(19) Евразийское патентное ведомство

(11) 043721 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.06.16

(21) Номер заявки
202200167

(22) Дата подачи заявки
2021.01.18

(51) Int. Cl. ***G06F 7/58*** (2006.01)

(54) ГЕНЕРАТОР ИСТИННО СЛУЧАЙНЫХ ЧИСЕЛ

(43) **2023.03.17**
(86) **PCT/RU2021/050010**
(87) **WO 2021/162586 2021.08.19**

(71)(73) Заявитель и патентовладелец:
ФИЗТЕХ ТЕХНОЛОДЖИЗ ТРУ РЭНДОМ АГ (CH)

(72) Изобретатель:
Гончаров Сергей Владимирович (CY)

(74) Представитель:
Суюндуков М.Ж. (KZ)

(56) WO-A1-2019222866
CN-A-107943451
US-A1-20090327381
US-B1-7389316

(57) Изобретение относится к устройствам для генерации истинно случайных чисел, включающих в себя цифровую хаотически осциллирующую автономную булеву сеть в качестве источника энтропии. Согласно изобретению цифровая хаотически осциллирующая автономная булева сеть состоит из трёх логических элементов, соединённых друг с другом, два из которых являются двухвходовыми логическими элементами "исключающее или" и/или "исключающее или-не", а третий логический элемент имеет три входа и один выход и реализует специальную логическую функцию "счёт единиц", при которой на его выходе устанавливается логическая единица, если не более чем на одном из его входов присутствует логическая единица, в противном случае устанавливается логический ноль. Достигаемый технический результат - увеличение скорости генерации истинно случайных чисел при снижении потребляемой энергии.

043721 B1

043721 B1

Область техники, к которой относится изобретение

Изобретение относится к устройствам для генерации истинно случайных чисел, включающих в себя цифровую хаотически осциллирующую автономную булеву сеть в качестве источника энтропии.

В данном описании используются следующие аббревиатуры:

ГСЧ - генератор случайных чисел;

ГПСЧ - генератор псевдослучайных чисел;

ПЛИС - программируемая логическая интегральная микросхема;

АБС - автономная булева сеть;

СХО - синхронный хаотический осциллятор;

СБИС - сверхбольшая интегральная схема;

ASIC - application specific integrated circuit (интегральная схема специального назначения).

Уровень техники

Из существующего уровня техники известны цифровые генераторы псевдослучайных чисел (ГПСЧ), основанные на какой-либо циклической функции, например, линейный конгруэнтный генератор, генератор на регистре сдвига с линейной обратной связью, на регистре сдвига с обобщенной обратной связью, вихрь Мерсенна. Самые лучшие результаты получаются при использовании простого счётчика чисел, последовательно соединённого с криптографическим алгоритмом, например, с блочным шифром или односторонней хэш-функцией.

Общим недостатком всех ГПСЧ является детерминизм полученной последовательности, что исключает, либо сильно затрудняет использование псевдослучайных чисел в криптографических целях, так как вся цепочка псевдослучайных чисел может быть предсказана, если известен алгоритм работы устройства и начальное, либо любое предыдущее состояние такого генератора. Также все эти методы являются вычислительно затратными, причём, чем большие требования предъявляются к качеству случайных чисел, тем больше вычислений необходимо совершить.

Известны генераторы истинно случайных чисел, основанных на специфических физических принципах. Исторически использовались игральные кости, радиоактивный распад, оцифровка через микрофон окружающего акустического шума, атмосферные шумы, уловленные радиоприёмником, и другие случайные физические явления.

Недостатком этих устройств является необходимость использования специальной физической установки, датчика или преобразователя и компьютерного интерфейса. Кроме того, работа таких устройств может сильно зависеть от окружающих условий, они требуют много энергии, а скорость генерации случайных чисел зачастую слишком мала.

Известны генераторы, основанные на физических принципах и при этом использующие только электронные компоненты. Например, установка ERNIE 1 и компьютер Ferranti Mark 1 использовали тепловой шум резистора. Часто применяются генераторы, использующие лавинный пробой обратно смещённого p-n перехода в диоде Зенера [1].

Недостатком таких устройств является необходимость изготовления отдельной аналоговой части прибора, что исключает или серьезно затрудняет изготовление цифровых интегральных микросхем (СБИС), содержащих ГСЧ. Такой генератор также невозможно реализовать в программируемой логической интегральной микросхеме (ПЛИС).

Известны ГСЧ, использующие разницу в частоте двух осцилляторов, обусловленную тепловым дрейфом. Например, микросхема хранения микропрограмм Intel 82802 имеет два осциллятора, - быстрый и медленный, -расположенные в разных частях кристалла, и замеряет разницу в их частоте. Такой ГСЧ возможно реализовать целиком средствами цифровой логики, поскольку в качестве осциллятора, как правило, используют инверторы с обратной связью и цепочкой буферных элементов в качестве линии задержки.

Недостатками таких генераторов являются необходимость размещения осцилляторов далеко друг от друга в топологии кристалла, чтобы снизить тепловую корреляцию между ними, низкая производительность, поскольку необходимо накапливать дрейф в течение некоторого времени работы, плохая предсказуемость качества случайных чисел. Также такой генератор практически затруднительно реализовать в ПЛИС, поскольку средства разработки не позволяют управлять физическим размещением элементов и, как правило, при автоматическом размещении, осцилляторы, будучи логически связанными, будут также расположены в непосредственной близости друг от друга, что влечёт большую корреляцию частоты между ними.

Последние несколько лет активно исследуются так называемые "автономные булевы сети" (АБС). Такая сеть представляет собой топологически связный граф логических элементов, на который извне не подаются никакие управляющие или тактовые сигналы. При этом на такую сеть накладываются очевидные дополнительные требования: ни у одного элемента не должно быть "висящих" (не подключённых ни к какому выходу) входов и никакие два выхода не должны быть связаны друг с другом. Эти требования обусловлены определённостью состояния логических элементов сети и электрической безопасностью её работы. В зависимости от топологии АБС может демонстрировать разное поведение: находиться в стабильном или квазистабильном состоянии, осциллировать с определённой частотой и формой сигнала,

либо находиться в состоянии так называемого "булева хаоса". Примером простейшей АБС является повторитель с выходом, подключённым ко входу. Такая сеть находится в квазистабильном состоянии: в зависимости от начального состояния, - 0 или 1, - она будет находиться в нём бесконечно долго. Другим примером является один или несколько инверторов, связанных друг с другом в кольцо. В зависимости от количества инверторов в кольце их поведение будет стабильным, квазистабильным или осциллирующим. Один инвертор, скорей всего, будет находиться в стабильном состоянии, промежуточном между 0 и 1, - это обусловлено физической реализацией инвертора как усилителя с большим коэффициентом усиления и отрицательной обратной связью, равной 1. По этой же причине возможно отсутствие генерации в очень маленьких сетях с элементами с малой скоростью нарастания выходного сигнала. При нечётном количестве инверторов сеть будет осциллировать с периодом, пропорциональным количеству инверторов. При чётном количестве инверторов сеть находится в квазистабильном состоянии. Отсюда видно, что генератор случайных чисел, реализованный в микросхеме Intel 82802 на двух осцилляторах и измерении дрейфа частоты между ними, по сути, является частным случаем АБС - в нём использованы два кольца с разным нечётным количеством инверторов. Более сложные сети часто могут порождать хаотическое поведение.

