

(19)



**Евразийское
патентное
ведомство**

(21) **202192769** (13) **A1**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2023.04.19

(51) Int. Cl. **G06F 7/58** (2006.01)
H01L 45/00 (2006.01)

(22) Дата подачи заявки
2021.11.09

(54) СПОСОБ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ЧИСЕЛ С ПОМОЩЬЮ МЕМРИСТОРНОГО ИСТОЧНИКА СТОХАСТИЧЕСКИХ СИГНАЛОВ И УСТРОЙСТВО ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ

(31) **2021131573**

(32) **2021.10.28**

(33) **RU**

(71) Заявитель:
**ФЕДЕРАЛЬНОЕ
ГОСУДАРСТВЕННОЕ
АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ
"НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ
НИЖЕГОРОДСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ИМ. Н.И.
ЛОБАЧЕВСКОГО" (RU)**

(72) Изобретатель:

**Михайлов Алексей Николаевич,
Белов Алексей Иванович, Гусейнов
Давуд Вадимович, Королев Дмитрий
Сергеевич, Шамшин Максим
Олегович, Шарапов Александр
Николаевич, Лукоянов Виталий
Игоревич (RU)**

(74) Представитель:

Ваулина Л.В. (RU)

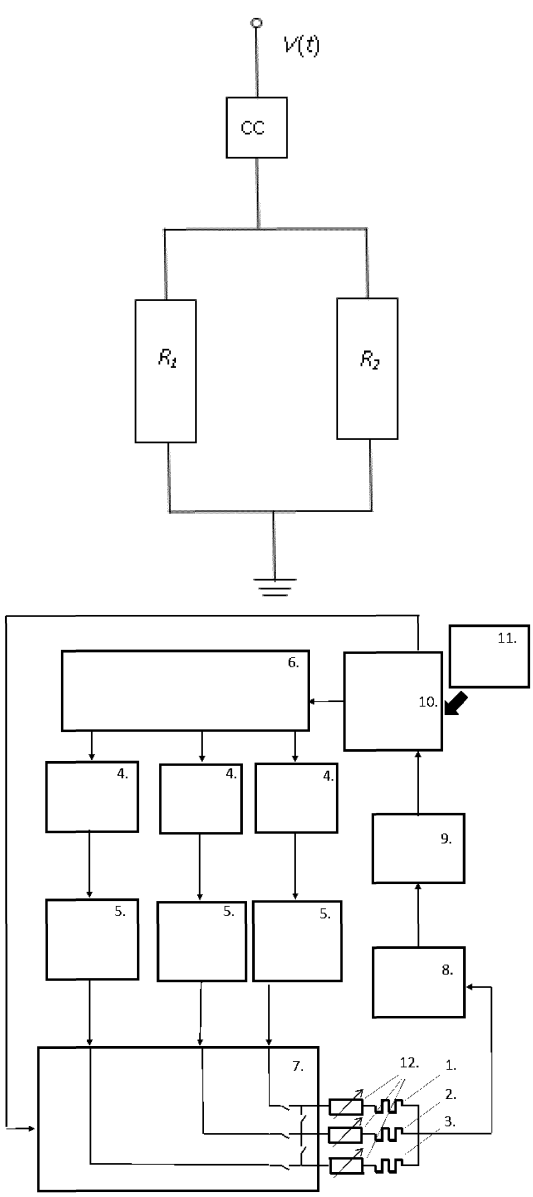
(57) Группа изобретений относится к мемристорной технологии генерации случайных чисел. Способ, включающий использование мемристорного источника стохастических сигналов и обработку последних в соответствии с алгоритмом формирования из них последовательности случайных чисел, характеризуется тем, что в качестве мемристорного источника стохастических сигналов используют параллельно соединённые мемристоры, максимально приближенные друг к другу по рабочим характеристикам их переключения из высокоомного в низкоомное состояние, в количестве как минимум двух, и обеспечивающие возможность съёма указанных стохастических сигналов в виде сигналов указанного переключения одного мемристора на выходе случайно включаемого первого из них при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения. Устройство для генерации случайных чисел, содержащее мемристорный источник стохастических сигналов и подключённый к нему модуль обработки указанных стохастических сигналов в соответствии с алгоритмом формирования из них последовательности случайных чисел, характеризуется тем, что мемристорный источник стохастических сигналов выполнен в виде параллельно соединённых мемристоров, максимально приближенных друг к другу по рабочим характеристикам их переключения из высокоомного в низкоомное состояние, в количестве как минимум двух, и оснащён блоком одновременной подачи на указанные мемристоры серии импульсов напряжения их переключения, а модуль обработки указанных стохастических сигналов снабжён блоком считывания сигналов указанного переключения снимаемых на выходе случайно включаемого первого из них при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения. Технический результат от использования предлагаемой группы изобретений заключается в упрощении подготовки стохастических сигналов и повышении эффективности и технологичности формирования последовательности случайных чисел за счёт возможности формирования разрядов битов на основе изменения количества мемристоров.

