РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 642 351** (13) **C1**

(51) МПК
G06F 7/04 (2006.01)
G06F 7/58 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 7/026 (2006.01); G06F 7/588 (2006.01); G06F 17/18 (2006.01); G06G 7/26 (2006.01)

(21)(22) Заявка: **2017101200, 16.01.2017**

(24) Дата начала отсчета срока действия патента:
16.01.2017

Дата регистрации:
24.01.2018

Приоритет(ы):
(22) Дата подачи заявки: **16.01.2017**

(45) Опубликовано: **24.01.2018** Бюл. № **3**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Андрущенко Алексей Сергеевич (RU),
Самоделов Андрей Сергеевич (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

(56) Список документов, цитированных в отчете о поиске: **RU 2216034 C2, 10.11.2003. RU 2363979 C2, 10.08.2009. RU 2417406 C2, 27.04.2011. US 6542014 B1, 01.04.2003. JP 2000298577 A, 24.10.2000.**

(54) Способ выбора шумовых диодов с использованием измерительного устройства для генератора случайных чисел

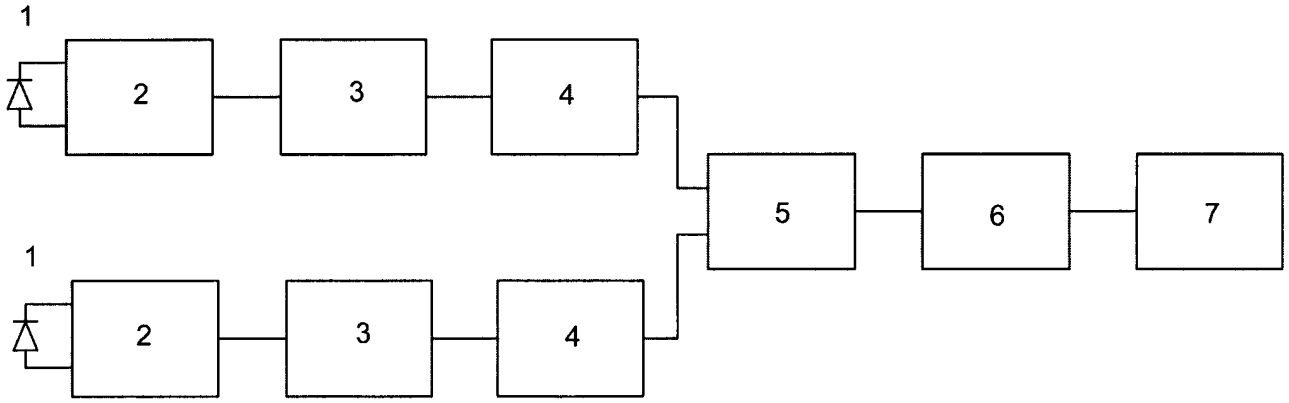
(57) Реферат:

Изобретение относится к генераторам случайных чисел (ГСЧ) и может быть использовано для генерации случайных цифровых последовательностей в различной радиоизмерительной аппаратуре и системах тестирования каналов обмена информацией, датчиков случайных чисел, средств криптографической защиты информации. Техническим результатом является упрощение процесса подготовки ГСЧ к последующей работе. Способ содержит этапы, на которых устанавливают перечень статистических характеристик числовой последовательности, включающий, по крайней мере, математическое ожидание и дисперсию частоты появления логической единицы в битовой числовой последовательности; для каждого диода из набора однотипных диодов: отмечают диод из набора однотипных диодов; устанавливают диод в генератор аналогового шума измерительного устройства; получают статистические характеристики числовой последовательности, относящиеся к отмеченному диоду, на выходе измерительного устройства; сохраняют данные о статистических характеристиках отмеченного диода; выбирают пару диодов из набора, осуществляя следующие действия: отмечают пары диодов, имеющих максимальную разницу математического ожидания с идеальным значением и минимальную разницу значений математического ожидания в паре; выбирают из совокупности пар диодов с минимальной разницей значений математического ожидания пару диодов, имеющих минимальную разницу значений дисперсии, определяют положение диодов выбранной пары в генераторах аналогового шума генератора случайных чисел, осуществляя следующие действия: устанавливают на основе случайного выбора диоды из выбранной пары в генераторы аналогового шума, отмечают сведения об установленных диодах для каждого генератора аналогового шума

RU 2642351 C1

RU 2642351 C1

(положение 1), получают математическое ожидание числовой последовательности на выходе генератора случайных чисел, сохраняют его значение, меняют местами диоды в генераторах аналогового шума, отмечают сведения об установленных диодах для каждого генератора аналогового шума (положение 2), получают математическое ожидание числовой последовательности на выходе генератора случайных чисел, сравнивают значения математического ожидания числовой последовательности на выходе генератора случайных чисел для положения 1 и положения 2, выбирают положение диодов с наименьшим отклонением от заданного значения математического ожидания и с наименьшим отклонением от заданного значения дисперсии числовой последовательности на выходе генератора случайных чисел, устанавливают диоды в выбранное положение в генераторы аналогового шума для последующего использования в генераторе случайных чисел. 2 ил., 4 табл.



