

(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
2022 年 3 月 10 日 (10.03.2022)



(10) 国际公布号
WO 2022/048231 A1

(51) 国际专利分类号:
G06F 7/58 (2006.01)

(21) 国际申请号: PCT/CN2021/099839

(22) 国际申请日: 2021 年 6 月 11 日 (11.06.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010911973.6 2020 年 9 月 2 日 (02.09.2020) CN

(71) 申请人: 长鑫存储技术有限公司 (CHANGXIN MEMORY TECHNOLOGIES, INC.) [CN/CN]; 中国安徽省合肥市经济技术开发区空港工业园兴业大道 388 号, Anhui 230000 (CN)。

(72) 发明人: 范习安 (FAN, Xian); 中国安徽省合肥市经济技术开发区空港工业园兴业大道 388 号, Anhui 230000 (CN)。

(74) 代理人: 北京名华博信知识产权代理有限公司 (BOXIN CHINA INTELLECTUAL PROPERTY); 中国北京市海淀区黑泉路 8 号 1 幢 4 层 101-10 号, Beijing 100192 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,

(54) Title: RANDOM NUMBER GENERATING CIRCUIT

(54) 发明名称: 随机数产生电路

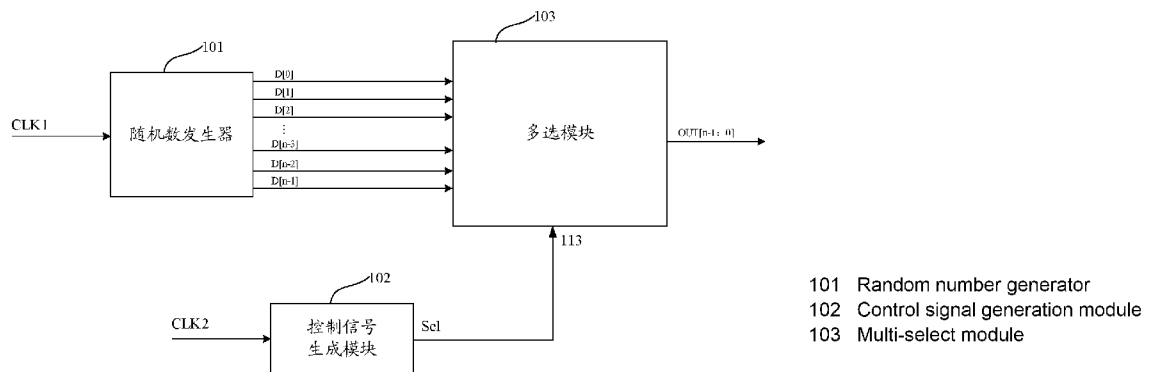


图 2

(57) Abstract: A random number generating circuit comprising: a random number generator (101), which is configured to output a plurality of first random numbers within every full cycle; a control signal generation module (102), which is configured to receive a trigger signal (CLK2) and output control signals (Sel) corresponding to different first random numbers on the basis of the trigger signal (CLK2); and a multi-select module (103), which is configured to receive the first random numbers and control signals (Sel) corresponding to the first random numbers, adjust at least one bit position of the first random numbers on the basis of the control signals (Sel), obtain second random numbers, and output a plurality of second random numbers.

(57) 摘要: 一种随机数产生电路, 包括: 随机数发生器 (101), 被配置为, 在每一计满周期内输出若干个第一随机数; 控制信号生成模块 (102), 被配置为, 接收触发信号 (CLK2), 并基于触发信号 (CLK2) 输出与不同的第一随机数对应的控制信号 (Sel); 多选模块 (103), 被配置为, 接收第一随机数以及与第一随机数对应的控制信号 (Sel), 基于控制信号 (Sel) 对第一随机数的至少一个比特位置进行调整, 获取第二随机数, 并输出若干第二随机数。

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))。

随机数产生电路

本公开要求在 2020 年 09 月 02 日提交中国专利局、申请号为 202010911973.6、发明名称为“随机数产生电路”的中国专利申请的优先权，其全部内容通过引用结合在本公开中。

技术领域

本公开实施例涉及但不限于一种随机数产生电路。

背景技术

处于信息时代的今天，关于信息的安全问题成为信息产品很关键的部分，加密模块是否具有良好的安全性能成为目前关注的重点之一。

对于加密模块而言，为了提高其安全性能需要提供具有良好随机性的随机数作为种子，从而形成伪随机数列。然而，目前的随机数产生电路产生的随机数的随机性仍然有待提高。

发明内容

以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

本公开提供一种随机数产生电路实现了，提高随机数的随机性。本公开实施例提供一种随机数产生电路，包括：随机数发生器，被配置为，在每一计满周期内输出若干个第一随机数；控制信号生成模块，被配置为，接收触发信号，并基于所述触发信号输出与不同的所述第一随机数对应的控制信号；多选模块，被配置为，接收所述第一随机数以及与所述第一随机数对应的所述控制信号，基于所述控制信号对所述第一随机数的至少一个比特位置进行调整，获取第二随机数，并输出若干所述第二随机数。

在一些实施例中，所述随机数发生器为 n -bit 随机数发生器，所述若干个第一随机数为 2^n-1 个第一随机数；所述随机数发生器具有 n 个第一输出端，且每一所述第一输出端具有固定的比特位置， n 为大于 1 的整数。

在一些实施例中，所述多选模块包括：片选输入端，用于接收所述控制信号；数据输入端，与 n 个所述第一输出端连接，用于接收所述第一随机数；所述多选模块具有 N 种不同比特位置调整方式，且每一所述比特位置调整方式与一所述控制信号对应，其中， N 为大于 1 的整数；所述多选模块还被配置为，对所述 n 个第一输出端的数据的比特位置进行调整，以获取所述第二随机数。

在一些实施例中，所述多选模块包括： N 个调整单元，每一所述调整电路定义一所述比特位置调整方式；每一所述调整单元均具有所述数据输入端，且每一所述调整单元均具有所述片选输入端。

在一些实施例中，所述 n 个第一输出端的数据的比特位置排列为第一比特位置排列，每一所述调整单元具有 n 个第二输出端，所述 n 个第二输出端的数据的比特位置排列为第二比特位置排列；每一所述第二比特位置排列各不相同，且所述第二比特位置排列与所述第一比特位置排列不同。

在一些实施例中， N 个所述调整单元被配置为， N 个所述第二比特位置排列中，一个比特位的数据对应的所述第二输出端的位置不同，其余比特位的数据对应的所述第二输出端的位置排列不变。

在一些实施例中，至少一个所述第二比特位置排列与所述第一比特位置排列相同。

在一些实施例中，所述 N 大于或等于 n 。

在一些实施例中，所述控制信号生成模块包括： m -bit 计数器；其中， N 与 m 的关系满足： $N \leq 2^m - 1$ ， m 为任意自然数， N 为大于等于 2 的任意自然数。

在一些实施例中，所述控制信号生成模块还被配置为，所述不同的第一随机数为在不同的所述计满周期内的所述第一随机数；在同一所述计满周期内，所述控制信号不变；一所述计满周期对应的所述控制信号与相邻的所述计满周期对应的所述控制信号不同。