A1

202192769

202192769

A1



Способ генерации случайных чисел с помощью мемристорного
источника стохастических сигналов и устройство для его
осуществления

Группа изобретений относится к мемристорной технологии генерации случайных чисел и может быть использована в широком спектре приложений для обеспечения безопасности современного цифрового оборудования в связи с полезными свойствами мемристоров, включающими их низкое энергопотребление, большую скорость переключения и высокую масштабируемость.

Работа генераторов случайных чисел на мемристорах со структурой «металл-оксид-металл», представляющих собой новую разновидность аналоговых генераторов случайных чисел, основана на использовании мемристорных источников стохастических сигналов, возникающих в связи с естественным случайным характером переключения мемристоров в проводящее состояние (при подаче на них импульсов напряжения их переключения из высокоомного в низкоомное состояние) в результате формирования проводящих каналов (филаментов) в расположенной между мемристорными электродами наноразмерной активной среде, и последующей обработке указанных стохастических сигналов в соответствии с алгоритмом формирования из них последовательности случайных чисел.

Актуальность разработки таких генераторов случайных чисел подтверждается всплеском интереса к созданию аппаратных систем информационных баз на основе мемристоров со стороны ведущих мировых научных групп (см. статьи на англ. яз. авторов Y. Pang and

other «Memristors for Hardware Security Applications». Adv. Electron. Mater, 2019, p.1800872 и авторов R. Carboni, D. Ielmini «Stochastic Memory Devices for Security and Computing». Adv. Electron. Mater, 2019, p.1900198).

Уровень техники в области мемристорной технологии генерации случайных чисел характеризуется генераторами случайных чисел на мемристорах, характеризующихся особенностями подготовки (съёма и преобразования) самих стохастических сигналов из мемристорных источников.

Так, известен генератор случайных чисел с мемристорным источником стохастических сигналов (см. заявку на изобретение «True random number generator (TRNG) circuit using a diffusive memristor» US201903031041, G06F7/58, G06F7/58, H01L45/00, H03K3/84, 2019) выполненный в виде энергозависимого мемристора, выдающего снимаемый с него стохастически переключаемый выходной сигнал в связи со случайным временем задержки порогового переключения этого мемристора с последующими преобразованием компаратором этого сигнала в сигнал со случайной шириной импульса и синхронной логической обработкой последнего перед входом в схему счётчика, генерирующего выходной сигнал случайной последовательности битов, которая выдержала все 15-ть статистических тестов NIST (National Institute of Standards and Technology, США) для проверки случайности генерируемых величин.

Основным недостатком этого аналога является усложнение подготовки самого стохастического сигнала, вырабатываемого мемристорным источником, состоящим из одного энергозависимого мемристора, из-за выбора в качестве указанного стохастического сигнала непосредственно времени задержки переключения

мемристора и необходимости его преобразования в сигнал со случайной шириной импульса.

Ещё более усложнена мемристорная технология генерации случайных чисел в статьях на англ. яз. авторов Balatti S. and other «Physical unbiased generation of random numbers with coupled resistive switching devices». Electron Devices, 2016, v. 63, p. 2029 и авторов Teng Zhang and other «High-speed true random number generation based on paired memristors for security». Electronics Nanotechnology, 2017, v. 2, p. 455202, в которых предлагается подготовка стохастических сигналов мемристорных источников на основе съёма разницы стохастики, соответственно, по очереди и вариативно-усложнённо переключаемых двух независимых мемристоров (при вариации параметров резистивного переключения, например, таких как напряжение переключения между резистивными состояниями при вариации от цикла к циклу переключения, а также от мемристора к мемристор, а также сопротивление в различных резистивных состояниях).

Вариативность параметров переключения мемристоров и возможность многоуровневого изменения резистивного состояния были использованы при реализации базового элемента аппаратной защиты с использованием двухслойного массива 10×10 металл-оксидных мемристоров в топологии «кросс-бар» (см. статью на англ. яз. авторов H. Nili and other «Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors». Nature Electronics, 2018, v. 1, p. 197-202). Реализация основных криптографических функций таких массивов мемристоров выглядит следующим образом. На несколько строк матрицы мемристоров подается напряжение, а затем производится сравнение токов, текущих в одной половине столбцов, с токами, текущими в другой половине столбцов. Если ток, например, левой группы столбцов выше,

чем ток правой, то на однобитовом выходе фиксируется значение «1», если ниже, то «0». В дальнейшем эти величины преобразуются в последовательности сигналов, которые могут служить в качестве ключа шифрования.