Фиг. 2

RU 2642351 C1

RU 2642351 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 642 351** (13) **C1**

(51) Int. Cl.
G06F 7/04 (2006.01)
G06F 7/58 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 7/026 (2006.01); G06F 7/588 (2006.01); G06F 17/18 (2006.01); G06G 7/26 (2006.01)

(21)(22) Application: **2017101200, 16.01.2017**

(24) Effective date for property rights:
16.01.2017

Registration date:
24.01.2018

Priority:
(22) Date of filing: **16.01.2017**

(45) Date of publication: **24.01.2018** Bull. № **3**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Andrushchenko Aleksej Sergeevich (RU),
Samodelov Andrej Sergeevich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

RU 2642351 C1

(54) METHOD OF SELECTING NOISE DIODES USING MEASURING DEVICE FOR GENERATOR OF RANDOM NUMBERS

(57) Abstract:

FIELD: physics.

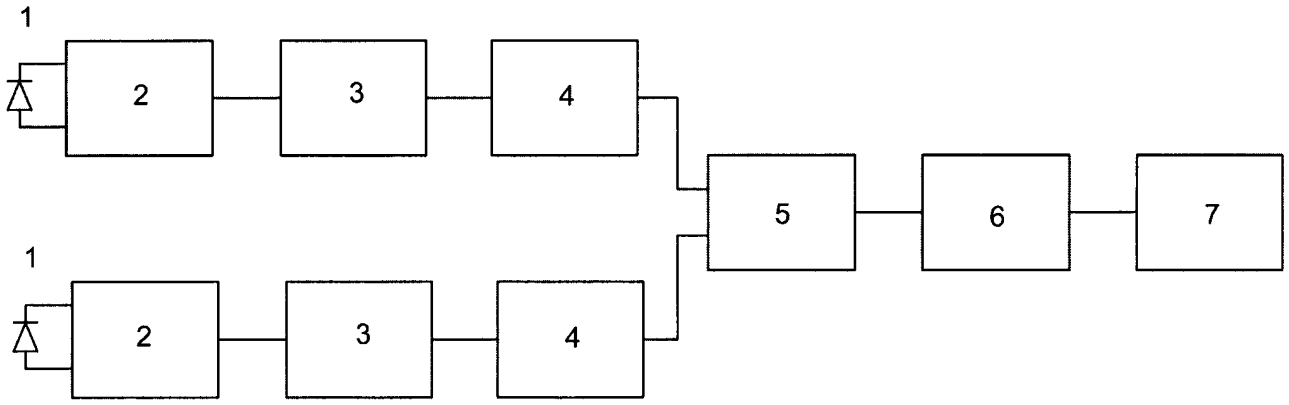
SUBSTANCE: method contains stages, at which the list of statistical characteristics of the numeric sequence is set, that includes at least an mathematical expectation and a dispersion of the logical unit occurrence frequency in a bit numerical sequence; for each diode from a set of the similar diodes: a diode is noted from a set of the similar diodes, the diode is set in the analogue noise generator of the measuring device; statistical characteristics of the numeric sequence is received, related to the detected diode, at the output of the measuring device; the data of the statistical characteristics of the detected diode is saved; a pair of diodes is selected from the set, performing the following actions: a pair of diodes is noted having the maximum difference of the mathematical expectation with a perfect value and the minimum difference of the expected values in the pair; a pair of the diodes having the minimum difference values of the dispersion is selected from the set of pairs of the diodes with a minimum difference of the mathematical expectations, the position of the selected pair diodes is determined in the analogue noise generators of the random number generator, performing the following actions: the diodes from the selected pair are set in the analogue noise generators based on the random selection, the details of the set diodes are noted for each of the analogue noise generator (position 1), the mathematical expectation of the number sequence is received at the output of the random number generator, its value is saved, the diodes are swapped in the analogue noise generators, the details of the set diodes are noted for each of the analogue noise generator (position 2), the mathematical expectation of the number sequence is received at the output of the random number generator, the value of the mathematical expectation of the numerical sequence is compared at the output of the random number generator for position 1 and position 2, the position of the diodes with the minimum deviation from the set value of the mathematical expectation and with the minimum deviation from the set value of the dispersion of the numeric sequence are selected at the

RU 2642351 C1

output of the random number generator, the diodes are set in the selected position in the analogue noise generators for use in the random number generator.

EFFECT: simplification of the process of preparing a random number generator for a subsequent work.

2 dwg, 4 tbl



Фиг. 2

RU 2642351 C1

RU 2642351 C1

Область техники, к которой относится изобретение

Предполагаемое изобретение относится к аппаратным генераторам случайных чисел и может быть использовано для генераторов случайных цифровых последовательностей различной радиоизмерительной аппаратуры и систем тестирования каналов обмена информацией, датчиков случайных чисел, средств криптографической защиты информации и т.п.