在一些实施例中，所述随机数发生器还被配置为，完成每一所述计满周期则输出计满信号；所述控制信号生成模块接收所述计满信号作为所述触发信号。

在一些实施例中，所述控制信号生成模块还被配置为，所述不同的第一随机数包括每一所述计满周期内的所述第一随机数，在同一所述计满周期内，不

同的所述第一随机数对应的所述控制信号不同。

在一些实施例中，所述随机数发生器还被配置为，接收驱动时钟信号产生所述第一随机数；所述控制信号生成模块还被配置为，接收所述驱动时钟信号作为所述触发信号。

在一些实施例中，所述控制信号生成模块包括：M-bit 伪随机数产生电路，且所述伪随机数产生电路与所述随机数发生器接收同一驱动时钟信号。

在一些实施例中，所述随机数发生器包括线性反馈移位寄存器。

本公开实施例提供一种结构性能优越的随机数产生电路，包括随机数发生器、控制信号生成模块以及多选模块，随机数发生器输出若干第一随机数，且控制信号生成模块向多选模块提供与不同第一随机数对应的控制信号，多选模块接收控制信号后对第一随机数的至少一个比特位置进行调整，获取第二随机数，第二随机数与第一随机数相比具有更好的随机性，从而提高随机数产生电路产生的随机数的随机性。

另外，多选模块具有 N 种不同比特位置调整方式，因此对于第一随机数的比特位置调整方式具有 N 种，基于具有一种随机序列的第一随机数而言，可以产生 N 种随机序列的第二随机数，从而进一步的增加了随机数的随机序列，进一步的提高了随机数的随机性。

在阅读并理解了附图和详细描述后，可以明白其他方面。

附图说明

并入到说明书中并且构成说明书的一部分的附图示出了本公开的实施例，并且与描述一起用于解释本公开实施例的原理。在这些附图中，类似的附图标记用于表示类似的要素。下面描述中的附图是本公开的一些实施例，而不是全部实施例。对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，可以根据这些附图获得其他的附图。

图 1 为 7 种不同的电路结构示意图；

图 2 为本公开一实施例提供的随机数产生电路的功能框图；

图 3 为本公开另一实施例提供的随机数产生电路的功能框图；

图 4 为图 3 中的随机数发生器的电路结构示意图;

图 5 为图 4 中多选模块的结构示意图;

图 6 为图 4 中控制信号生成模块的一种结构示意图;

图 7 为图 4 中控制信号生成模块的另一种结构示意图;

图 8 为图 4 中控制信号生成模块的又一种结构示意图。

具体实施方式

为使本公开实施例的目的、技术方案和优点更加清楚，下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本公开一部分实施例，而不是全部的实施例。基于本公开中的实施例，本领域技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本公开保护的范围。需要说明的是，在不冲突的情况下，本公开中的实施例及实施例中的特征可以相互任意组合。

由背景技术可知，现有技术的随机数产生电路的随机性仍有待提高。

分析发现，目前的随机数产生电路虽然对输出进行了乱序处理，但是前后数之间还是具有一定的前后关系，很难做到真正意义上的随机。以线性移位寄存器（Linear Feedback Shift Registers, LFSR）作为随机数产生电路，以产生 7-bit 的随机数作为示例。对于一个固定的随机数产生电路而言，其抽头（the output of affect on the input, tap）位置是固定的，那么这个随机数产生电路只能产生一种随机序列，在一个计数周期内前后数的顺序是固定的，其中影响下一个状态的比特位置叫做抽头位置。

若需要产生多种随机序列，则需要设置多种随机数产生电路，且每一随机数产生电路的抽头位置不同，例如，对于 7-bit 的 LFSR 而言具有 7 种不同的抽头位置，则可设计 7 个具有不同抽头位置的 LFSR，从而实现 7 种随机序列，每一种随机序列可产生 2^7-1 个随机数，以增加随机数的随机性。

图 1 为 7 种不同的电路结构示意图，如图 1 所示，标示 1-7 的 7 种不同的电路图各自对应的抽头位置不同，随机数产生电路包括：7 个串联的触发器 10，该触发器 10 为 D 触发器，且前一级触发器 10 的输出作为后一级触发器 10 的输

入，且各触发器 10 接收驱动时钟信号 clk；异或门 11，异或门 11 的两个输入端分别与一触发器 10 的输入端与输出端连接，且异或门 11 的输出端作为另一触发器 10 的输入端；该异或门 11 的位置决定随机数产生电路的抽头位置；从左往右将触发器 10 称为第零级/第一级.....第六级触发器 10，且各触发器 10 的输出相应即为 D[0]D[1].....D[6]。

对于标示为 1 的电路图，该随机数产生电路产生第一种随机序列的随机数：抽头位置为第零级触发器 10，随机数产生电路的输出按照比特位的高低依次排布为 D[0]D[6]D[5]D[4]D[3]D[2]D[1]。

对于标示为 2 的电路图，该随机数产生电路产生第二种随机序列的随机数：抽头位置为第一级触发器 10，随机数产生电路的输出按照比特位的高低依次排布为 D[1]D[0]D[6]D[5]D[4]D[3]D[2]。

对于标示为 3 的电路图，该随机数产生电路产生第三种随机序列的随机数：抽头位置为第二级触发器 10，随机数产生电路的输出按照比特位的高低依次排布为 D[2]D[1]D[0]D[6]D[5]D[4]D[3]。

对于标示为 4 的电路图，该随机数产生电路产生第四种随机序列的随机数：抽头位置为第三级寄存器 10，随机数产生电路的输出按照比特位的高低依次排布为 D[3]D[2]D[1]D[0]D[6]D[5]D[4]。

对于标示为 5 的电路图，该随机数产生电路产生第五种随机序列的随机数：抽头位置为第四级寄存器 10，随机数产生电路的输出按照比特位的高低依次排布为 D[4]D[3]D[2]D[1]D[0]D[6]D[5]。

对于标示为 6 的电路图，该随机数产生电路产生第六种随机序列的随机数：抽头位置为第五级寄存器 10，随机数产生电路的输出按照比特位的高低依次排布为 D[5]D[4]D[3]D[2]D[1]D[0]D[6]。

对于标示为 7 的电路图，该随机数产生电路产生第七种随机序列的随机数：抽头位置为第六级寄存器 10，随机数产生电路的输出按照比特位的高低依次排布为 D[6]D[5]D[4]D[3]D[2]D[1]D[0]。

由上述分析不难发现，为达到不同的随机序列，需要改过电路图的抽头位置，即需要提供 7 种电路，增加电路复杂性。此外，由上述分析可知，对于随

机数的比特位固定的电路而言，且抽头位置可变化的量也是固定的，导致可变化的随机序列的数量也是固定的，如图 1 为产生 7-bit 的随机数，那么抽头位置变化的最大量也是 7，能够产生的随机序列的最大种类也是 7，因此采用这种方式来增加随机序列的能力也是有限的。