Есть прямая физическая аналогия по существу, которая помогает наглядно понять поведение АБС в различных ситуациях. Это - маятник. Простой маятник, будучи отклонённым и отпущенным, начинает колебаться со стабильным периодом - это осциллирующее поведение. Если мы перевернём маятник вверх, то верхняя точка представляет собой квазистабильное состояние, при любом малом отклонении маятник упадёт влево или вправо. Если же разделить плечо маятника на две части, соединённые шарниром, то получится так называемый хаотический маятник, эволюцию которого во времени невозможно точно предсказать, поскольку любое бесконечно малое изменение начального состояния (вплоть до квантового уровня) со временем усиливается и приводит к произвольно большим изменениям в поведении маятника. По этой аналогии можно замерять случайные отклонения в частоте двух маятников, возникающие из-за хаотических внешних воздействий, но это потребует длительного анализа, а можно отклонить хаотический маятник и в кратчайшее время получить случайную величину.

Из приведённого примера видно, что для генерации случайных чисел действительно можно использовать осциллирующие АБС, но гораздо более перспективными являются АБС, изначально проявляющие хаотическое поведение. Скорость наступления булева хаоса и его качественные характеристики определяются рядом факторов, и важнейшим из всех является характеристическая экспонента Ляпунова. Если её показатель отрицателен, то отклонения со временем затухают. Если больше нуля, то случайные отклонения усиливаются системой. При равенстве нулю отклонения не затухают и не усиливаются, но накапливаются, если попадают в систему извне. Для быстрой физической генерации случайных чисел показатель должен быть неотрицательным. Простой маятник имеет отрицательный показатель экспоненты Ляпунова, что выражается в том, что частота колебаний мгновенно стабилизируется при отсутствии внешних воздействий. Хаотический маятник является частным примером системы с положительным показателем, так что любое малое воздействие приводит к совершенно другой динамике уже через короткое время. В двоичной логике не существует логических функций, которые усиливали бы малые отклонения, но существуют функции, которые не позволяют возникающим изменениям исчезать, - для случая двух аргументов это функции XOR (исключающее "или") и XNOR (эквивалентность). Любое изменение любого входного сигнала в них вызывает изменение выходного сигнала, по этой причине использование этих функций предпочтительно в ГСЧ.

Из текущего состояния науки известны схемы АБС, которые демонстрируют хаотическое поведение. Хаос возникает в условиях, когда работа сети определяется мельчайшими отклонениями в питающем напряжении, сдвигам фронтов из-за тепловых флуктуаций, наводок и других дестабилизирующих факторов. В литературе [3] рассматриваются двух- и трёхвходовые логические элементы XOR или XNOR, в которых выход заведен обратно на входы через две (или, соответственно, три) линии задержки. В таких сетях при определённом соотношении длин линий задержки может наблюдаться хаотическое поведение. Проблемой данной сети является сильная зависимость поведения не только от соотношения длин линий задержки, но и от их физической реализации, при этом вместо хаоса могут возникать осцилляции. Также, несмотря на кажущуюся схематическую простоту устройства, она требует большого количества логических элементов, так как каждая линия задержки - это цепочка инверторов. В результате простая на вид схема может содержать несколько десятков элементов. Более того, у трёх из четырёх вариантов такого генератора есть фундаментальный недостаток - пропадание генерации через некоторое время. Элемент XOR, независимо от количества входов, приходит в стабильное состояние с нулём на выходе, а элемент XNOR с двумя входами - с единицей на выходе. Элемент XOR с тремя входами имеет дополнительное стабильное состояние - с единицей на выходе. В работе [4] показано, что более-менее стабильная генерация наблюдается с трёхвходовым элементом XNOR и линиями задержки из 18, 6 и 2 инверторов.

Руи Жанг (Rui Zhang et al.) в 2009 году предложил [2] схему из трёх двухвходовых логических элементов, в которой возникает булев хаос, - двух элементов XOR и одного XNOR. Для реализации схемы он использовал дискретные элементы. Такая схема также обладает внутренне присущими недостатками,

которые далее будут рассмотрены. При реализации такой сети в ПЛИС генерация может пропадать или вместо случайного поведения могут возникать осцилляции.

В своей диссертации [4] Дэвид Розин (David Rosin) предложил более сложную схему, также демонстрирующую хаотическое поведение - большие кольца трёхвходовых элементов XOR, в которых каждый элемент получает на вход сигнал от самого себя и от двух ближайших соседей. При этом результирующий сигнал снимается с нескольких точек кольца и также объединяется через элементы XOR. Однако в чистом виде такая схема неработоспособна, поскольку кольца с чётным количеством элементов имеют целых четыре разных стабильных состояния, и неизбежно стабилизируются в одном из них: это состояния со всеми нулями, всеми единицами и два варианта чередования нулей и единиц.

Для устранения стабильного состояния Розин заменяет в генераторе один элемент XOR на элемент XNOR. Качество возникающего хаоса в таком генераторе зависит от количества логических элементов в кольце. Розин предлагает использовать 16 элементов. Однако возбуждение, возникшее в такой системе, должно пройти через восемь логических элементов, прежде чем дойдёт до противоположной стороны кольца, что по времени сопоставимо с одним тактом микропроцессора. Следовательно, при аппаратной реализации желательно ждать несколько тактов, чтобы исключить корреляцию между последовательными значениями. Недостатком как генератора Розина, так и генератора Жанга является невозможность дестабилизирующего внешнего воздействия на сеть.

Из уровня техники известен генератор истинно случайных чисел, включающий в себя цифровую хаотически осциллирующую автономную булеву сеть в качестве источника энтропии, см. описание заявки на патент на изобретение WO 2019222866, опубликованный в 2019 году. Как и в генераторе Розина, в этом генераторе используется кольцо из трёх элементов XOR и одного элемента XNOR, и элемент XOR для сбора сигналов с кольца. В отличие от генератора Розина, этот генератор использует дополнительный инвертор для генерации высокочастотного периодического сигнала и дестабилизации автономной булевой сети.