Известен другой подход, который состоит в использовании шумов и флуктуаций тока в каком-либо резистивном состоянии, в основном – в высокопроводящем состоянии (см. инф. материал на англ. яз. авторов Nikolaos Vasileiadis and other «Random Number Generator Based on Multi-State Silicon Nitride Memristor Entropy Sources Combination». Proc. IEEE International Conference on Electronics, Information, and Communication (ICEIC), 2021).

К общим недостаткам рассмотренных аналогов реализации генераторов случайных чисел на мемристорах относятся сложность обслуживающих схем, включающих счетчики, компараторы, ключи и специальные логические схемы (см. инф. материал на англ. яз. авторов Nikolaos Vasileiadis and other «Random Number Generator Based on Multi-State Silicon Nitride Memristor Entropy Sources Combination». Proc. IEEE International Conference on Electronics, Information, and Communication (ICEIC), 2021) или необходимость организации программирования и считывания состояний в больших массивах мемристоров (см. статью на англ. яз. авторов H. Nili and other «Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors». Nature Electronics, 2018, v. 1, p. 197-202).

При этом, когда для генерации случайных чисел используется сравнение параметра переключения со средним значением, требуется тонкий подбор порога срабатывания компаратора для обеспечения равных вероятностей генерации значений «1» и «0» (см. инф. материал на англ. яз. авторов Nikolaos Vasileiadis and other «Random Number

Generator Based on Multi-State Silicon Nitride Memristor Entropy Sources Combination». Proc. IEEE International Conference on Electronics, Information, and Communication (ICEIC), 2021).

Недостатком упомянутых схем на основе спаренных мемристоров (см. статьи на англ. яз. авторов Balatti S. and other «Physical unbiased generation of random numbers with coupled resistive switching devices». Electron Devices, 2016, v. 63, p. 2029 и авторов Teng Zhang and other «High-speed true random number generation based on paired memristors for security». Electronics Nanotechnology, 2017, v. 2, p. 455202) является также то, что для генерации случайных чисел используется пара мемристоров с подачей электрических импульсов на каждый из них независимо, после чего проводится сравнение полученных значений сопротивления с заданной величиной, что также может приводить к отклонениям от равновероятного распределения сгенерированных случайных чисел и требует их дополнительной корректировки с использованием специальных схем.

В связи с отсутствием источников информации, содержащих близкую по механизму подготовку стохастических сигналов, которая в предлагаемых способе и устройстве для его осуществления предусматривает совместное одновременное участие двух или более запаралеленных мемристоров в расширении стохастических возможностей на основе качественно новой простой и эффективной конкуренции автономных стохастик этих мемристоров (когда филаментарный механизм автономного переключения каждого мемристора обеспечивает случайное равновероятное переключение в проводящее состояние одного из двух или более мемристоров при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения) заявителем выбрана форма раскрытия

сущности заявляемых способа и устройства для его осуществления без прототипа.

Технический результат от использования предлагаемых способа генерации случайных чисел с помощью мемристорного источника стохастических сигналов и устройства для его осуществления – упрощение подготовки стохастических сигналов и повышение эффективности и технологичности формирования последовательности случайных чисел за счёт возможности формирования разрядов битов на основе изменения количества мемристоров.

Для достижения указанного технического результата предлагаются

способ генерации случайных чисел, включающий использование мемристорного источника стохастических сигналов и обработку последних в соответствии с алгоритмом формирования из них последовательности случайных чисел, характеризующийся тем, что в качестве мемристорного источника стохастических сигналов используют параллельно соединённые мемристоры, максимально приближенные друг к другу по рабочим характеристикам их переключения из высокоомного в низкоомное состояние, в количестве, как минимум двух, и обеспечивающие возможность съёма указанных стохастических сигналов в виде значений тока, протекающего через один мемристор, после случайного равновероятного переключения в проводящее состояние одного из указанных мемристоров при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения,

и устройство для изложенной генерации случайных чисел, содержащее мемристорный источник стохастических сигналов и подключённый к нему модуль обработки указанных стохастических

сигналов в соответствии с алгоритмом формирования из них последовательности случайных чисел, характеризующийся тем, что мемристорный источник стохастических сигналов выполнен в виде параллельно соединённых мемристоров, максимально приближенных друг к другу по рабочим характеристикам их переключения из высокоомного в низкоомное состояние, в количестве, как минимум двух, и оснащён блоком одновременной подачи на указанные мемристоры серии импульсов напряжения их переключения, а модуль обработки указанных стохастических сигналов снабжён блоком считывания сигналов указанного переключения, снимаемых на выходе случайно включаемого одного из них при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения.