本公开实施例提供一种随机数产生电路，包括随机数发生器、控制信号生成模块以及多选模块，该多选模块可用于对随机数发生器产生的第一随机数的比特位置进行重新排序，从而增加随机数产生电路产生的随机数的随机序列，提高随机数的随机性。

图 2 为本公开一实施例提供的随机数产生电路的功能框图。

参考图 2，本实施例中，随机数产生电路包括：随机数发生器 101，被配置为，在每一计满周期内输出若干个第一随机数；控制信号生成模块 102，被配置为，接收触发信号 CLK2，并基于触发信号 CLK2 输出与不同的第一随机数对应的控制信号 Sel；多选模块 103，被配置为，接收第一随机数以及与第一随机数对应的控制信号 Sel，基于控制信号 Sel 对第一随机数的至少一个比特位置进行调整，获取第二随机数，并输出若干所述第二随机数。

以下将结合附图对本实施例提供的随机数产生电路进行详细说明。

随机数发生器 101 为 n-bit 随机数发生器，相应的，若干个第一随机数为 2^n-1 个第一随机数；随机数发生器 101 接收驱动时钟信号 CLK1 产生第一随机数。其中，随机数发生器 101 产生所有不同的第一随机数的周期为计满周期。

随机数发生器 101 具有 n 个第一输出端，且每一所述第一输出端具有固定的比特位置，n 为大于 1 的整数，例如为 4、7、10 等。随机数发生器 101 可以为线性反馈移位寄存器，且包括 n 个串联的触发器，每一个触发器的输出端作为 n 个第一输出端中的一个，且每一触发器的输出端所处的比特位置不同。

在一个例子中，以 D[0]、D[1]、D[2].....D[n-3]、D[n-2]、D[n-1] 标示各第一输出端（即各触发器的输出端），且各第一输出端的比特位置从高到低的排布可以为以 D[0]、D[n-1]、D[n-2]、D[n-3].....D[2]、D[1] 的顺序，n 大于 3。本实施例中，随机数发生器 101 可产生一种随机序列的第一随机数，也就是说，随机数发生器 101 可以为具有固定抽头位置的线性移位寄存器。可以理解的是，

在其他实施例中，随机数发生器也可以产生具有多种随机序列的第一随机数。

控制信号生成模块 102 具有用于接收触发信号 CLK2 的触发端 112，且还具有用于输出控制信号 Sel 的信号输出端 122。

为了提高控制信号 Sel 与第一输出端输出数据的同步性，本实施例中，触发信号 CLK2 与随机数发生器 101 相关联。如此，可以提高第一随机数发生变化时控制信号 Sel 变化的同步性。

在一个例子中，控制信号生成模块 102 可以被配置为，不同的第一随机数为在不同的计满周期内的第一随机数；在同一计满周期内，控制信号 Sel 不变；一计满周期对应的控制信号 Sel 与相邻的计满周期对应的控制信号 Sel 不同。如此，在同一计满周期内，多选模块 103 对同一计满周期内的若干第一随机数的比特位置调整的方式相同，即基于第一随机数获取第二随机数的方式相同，有利于降低电路的复杂程度。

触发信号 CLK2 可以为触发驱动时钟信号，且触发驱动时钟信号的时钟周期与计满周期相同。或者，触发信号 CLK2 也可以由随机数发生器 101 输出提供，即随机数发生器 101 完成一个计满周期则输出计满信号，控制信号生成模块 102 接收该计满信号作为触发信号。

在另一个例子中，控制信号生成模块 102 可以被配置为，不同的第一随机数包括每一计满周期内的第一随机数，在同一计满周期内，不同的第一随机数对应的控制信号 Sel 不同。如此，由于在单个计满周期内，控制信号 Sel 不同，因此多选模块 103 对同一计满周期内的每一第一随机数的比特位置调整方式也可以不同，从而有利于进一步的增加第二随机数的随机性。更具体地，由于同一计满周期内的控制信号 Sel 也不相同，能够在增加不同计满周期的第一随机数的随机性的同时，还增加同一计满周期的第一随机数的随机性。

随机数发生器 101 接收驱动时钟信号 CLK1 产生第一随机数，控制信号生成模块 102 接收该驱动时钟信号 CLK1 作为触发信号 CLK2。

本实施例中，多选模块 103 包括：片选输入端 113，用于接收控制信号 Sel；数据输入端，与 n 个第一输出端连接，用于接收第一随机数；多选模块 103 具有 N 种不同比特位置调整方式，且每一比特位置调整方式与一控制信号对应，

其中，N 为大于 1 的整数；多选模块 103 还被配置为：对 n 个第一输出端的比特位置进行调整，以获取第二随机数。

多选模块 103 包括数据输出端 OUT[n-1: 0]，输出 n-bit 的第二随机数。

相较于随机数产生电路 101 产生的第一随机性的随机序列而言，多选模块 103 输出的第二随机数的随机序列增加了 N 倍。

控制信号 Sel 的种类大于或等于 N，保证会用到所有的不同比特位置调整方式来调整第一随机数的比特位置，从而增加第二随机数的随机序列。因此，可以根据 N 合理设置控制信号生成模块 102，保证产生的控制信号 Sel 的种类符合需求。

本实施例中，N 大于或等于 n，有利于增加第二随机数的随机序列。具体地，n 个第一输出端的数据的比特位置排列为第一比特位置排列，多选模块 103 的输出端输出的数据可以具有 N 个第二比特位置排列，每一第二比特位置排列为基于一种比特位置调整方式对第一比特位置进行调整后获取的。

需要说明的是，为了保留随机数发生器 101 产生的第一随机数的随机序列，至少一个第二比特位置排列与第一比特位置排列相同。还需要说明的是，在其他实施例中，N 也可以为 1。

此外，为了减小多选模块 103 的电路复杂度，多选模块 103 还可以被配置为：对于 N 各第二比特位置排列中，一个比特位的数据对应的多选模块 103 的输出端的位置不同，而其余比特位的数据对应的多选模块 103 的输出端的位置排列不变。举例来说，由最高位到最低位，第一比特位置排列为 D[0]、D[n-1]、D[n-2]...D[3]、D[2]、D[1]；由最高位到最低位，第二比特位置排列包括表一中的多种排列方式。

1	D[0]	D[n-1]	D[n-2]	D[n-3]	...	D[3]	D[2]	D[1]
2	D[1]	D[0]	D[n-1]	D[n-2]	...	D[4]	D[3]	D[2]
3	D[2]	D[1]	D[0]	D[n-1]	...	D[5]	D[4]	D[3]
...	...	...	...	...	...	...	...	...
n-1	D[n-2]	D[n-3]	D[n-4]	D[n-5]	...	D[1]	D[0]	D[n]

n	D[n-1]	D[n-2]	D[n-3]	D[n-4]	...	D[2]	D[1]	D[0]
---	--------	--------	--------	--------	-----	------	------	------

表一

可以理解的是，在其他实施例中，也可以为至少两个比特位的数据对应的多选模块 103 的输出端的位置不同。对于 n 个第一输出端而言，各第一输出端对应的数据的比特位均可以发生变化，根据不同的排列组合一共具有 C_n^{n-1} 种变化，也就是说， N 与 n 满足： $N \leq C_n^{n-1}$ ，即， $N \leq n \times (n-1) \times (n-2) \dots 2 \times 1$ 。