Данное устройство является наиболее близким по технической сути и достигаемому техническому результату и выбрано в качестве прототипа предлагаемого изобретения.

Недостатком этого прототипа также является то, что он производит генерацию истинно случайных чисел длительное время, содержит много элементов и потребляет много энергии.

Раскрытие изобретения

Опирающееся на это оригинальное наблюдение, настоящее изобретение, главным образом, имеет целью предложить генератор истинно случайных чисел, включающий в себя цифровую хаотически осциллирующую автономную булеву сеть в качестве источника энтропии, позволяющий, по меньшей мере, сгладить, как минимум, один из указанных выше недостатков, а именно обеспечить увеличение скорости генерации истинно случайных чисел при снижении потребляемой энергии, что и является поставленной задачей.

Целью данного изобретения является построение такой частично управляемой АБС, которая при минимальном размере гарантированно и с наибольшей возможной скоростью приходит в состояние булева хаоса. Наиболее важным требованием является невозможность стабильного, квазистабильного или осциллирующего состояния сети. Далее, скорость возрастания хаоса напрямую зависит от размера имеющихся в сети циклических путей распространения сигнала, Чем больше размер пути, тем дольше должен распространяться по ней сигнал, чтобы вернуться в исходную точку, следовательно, сеть должна иметь как можно меньший размер. Это очевидно из рассмотрения осциллятора, состоящего из нечётного количества инверторов, - период осцилляций прямо пропорционален длине кольца.

Для дальнейшего анализа лучше рассматривать синхронную булеву сеть. Фактическое отличие синхронной булевой сети от АБС состоит в том, что сигнал на выводах всех логических элементов изменяется одновременно, поэтому можно считать, что сеть проходит через ряд состояний. Теоретически, при абсолютно одинаковой скорости работы элементов, одинаковой длине всех проводников и идентичных условий работы элементов, АБС становится синхронной булевой сетью. Более того, в работе [3] показано, что взаимное влияние разных фрагментов сети может приводить к их принудительной синхронизации. Это очень важный эффект, который также необходимо исключить или минимизировать. Поскольку ищется минимальная возможная сеть, их можно анализировать в порядке увеличения количества логических элементов. Так как множество возможных логических функций и сетей на их основе является счётным и упорядоченным, можно провести исчерпывающий анализ.

Сеть с одним элементом может состоять из одного повторителя или одного инвертора. В первом случае нет никакой генерации, во втором случае мы имеем периодические осцилляции. Поэтому сеть из одного логического элемента не может генерировать хаос.

Рассмотрим сеть с двумя элементами. Каждый элемент может содержать не более двух входов, и всего возможны четыре разных состояния сети. Возможно большое количество сочетаний переходов между этими состояниями, но их можно сгруппировать по свойствам. Первая категория - когда имеется одно вырожденное состояние, в котором сеть находится бесконечно долго. Они, очевидно, непригодны. Вторая категория - когда присутствует как минимум один цикл из двух или трёх состояний. В этом случае один элемент находится в стабильном состоянии, а второй осциллирует, либо оба осциллируют с

одинаковым периодом. Такие сети также непригодны. Последний возможный случай - когда сеть эволюционирует через все четыре состояния. Таких разных циклов всего 3! = 6. Перебор всех вариантов показывает, что при этом один элемент осциллирует с периодом T, а другой 2T, либо оба элемента осциллируют с одинаковым периодом 2T. Поэтому сеть из двух элементов не может быть надёжным источником хаоса.

Таким образом, для хаотического поведения требуется сеть не менее чем из трёх элементов. В обобщённом случае; это должны быть двух- или трёхвходовые элементы, так как наличие одновходового элемента превращает сеть в сеть с двумя элементами. Соответственно, сеть в каждый момент времени может находиться в одном из восьми разных состояний. Генератор Жанга как раз относится к сетям из трёх элементов. Однако анализ графа смены состояний генератора Жанга показывает, что при любом начальном состоянии он приходит в цикл из четырёх состояний, в котором один элемент осциллирует с периодом в T, остальные два элемента с периодом в 2T. Конечно, этот факт не исключает наступления хаоса, однако свидетельствует о чувствительности сети к реализации и к перекрёстному влиянию элементов друг на друга.

Для поиска необходимой сети сразу можно отбросить все сети с наличием стабильного состояния. Также сразу исключаются все сети, в которых цикл имеет меньше восьми состояний, поскольку в таких сетях возможны осцилляции и перекрёстное влияние. Остаются только сети, эволюционирующие через все восемь состояний. Всего возможно 7! = 5040 разных циклов, начинающихся состоянием 000, проходящих через все возможные состояния и через восемь итераций возвращающихся к состоянию 000.

Для дальнейшего рассмотрения необходимо ввести понятие автокорреляции выходного сигнала логического элемента. В процессе эволюции сети выход каждого элемента циклически проходит через восемь состояний, которые мы можем обозначить через восьмизначное двоичное число, например, 01010101b. Для расчёта автокорреляции мы семь раз циклически сдвигаем это число на один бит (переносим младший бит в старшую позицию) и каждый раз считаем количество совпадений бит с исходным значением в соответствующих позициях. Если при сопоставлении мы получили, что все восемь позиций отличаются, то такой сигнал коррелирует столь же хорошо, как и при совпадении во всех восьми позициях. Минимальной корреляцией будет случай с четырьмя совпадениями и четырьмя отличиями. Полную корреляцию определим как сумму семи модулей разности количества совпадений и 4, делённую пополам, так как такая сумма всегда четна.

Для некоторых последовательностей действительно возможна автокорреляция равная нулю. Однако в таких последовательностях количество нулей и единиц отличается, а в случае сети, проходящей полный цикл из всех восьми состояний, каждый элемент должен иметь на выходе одинаковое количество состояний с единицами и с нулями. Среди всех таких последовательностей минимальная возможная автокорреляция равна двум. Всего существует только четыре фундаментальных последовательности с такой автокорреляцией: 00010111b, 00011011b, 00100111b, 00101011b, все остальные последовательности с минимальной возможной автокорреляций являются производными от них циклическим сдвигом и инверсией.

Для сети из трёх элементов минимальная теоретически возможная суммарная автокорреляция равна 6, а максимальная 26. Трёхразрядный двоичный счётчик обладает автокорреляцией 18, а при реализации соответствующей ему АБС в ней никогда не возникает хаотическое поведение.

