



УКРАЇНА

(19) UA (11) 6822 (13) C1

(51) G 06 F 7/58

ДЕРЖАВНЕ  
ПАТЕНТНЕ  
ВІДОМСТВООПИС ДО ПАТЕНТУ  
НА ВІНАХІД

(54) ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

1

(20) 94270901, 11.03.93

(21) 4776155/24

(22) 09.11.89, SU

(46) 31.03.95, Бюл. № 1

(56) 1.А.с.СССР № 907547,

кл. G 06 F 7/58, 1981.

2.А.с.СССР № 920718,

кл. G 06 F 7/58, 1980 (прототип).

(71) Виробниче об'єднання "Луганський верстатобудівний завод"

(72) Биков Олександр Сергійович, Умеренко Ігор Віталійович, Жабський Юрій Олександрович

(73) Виробниче об'єднання "Луганський верстатобудівний завод", UA

(57) Генератор псевдослучайных чисел, содержащий блок формирования равномерно распределенных псевдослучайных чисел и коммутатор, информационные входы которого соединены с разрядными выходами блока формирования равномерно распределенных псевдослучайных чисел, отличающемся тем, что в него введены первая и вторая схемы сравнения, счетчик, два элемента И, элемент ИЛИ, блок управления и генератор тактовых импульсов, первый выход которого соединен с первыми входами первого и второго элементов И, а второй

2

выход - с входом синхронизации блока управления, первый выход которого соединен с управляющим входом коммутатора, первый выход которого соединен с первым входом первой схемы сравнения, а второй выход - со вторым входом первой схемы сравнения и первым входом второй схемы сравнения, второй вход которой является входом задания верхнего граничного значения, а выход "больше" соединен со вторым входом второго элемента И, выход которого соединен с первым входом элемента ИЛИ, второй вход которого является входом запуска генератора, а выход соединен с тактовым входом блока формирования равномерно распределенных псевдослучайных чисел и с входом "сброс" блока управления, второй выход которого соединен с вторым входом первого элемента И, третий вход которого соединен с выходом "равно" первой схемы сравнения, а выход - с счетным входом счетчика, вход сброса которого соединен с третьим выходом блока управления, а выход переполнения - с третьим входом элемента ИЛИ, четвертый выход блока управления является выходом "готовность" генератора и соединен с входом "запрет" генератора тактовых импульсов.

Изобретение относится к вычислительной технике и может быть использовано в аппаратуре контроля и диагностики цифровых блоков, в системах программного управления фрезерным станком при фрезеровании пазов в ключе дверных замков повышенной секретности.

Известен генератор псевдослучайных чисел, содержащий регистр сдвига, счетчик,

элемент И, элемент ИЛИ, элемент задержки, сумматор по модулю два и триггер [1].

В процессе эксплуатации генератора формируемые на разрядных выходах регистра сдвига коды носят псевдослучайный характер и равномерно распределены во времени, однако использование данного устройства в качестве генератора псевдослучайных размещений чисел для фрезерования пазов с ограниченным числом

(19) UA (11) 6822 (13) C1

одинаковых углов невозможно из-за многократного повторения генерируемых кодов.

Известен также генератор псевдослучайных чисел (прототип), содержащий блок формирования равномерно распределенных псевдослучайных чисел и коммутатор, информационные входы которого соединены с разрядными выходами блока формирования равномерно распределенных псевдослучайных чисел [2].

Такая конструкция генератора также не исключает возможность многократного повторения кодов и кроме этого не обеспечивает возможность регулирования верхней границы кодов, не используя перезапись информации в памяти. Это ограничивает применение данного генератора, в частности, в качестве программирующего устройства в системе программного управления фрезерным станком для фрезерования пазов в ключе дверных замков повышенной секретности.

В основу изобретения поставлена задача создания генератора псевдослучайных чисел в котором достигается выделение комбинаций псевдослучайных чисел, соответствующих поставленным условиям, из всех возможных формируемых комбинаций, в результате чего обеспечивается исключение многократного повторения генерируемых кодов и реализация возможности регулирования их верхней границы, что позволяет применить данный генератор в качестве программирующего устройства в системе программного управления фрезерным станком для фрезерования пазов в ключе дверных замков повышенной секретности.