为了降低多选模块 103 的复杂度， N 可以与 n 相同。

可以理解的是，在其他实施例中， N 也可以小于 n 。

本实施例中，随机数发生器 101 输出二进制的第一随机数，相应的多选模块 103 输出二进制第二随机数。

本实施例提供的随机数产生电路，由于多选模块 103 能够对第一随机数的比特位进行重新排序，从而产生更多的随机序列，提高随机数产生电路的随机数的随机性。此外，相较于需要多种具有不同抽头位置的随机数发生器而言，本实施例的电路结构更为简单，且功耗更低。

本公开另一实施例还提供一种随机数产生电路，该随机数产生电路与前述的实施例的大致相同，主要区别包括对各模块做了更详细的说明。以下将结合附图对本公开另一实施例提供的随机数产生电路进行详细说明，与前述实施例相同或者相应的部分，可参考前述实施例，以下将不做详细赘述。

图 3 为本公开另一实施例提供的随机数产生电路的功能框图。

参考图 3，本实施例中，随机数产生电路包括： n -ibt 的随机数发生器 201，具有 n 个第一输出端 211；控制信号生成模块 202；多选模块 203，多选模块 203 具有片选输入端以及数据输入端，多选模块 203 具有数据输出端 OUT[n-1:0]。

多选模块 203 包括： N 个调整单元 204，每一调整单元 204 定义一比特位置调整方式；且每一调整单元 204 均具有数据输入端，且每一调整单元 204 均具有片选输入端。每一调整单元 204 被配置为，接收控制信号 Sel，且与控制信号 Sel 对应的调整单元 204 输出第二随机数。

也就是说，每一调整单元 204 的输出端均为多选模块 203 的数据输出端

OUT[n-1:0]，且控制信号 Sel 作为调整单元 204 的片选信号，基于控制信号 Sel 选中对应的调整单元 204 的输出端作为多选模块 203 的数据输出端 OUT[n-1:0]。

按照各自输出的数据的比特位置，将 n 个第一输出端 211 中的每一第一输出端 211 标记为 D[n-1]、D[n-2]...D[3]、D[2]、D[1]、D[0]。

n 个第一输出端 211 的数据的比特位置排列为第一比特位置排列，例如为 D[0]D[n-1]D[n-2]...D[3]D[2]D[1]。每一调整单元 204 具有 n 个第二输出端 214，且 n 个第二输出端 214 的数据的比特位置排列为第二比特位置排列，第二比特位置排列各不相同，且第二比特位置排列与第一比特位置排列不同，例如第二比特位置排列可以为 D[n-1]D[n-2]...D[3]D[2]D[1]D[0]等，有关第二比特位置排列以及第一比特位置排列的详细说明，可参考前述实施例。

本实施例中，以调整单元 204 的数量与随机数产生器 201 的第一随机数的比特位数量相同作为示例，即 N 与 n 相同。在其他实施例中，调整单元的数量可以大于或小于随机数发生器的比特位数量。

图 4 为本实施例提供的随机数发生器 201 的电路结构示意图。

参考图 4，随机数发生器 201 为线性移位寄存器，包括：n 个触发器 211，异或门 231，一触发器 211 的输入端以及输出端作为异或门 231 的两个输入端，且异或门 231 的输出端连接另一触发器 211 的输入端。异或门 231 的位置定义随机数发生器 201 的抽头位置，每一触发器 211 的输出端作为一第一输出端 211（参考图 3）。

根据串联的顺序，触发器 211 依次记为第零级触发器、第一级触发器、第二级触发器...第 n-1 级触发器。

本实施例中，以随机数发生器 201 为 7-bit 随机数发生器，且为二进制的 7-bit 随机数发生器作为示例进行详细说明，在一个计满周期内产生 127 个第一随机数。图 4 中，随机数发生器 201 具有 7 个触发器 211，且异或门 231 的位置决定了 n 个第一输出端 211 的数据的比特位置排列，例如，图 4 中，7 个第一输出端 211 的数据的比特位置排列为 D[0]D[6]D[5]D[4]D[3]D[2]D[1]。

需要说明的是，在其他实施例中，异或门 231 的输入端、输出端也可以与其他的触发器相应连接。

图 5 为本实施例提供的多选模块 203 的结构示意图, 包括 7 个调整单元 204 (参考图 3)。n 个第一输出端 211 作为每一调整单元 204 的输入端, 为了便于图示的简洁性, 图 5 中每一调整单元 204 的输入端以 0 代替 D[0]、以 1 代替 D[1], 依次类推, 且第二输出端 214 以 0 代替 D[0], 依次类推。需要说明的是, 标示为 D[0] 的标示为第零个第一输出端 211 的数据, 标示为 D[1] 的为第一个第一输出端 211 的数据, 依次类推。

图 5 中, 为了便于说明, 以 20/21/22/23/24/25/26 标示不同的调整单元 204。每一调整单元 204 的第二输出端的排列方式不同, 作为示例, 按照从上往下的排列表示各数据的比特位由高到低的排序, 标示为 20 的调整单元 204 的第二输出端输出的数据为 D[0]D[6]D[5]D[4]D[3]D[2]D[1], 标示为 21 的调整单元 204 的第二输出端输出的数据为 D[1]D[0]D[6]D[5]D[4]D[3]D[2]。

本实施例中, 随机数发生器 201 具有固定的抽头位置, 多选模块 203 应用于模拟随机数发生器 201 的抽头位置调整产生的随机数。相应的, 多选模块 203 具有 n 种不同的调整单元 204。如图 5 所示, 标示为 21 的调整单元 204 用于模拟图 4 中随机数发生器 201 的抽头位置在第零级触发器的 LFSR, 标示为 22 的调整单元 204 用于模拟图 4 中抽头位置在第一级触发器的 LFSR, 标示为 23 的调整单元 204 用于模拟图 4 中抽头位置在第二级触发器的 LFSR, 依次类推。

需要说明的是, 本实施例中以随机数发生器 201 为 7-bit 的随机数发生器作为示例。在其他实施例中, 随机数发生器也可以为任意 bit 的随机数发生器, 如 3-bit、4-bit、10-bit、20-bit 等。

本实施例中, 控制信号生成模块 202 包括: m-bit 计数器 212; 其中, N 与 m 的关系满足: $N \leq 2^m - 1$, m 为任意自然数, N 为大于等于 2 的任意自然数。具体地, m 大于或等于 $\lg N / \lg 2 + 1$ 的结果向下取整。举例来说, N 为 7 时, m 大于或等于 3。

如图 6 所示, m-bit 计数器 212 包括 m 个触发器 222; 触发信号 CLK2 作为第一级的触发器 222 的时钟输入信号, 前一级的触发器 222 的输出端作为后一级即触发器 222 的时钟输入信号, m 个触发器 222 的输出端共同输出控制信号 Sel。