Всего существует 648 топологически разных сетей, проходящих полный цикл из всех восьми состояний. Среди них 216 сетей имеют минимальную возможную суммарную автокорреляцию - 6. Из этих сетей необходимо отбросить такие, у которых сигнал на выходах двух разных элементов коррелирует друг с другом, в этих сетях теоретически возможна фазовая подстройка работы элементов, что приведёт к упорядочиванию сигнала. Существуют даже такие сети, в которых коррелирует друг с другом сигнал на всех трёх элементах, такие сети особенно опасны. Среди отобранных сетей только у 80 отсутствует корреляция между сигналами элементов. Поскольку мы ищем минимальную возможную сеть, то отдадим предпочтение сетям, имеющим двухвходовые элементы. Таких сетей только 24.

Есть ещё одно важное обстоятельство для предпочтения двухвходовых элементов. Все рассмотренные ранее генераторы неуправляемы, в том смысле, что к ним нельзя подключить внешний дестабилизирующий сигнал, форсирующий наступление хаоса и позволяющий каскадировать сети друг с другом. Добавление дополнительного входа должно превращать одну сеть в другую, также полностью удовлетворяющую указанным критериям. Это проще всего сделать, добавив третий вход к двухвходовым элементам. Поскольку двухвходовые элементы могут быть только XOR или XNOR, добавление нового входа возможно только с получением трёхвходовых элементов XOR и XNOR. При этом при подаче логической единицы на третий вход происходит взаимное превращение двухвходовых элементов XOR и XNOR.

Оказывается, что из двадцати четырёх оставшихся сетей только восемь могут быть перестроены таким образом с изменением характера генерации и сохранением всех основных характеристик. Более того, эти сети одновременно обладают рекордно низким уровнем сложности, - каждая такая сеть имеет по два двухвходовых элемента. Все эти восемь сетей попарно группируются в четыре перестраиваемые сети, каждая из которых состоит из трёх трёхвходовых логических элементов. Каждая перестраиваемая

сеть соответствует двум исходным сетям. Эти четыре сети функционально полностью эквивалентны, но среди них одна сеть обладает уникальным свойством - все её логические элементы симметричны относительно назначения входов (входы элементов эквивалентны), что упрощает реализацию сети и позволяет избежать ошибок.

Сущностью изобретения являются эти четыре булевых сети, удовлетворяющие всем перечисленным ранее требованиям и имеющие дополнительное свойство модуляции. Все они состоят из трёх логических элементов, - двух элементов 3-XOR или 3-XNOR, и одного выходного трёхвходового элемента с более сложной, специальной функцией, называемой "счёт единиц". Эти четыре сети по способу соединения элементов друг с другом абсолютно одинаковы и отличаются только типом используемых элементов. Они объединяются в две группы - "A" и "B". В группе "A" используются одинаковые элементы, оба 3-XOR или оба 3-XNOR, в группе "B" - разные, один 3-XOR, другой 3-XNOR. Логическая схема всех этих сетей изображена на фигурах, прилагаемых далее.

Элемент "счёт единиц" можно описать так: на выходе элемента устанавливается 1, если не более чем на одном входе присутствует 1, в противном случае на выходе 0. Таким образом, если на трёх входах - ноль, то на выходе тоже логическая единица. См. таблицу.

Таблица истинности третьего логического элемента "счёт единиц"

Вход 3	Вход 2	Вход 1	Выход
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

В зависимости от варианта сети один или два входа этого элемента могут быть инвертированы. На вход элемента "счёт единиц" подаются сигналы со всех трёх логических элементов. На два входа первого элемента XOR/XNOR подаётся сигнал с него же и с другого элемента XOR/XNOR. На два входа второго элемента XOR/XNOR подаётся сигнал с первого элемента XOR/XNOR и с выхода элемента "счёт единиц". Оставшиеся свободные входы обоих элементов XOR/XNOR объединяются вместе и представляют собой модуляционный вход булевой сети.

Каждая из описанных булевых сетей является базовым блоком, на котором строится генератор случайных чисел. Назовём этот базовый блок "хаотическим осциллятором". У него есть выход и модуляционный вход. Хаотический осциллятор не может модулировать сам себя. Легко проверить, что при такой модуляции хаотический осциллятор вырождается либо в обычный осциллятор, либо в источник стабильного уровня. Также хаотический осциллятор не рекомендуется оставлять без модуляции вообще, поскольку в силу особенностей физической реализации поведение двух осцилляторов без модуляции может серьёзно отличаться. Желательно использовать блок осцилляторов, модулирующих друг друга, причём, желательно, чтобы петля, образуемая модуляцией, была как можно больше для уменьшения взаимной корреляции осцилляторов.

В теории сигнал немодулированного осциллятора можно снимать с любого из трёх логических элементов, однако для уменьшения взаимной корреляции сигнала с разных осцилляторов хаотический сигнал необходимо снимать с элемента "счёт единиц".

Автономная булева сеть всегда находится в состоянии хаотической осцилляции и при этом потребляет энергию. Чтобы остановить генерацию, надо изменить сеть так, чтобы при любом начальном состоянии она гарантированно приходила в единственно возможное детерминированное состояние. Для указанных сетей этого невозможно добиться выключением только одного логического элемента. Необходимо выключить как минимум два элемента и в наилучшем случае это те же входные элементы XOR или XNOR. Сеть можно выключать принудительным переводом выходов этих элементов как в 0, так и в 1. При этом если на выходах элементов XOR/XNOR устанавливается 0, то на выходе сети будет 1, и наоборот.

Сам по себе хаотический осциллятор нельзя использовать в качестве генератора случайных чисел, так как он имеет только асинхронный выход, на котором присутствует широкополосный хаотический аналоговый сигнал. Каждый хаотический осциллятор, независимо от его внутренней структуры, необходимо поместить в синхронную "обёртку", которая выполняет сразу две функции. С одной стороны, она обеспечивает стабильный выходной логический сигнал, с другой стороны, хранит предыдущее состояние, которое при желании можно использовать через модуляционные входы в качестве "посева" для получения следующего случайного числа. Обозначение и внутренняя схема такого синхронного хаотического осциллятора (СХО) приведены на фигурах далее.

СХО имеет тактовый и модуляционный входы и два выхода - синхронный, используемый для получения случайного числа, и асинхронный, необходимый для модуляции других СХО. По каждому фронту

тактового сигнала D-триггер фиксирует значение асинхронного сигнала. Полученное значение с одной стороны подаётся на синхронный выход, с другой стороны, может использоваться для модуляции совместно с внешним сигналом при помощи двухвходового элемента XOR. Генератор случайных чисел строится на таких блоках СХО.

Несмотря на взаимную модуляцию, блоки СХО могут обладать смещением распределения между количеством нулей и единиц на выходе, т.е. появление на выходе одного типа величин более вероятно, чем другого. Это также обусловлено особенностями физической работы логических элементов схемы. Для устранения этого смещения может потребоваться процедура так называемого "отбеливания" полученных случайных чисел.