Уровень техники

Аппаратные генераторы случайных чисел широко используются в различных устройствах измерительной и криптографической техники. Основой таких генераторов является генераторы равномерно распределенных случайных чисел, формирующие поток чисел с математическим ожиданием (МО), близким к идеальному значению 0,5.

В качестве источника шума в таких генераторах используются резисторы, диоды или транзисторы различного типа. Разработаны и применяются в практике специальные шумовые диоды

Так, известен способ генерации случайных чисел (патент РФ №2363979, приоритет от 23.07.2004 г.), заключающийся в том, что

- генерируют случайные числа, имеющие регулируемое распределение на основе, по меньшей мере, одного регулируемого входного значения;
- формируют выборку генерированных случайных чисел;
- вычисляют, по меньшей мере, одну метрику на основе выборки;
- сравнивают метрику с соответствующим опорным значением; и
- регулируют регулируемое входное значение на основе результата сравнения так, чтобы генерированные случайные числа достигали требуемого распределения;
- при этом регулировка регулируемого входного значения на основе упомянутого сравнения содержит этапы, на которых

○ регулируют значение сдвига постоянной составляющей для генерации аналогового напряжения шумов для того, чтобы вызвать достижение генерированными случайными числами требуемого числового среднего значения; и

○ регулируют значение опорного напряжения для того, чтобы вызвать достижение генерированными случайными числами требуемого числового диапазона.

В качестве метрики может использоваться среднее значение (МО) и среднеквадратическое отклонение (СКО).

Для реализации способа используется устройство для генерации случайных чисел, содержащее

- средство для генерации случайных чисел, имеющих регулируемое распределение на основе, по меньшей мере, одного регулируемого входного значения;
- средство для формирования выборки генерированных случайных чисел;
- средство для вычисления, по меньшей мере, одной метрики на основе выборки;
- средство для сравнения метрики с соответствующим опорным значением; и
- средство для регулировки регулируемого входного значения на основе результата упомянутого сравнения так, чтобы генерированные случайные числа достигали требуемого распределения;

при этом средство для регулировки регулируемого входного значения на основе упомянутого сравнения содержит

- средство для регулировки значения сдвига постоянной составляющей для генерации аналогового напряжения шумов для того, чтобы вызвать достижение генерированными случайными числами требуемого числового среднего значения; и
- средство для регулировки значения опорного напряжения для того, чтобы вызвать

достижение генерированными случайными числами требуемого числового диапазона.

Таким образом, для реализации известного способа используется одиночное средство для генерации случайных чисел, а в качестве источника шума используется один ШД.

Для обеспечения необходимого распределения случайных чисел используются аппаратные регулировки постоянного опорного напряжения для аналого-цифрового преобразователя (АЦП) и постоянного напряжения смещения в дифференциальном усилителе (ДУ).

Для реализации известного способа и обеспечения последующей работы ГСЧ требуется дополнительный этап достаточно длительной и трудоемкой регулировки, с привлечением квалифицированного персонала.

Недостатками известного способа являются

1) необходимость сложного дополнительного аппаратного и программного обеспечения получения на выходе необходимого распределения случайных чисел,

2) необходимость выполнения нескольких регулировок.

Известен также способ генерации случайных чисел (патент США №6857003, приоритет от 12.07.2001 г.), включающий следующие шаги:

- генерация 1-го шумового сигнала и прохождение 1-го шумового сигнала через 1-й фильтр высоких частот, который удаляет периодический компонент, содержащийся в 1-м шумовом сигнале, чтобы сформировать 1-й шумовой сигнал, имеющий 1/f зависимость, в 1-м блоке генератора шума и;

- генерация 2-го шумового сигнала и прохождение 2-го шумового сигнала через 2-й фильтр высоких частот, который удаляет периодический компонент, содержащийся во 2-м [шумовом сигнале], чтобы сформировать 2-й шумовой сигнал, имеющий 1/f зависимость, во 2-м блоке генератора шума и;

- передача 1-го и 2-го шумовых сигналов, имеющих 1/f зависимость, в дифференциальный блок, чтобы получить разностный сигнал между 1-м и 2-м шумовыми сигналами, и

- генерация из разностного сигнала случайных чисел, у которых нет периодичности из-за 1/f зависимости 1-го и 2-го шумовых сигналов.

Разностный сигнал, сформированный дифференциальным блоком, преобразуется АЦП в цифровой сигнал, и преобразованный таким образом цифровой сигнал является источником случайных чисел.

Для реализации данного способа используются два одинаковых средства (блока) для генерации случайных чисел, затем производится вычитание сигнала в ДУ и последующая обработка разностного сигнала, а в качестве источников шума используются ШД или резисторы.

Для обеспечения необходимого распределения случайных чисел используются аппаратные регулировки постоянного опорного напряжения для аналого-цифрового преобразователя (АЦП) и объем выборки выходного цифрового сигнала.

В качестве источника шума в известном способе предпочтительно используются ШД, также могут применяться резисторы.

Известный способ принимается за прототип.

Недостатками известного способа являются

1) необходимость дополнительного аппаратного обеспечения для получения на выходе необходимого распределения случайных чисел,

2) необходимость выполнения нескольких регулировок в зависимости от использованной пары ШД.