本实施例中, N 为 7, 则计数器 212 包括三个触发器 222, 分别标示为 DFF#0、DFF#1、DFF#2。

随机数发生器 201 还被配置为，完成每一计满周期则输出计满信号，控制信号生成模块 202 接收该计满信号作为触发信号。如此，在同一计满周期内，控制信号 Sel 不变；不同的计满周期对应的控制信号 Sel 不同。

本实施例中，控制信号生成模块 202 为 3-bit 计数器，具有三个输出端 S0/S1/S2，控制信号 Sel 如表二所示：

S2 (最高比特位)	S1	S0 (最低比特位)	Sel
0	0	0	0
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6

表二

以下将结合附图对本实施例提供的随机数产生电路的工作原理进行说明：

在第一个计满周期内，随机数发生器 201 产生若干第一随机数，且控制信号 Sel 保持不变为 0，相应的多选模块 203 中标示为 20 的调整单元 204 被选中，其第二输出端 214 输出若干第二随机数，各第二随机数的顺序与第一随机数的顺序相同。

第一计满周期完成，随机数发生器 201 输出计满信号，该计满信号作为计数器的触发信号，S2S1S0 由 000 变为 001，控制信号 Sel 由 0 变为 1，相应的标示为 21 的调整单元 204 被选中，在第二个计满周期内，标示为 21 的调整单元 203 的第二输出端输入若干第二随机数，各第二随机数的顺序与第一随机数的顺序不同。

依次类推，每一次计满周期完成后，计数器输出端输出的控制信号 Sel 为上一个计满周期对应的数值+1，从而选中另一个调整单元 203 的第二输出端作为

多选模块 203 的输出端。

如此，对于 7 个计满周期而言，每个计满周期内的第二随机数的顺序都发生了变化，第二随机数的随机序列为 7 种，从而增加了随机数产生电路产生的随机数的随机性。

在另一例子中，如图 7 所示，计数器的触发信号与随机数发生器 201 的驱动时钟信号相同。在每个计满周期内，不同的第一随机数对应不同的控制信号 Sel，因此在每个计满周期内也能调用不同的调整单元 204 进行比特位置的重新排列，从而进一步的增加了随机数的随机性，有利于产生更多的随机序列。随机数产生电路的工作原理如下：

在每一个计满周期内，随机数发生器 201 产生第一个随机数，计数器输出的控制信号 Sel 为 0，选中标号为 20 的调整单元 204 产生第二随机数；随机数发生器 201 产生第二个随机数，计数器输出的控制信号 Sel 为 1，选中标号为 21 的调整单元 204 产生第二随机数；计数器输出的控制信号 Sel 为 2，选中标号为 22 的调整单元 204 产生第二随机数；依次类推；当计数器输出的控制信号为 7 之后，计数器又重新从 0 开始计数。可以理解的是，多选模块 203 中的调整单元 204 的数量可以与每一计满周期产生的第一随机数的数量相同，且根据调整电路 203 的数量设置计数器。需要说明的是，前述的控制信号 Sel 与对应选中的调整单元 204 仅为示例，只有保证不同的控制信号 Sel 对应选中不同的调整单元 204 即可。

在又一个例子中，如图 8 所示，控制信号生成模块 202 可以为：M-bit 伪随机数产生电路，且伪随机数产生电路与随机数发生器 201 接收同一驱动时钟信号 CLK。相较于计数器而言，伪随机数产生电路输出的控制信号更具有随机性，因此不同的第一随机数对应的调整单元 204 也相应更具有随机性。

伪随机数产生电路包括 M 个 D 触发器 232 以及第一异或门 231，伪随机数产生电路具有输出端 S0/S1/S2，该输出端的信号作为控制信号。

本实施例提供的随机数产生电路，基于一种具有固定随机序列的随机数发生器 201，能够产生具有 N 种不同随机序列的随机数，提高了使用该随机数产生电路的安全性。

本领域技术人员在考虑说明书及实践的公开后，将容易想到本公开的其它实施方案。本公开旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

工业实用性

本公开所提供的随机数产生电路，结构简单，功耗低，通过多选模块对随机数发生器输出的若干第一随机数的至少一个比特位置进行重新排序，获取第二随机数，从而增加随机数产生电路产生的随机数的随机序列，产生更多的随机序列，提高随机数的随机性。

权利要求

1. 一种随机数产生电路，其中，包括：

随机数发生器，被配置为，在每一计满周期内输出若干个第一随机数；

控制信号生成模块，被配置为，接收触发信号，并基于所述触发信号输出与不同的所述第一随机数对应的控制信号；

多选模块，被配置为，接收所述第一随机数以及与所述第一随机数对应的所述控制信号，基于所述控制信号对所述第一随机数的至少一个比特位置进行调整，获取第二随机数，并输出若干所述第二随机数。

2. 如权利要求 1 所述的随机数产生电路，其中，所述随机数发生器为 n -bit 随机数发生器，所述若干个第一随机数为 2^n-1 个第一随机数；所述随机数发生器具有 n 个第一输出端，且每一所述第一输出端具有固定的比特位置， n 为大于 1 的整数。

3. 如权利要求 2 所述的随机数产生电路，其中，所述多选模块包括：

片选输入端，用于接收所述控制信号；

数据输入端，与 n 个所述第一输出端连接，用于接收所述第一随机数；

所述多选模块具有 N 种不同比特位置调整方式，且每一所述比特位置调整方式与一所述控制信号对应，其中， N 为大于或等于 1 的整数；所述多选模块还被配置为，对所述 n 个第一输出端的数据的比特位置进行调整，以获取所述第二随机数。

4. 如权利要求 3 所述的随机数产生电路，其中，所述多选模块包括： N 个调整单元，每一所述调整电路定义一所述比特位置调整方式；每一所述调整单元均具有所述数据输入端，且每一所述调整单元均具有所述片选输入端。

5. 如权利要求 4 所述的随机数产生电路，其中，所述 n 个第一输出端的数据的比特位置排列为第一比特位置排列，每一所述调整单元具有 n 个第二输出端，所述 n 个第二输出端的数据的比特位置排列为第二比特位置排列；每一所述第二比特位置排列各不相同，且所述第二比特位置排列与所述第一比特位置排列不同。

6. 如权利要求 5 所述的随机数产生电路，其中， N 个所述调整单元被配置

为，N 个所述第二比特位置排列中，一个比特位的数据对应的所述第二输出端的位置不同，其余比特位的数据对应的所述第二输出端的位置排列不变。

7. 如权利要求 5 所述的随机数产生电路，其中，至少一个所述第二比特位置排列与所述第一比特位置排列相同。

8. 如权利要求 4 所述的随机数产生电路，其中，所述 N 大于或等于 n。

9. 如权利要求 3 所述的随机数产生电路，其中，所述控制信号生成模块包括：m-bit 计数器；其中，N 与 m 的关系满足： $N \leq 2m-1$ ，m 为任意自然数，N 为大于等于 2 的任意自然数。

10. 如权利要求 1 所述的随机数产生电路，其中，所述控制信号生成模块还被配置为，所述不同的第一随机数为在不同的所述计满周期内的所述第一随机数；在同一所述计满周期内，所述控制信号不变；一所述计满周期对应的所述控制信号与相邻的所述计满周期对应的所述控制信号不同。