Таким образом, сутью изобретения является то, что цифровая хаотически осциллирующая автономная булева сеть включает в себя три логических элемента, соединённые друг с другом, два из которых являются двухвходовыми логическими элементами "исключающее или" и/или "исключающее или-не", а третий логический элемент имеет три входа и один выход и реализует специальную логическую функцию "счёт единиц", при которой на его выходе устанавливается логическая единица, если не более чем на одном из его входов присутствует логическая единица, в противном случае устанавливается логический ноль.

Благодаря данным выгодным характеристикам появляется возможность получать истинно случайные числа за очень короткое время с использованием генератора, состоящего всего из трёх элементов.

Существует преимущественный вариант исполнения устройства, при котором выход первого двухвходового логического элемента соединен с первым входом второго двухвходового логического элемента и со вторым входом третьего логического элемента "счёт единиц", выход второго двухвходового логического элемента соединен с его вторым входом, со вторым входом первого двухвходового логического элемента и с третьим входом третьего логического элемента "счёт единиц", а выход третьего логического элемента "счёт единиц" соединен с его первым входом, с первым входом первого двухвходового логического элемента и с выходом всей сети.

Благодаря данным выгодным характеристикам появляется возможность гарантировать хаотическое поведение автономной булевой сети, являющейся основной генератора истинно случайных чисел.

Существует ещё один вариант исполнения устройства, при котором второй и/или третий входы третьего логического элемента "счёт единиц" инвертированы.

Благодаря данным выгодным характеристикам появляется возможность конкретной реализации генератора истинно случайных чисел.

Существует также вариант исполнения устройства, при котором оба двухвходовых логических элемента "исключающее или" и/или "исключающее или-не" имеют дополнительные третьи логические входы, которые объединены вместе и подключены к дополнительному входу внешней модуляции цифровой хаотически осциллирующей автономной булевой сети.

Благодаря данным выгодным характеристикам появляется возможность улучшения статистических свойств генератора истинно случайных чисел.

Существует, кроме того, вариант исполнения устройства, при котором генератор имеет вход выключения, а оба логических элемента "исключающее или" и/или "исключающее или-не" имеют дополнительные входы выключения с возможностью принудительного перевода выхода обоих указанных логических элементов в состояние логического нуля либо логической единицы независимо от состояния остальных входов, причём эти входы объединены вместе и подключены к указанному входу выключения генератора.

Благодаря данным выгодным характеристикам появляется возможность включать и выключать генератор истинно случайных чисел.

Существует также вариант исполнения устройства, при котором цифровая хаотически осциллирующая автономная булева сеть объединена с D-триггером в блок синхронного хаотического осциллятора, имеющий тактовый вход, подключённый к тактовому входу D-триггера, вход модуляции, подключённый ко входу модуляции автономной булевой сети, асинхронный выход, подключённый к выходу автономной булевой сети, синхронный выход, подключённый к выходу D-триггера, при этом выход автономной булевой сети подключен ко входу данных D-триггера.

Благодаря данным выгодным характеристикам появляется возможность подключения генератора истинно случайных чисел к внешним тактируемым схемам.

Существует кроме того вариант исполнения устройства, при котором включает в себя дополнительный двухвходовой элемент "исключающее или" и/или "исключающее или-не", первый вход которого подключён ко входу внешней модуляции, второй вход которого подключён к выходу D-триггера, а выход подключён ко входу модуляции автономной булевой сети.

Благодаря данным выгодным характеристикам появляется возможность улучшения статистических свойств генератора истинно случайных чисел за счёт изменения его начального состояния.

Наконец, существует вариант исполнения устройства, при котором оно включает в себя множество из N блоков синхронных хаотических осцилляторов, объединённых в кольцевую структуру, тактовые входы которых объединены вместе и подключены к общему тактовому сигналу, а их синхронные выхо-

ды подключены к N-битному выходу генератора, и множество из N дополнительных двухвходовых элементов "исключающее или" и/или "исключающее или-не", таких, что выход каждого из указанных логических элементов подключён ко входу модуляции соответствующего ему блока синхронного хаотического осциллятора, его первый вход подключён к асинхронному выходу предыдущего в цепочке блока синхронного хаотического осциллятора, а второй вход подключён к асинхронному выходу последующего в цепочке блока синхронного хаотического осциллятора.

Благодаря данным выгодным характеристикам появляется возможность генерировать многобитные истинно случайные числа.

Совокупность существенных признаков предлагаемого изобретения неизвестна из уровня техники для способов аналогичного назначения, что позволяет сделать вывод о соответствии критерию "новизна" для изобретения в отношении способа. Кроме того, данное решение неочевидно для специалиста в данной области.

Краткое описание фигур

Другие отличительные признаки и преимущества данного изобретения ясно вытекают из описания, приведённого ниже для иллюстрации и не являющегося ограничительным, со ссылками на прилагаемые рисунки, на которых:

фиг. 1 изображает функциональную схему автономной булевой сети, согласно изобретению,

фиг. 2 изображает логическую схему автономной булевой сети с использованием элементов XOR, согласно изобретению,

фиг. 3 изображает логическую схему автономной булевой сети с использованием элементов XNOR, согласно изобретению,

фиг. 4 изображает логическую схему автономной булевой сети с использованием элементов XOR и инверсией входа элемента "счёт единиц", согласно изобретению,

фиг. 5 изображает логическую схему автономной булевой сети с использованием элементов XNOR и инверсией входа элемента "счёт единиц", согласно изобретению,

фиг. 6 изображает логическую схему автономной булевой сети с использованием элементов XOR и XNOR, согласно изобретению,

фиг. 7 изображает логическую схему автономной булевой сети с использованием элементов XNOR и XOR, согласно изобретению,

фиг. 8 изображает логическую схему автономной булевой сети с использованием элементов XOR и XNOR и инверсией входов элемента "счёт единиц", согласно изобретению,

фиг. 9 изображает логическую схему автономной булевой сети с использованием элементов XNOR и XOR и инверсией входов элемента "счёт единиц", согласно изобретению,

фиг. 10 изображает логическую схему автономной булевой сети со входом модуляции, согласно изобретению,

фиг. 11 изображает логическую схему автономной булевой сети со входом модуляции и разрешением генерации, согласно изобретению,

фиг. 12 изображает построение синхронного хаотического осциллятора на основе описанных булевых сетей, согласно изобретению,

фиг. 13 изображает обозначение синхронного хаотического осциллятора, согласно изобретению,

фиг. 14 изображает вариант синхронного хаотического осциллятора с использованием предыдущего значения в качестве посева, согласно изобретению,

фиг. 15 изображает схему генератора случайных чисел на основе синхронного хаотического осциллятора, согласно изобретению.