Поставленная задача решается тем, что в генератор псевдослучайных чисел, содержащем блок формирования равномерно распределенных псевдослучайных чисел и коммутатор, информационные входы которого соединены с разрядными выходами блока формирования равномерно распределенных псевдослучайных чисел, согласно изобретению, введены первая и вторая схемы сравнения, счетчик, два элемента И, элемент ИЛИ, блок управления и генератор тактовых импульсов, первый выход которого соединен с первыми входами первого и второго элементов И, а второй выход — с входом синхронизации блока управления, первый выход которого соединен с управляющим входом коммутатора, первый выход которого соединен с первым входом первой схемы сравнения, а второй выход — со вторым входом первой схемы сравнения и первым входом второй схемы сравнения, второй вход которого является входом задания верхнего граничного значения, а выход "больше" сое-

динен с вторым входом второго элемента И, выход которого соединен с первым входом элемента ИЛИ, второй вход которого является входом запуска генератора, а выход соединен с тактовым входом блока формирования равномерно распределенных псевдослучайных чисел и с входом "сброс" блока управления, второй выход которого соединен с вторым входом первого элемента И, третий вход которого соединен с выходом "равно" первой схемы сравнения, а выход — с счетным входом счетчика, вход сброса которого соединен с третьим выходом блока управления, а выход переполнения с третьим входом элемента ИЛИ, четвертый выход блока управления является выходом "готовность" генератора и соединен с входом "запрет" генератора тактовых импульсов.

Благодаря такому выполнению данный генератор обеспечивает выделение комбинаций псевдослучайных, соответствующих поставленным условиям, из всех возможных комбинаций формируемых в регистре сдвига с сумматором по модулю два в обратной связи. Комбинации формируются путем сдвига содержимого  $m \times n$  — разрядного регистра сдвига, выходы которого объединены в  $n$ -групп по  $m$ -разрядов. Если комбинация не отвечает заданным требованиям осуществляется очередной сдвиг и новая проверка. За счет этого данный генератор обладает дополнительными возможностями, позволяющими получить комбинации чисел, обладающие определенными свойствами, в частности получать комбинации с однократными повторениями, причем имеется возможность легко изменять верхнюю границу ряда чисел без аппаратных изменений устройства.

На чертеже приведена функциональная схема генератора.

Генератор псевдослучайных чисел содержит блок 1 формирования равномерно распределенных случайных чисел, коммутатор 2, первую и вторую 3 и 4 схемы сравнения, счетчик 5, первый 6 и второй 7 элементы И, элемент ИЛИ 8, блок управления 9, генератор 10 тактовых импульсов, вход запуска 11, выход "готовность" 12. Первый выход генератора 10 соединен с первыми входами элементов 6 и 7, а второй выход — с входом синхронизации блока 9. Первый выход блока 9 связан с управляющим входом коммутатора 2, первый выход которого соединен с первым входом схемы 3, а второй выход — со вторым входом схемы 3 и с первым входом схемы 4. Второй вход последней является входом задания "верхнего граничного значения", а выход "больше" связан со вторым входом элемента 7, выход которого соеди-

нен с первым входом элемента 8, второй вход которого служит входом 11 запуска генератора 10. Выход элемента 8 связан с тактовым входом блока 1 и с входом "сброс" блока 9. Второй выход блока 9 подключен к второму входу элемента 6, третий вход которого связан с выходом "равно" схемы 3, а выход — со счетным входом счетчика 5, имеющего вход сброса от третьего выхода блока 9. Выход переполнения счетчика 5 подключен к третьему входу элемента 8. Четвертый выход блока 9 является выходом "готовность" генератора псевдослучайных чисел и соединен с входом "запрет" генератора 10.

Назначение генератора — одновременное получение  $n$  кодов ( $n$  двоичных чисел), содержащих  $m$  двоичных разрядов, причем общее число совпадающих кодов не должно превышать выбранного предельного значения  $N$ , а каждое число не должно быть больше заданной граничной величины  $A < 2^m$ .

Генератор работает следующим образом.

Сигнал со входа запуска 11 генератора поступает через элемент ИЛИ 8 на тактовый вход блока 1 формирования равномерно распределенных псевдослучайных чисел.