11. 如权利要求 10 所述的随机数产生电路，其中，所述随机数发生器还被配置为，完成每一所述计满周期则输出计满信号；所述控制信号生成模块接收所述计满信号作为所述触发信号。

12. 如权利要求 1 所述的随机数产生电路，其中，所述控制信号生成模块还被配置为，所述不同的第一随机数包括每一所述计满周期内的所述第一随机数，在同一所述计满周期内，不同的所述第一随机数对应的所述控制信号不同。

13. 如权利要求 12 所述的随机数产生电路，其中，所述随机数发生器还被配置为，接收驱动时钟信号产生所述第一随机数；所述控制信号生成模块还被配置为，接收所述驱动时钟信号作为所述触发信号。

14. 如权利要求 1 所述的随机数产生电路，其中，所述控制信号生成模块包括：M-bit 伪随机数产生电路，且所述伪随机数产生电路与所述随机数发生器接收同一驱动时钟信号。

15. 如权利要求 1 所述的随机数产生电路，其中，所述随机数发生器包括线性反馈移位寄存器。

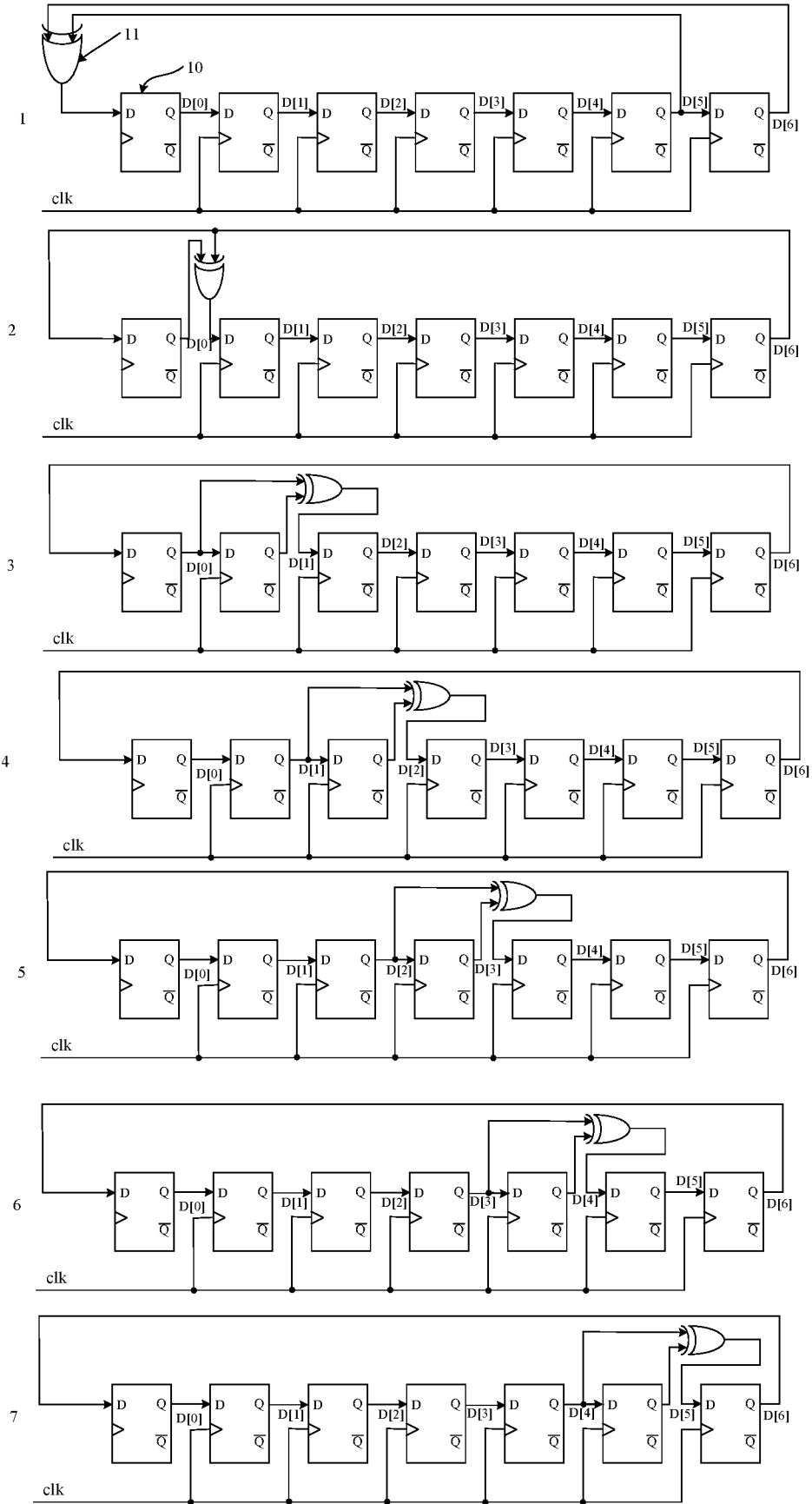


图 1

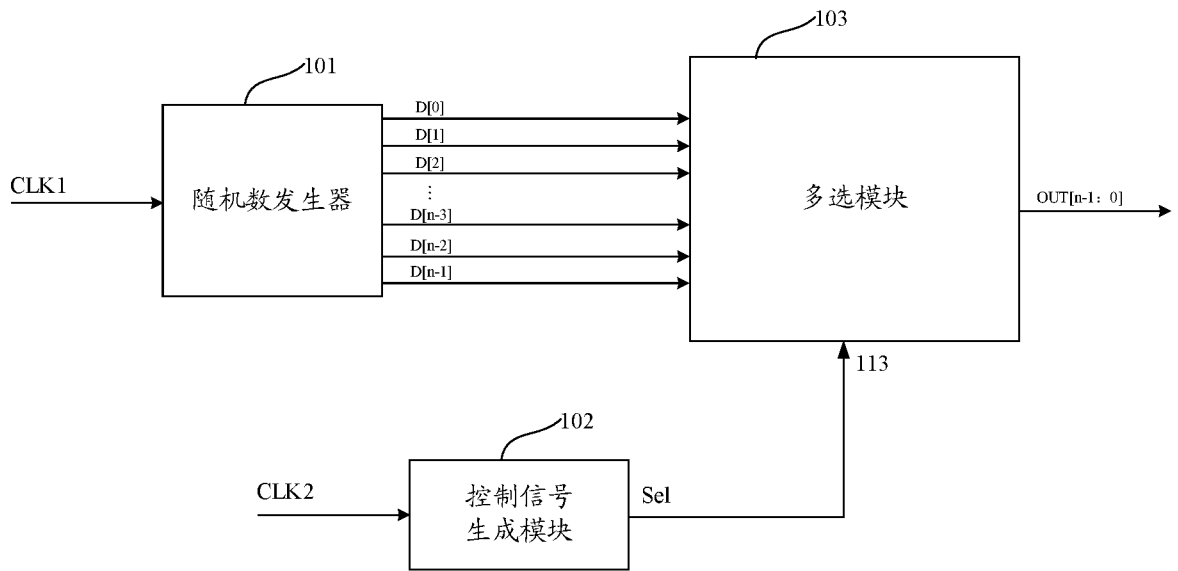


图 2

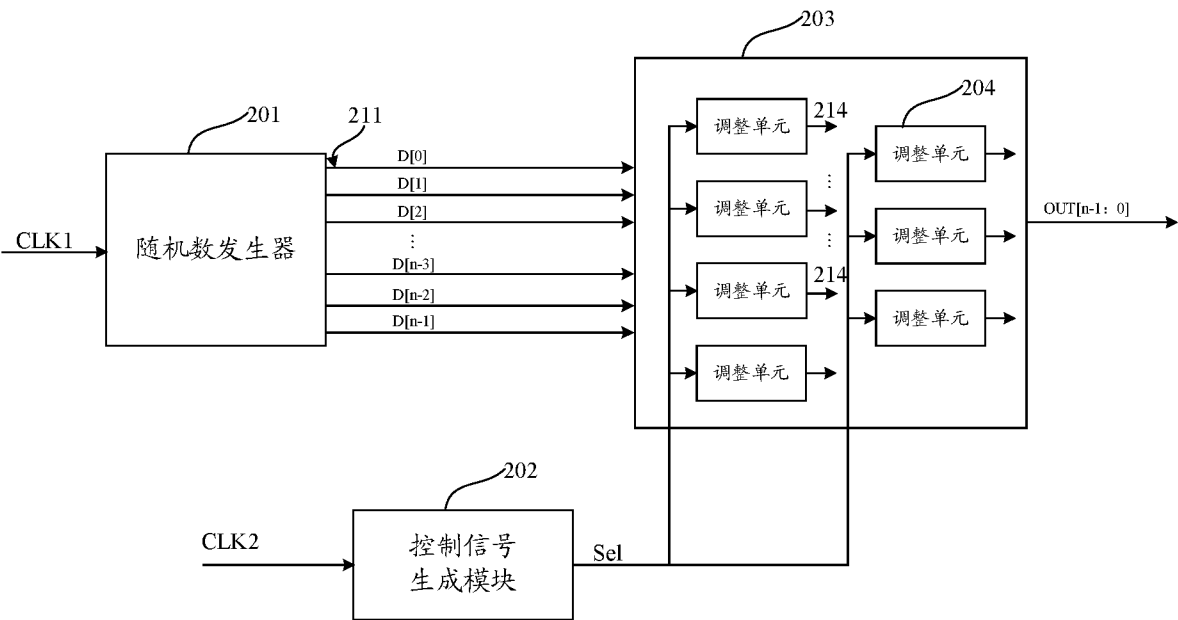


图 3

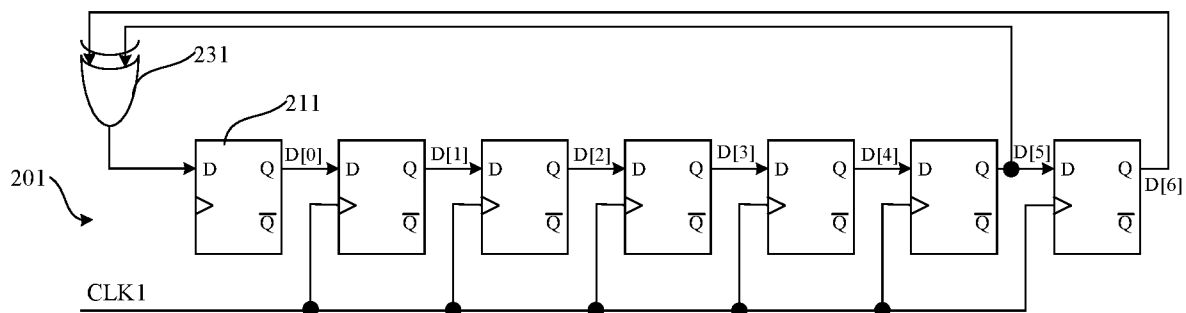


图 4

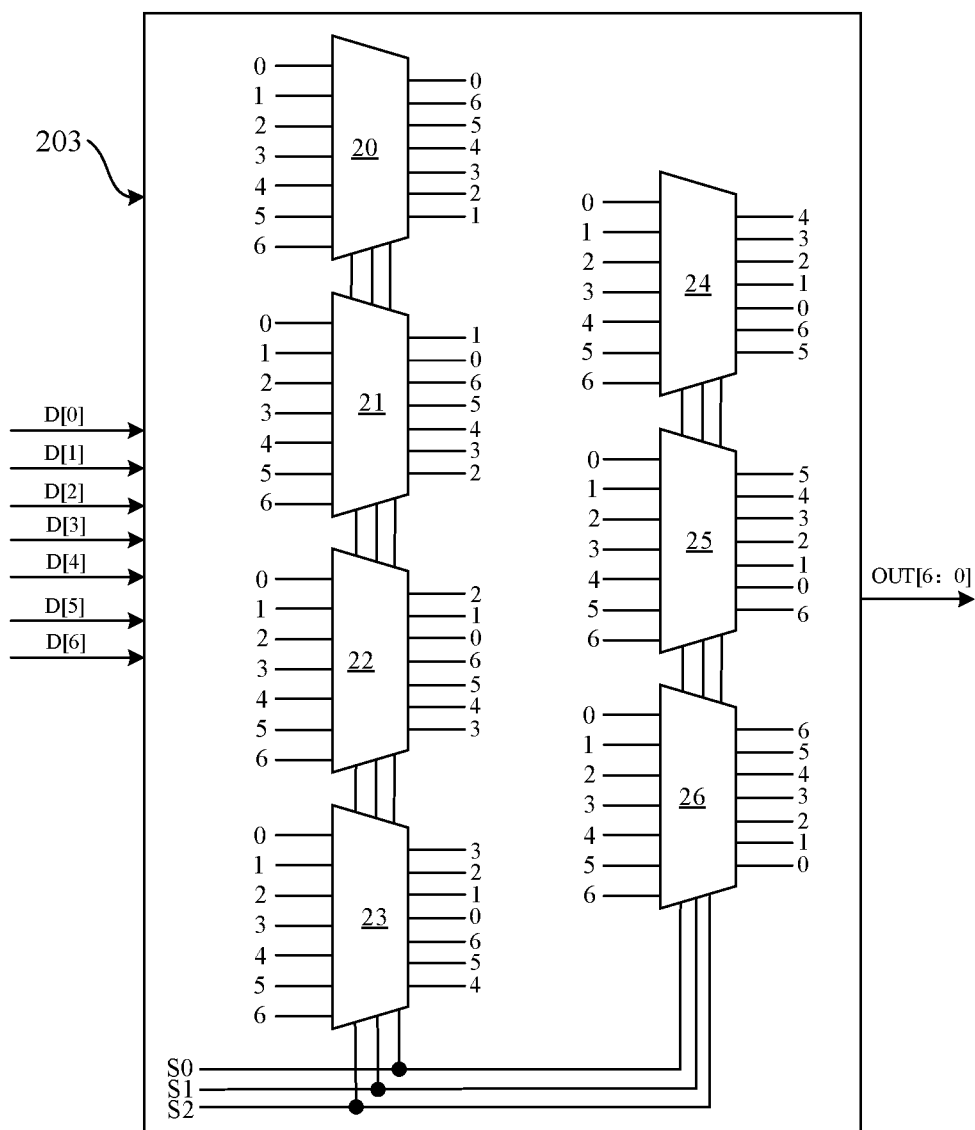


图 5

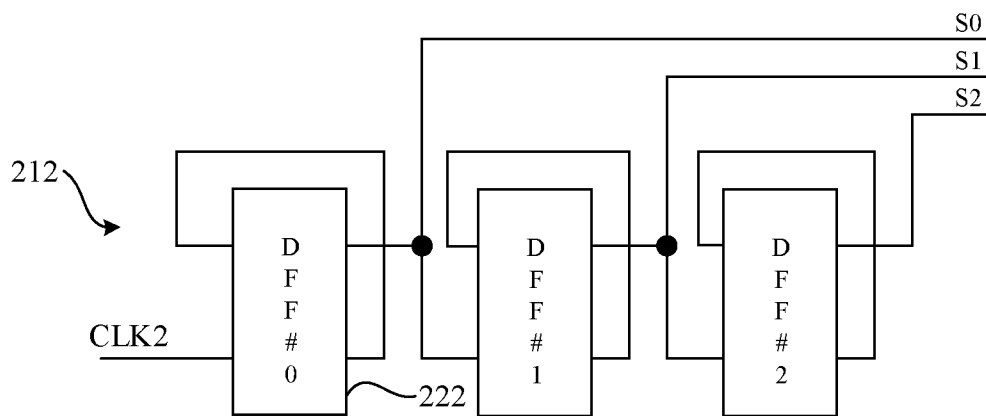


图 6

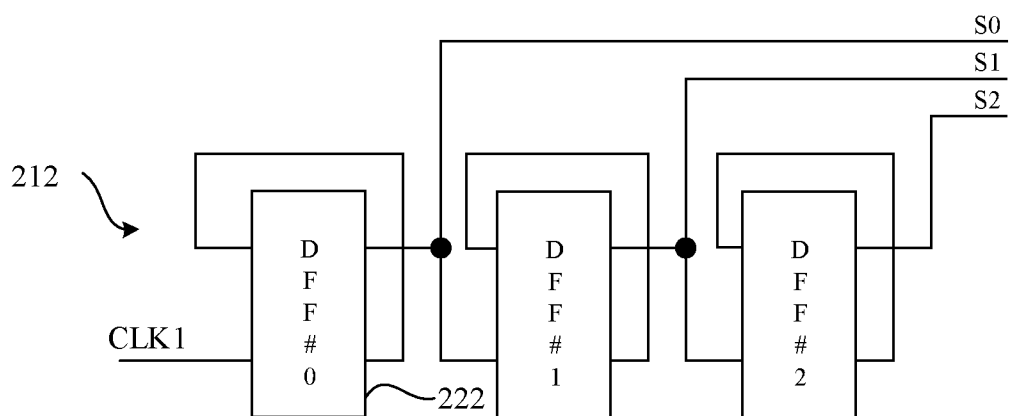


图 7

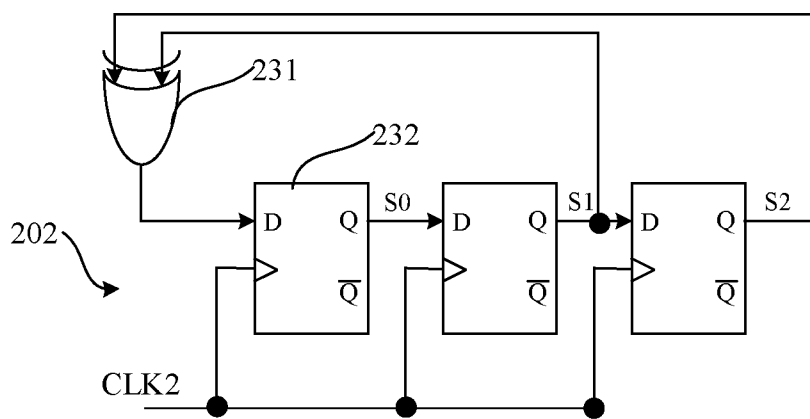


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/099839

A. CLASSIFICATION OF SUBJECT MATTER

G06F 7/58(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