На фигурах обозначены:

1 - первый логический элемент;

2 - второй логический элемент;

3 - третий логический элемент;

4 - логический элемент XOR;

5 - логический элемент XNOR;

6 - синхронный хаотический осциллятор;

7 - хаотический осциллятор;

8 - D-триггер;

Modulation - вход модуляции;

Enable - вход разрешения генерации;

Out - выход;

Sync out - синхронный выход;

Async out - асинхронный выход;

Clock - тактовый сигнал.

Согласно фигурам 1-15 генератор истинно случайных чисел, включающий в себя цифровую хаотически осциллирующую автономную булеву сеть в качестве источника энтропии, включает в себя следующее. Цифровая хаотически осциллирующая автономная булева сеть включает в себя три логических

элемента 1 - первый, 2 - второй, и 3 - третий, соединённые друг с другом, два из которых 1 и 2 являются двухвходовыми логическими элементами "исключающее или" и/или "исключающее или-не", а третий логический элемент 3 имеет три входа (входы всех логических элементов обозначены римскими цифрами I, II и III) и один выход.

Логический элемент 3 реализует специальную логическую функцию "счёт единиц", при которой на его выходе устанавливается логическая единица, если не более чем на одном из его входов присутствует логическая единица, в противном случае устанавливается логический ноль.

Преимущественно выход первого двухвходового логического элемента 1 соединен с первым входом второго двухвходового логического элемента 2 и со вторым входом третьего логического элемента "счёт единиц" 3. Выход второго двухвходового логического элемента 2 соединен с его вторым входом, со вторым входом первого двухвходового логического элемента 1 и с третьим входом третьего логического элемента "счёт единиц" 3. Выход третьего логического элемента "счёт единиц" 3 соединен с его первым входом, с первым входом первого двухвходового логического элемента 1 и с выходом всей сети.

Второй и/или третий входы третьего логического элемента "счёт единиц" 3 могут быть инвертированы.

В частном варианте реализации изобретения оба двухвходовых логических элемента 1 и 2 ("исключающее или" и/или "исключающее или-не") имеют дополнительные третьи логические входы, которые объединены вместе и подключены к дополнительному входу внешней модуляции цифровой хаотически осциллирующей автономной булевой сети. См. фиг. 10.

В частном варианте реализации изобретения генератор имеет вход выключения, а оба логических элемента "исключающее или" и/или "исключающее или-не" имеют дополнительные входы выключения с возможностью принудительного перевода выхода обоих указанных логических элементов в состояние логического нуля либо логической единицы независимо от состояния остальных входов, причём эти входы объединены вместе и подключены к указанному входу выключения генератора. См. фиг. 11.

В частности, цифровая хаотически осциллирующая автономная булева сеть может быть объединена с D-триггером в блок синхронного хаотического осциллятора, имеющий тактовый вход, подключённый к тактовому входу D-триггера, вход модуляции, подключённый ко входу модуляции автономной булевой сети, асинхронный выход, подключённый к выходу автономной булевой сети, синхронный выход, подключённый к выходу D-триггера, при этом выход автономной булевой сети подключен ко входу данных D-триггера. См. фигуры 12, 13.

В частном варианте реализации изобретения генератор включает в себя дополнительный двухвходовой элемент "исключающее или" и/или "исключающее или-не", первый вход которого подключён ко входу внешней модуляции, второй вход которого подключён к выходу D-триггера, а выход подключён ко входу модуляции автономной булевой сети. См. фиг. 14.

В частном варианте реализации изобретения включает в себя множество из N блоков синхронных хаотических осцилляторов, объединённых в кольцевую структуру, тактовые входы которых объединены вместе и подключены к общему тактовому сигналу, а их синхронные выходы подключены к N-битному выходу генератора, и множество из N дополнительных двухвходовых элементов "исключающее или" и/или "исключающее или-не", таких, что выход каждого из указанных логических элементов подключён ко входу модуляции соответствующего ему блока синхронного хаотического осциллятора, его первый вход подключён к асинхронному выходу предыдущего в цепочке блока синхронного хаотического осциллятора, а второй вход подключён к асинхронному выходу последующего в цепочке блока синхронного хаотического осциллятора. См. фиг. 15.

Осуществление изобретения

Генератор истинно случайных чисел работает следующим образом. Приведем наиболее исчерпывающий пример реализации изобретения, имея в виду, что данный пример не ограничивает применения изобретения.

Формируют цифровую хаотически осциллирующую автономную булеву сеть из трёх логических элементов, соединённых друг с другом, в качестве двух из которых используют двухвходовые логические элементы "исключающее или" и/или "исключающее или-не", а посредством третьего логического элемента реализуют специальную логическую функцию "счёт единиц", при которой на его выходе устанавливают логическую единицу, если не более чем на одном из его входов присутствует логическая единица, в противном случае устанавливают логический ноль.

Формируют синхронный хаотический осциллятор (СХО) - он имеет тактовый и модуляционный входы и два выхода - синхронный, используемый для получения случайного числа, и асинхронный, необходимый для модуляции других СХО. По каждому фронту тактового сигнала D-триггер фиксирует значение асинхронного сигнала. Полученное значение с одной стороны подаётся на синхронный выход, с другой стороны, используется для условной инверсии входного модуляционного сигнала при помощи двухвходового элемента XOR.

Генератор случайных чисел строят на таких блоках СХО.

Многобитный генератор истинно случайных чисел строят по схеме, в которой использовано кольцо блоков СХО, модулирующееся во встречных направлениях. На модуляционный вход каждого блока

СХО подаётся сигнал с логического элемента "исключающее или", ко входам которого подключены асинхронные выходы предыдущего и последующего в кольце блоков СХО.

Промышленная применимость

Предлагаемый генератор истинно случайных чисел может быть осуществлен специалистом на практике и при осуществлении обеспечивает реализацию заявленного назначения, что позволяет сделать вывод о соответствии критерию "промышленная применимость" для изобретения.

В соответствии с предложенным изобретением изготовлен опытный образец генератора истинно случайных чисел. В ходе работы экспериментально исследованы в ПЛИС как уже упоминавшиеся генераторы Жанга и Роэина, так и генератор на основе описанной булевой сети. Случайная природа чисел нашего генератора подтверждается следующим экспериментом, который проводился с использованием ПЛИС Altera Cyclone IV EP4CE22F17C6N. Сеть находится в состоянии "сброса", т.е. выводы всех логических элементов установлены в предопределённом состоянии "ноль". Далее в одном такте снимается сигнал сброса, а в следующем такте фиксируется состояние выхода хаотического осциллятора. Данные, снятые при многократном перезапуске сети удовлетворяли критериям случайности и не обнаруживали значимой корреляции друг с другом при тактовой частоте до 150 мегагерц, что свидетельствует о наступлении хаоса за время, меньшее 7 наносекунд. После процедуры отбеливания полученные случайные числа полностью проходили тесты на случайность NIST.