Здесь также для реализации известного способа и обеспечения последующей работы

ГСЧ требуется дополнительный этап достаточно длительной и трудоемкой регулировки, с привлечением квалифицированного персонала.

В прототипе используется пара ШД, в общем случае, выбираемая случайным образом из партии однотипных ШД. Как показывает опыт, такая пара ШД, в общем случае, может дать последовательность на выходе, которая не обеспечивает необходимых статистических характеристик распределения случайных чисел, в частности, неприемлемое отличие от заданного идеального значения МО=0,5.

Раскрытие сущности изобретения

Техническим результатом является

1) получение пары диодов, обеспечивающих на выходе ДСЧ последовательность случайных чисел с заданными статистическими характеристиками,

2) упрощение процесса подготовки ГСЧ к последующей работе за счет отказа от регулировок используемого аппаратного обеспечения.

Для этого предлагается способ выбора шумовых диодов с близкими характеристиками с использованием измерительного устройства для генератора случайных чисел,

причем измерительное устройство выполнено с возможностью формирования числовой последовательности и включает

- генератор аналогового шума на основе шумового диода;
- усилитель;
- фильтр высоких частот;
- компаратор с цифровым выходом;
- блок выборки;
- блок обработки, выполненный с возможностью
  - задавать частоту выборки для блока выборки;
  - получать цифровой сигнал от блока выборки;
  - обрабатывать цифровой сигнал для получения заданных статистических характеристик числовой последовательности;

а генератор случайных чисел выполнен с возможностью формирования числовой последовательности и содержит

- два одинаковых генератора аналогового шума на основе шумовых диодов;
- два одинаковых усилителя;
- два одинаковых фильтра высоких частот;
- компаратор с цифровым выходом;
- блок выборки;
- блок обработки, выполненный с возможностью
  - задавать частоту выборки для блока выборки;
  - получать цифровой сигнал от блока выборки;
  - обрабатывать цифровой сигнал для получения заданных статистических характеристик числовой последовательности;

способ, заключающийся в том, что

- устанавливают перечень статистических характеристик числовой последовательности, включающий, по крайней мере,
  - математическое ожидание частоты появления логической единицы в битовой числовой последовательности;
  - дисперсия частоты появления логической единицы в битовой числовой

последовательности;

- для каждого диода из набора однотипных диодов выполняют следующие действия:

○ отмечают диод из набора однотипных диодов; о устанавливают диод в генератор аналогового шума измерительного устройства;

○ получают статистические характеристики числовой последовательности, относящиеся к отмеченному диоду, на выходе измерительного устройства;

○ сохраняют данные о статистических характеристиках отмеченного диод;

- выбирают пару диодов из набора, осуществляя следующие действия:

○ отмечают пары диодов, имеющих максимальную разницу математического ожидания с идеальным значением и минимальную разницу значений математического ожидания в паре;

○ выбирают из совокупности пар диодов с минимальной разницей значений математического ожидания пару диодов, имеющих минимальную разницу значений дисперсии;

- определяют положение диодов выбранной пары в генераторах аналогового шума генератора случайных чисел, осуществляя следующие действия:

○ устанавливают на основе случайного выбора диоды из выбранной пары в генераторы аналогового шума;

○ отмечают сведения об установленных диодах для каждого генератора аналогового шума (положение 1);

○ получают математическое ожидание числовой последовательности на выходе генератора случайных чисел;

○ сохраняют значение полученного математического ожидания;

○ меняют местами диоды в генераторах аналогового шума;

○ отмечают сведения об установленных диодах для каждого генератора аналогового шума (положение 2);

○ получают математическое ожидание числовой последовательности на выходе генератора случайных чисел;

○ сравнивают значения математического ожидания числовой последовательности на выходе генератора случайных чисел для положения 1 и положения 2;

○ выбирают положение диодов с наименьшим отклонением от заданного значения математического ожидания и с наименьшим отклонением от заданного значения дисперсии числовой последовательности на выходе генератора случайных чисел;

- устанавливают диоды в выбранное положение в генераторы аналогового шума для последующего использования в генераторе случайных чисел.

Блок-схема измерительного устройства показана на фиг. 1, а блок-схема генератора случайных чисел показана на фиг. 2, где цифрами обозначены: 1 - шумовой диод, 2 - генератор аналогового шума, 3 - усилитель, 4 - фильтр высоких частот, 5 - компаратор, 6 - блок выборки, 7 - блок обработки.

Для генератора случайных чисел выбирается подходящая пара диодов из нескольких однотипных единиц (партии диодов), причем размер партии может быть различным, в зависимости от условий изготовления или производства генераторов случайных чисел, - от 3-5 до 50-100 штук.

Сначала все диоды последовательно помечаются, например, путем присвоения условного номера в партии, и помещаются в измерительное устройство, и для каждого

диода в ходе его работы проводятся измерения параметров и расчет статистических характеристик выходной числовой битовой последовательности, в результате чего для каждого диода получают два значения - МО и дисперсию.