Указанный блок формирует очередное  $m \cdot n$  — разрядное двоичное число, рассматриваемое в дальнейшем как  $n$  кодов (чисел) по  $m$ -разрядов в каждом.

Запускающий сигнал попадает также на вход "сброс" блока управления 9, переводя его в начальное состояние.

При этом на четвертом выходе блока управления появляется нулевой сигнал, разрешающий работу генератора тактовых импульсов, а на третьем выходе блока управления — сигнал, осуществляющий сброс счетчика 5 в исходное нулевое состояние.

Одновременно сигнал с первого выхода блока управления обеспечивает подачу первого  $m$  разрядного числа  $a_1$  с блока 1 на второй выход коммутатора 2.

Это число сравнивается во второй схеме сравнения 4 с заданной граничной величиной  $A_{гр}$ .

Если  $a_1 \leq A_{гр}$ , то сигнал на выходе схемы сравнения 4 не появляется, вследствие чего блок управления синхронно с тактовыми импульсами, поступающими со второго выхода генератора тактовых импульсов, вырабатывает на своем первом выходе последовательность  $K$  — разрядных сигналов ( $K$  — удовлетворяет условию  $2^K \geq \frac{n(n+1)}{2}$ ).

Эти сигналы осуществляют управление коммутатором 2, обеспечивая следующий порядок коммутации:

— в течение первых  $(n-1)$  тактов на первый вход коммутатора 2 поступает первое число  $a_1$  на второй выход — поочередно  $a_2, a_3, \dots, a_n$ ;

— в течение последующих  $(n-2)$  тактов на первый вход коммутатора 2 поступает второе число  $a_2$ , на второй выход поочередно  $a_3, a_4, \dots, a_n$  и т.д. вплоть до случая, когда на первом входе будет число  $a_{n-1}$ , а на втором  $a_n$ . Одновременно на первом такте появляется единичный сигнал, на втором такте блока управления, разрешающий подсчет числа совпадающих кодов счетчиком 5.

Поскольку второй выход коммутатора 2 соединен с первым входом второй схемы сравнения 4, то в течение указанных  $(n-1)$  тактов происходит последовательное сопоставление чисел  $a_2, a_3, \dots, a_n$  с  $A_{гр}$ . Первая схема сравнения осуществляет попарное сопоставление чисел  $a_i, i = 1, n$ , выдавая на своем выходе "равно" сигнал каждый раз, когда коды совпадают, т.е. если  $a_i = a_j$  ( $i < j$ ;  $i = 1, n-1, j = 2, n$ ).

Для проведения такого сопоставления требуется  $\frac{n(n-1)}{2}$  тактов.

Количество таких совпадений фиксируется счетчиком 5 синхронно с поступлением тактовых импульсов с первого выхода генератора 10 тактовых импульсов.

Коэффициент  $N$  пересчета счетчика 5 устанавливается предварительно исходя из предельно допустимого числа совпадающих кодов.

Если число совпадения оказывается больше  $n$ , на выходе переполнения счетчика 5 возникает сигнал, появляющийся затем на выходе элемента ИЛИ 8, схематичный сигнал возникает на элементе ИЛИ 8 и при первом же нарушении условия  $a_i \leq A_{гр}$  ( $i = 1, n$ ).

При  $a_i > A_{гр}$  появляется единичный сигнал на выходе "больше" второй схемы сравнения, а затем синхронно с тактовым импульсом и на выходе второго 7 элемента И.