В частном случае выполнения мемристорного источника стохастических сигналов в виде трёх параллельно соединённых мемристоров, имеющих структуру $\text{Au/Zr/ZrO}_2(\text{Y})/\text{TiN/Ti}$, максимально приближенных друг к другу по рабочим вольт-амперным характеристикам их переключения из высокоомного в низкоомное состояние, блок одновременной подачи на указанные мемристоры серии импульсов напряжения их переключения выполнен трёхканальным, в каждом канале которого смонтированы последовательно соединённые масштабирующий усилитель и ограничитель обратного тока мемристора, соединённые на канальном входе с цифро-аналоговым преобразователем (ЦАП) и подключённые на канальном выходе с многоканальным входом мультиплексора настройки топологии цепи одновременной подачи на входы указанных мемристоров серии импульсов напряжения их переключения, а модуль обработки указанных стохастических сигналов в соответствии с алгоритмом формирования из них последовательности случайных чисел, снабжённый блоком считывания сигналов указанного

переключения, снимаемых на выходе случайно включаемого первого из них при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения, выполнен в виде одноканальной измерительной цепи, в которой смонтированы последовательно соединённые инвертирующий и масштабирующий усилители, соединённые на входе этой цепи с выходами мемристоров в составе мемристорного источника стохастических сигналов, подключенными на выходе этой цепи к аналого-цифровому преобразователю (АЦП) в составе контроллера, включённого в интерфейс «компьютер-контроллер» и подключённого с помощью цепи управления к входу указанного мультиплексора.

При этом для предэксплуатационной настройки мемристоров в составе мемристорного источника стохастических сигналов в связи возможными технологическими расхождениями в напряжениях переключения указанные мемристоры могут быть снабжены последовательными подстроечными резисторами.

На фиг. 1 показана принципиальная схема мемристорного источника стохастических сигналов, поясняющая на примере исполнения указанного источника на 2-х мемристорах механизм работы устройства для осуществления предлагаемого способа генерации случайных чисел; на фиг. 2 – блок-схема устройства для осуществления предлагаемого способа генерации случайных чисел с мемристорным источником стохастических сигналов, выполненным на 3-х мемристорах.

Предлагаемый способ генерации случайных чисел включает использование мемристорного источника стохастических сигналов, выполненного в виде параллельно соединённых мемристоров, максимально приближенных друг к другу по рабочим характеристикам их переключения из высокоомного в низкоомное состояние, в

количестве, как минимум двух (в примере выполнения в количестве трёх мемристоров), и обеспечивающих возможность съёма указанных стохастических сигналов в виде сигналов указанного переключения одного мемристора на выходе случайно включаемого первого из них при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения, и последующую обработку адресно снимаемых стохастических сигналов с мемристоров в соответствии с алгоритмом формирования из указанных сигналов последовательности случайных чисел, причём количество упомянутых мемристоров может быть два, три, четыре, восемь, шестнадцать и иное количество в зависимости от алгоритма указанного формирования.

При этом принцип осуществления предлагаемого способа можно рассмотреть на примере использования мемристорного источника стохастических сигналов на двух параллельных мемристорах с текущими значениями сопротивлений R_1 и R_2 (см. фиг. 1), подключенных к источнику внешнего напряжения через ограничитель тока «СС» (рис 1).

Напряжение, падающее на мемристорах, описывается следующим выражением:

$$\begin{cases} V = V_{in}, I < I_{cc} \\ V = I_{cc} \frac{R_1 R_2}{R_1 + R_2}, I \geq I_{cc} \end{cases}, \quad (1)$$

где V – напряжение на мемристорах, R_1 и R_2 – сопротивления мемристоров 1 и 2, а $I = V_{in} \cdot (R_1 + R_2) / (R_1 R_2)$ – ток в цепи, I_{cc} – ток ограничения.

Сопротивление мемристора может изменяться под действием внешнего напряжения в том случае, если оно превышает значение

напряжения переключения SET (порога) V_{th} . Так как в мемристорах процессы переключения имеют случайный характер, то даже при одновременном воздействии на оба мемристора напряжения $V \geq V_{th}$, один из мемристоров может переключиться раньше другого.

Приведем пример работы данного устройства при правильном выборе параметров схемы. Допустим, что на систему подается внешнее напряжение V_{in} в виде прямоугольных импульсов, а мемристоры в начальный момент находятся в состоянии с одинаковым сопротивлением $R_1 = R_2 = R$, таким, что ток, протекающий через ограничитель тока СС, не превышает I_{cc} . Тогда, согласно (1), напряжение на мемристорах равно внешнему напряжению $V = V_{in}$. Пусть при достижении порога $V_{in} = V_{th}$ мемристор 1 переключается и уменьшает свое сопротивление так, что ток в цепи $I = V_{in} \cdot (R_1 + R_2) / (R_1 R_2)$ достигает величины тока ограничения. В таком случае напряжение V на мемристорах падает ниже порогового значения V_{th} при любом значении V_{in} , и мемристор 2 уже не может переключиться. Далее с помощью импульса инициализации (RESET) система возвращается в исходное состояние, и процесс повторяется. При этом, вследствие случайности процесса переключения первым может переключиться уже мемристор 2. Таким образом реализуется генерация случайных чисел на схеме с двумя мемристорами по принципу «победитель забирает все».