Расчет МО и дисперсии может быть проведен по известным формулам (Маркин Н.С. Основы теории обработки результатов измерений, М., Издательство стандартов, 1991)

$$x_0 = \frac{\sum_{i=1}^{n} x_i}{n},$$

$$D = \sigma^2 = \frac{\sum_{i=1}^{n} (x_i - x_0)^2}{n-1},$$

где x_0 - МО;

x_i - значение случайной величины на выходе;

n - количество измерений случайной величины на выходе;

σ - СКО.

После проведения измерений и расчетов для всех диодов получается совокупность значений МО и дисперсии. Этот набор значений удобно поместить в таблицу и затем ранжировать по возрастанию величины МО. Из-за разброса физических характеристик диодов значения МО и дисперсии находятся в определенном интервале.

Затем выбирают пару диодов из набора, осуществляя следующие действия:

- отмечают пары диодов, имеющих максимальную абсолютную разницу математического ожидания с идеальным значением и минимальную разницу значений математического ожидания в паре;

- выбирают из совокупности пар диодов с минимальной разницей значений математического ожидания пару диодов, имеющих минимальную разницу значений дисперсии.

Как показали проведенные измерения для генератора случайных чисел на основе двух диодов, статистические характеристики выходной числовой последовательности зависят от размещения пары диодов в генераторах аналогового шума, несмотря на все усилия по достижению максимальной идентичности элементов схем этих генераторов. Если изначально провести случайный выбор диодов из пары, поместить их в генераторы аналогового шума (положение диодов 1) и измерить статистические характеристики выходной числовой последовательности, то получится определенный результат. Если затем поменять диоды из пары местами в в генераторах аналогового шума (положение диодов 2) и снова измерить статистические характеристики, то выяснится, что результат будет отличаться по сравнению с полученным для положения диодов 1.

Поэтому целесообразно проделать описанную процедуру для выбранной из партии пары диодов и затем окончательно установить диоды в генератор случайных чисел в том положении, в котором обеспечиваются лучшие статистические характеристики выходной числовой последовательности.

Таким образом, при реализации предложенного способа обеспечивается выбор пары диодов, обеспечивающих на выходе генератора случайных чисел последовательность случайных чисел с заданными статистическими характеристиками.

При этом существенно упрощается процесс подготовки генератора случайных чисел к последующей работе, поскольку не требуется никаких регулировок в схеме генератора.

Краткое описание чертежей

На фиг. 1 показана блок-схема измерительного устройства.

На фиг. 2 показана блок-схема генератора случайных чисел.

Осуществление изобретения Для осуществления способа необходимы два устройства, представляющих собой аппаратные генераторы случайных чисел на основе шумовых диодов:

- одноканальный - для снятия статистических характеристик одиночных диодов (измерительное устройство),

- двухканальный - для снятия статистических характеристик пары диодов. Допустимо для снятия статистических характеристик одиночных диодов использование одного из каналов двухканального генератора случайных чисел.

Одноканальный генератор случайных чисел (фиг. 1) включает

- генератор аналогового шума 2 на основе шумового диода 1,

- усилитель 3, предназначенный для уменьшения влияния последующих каскадов на генератор аналогового шума 2,

- фильтр высоких частот 4, предназначенного для устранения влияния на выходной сигнал низкочастотных составляющих шумового сигнала и наводок,

- компаратор 5 с цифровым выходом, предназначенный для преобразования аналогового шумового сигнала от генератора аналогового шума 2 в случайную цифровую последовательность,

- блок выборки 6, предназначенный для выборки отсчетов цифрового сигнала из случайной цифровой последовательности с выхода компаратора 5 с задаваемой блоком обработки 7 частотой.

Двухканальный генератор случайных чисел (фиг. 2) включает

- два идентичных генератора аналогового шума 2 на основе шумовых диодов 1,

- два идентичных усилителя 3, предназначенных для уменьшения влияния последующих каскадов на генераторы аналогового шума 2,

- два идентичных фильтра высоких частот 4, предназначенных для устранения влияния на выходной сигнал низкочастотных составляющих шумового сигнала и наводок,

- компаратор 5 с цифровым выходом, предназначенный для вычитания аналоговых шумовых сигналов с генераторов аналогового шума 2 и преобразования разностного аналогового шумового сигнала в случайную цифровую последовательность,

- блок выборки 6, предназначенный для выборки отсчетов цифрового сигнала из случайной цифровой последовательности с выхода компаратора 5 с задаваемой блоком обработки 7 частотой.

Для получения статистических характеристик случайной цифровой последовательности с выхода блока выборки служит блок обработки 7, в состав которого входят

- блок ввода данных в персональный компьютер (ПК), позволяющий вводить в ПК случайную цифровую последовательность с одно- или двухканального генератора случайных чисел,

- программное обеспечение, позволяющее анализировать статистические характеристики вводимой в ПК через устройство сопряжения цифровой последовательности.

Блок обработки выполнен с возможностью

- задавать частоту выборки для блока выборки 6,

- получать цифровой сигнал от блока выборки 6,

- обрабатывать цифровой сигнал для получения выбранных статистических характеристик случайной цифровой последовательности.