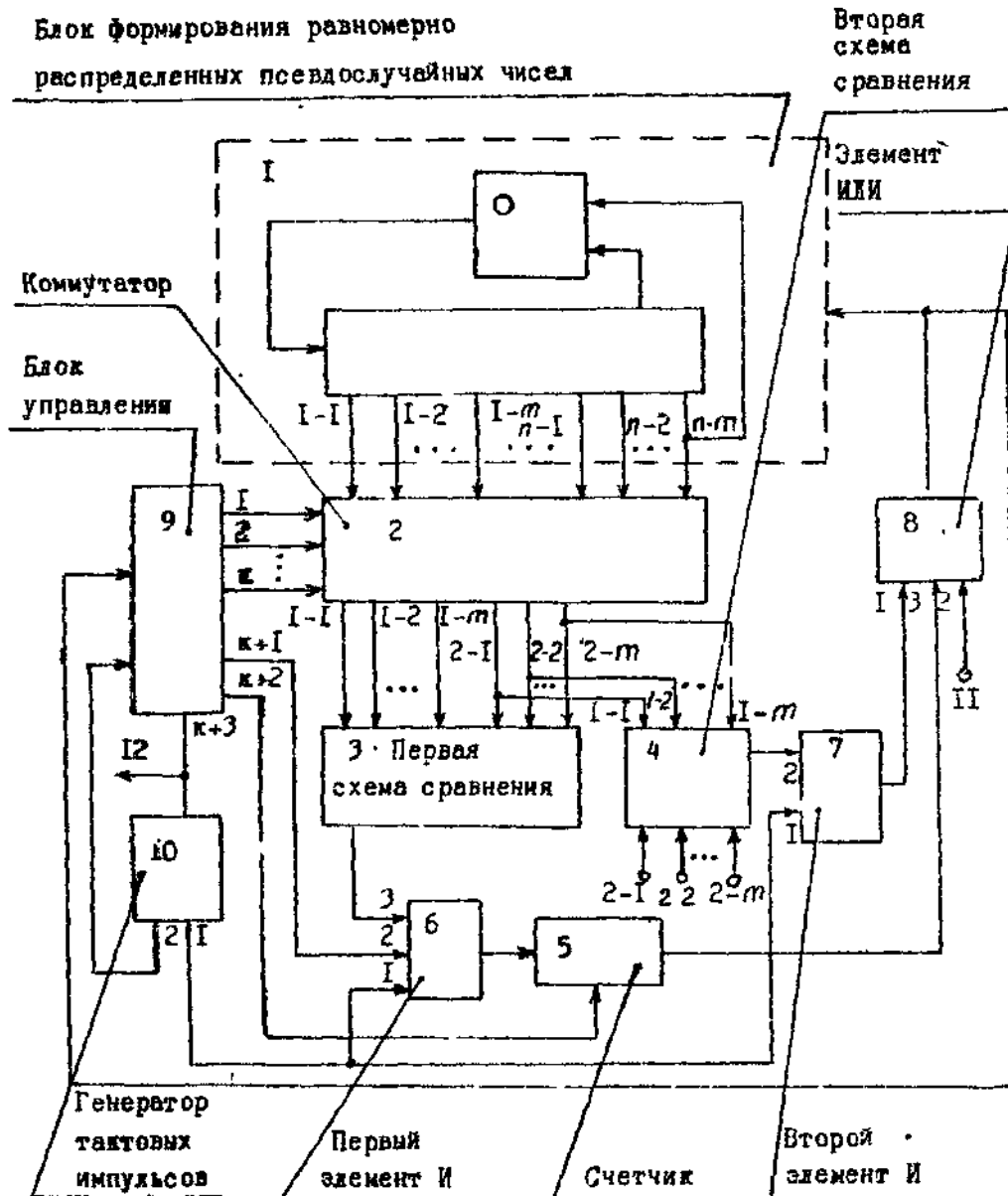
Появление сигнала на выходе элемента ИЛИ 8 означает, что сгенерированный набор кодов является неудовлетворительным, сигнал с выхода элемента ИЛИ 8 осуществляет перезапуск блока и сброс блока управления в исходное состояние, после чего осуществляется генерация очередного набора кодов и их последующая проверка.

Если же сигнал на выходе элемента ИЛИ 8 не появляется, то после завершения  $\frac{n(n-1)}{2}$  —го такта проверки заканчиваются и появляется единичный сигнал на четвертом выходе блока управления.

Этот сигнал разрешает работу генератора тактовых импульсов и служит сигналом "готовность", свидетельствующим о том, что на выходах блока 1 имеют место  $n$  двоичных

кодов псевдослучайных чисел по  $m$  разрядов  $8$  в каждом, причем число совпадающих кодов не превышает  $N$ , а каждое число не больше  $\text{Agr}$ .

5



Упорядник

Техред М.Моргентал

Коректор Н.Мілюкова

Замовлення 4501

Тираж  
Державне патентне відомство України,  
254655, ГСП, Київ-53, Львівська пл., 8

Підписне

Виробничо-видавничий комбінат "Патент", м. Ужгород, вул.Гагаріна, 101