В случае выполнения мемристорного источника стохастических сигналов (см. фиг. 2) в виде трёх параллельно соединённых мемристоров 1-3, имеющих структуру $Au/Zr/ZrO_2(Y)/TiN/Ti$, максимально приближенных друг к другу по рабочим вольт-амперным характеристикам их переключения из высокоомного в низкоомное состояние, блок одновременной подачи на указанные мемристоры серии импульсов напряжения их переключения выполнен трёхканальным, в каждом канале которого смонтированы

последовательно соединённые масштабирующий усилитель 4 и ограничитель обратного тока мемристора 5, соединённые на канальном входе с ЦАП 6 и подключённые на канальном выходе с многоканальным входом мультиплексора 7 для настройки топологии цепи одновременной подачи на входы указанных мемристоров серии импульсов напряжения их переключения, а модуль обработки указанных стохастических сигналов в соответствии с алгоритмом формирования из них последовательности случайных чисел, снабжённый блоком считывания сигналов указанного переключения, снимаемых на выходе случайно включаемого первого из них при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения, выполнен в виде одноканальной измерительной цепи, в которой смонтированы последовательно соединённые инвертирующий и масштабирующий усилители 8 и 9, соединённые на входе этой цепи с выходами мемристоров 1-3 в составе мемристорного источника стохастических сигналов подключенными на выходе этой цепи через инвертирующий и масштабирующий усилители к АЦП контроллера 10 (с функцией считывания сигналов переключения, снимаемых на выходе случайно включаемого одного из мемристоров 1-3 при одновременной подаче на них серии импульсов напряжения их переключения), включённого в интерфейс «компьютер-контроллер» 11 и подключённого с помощью цепи управления к входу мультиплексора 7.

При этом для предэксплуатационной настройки мемристоров 1-3 в составе мемристорного источника стохастических сигналов указанные мемристоры снабжены подстроечными резисторами 12, последовательно подключёнными к ним с возможностью предэксплуатационной компенсации технологических расхождений в напряжениях переключения этих мемристоров.

Входящие в состав изложенного устройства составляющие имеют особенности выполнения.

Интерфейс 11, реализован при помощи адаптера USB-UART (CP2102). Обеспечивает возможность управления устройством через специальную desktop-программу (разработана в среде Qt Creator).

8-ми битный контроллер 10 фирмы Atmel Atmega328p со встроенным 10-ти битным АЦП. Используется для управления периферийными узлами устройства.

Восьмиканальный 12-ти битовый ЦАП 6 фирмы Analog Devices AD5308.

Масштабирующий усилитель напряжения 4 на основе мощностного операционного усилителя TCA0372. Используется для преобразования исходного униполярного маломощного сигнала отдельного канала ЦАП 6 в достаточно мощный (номинальный максимальный выходной ток ОУ – 1 А) биполярный сигнал, способный производить настройку состояния мемристоров 1-3 в широких пределах.

Ограничитель обратного тока мемристора 5 (ограничение до 250 мкА). Используется для безопасного управления мемристорами 1-3. Состоит из диода Шоттки (1PS76SB10, 115) и *p*-канального *j*FET (MMBFJ177);

Мультиплексор 7 на основе аналоговых 4-х канальных ключей DG445DY. Позволяет менять топологию цепи, переходя от цепи обычного конфигулятора к цепи мемристорного источника стохастических сигналов.

Подстроечные резисторы 12, элементы для предэксплуатационной настройки мемристоров 1-3, имеющих

технологические отклонения от номинала вольтамперной характеристики (последовательные сопротивления).

Инвертирующий усилитель 8 на основе ОУ ТСА0372. Обеспечивает суммирование токов всех используемых каналов одновременной подачи на мемристоры 1-3 серии импульсов напряжения их переключения.

Масштабирующий усилитель напряжения 9 на основе прецизионного усилителя фирмы National Instruments, используемый для перевода измеряемого биполярного сигнала в маломощный униполярный с диапазоном напряжений, приемлемым для встроенного в контроллер 10 АЦП.

Управление устройством для осуществления предлагаемого способа в примере выполнения производится с компьютера через специальную desktop-программу, разработанную в среде Qt Creator. Программа позволяет переключаться между режимами управления мемристорами 1-3 (режим измерения вольт-амперной характеристики мемристоров 1-3, режим задания целевого сопротивления и режим генерации случайных значений). Режим измерения вольт-амперной характеристики указанной программой производится путем подачи пилообразного напряжения на вход отдельных мемристоров 1-3.