Таким образом, испытания опытного образца генератора истинно случайных чисел показали, что за счет того, что цифровая хаотически осциллирующая автономная булева сеть включает в себя три логических элемента, соединённые друг с другом, два из которых являются двухвходовыми логическими элементами "исключающее или" и/или "исключающее или-не", а третий логический элемент имеет три входа и один выход и реализует специальную логическую функцию "счёт единиц", при которой на его выходе устанавливается логическая единица, если не более чем на одном из его входов присутствует логическая единица, в противном случае устанавливается логический ноль, и достигается заявленный технический результат, а именно: увеличение скорости генерации истинно случайных чисел при снижении потребляемой энергии.

Кроме того, техническим результатом изобретения является набор единственно возможных сетей логических элементов, каждая из которых обладает следующими свойствами:

1) она не обладает стабильными состояниями и короткими циклами, которые вызывали бы упорядочивание работы сети и исчезновение булева хаоса;

2) сигналы на выходе всех элементов имеют наименьшую теоретически возможную автокорреляцию, что вынуждает сеть сваливаться в хаотическое поведение;

3) отсутствует корреляция формы выходных сигналов всех элементов, что исключает перекрёстную фазовую модуляцию элементов при работе сети;

4) она имеет наименьший возможный размер, что обеспечивает наибольшую возможную скорость нарастания хаоса из-за коротких петель распространения сигнала внутри сети;

5) она имеет внешний модуляционный вход, который позволяет дестабилизировать сеть, предотвращая наступление физического равновесия, и объединять сети в масштабируемые кластеры при помощи перекрёстной модуляции.

Одна сеть из этого набора к тому же использует только симметричные по входам логические элементы.

Таким образом, эти сети позволяют создать генератор случайных чисел с уникальными характеристиками:

1) полученные числа являются истинно случайными, что позволяет использовать их для криптографических целей;

2) скорость генерации случайного числа столь высока, что поведение сети непредсказуемо уже за время распространения сигнала через несколько логических элементов. Таким образом, при реализации в микропроцессорных системах случайное число можно получить за один такт. Такая скорость генерации фактически удовлетворяет любые возможные потребности;

3) модуляционный вход позволяет дополнительно улучшить характеристики, так как на него можно подавать другое случайное число, так называемый "посев" предлагаемого генератора случайных чисел. Это заставляет сеть каждый раз стартовать из нового состояния;

4) этот же вход позволяет осуществлять перекрёстную модуляцию разрядов предлагаемого генератора, увеличивая этим скорость нарастания хаоса;

5) минимальный размер сети делает предлагаемый генератор наиболее экономичным по потреблению энергии;

6) предлагаемый генератор можно одинаково эффективно реализовать как на дискретных элементах, так и в ПЛИС или ASIC;

7) конструкция предлагаемого генератора проста и затраты на его реализацию ничтожно малы, что позволяет использовать его повсеместно, включая дешёвые и энергосберегающие устройства.

Литература

[1] Maxim Semiconductors. Building a Low-Cost White-Noise Generator. Application note 3469.

[2] R. Zhang, H. L. D. de S. Cavalcante, Z. Gao, D. J. Gauthier, J. E. S. Socolar, M. M. Adams, and D. P. Lathrop. Boolean Chaos. Phys. Rev. E 80, 045202 (2009).

[3] David P. Rosin, Damien Rontani, Daniel J. Gauthier, and Eckehard Schöll. Experiments on autonomous Boolean networks. Chaos 23, 025102 (2013).

[4] Hugo L. D. de S. Cavalcante, Daniel J. Gauthier, Joshua E. S. Socolar and Rui Zhang. On the origin of chaos in autonomous Boolean networks. Phil. Trans. R. Soc. A (2010) 368, 495–513.

[5] David Rosin. Dynamics of Complex Autonomous Boolean Networks. Doctoral dissertation. Technische Universität Berlin.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Генератор истинно случайных чисел, включающий в себя цифровую хаотически осциллирующую автономную булеву сеть в качестве источника энтропии, отличающийся тем, что цифровая хаотически осциллирующая автономная булева сеть включает в себя три логических элемента, соединённые друг с другом, первый из которых является двухвходовым логическим элементом "исключающее или" или "исключающее или-не", второй является двухвходовым логическим элементом "исключающее или" или "исключающее или-не", а третий логический элемент имеет три входа и один выход и реализует логическую функцию "счёт единиц", при которой на его выходе устанавливается логическая единица, если не более чем на одном из его входов присутствует логическая единица, в противном случае устанавливается логический ноль, при этом выход первого двухвходового логического элемента соединен с первым входом второго двухвходового логического элемента и со вторым входом третьего логического элемента "счёт единиц", выход второго двухвходового логического элемента соединен с его вторым входом, со вторым входом первого двухвходового логического элемента и с третьим входом третьего логического элемента "счёт единиц", а выход третьего логического элемента "счёт единиц" соединен с его первым входом, с первым входом первого двухвходового логического элемента и с выходом всей сети.

2. Генератор по п.1, отличающийся тем, что второй и/или третий входы третьего логического элемента "счёт единиц" инвертированы.

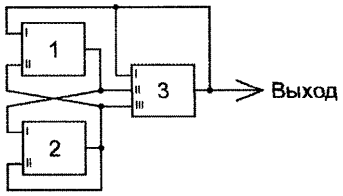
3. Генератор по любому из пп.1, 2, отличающийся тем, что оба двухвходовых логических элемента "исключающее или" и/или "исключающее или-не" имеют дополнительные третьи логические входы, которые объединены вместе и подключены к дополнительному входу внешней модуляции цифровой хаотически осциллирующей автономной булевой сети.

4. Генератор по любому из пп.1-3, отличающийся тем, что генератор имеет вход выключения, а оба логических элемента "исключающее или" и/или "исключающее или-не" имеют дополнительные входы выключения с возможностью принудительного перевода выхода обоих указанных логических элементов в состояние логического нуля либо логической единицы независимо от состояния остальных входов, причём эти входы объединены вместе и подключены к указанному входу выключения генератора.

