 全文	1-12

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2017年 10月 16日

国际检索报告邮寄日期

2017年 10月 27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

范晓寒

电话号码 (86-10)62089546

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/097350

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	105227259	A	2016年 1月 6日	无			
CN	101132383	A	2008年 2月 27日	CN	101132383	B	2014年 9月 10日
CN	101394266	A	2009年 3月 25日	CN	101394266	B	2010年 12月 8日
US	2007273401	A1	2007年 11月 29日	US	7681098	B2	2010年 3月 16日
US	2007294508	A1	2007年 12月 20日	US	8756264	B2	2014年 6月 17日

表 PCT/ISA/210 (同族专利附件) (2009年7月)