Причём, значения максимума и минимума входного напряжения могут быть изменены непосредственно во время измерения вольт-амперной характеристики мемристоров 1-3. Такой подход измерения оказывает воздействие на состояния проводимости мемристора, что позволяет, в конечном счете, получить ярко выраженную гистерезисную картину, а также повлиять на состояния ветвей гистерезиса. Режим указанной программы для задания целевого сопротивления основывается на следующей идее: достаточно

большим отрицательным импульсом напряжения (3-8 В) устанавливается открытое состояние мемристора (ON), далее подаётся последовательная серия возрастающих положительных импульсов, каждый из которых уменьшает текущее значение проводимости мемристоров 1-3, приближая его к целевому, что контролируется путем повторяющихся измерений проводимости. Наконец, режим генерации случайных значений проводимости выполняется путём чередования 2-х коммутационных режимов при помощи мультиплексора 7. Режим мультиплексации обеспечивает общее соединение между входами мемристоров 1-3, а также последовательное соединение этих мемристоров, каждого со своим резистором 12. На выведенные в закрытое состояние (OFF) мемристоры 1-3 приходит общий отрицательный импульс, переводя один из трёх мемристоров в открытое состояние так, что с учётом ограничения тока на ограничителе тока 5 остальные мемристоры шунтируются открывшимся и, таким образом, остаются закрытыми. Номер случайно открытого мемристора в таком случае и есть случайное число, сгенерированное устройством.

Реализация интерфейса «компьютер-контроллер» 11 выполнена за счет адаптера USB-UART (CP2102). Команды, отправляемые описываемому устройству, поступают на контроллер 10 Atmel Atmega328p при помощи встроенного в контроллер 10 uart-модуля (BAUDRATE = 115200). Таким образом в устройстве осуществляется переключение между режимами указанной ранее программы и отсылка измеренных величин тока этой программе. Измерение величины тока производится при помощи встроенного в контроллер 10 АЦП (10 бит). Подача импульсов напряжений на мемристоры 1-3 производится с помощью восьмиканального 12-ти битового ЦАП 6 фирмы Analog Devices AD5308, соединенного с контроллером 10 через SPI-

интерфейс. ЦАП 6 представляет собой основное звено канала подачи на мемристоры 1-3 серии импульсов напряжения их переключения. Следующий элемент указанного канала – масштабирующий усилитель 4, выполненный на основе мощностного операционного усилителя TCA0372. Используется для преобразования исходного униполярного маломощного сигнала отдельного канала ЦАП 6 в достаточно мощный (номинальный максимальный выходной ток ОУ – 1 А) биполярный сигнал, способный производить настройку состояния мемристоров 1-3 в широких пределах. Полученный таким образом биполярный сигнал подается на ограничитель обратного тока мемристора 6 (ограничение до 250 мкА). Ограничитель 6 используется для безопасного управления мемристорами 1-3 и состоит из диода Шоттки (1PS76SB10, 115) и *p*-канального *j*FET (MMBFJ177). Каналы блока одновременной подачи на мемристоры 1-3 серии импульсов напряжения их переключения соединяются со входами мемристоров 1-3, мультиплексируясь с ними должным образом согласно режимам указанной выше программы. Токи всех этих каналов суммируются при помощи инвертирующего усилителя 8, реализованного за счет микросхемы TCA0372. Суммарный ток подлежит измерению при помощи АЦП, о чем упоминалось выше. Для измерения тока его значение масштабируется до приемлемого АЦП значения (используется прецизионный усилитель 9 фирмы National Instruments для перевода измеряемого биполярного сигнала в маломощный униполярный).

Изложенное позволяет сделать вывод в отношении предлагаемых способа и устройства для его осуществления о повышении эффективности генерации случайных чисел с помощью мемристоров в результате упрощения подготовки стохастических сигналов и повышения технологичности формирования

последовательности случайных чисел за счёт возможности формирования разрядов битов в связи с возможностью изменения количества мемристоров (наиболее оптимальным для современной микроэлектроники является количество мемристоров – 16) .