Реализация предложенного способа может быть показана на конкретном примере выбора подходящей пары диодов из партии объемом 50 штук ШД типа 2Г401Б (Кремниевые шумовые диоды 2Г401А-В, КГ401А-В, статья по адресу http://asest.com/196-2g401a-2g401b-2g401v-kg401a-kg401b-kg401v).

Для измерения характеристик диодов устанавливалась частота выборки для измерительного устройства порядка 1 МГц, которая обеспечивала проведение измерений для одного диода в течение 3-5 минут, так что вся партия может быть исследована за половину рабочего дня. При этом в ходе измерений для каждого диода анализировалось $n=10^6$ значений битовой последовательности.

Ошибка вычисления МО ожидания рассчитывалась по формуле (ГОСТ Р 8.736-2011):

$$\Delta \text{МО} = K_{\alpha,n}\sqrt{\frac{D}{n}} \quad ,$$

где $K_{\alpha,n}$ - коэффициент Стьюдента;

α - уровень значимости (принимался равным 5%).

Для принятых значений $K_{\alpha,n}=1,96$, соответственно, погрешность вычисления МО не превышает 1×10^{-3}.

Можно также отметить, что, поскольку на выходе генератора могут быть только два значения случайного числа - 0 или 1, то, на основе указанной выше формулы для расчета D, идеальное значение дисперсии составляет D=0,25.

Для проведения измерений для каждого диода из набора однотипных диодов выполняют следующие действия:

- отмечают диод из набора однотипных диодов,
- устанавливают диод в генератор аналогового шума измерительного устройства,
- получают статистические характеристики числовой последовательности, относящиеся к отмеченному диоду, на выходе измерительного устройства,
- сохраняют данные о статистических характеристиках отмеченного диода.

Результаты измерений для 50 диодов приведены в табл. 1 (диодам были присвоены условные номера от 51 до 100)

Таблица 1

№ диода	MO	D
51	0.4384	0.199
52	0.4276	0.191
53	0.4638	0.220
54	0.4488	0.207
55	0.4425	0.202
56	0.4328	0.195
57	0.4334	0.195
58	0.4301	0.193
59	0.4529	0.211
60	0.4419	0.202
61	0.4453	0.205
62	0.4242	0.188
63	0.4772	0.231
64	0.4387	0.199
65	0.4253	0.189
66	0.4419	0.202
67	0.4406	0.201
68	0.4589	0.216
69	0.4273	0.191
70	0.4339	0.196
71	0.4432	0.203
72	0.4287	0.192
73	0.4318	0.194
74	0.4402	0.201
75	0.4431	0.203
76	0.4345	0.196
77	0.4340	0.196
78	0.4453	0.205
79	0.4325	0.195
80	0.4340	0.196
81	0.4369	0.198
82	0.4405	0.201
83	0.4660	0.221
84	0.4685	0.223
85	0.4461	0.205

Таблица 1 (продолжение)

№ диода	MO	D
86	0.4448	0.204
87	0.4260	0.190
88	0.4282	0.191
89	0.4265	0.190
90	0.4441	0.204
91	0.4333	0.195
92	0.4365	0.198
93	0.4432	0.203
94	0.4392	0.120
95	0.4311	0.194
96	0.4379	0.199
97	0.4384	0.199
98	0.4572	0.214
99	0.4388	0.199
100	0.4556	0.213

Результаты, приведенные в табл. 1, позволяют сделать следующие выводы:

1) генератор на одном диоде дает сниженные по сравнению с идеальными значения MO и D,

2) значения MO и D могут ощутимо отличаться для разных диодов из одной партии.

Для более удобного анализа результаты измерений можно осуществить сортировку по нарастанию среди данных о математическом ожидании диодов (табл. 2).

Таблица 2

№ диода	MO	D
62	0.4242	0.188
65	0.4253	0.189
87	0.4260	0.190
89	0.4265	0.190
69	0.4273	0.191
52	0.4276	0.191
88	0.4282	0.191
72	0.4287	0.192
58	0.4301	0.193
95	0.4311	0.194
73	0.4318	0.194
79	0.4325	0.195
56	0.4328	0.195

Таблица 2 (продолжение)

№ диода	MO	D
91	0.4333	0.195
57	0.4334	0.195
70	0.4339	0.196
77	0.434	0.196
80	0.4340	0.196
76	0.4345	0.196
92	0.4365	0.198
81	0.4369	0.198
96	0.4379	0.199
51	0.4384	0.199
97	0.4384	0.199
64	0.4387	0.199
99	0.4388	0.199
94	0.4392	0.200
74	0.4402	0.201
82	0.4405	0.201
67	0.4406	0.201
60	0.4419	0.202
66	0.4419	0.202
55	0.4425	0.202
75	0.4431	0.203
71	0.4432	0.203
93	0.4432	0.203
90	0.4441	0.204
86	0.4448	0.204
61	0.4453	0.205
78	0.4453	0.205
85	0.4461	0.205
54	0.4488	0.207
59	0.4529	0.211
100	0.4556	0.213
98	0.4572	0.214
68	0.4589	0.216
53	0.4638	0.220
83	0.4660	0.221
84	0.4685	0.223
63	0.4772	0.231

На основе данных табл. 2 выбирают пару диодов из набора, осуществляя следующие действия:

- отмечают пары диодов, имеющих максимальную разницу математического ожидания с идеальным значением и минимальную разницу значений математического ожидания в паре;
- выбирают из совокупности пар диодов с минимальной разницей значений математического ожидания пару диодов, имеющих минимальную разницу значений дисперсии.