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: 随机数, 多工, 多选, 复用器, 多路器, 选择器, 复选, 片选, 移位, 位移, 比特, random number, MUX, multi+, shift+, selector+, counter+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 110597488 A (WINBOND ELECTRONICS CORPORATION) 20 December 2019 (2019-12-20) description, paragraphs [0036]-[0048], and figures 1-7	1-15
A	CN 108809294 A (BEIJING NEURON NETWORK TECHNOLOGY CO., LTD.) 13 November 2018 (2018-11-13) entire document	1-15
A	CN 109656514 A (WINBOND ELECTRONICS CORPORATION) 19 April 2019 (2019-04-19) entire document	1-15
A	US 5966313 A (NEC CORPORATION) 12 October 1999 (1999-10-12) entire document	1-15



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

31 August 2021

Date of mailing of the international search report

22 September 2021

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/099839

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110597488	A	20 December 2019	None			
CN	108809294	A	13 November 2018	None			
CN	109656514	A	19 April 2019	US	2019107999	A1	11 April 2019
US	5966313	A	12 October 1999	JP	H1027088	A	27 January 1998

国际检索报告

国际申请号

PCT/CN2021/099839

A. 主题的分类

G06F 7/58 (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

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, EPDOC, CNKI, IEEE: 随机数, 多工, 多选, 复用器, 多路器, 选择器, 复选, 片选, 移位, 位移, 比特, random number, MUX, multi+, shift+, selector+, counter+

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 110597488 A (华邦电子股份有限公司) 2019年 12月 20日 (2019 - 12 - 20) 说明书第[0036]-[0048]段, 图1-7	1-15
A	CN 108809294 A (北京神经网络技术有限公司) 2018年 11月 13日 (2018 - 11 - 13) 全文	1-15
A	CN 109656514 A (华邦电子股份有限公司) 2019年 4月 19日 (2019 - 04 - 19) 全文	1-15
A	US 5966313 A (NEC CORPORATION) 1999年 10月 12日 (1999 - 10 - 12) 全文	1-15

☐ 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

2021年 8月 31日

国际检索报告邮寄日期

2021年 9月 22日

ISA/CN的名称和邮寄地址

中国国家知识产权局(ISA/CN)

中国 北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

杨莹莹

电话号码 86-(10)-53961527

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/099839

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	110597488	A	2019年 12月 20日	无	
CN	108809294	A	2018年 11月 13日	无	
CN	109656514	A	2019年 4月 19日	US 2019107999 A1	2019年 4月 11日
US	5966313	A	1999年 10月 12日	JP H1027088 A	1998年 1月 27日