Формула изобретения

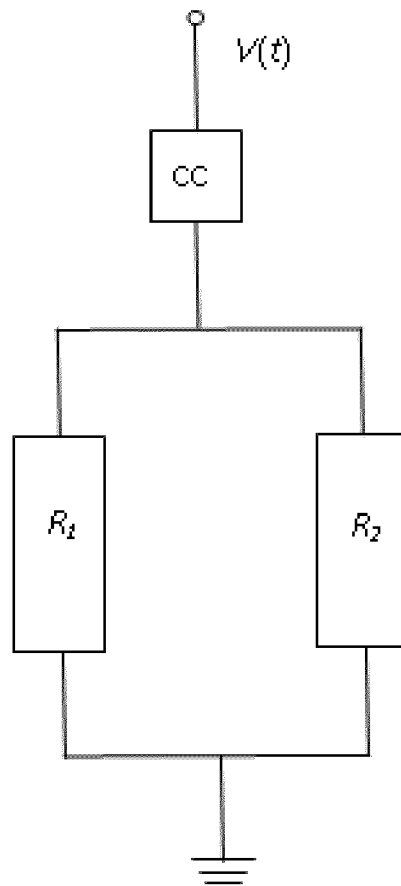
1. Способ генерации случайных чисел, включающий использование мемристорного источника стохастических сигналов и обработку последних в соответствии с алгоритмом формирования из них последовательности случайных чисел, характеризующийся тем, что в качестве мемристорного источника стохастических сигналов используют параллельно соединённые мемристоры, максимально приближенные друг к другу по рабочим характеристикам их переключения из высокоомного в низкоомное состояние, в количестве, как минимум двух, и обеспечивающие возможность съёма указанных стохастических сигналов в виде сигналов указанного переключения одного мемристора на выходе случайно включаемого первого из них при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения.

2. Устройство для генерации случайных чисел по п. 1, содержащее мемристорный источник стохастических сигналов и подключённый к нему модуль обработки указанных стохастических сигналов в соответствии с алгоритмом формирования из них последовательности случайных чисел, характеризующийся тем, что мемристорный источник стохастических сигналов выполнен в виде параллельно соединённых мемристоров, максимально приближенных друг к другу по рабочим характеристикам их переключения из высокоомного в низкоомное состояние, в количестве, как минимум двух, и оснащён блоком одновременной подачи на указанные мемристоры серии импульсов напряжения их переключения, а модуль обработки указанных стохастических сигналов снабжён блоком считывания сигналов указанного переключения снимаемых на выходе случайно включаемого первого из них при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения.

3. Устройство по п. 2, отличающееся тем, что в случае выполнения мемристорного источника стохатических сигналов в виде трёх параллельно соединённых мемристоров, имеющих структуру $\text{Au/Zr/ZrO}_2(\text{Y})/\text{TiN/Ti}$, максимально приближенных друг к другу по рабочим вольт-амперным характеристикам их переключения из высокоомного в низкоомное состояние, блок одновременной подачи на указанные мемристоры серии импульсов напряжения их переключения выполнен трёхканальным, в каждом канале которого смонтированы последовательно соединённые масштабирующий усилитель и ограничитель обратного тока мемристора соединённые на канальном входе с цифро-аналоговым преобразователем и подключённые на канальном выходе с многоканальным входом мультиплексора настройки топологии цепи одновременной подачи на входы указанных мемристоров серии импульсов напряжения их переключения, а модуль обработки указанных стохастических сигналов в соответствии с алгоритмом формирования из них последовательности случайных чисел, снабжённый блоком считывания сигналов указанного переключения, снимаемых на выходе случайно включаемого первого из них при одновременной подаче на эти мемристоры серии импульсов напряжения их переключения, выполнен в виде одноканальной измерительной цепи, в которой смонтированы последовательно соединённые инвертирующий и масштабирующий усилители, соединённые на входе этой цепи с выходами мемристоров в составе мемристорного источника стохатических сигналов и подключённые на выходе этой цепи к аналого-цифровому преобразователю в составе контроллера, включённого в интерфейс «компьютер-контроллер» и подключённого с помощью цепи управления к входу указанного мультиплексора.