В результате, выбирается пара диодов с номерами 65 и 87.

В целом, из имеющегося набора можно выбрать пары диодов 52-69, 72-88, 73-95, 56-79, 57-91, 77-80, 51-97, 64-99, 82-67 (приведены первые 10 пар, номера выбранных диодов в ячейках табл. 2 смещены к правому краю). Такой выбор среди одной партии может быть полезен, если из партии выбирается не одна пара диодов, а, например, решается задача последовательного неоднократного выбора пар диодов (с изъятием из состава партии диодов) для последующей установки в изготавливаемые генераторы.

После этого определяют положение диодов выбранной пары в генераторах аналогового шума генератора случайных чисел, осуществляя следующие действия:

- устанавливают на основе случайного выбора диоды из выбранной пары в генераторы аналогового шума,
- отмечают сведения об установленных диодах для каждого генератора аналогового шума (положение 1),
- получают математическое ожидание числовой последовательности на выходе генератора случайных чисел,
- сохраняют значение полученного математического ожидания,
- меняют местами диоды в генераторах аналогового шума,
- отмечают сведения об установленных диодах для каждого генератора аналогового шума (положение 2),
- получают математическое ожидание числовой последовательности на выходе генератора случайных чисел,
- сравнивают значения математического ожидания числовой последовательности на выходе генератора случайных чисел для положения 1 и положения 2,
- выбирают положение диодов с наименьшим отклонением от заданного значения математического ожидания и с наименьшим отклонением от заданного значения дисперсии числовой последовательности на выходе генератора случайных чисел.

Результаты измерений для двух положений выбранной пары диодов 65-87 приведены в табл. 3. В этой же таблице для сравнения приведены также результаты измерений для пар диодов 52-69, 72-88, 73-95, 56-79, 57-91, 77-80, 51-97, 64-99, 82-67.

Таблица 3

№№ диодов в паре	MO	D
65-87	0.499	0.249
87-65	0.503	0.253
52-69	0.501	0.251
69-52	0.500	0.250
72-88	0.502	0.252
88-72	0.500	0.250
73-95	0.498	0.248
95-73	0.505	0.254
56-79	0.500	0.250
79-56	0.504	0.254
57-91	0.499	0.249
91-57	0.504	0.253
77-80	0.501	0.251
80-77	0.503	0.253
51-97	0.502	0.252
97-51	0.503	0.253
99-64	0.500	0.250
64-99	0.505	0.254
67-82	0.500	0.250
82-67	0.503	0.253

Результаты, приведенные в табл. 3, показывают, что перестановка диодов из одной пары позволяет выбрать положение диодов, при котором снижается отклонение от заданного идеального значения MO и отклонение от заданного идеального значения дисперсии числовой последовательности на выходе генератора случайных чисел.

Для иллюстрации эффективности предложенного способа подбора диодов в табл. 4 приведены результаты измерений для случайно выбранных из партии пар диодов. При этом выбор проводился из сортированного списка табл. 2, в которой весь список разделялся на условные группы, которые находились в начале списка, в середине, в конце.

Таблица 4

№№ диодов в паре	MO	D	Группы диодов в списке
62-72	0.500	0.250	начало - начало
72-62	0.502	0.252	
81-62	0.511	0.260	начало - середина
62-81	0.493	0.244	
81-72	0.508	0.257	
72-81	0.495	0.246	
85-62	0.505	0.255	начало - конец
62-85	0.498	0.249	
98-62	0.518	0.266	
62-98	0.487	0.238	
98-72	0.517	0.265	
72-98	0.488	0.239	
85-72	0.504	0.254	
72-85	0.499	0.249	
63-72	0.497	0.248	
72-63	0.504	0.254	
98-81	0.511	0.260	середина - конец
81-98	0.493	0.244	
85-81	0.497	0.247	
81-85	0.507	0.256	
63-81	0.485	0.237	
81-63	0.516	0.264	
63-82	0.501	0.251	
82-63	0.499	0.249	
98-85	0.514	0.263	конец - конец
85-98	0.489	0.240	
63-53	0.483	0.235	
53-63	0.520	0.267	
63-98	0.478	0.231	
98-63	0.523	0.271	
63-85	0.484	0.236	
85-63	0.516	0.265	

Результаты, приведенные в табл. 4, показывают, что

1) случайный выбор может оказаться удачным, что видно на примере пары диодов 63-82,

2) у большей части случайно выбранных пар диодов характеристики оказываются хуже, чем у пар диодов, выбранных согласно предложенному способу.