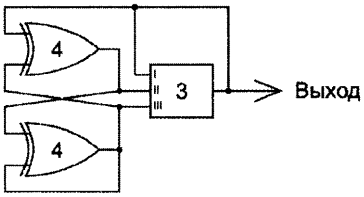
5. Генератор по любому из пп.3, 4, отличающийся тем, что цифровая хаотически осциллирующая автономная булева сеть объединена с D-триггером в блок синхронного хаотического осциллятора, имеющий тактовый вход, подключённый к тактовому входу D-триггера, вход модуляции, подключённый ко входу модуляции автономной булевой сети, асинхронный выход, подключённый к выходу автономной булевой сети, синхронный выход, подключённый к выходу D-триггера, при этом выход автономной булевой сети подключен ко входу данных D-триггера.

6. Генератор по п.5, отличающийся тем, что включает в себя дополнительный двухвходовой элемент "исключающее или" и/или "исключающее или-не", первый вход которого подключён ко входу внешней модуляции, второй вход которого подключён к выходу D-триггера, а выход подключён ко входу модуляции автономной булевой сети.

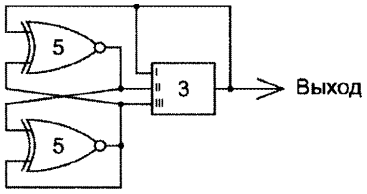
7. Генератор по любому из пп.5, 6, отличающийся тем, что включает в себя множество из N блоков синхронных хаотических осцилляторов, объединённых в кольцевую структуру, тактовые входы которых объединены вместе и подключены к общему тактовому сигналу, а их синхронные выходы подключены к N-битному выходу генератора, и множество из N дополнительных двухвходовых элементов "исключающее или" и/или "исключающее или-не", таких, что выход каждого из указанных логических элементов подключён ко входу модуляции соответствующего ему блока синхронного хаотического осциллятора, его первый вход подключён к асинхронному выходу предыдущего в цепочке блока синхронного хаотического осциллятора, а второй вход подключён к асинхронному выходу последующего в цепочке блока синхронного хаотического осциллятора.



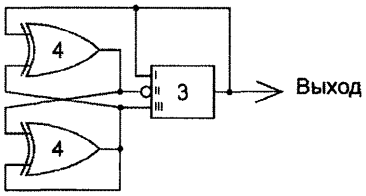
Фиг. 1



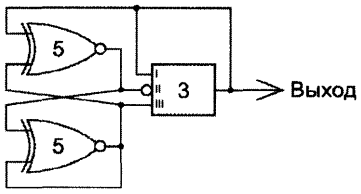
Фиг. 2



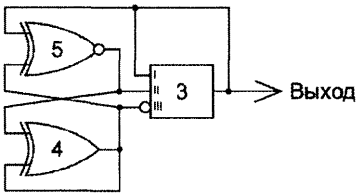
Фиг. 3



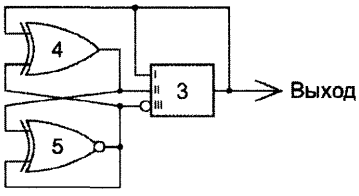
Фиг. 4



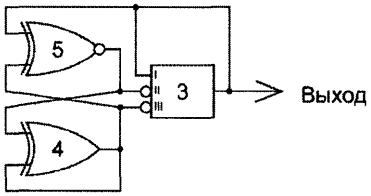
Фиг. 5



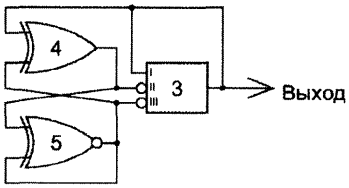
Фиг. 6



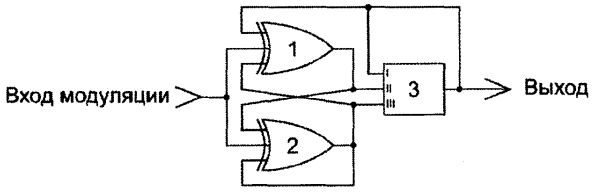
Фиг. 7



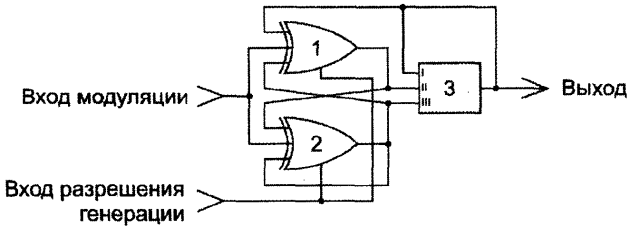
Фиг. 8



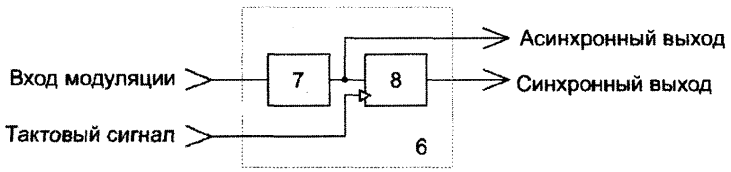
Фиг. 9



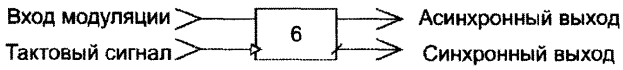
Фиг. 10



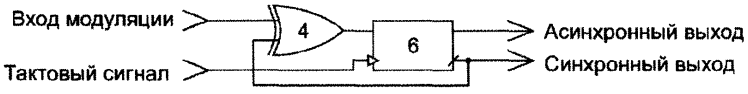
Фиг. 11



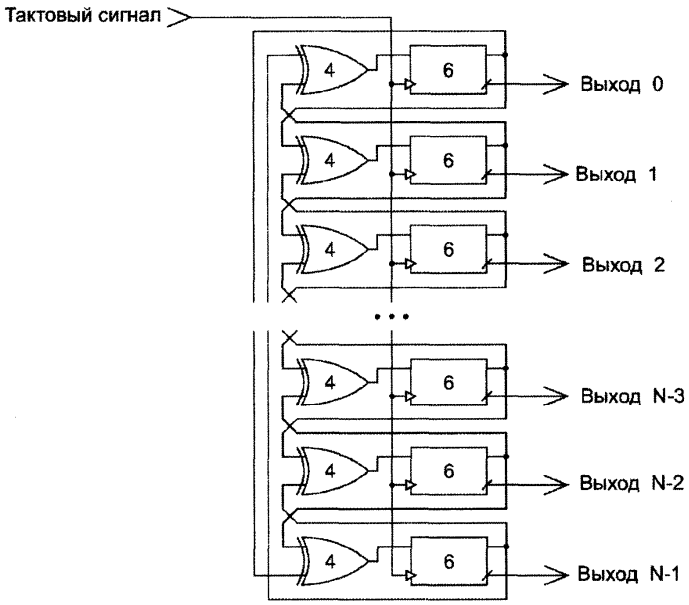
Фиг. 12



Фиг. 13



Фиг. 14



Фиг. 15

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2