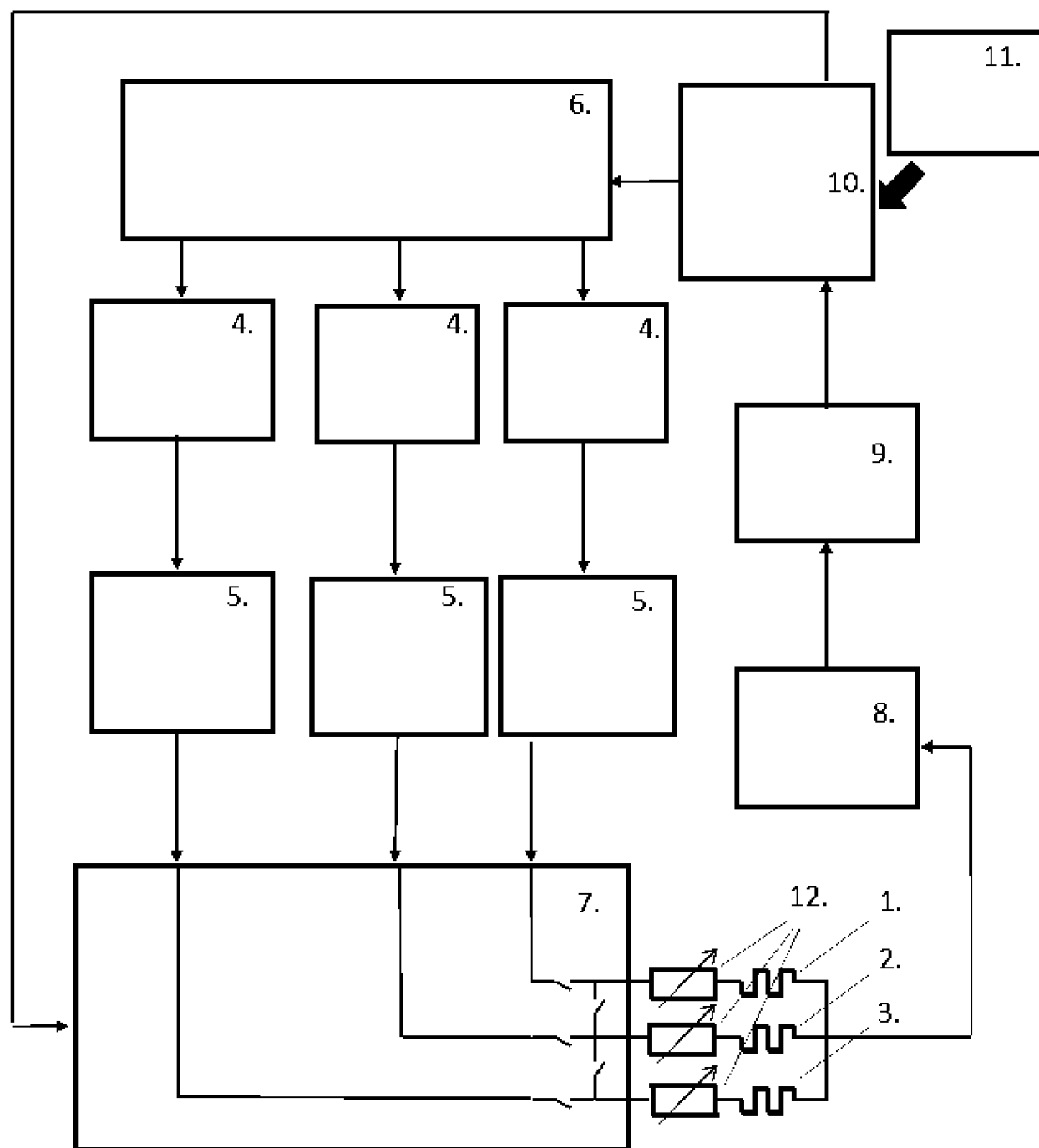
4. Устройство по п. 2, отличающееся тем, что мемристоры в составе мемристорного источника стохастических сигналов снабжены подстроечными резисторами.

Способ генерации случайных чисел
с помощью мемристорного источника стохастических сигналов
и устройство для его осуществления



Фиг. 1

Способ генерации случайных чисел
с помощью мемристорного источника стохастических сигналов
и устройство для его осуществления



Фиг. 2.

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ
(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки:

202192769

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

G06F 7/58 (2006.01)

H01L 45/00 (2006.01)

Согласно Международной патентной классификации (МПК)

Б. ОБЛАСТЬ ПОИСКА:

Просмотренная документация (система классификации и индексы МПК)

G06F 7/00 - G06F 7/78, H01L 45/00, H03K 19/00 - H03K 19/23, H04L9/00

Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, используемые поисковые термины)
EPO Espacenet, WIPO Patentscope, ЕАПАТИС

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	RU 2744246 (Федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского"), 04.03.2020, весь документ	1-4
A	US 2020/0335162 A1 (UNIV KING ABDULLAH SCI & TECH), 22.10.2020, весь документ	1-4
A	CN 111294197 A (UNIV EAST CHINA JIAOTONG), 16.06.2020, весь документ	1-4
A	US 2019/0042201 A1 (MILANO POLITECNICO), 07.02. 2019, пар. 0030-0045	1-4

☐ последующие документы указаны в продолжении

* Особые категории ссылочных документов:

«А» - документ, определяющий общий уровень техники

«D» - документ, приведенный в евразийской заявке

«Е» - более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее

«О» - документ, относящийся к устному раскрытию, экспонированию и т.д.

"Р" - документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета"

«Т» - более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения

«Х» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности

«У» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории

«&» - документ, являющийся патентом-аналогом

«L» - документ, приведенный в других целях

Дата проведения патентного поиска: **09/11/2022**

Уполномоченное лицо:

Начальник отдела механики,
физики и электротехники



Д.Ф. Крылов