Необходимо отметить, что возможны и другие варианты реализации предложенного способа, отличающиеся от описанного выше и зависящие от личных предпочтений при программировании отдельных действий и функций.

(57) Формула изобретения

Способ выбора шумовых диодов с использованием измерительного устройства для генератора случайных чисел,

причем измерительное устройство выполнено с возможностью формирования числовой последовательности и включает

генератор аналогового шума на основе шумового диода;

усилитель;
фильтр высоких частот;
компаратор с цифровым выходом;
блок выборки;
блок обработки, выполненный с возможностью
задавать частоту выборки для блока выборки;
получать цифровой сигнал от блока выборки;
обрабатывать цифровой сигнал для получения заданных статистических характеристик числовой последовательности;
а генератор случайных чисел выполнен с возможностью формирования числовой последовательности и содержит
два одинаковых генератора аналогового шума на основе шумовых диодов;
два одинаковых усилителя;
два одинаковых фильтра высоких частот;
компаратор с цифровым выходом;
блок выборки;
блок обработки, выполненный с возможностью
задавать частоту выборки для блока выборки;
получать цифровой сигнал от блока выборки;
обрабатывать цифровой сигнал для получения заданных статистических характеристик числовой последовательности;
способ, заключающийся в том, что
устанавливают перечень статистических характеристик числовой последовательности, включающий, по крайней мере,
математическое ожидание частоты появления логической единицы в битовой числовой последовательности;
дисперсия частоты появления логической единицы в битовой числовой последовательности;
для каждого диода из набора однотипных диодов выполняют следующие действия:
отмечают диод из набора однотипных диодов;
устанавливают диод в генератор аналогового шума измерительного устройства;
получают статистические характеристики числовой последовательности, относящиеся к отмеченному диоду, на выходе измерительного устройства;
сохраняют данные о статистических характеристиках отмеченного диод;
выбирают пару диодов из набора, осуществляя следующие действия:
отмечают пары диодов, имеющих максимальную разницу математического ожидания с идеальным значением и минимальную разницу значений математического ожидания в паре;
выбирают из совокупности пар диодов с минимальной разницей значений математического ожидания пару диодов, имеющих минимальную разницу значений дисперсии;
определяют положение диодов выбранной пары в генераторах аналогового шума генератора случайных чисел, осуществляя следующие действия:
устанавливают на основе случайного выбора диоды из выбранной пары в генераторы аналогового шума;
отмечают сведения об установленных диодах для каждого генератора аналогового шума (положение 1);
получают математическое ожидание числовой последовательности на выходе

генератора случайных чисел;

сохраняют значение полученного математического ожидания; меняют местами диоды в генераторах аналогового шума;

отмечают сведения об установленных диодах для каждого генератора аналогового шума (положение 2);

получают математическое ожидание числовой последовательности на выходе генератора случайных чисел;

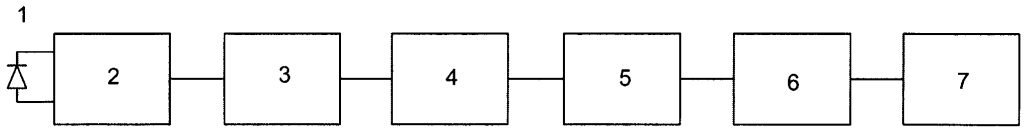
сравнивают значения математического ожидания числовой последовательности на выходе генератора случайных чисел для положения 1 и положения 2;

выбирают положение диодов с наименьшим отклонением от заданного значения математического ожидания и с наименьшим отклонением от заданного значения дисперсии числовой последовательности на выходе генератора случайных чисел;

устанавливают диоды в выбранное положение в генераторы аналогового шума для последующего использования в генераторе случайных чисел.

1

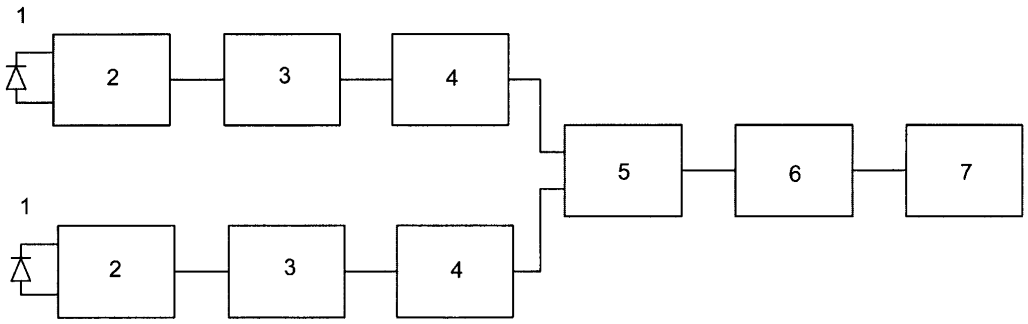
Способ выбора шумовых диодов с использованием измерительного устройства для генератора случайных чисел



Фиг. 1

2

Способ выбора шумовых диодов с использованием измерительного устройства для генератора случайных чисел



Фиг. 2