О. К. БАРАНОВСКИЙ, д. ф.-м. н. П. В. КУЧИНСКИЙ, к. ф.-м. н. И. З. РУТКОВСКИЙ

Республика Беларусь, г. Минск, НИИ ПФП им. А. Н. Севченко
E-mail: baranouski@bsu.by

Дата поступления в редакцию
14.03—25.10 2006 г.
Оппонент *д. т. н. В. С. СИТНИКОВ*
(ОНПУ, г. Одесса)

КОМПЬЮТЕРНАЯ СИСТЕМА ОТБОРА КРЕМНИЕВЫХ ДИОДОВ ДЛЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Разработана компьютерная система для анализа характеристик случайных потоков шумовых импульсов кремниевых диодов с микроплазмами, используемых в генераторах случайных числовых последовательностей.

При генерации случайных числовых последовательностей (**СЧП**) с заданными статистическими свойствами необходимо использовать физические источники шума согласно современным стандартам для криптографических алгоритмов. Полупроводниковые диоды, работающие в режиме микроплазменного пробоя [1], применяются в генераторах случайных числовых последовательностей (**ГСЧП**) в качестве первичного источника случайности. В соответствии с алгоритмом генерации на последовательно расположенных интервалах времени фиксированной длительности $(0, T]$ подсчитывается количество шумовых импульсов $N(T)$ и формируется «0», если $N(T)$ четное, и «1», если $N(T)$ нечетное число [2, 3].

Обычно предполагается, что количество зарегистрированных шумовых импульсов $N(T)$ подчиняется распределению Пуассона

$$P\{N(T)=i\}=(\lambda T)^i/i!\cdot\exp\{-\lambda T\},\ i=0, 1, \ldots,$$

где λ — интенсивность потока шумовых импульсов.

Однако вероятностные свойства сигналов реальных диодов отличаются от модели идеального источника вследствие физических принципов их функционирования. Любые функциональные преобразования, действующие на первичный пуассоновский поток событий, вносят корреляцию между элементами последовательности $\{N(T)\}$, что уменьшает энтропию СЧП. Методики измерений и анализа характеристик шумовых сигналов являются уникальными для каждой из научных групп, занимающихся разработкой ГСЧП, и авторам неизвестны.

В связи с этим актуальной является задача разработки комплекса аппаратуры и методики, позволяющих автоматизировать процесс анализа случайных сигналов полупроводниковых источников шума в целях их отбора и выбора режимов работы для применения в ГСЧП.

Компьютерная система и методика анализа

Для измерения и анализа характеристик случайных сигналов диодов разработана и изготовлена компьютерная система, включающая аппаратную и программную части. Аппаратная часть (**рис. 1**) состоит из блока установки рабочих режимов и блока регистрации и анализа сигнала. Первый блок содержит генератор тока (*1*), схему контроля напряжения на полупроводниковом генераторе шума и термостат (*2*).

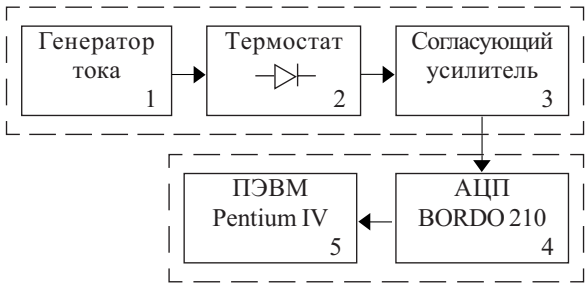

Рис. 1. Структурная схема системы регистрации шумового сигнала

Установка режимов измерения проводится в диапазоне токов 0,1—400 мкА и температур от комнатной до 90°С. Широкополосное согласование генератора шума с АЦП ПЭВМ осуществляется с помощью усилителя тока на быстродействующем операционном усилителе (*3*). В качестве АЦП (*4*) используется блок осциллографический BORDO 210 с шиной PCI. Блок имеет 10-разрядный АЦП с максимальной частотой дискретизации 100 Мвыб/с, емкость буферной памяти составляет 128 Кбайт.

Программная часть системы предназначена для записи и математической обработки электрического сигнала в режиме реального времени и представляет собой Windows-приложение, работающее на ПЭВМ (*5*) класса Pentium IV.

В основе методики анализа качества источников шума, применяемых в указанном выше алгоритме генерации, лежит представление последовательности шумовых импульсов на выходе диодов как случайного потока событий на временной оси, для анализа характеристик которого применяется аппарат математической статистики и теории вероятностей. Задача оператора компьютерной системы состоит в установлении меры отклонения вероятностных свойств последовательности $\{N(T)\}$ от свойств идеальной последовательности при заданных рабочем режиме источника шума и условиях селекции импульсов из суммарного шума [2, 3].

Так как оценка функции распределения последовательности $\{N(T)\}$ является сложной задачей, для решения которой необходимо установить вносимые в исходный пуассоновский поток типы функциональных преобразований и их законы распределения, то в системе присутствует возможность измерения амплитуды U и интервалов времени следования ΔT шумовых импульсов, подсчета количества шумовых импульсов $N(T)$ на последовательных интервалах времени.

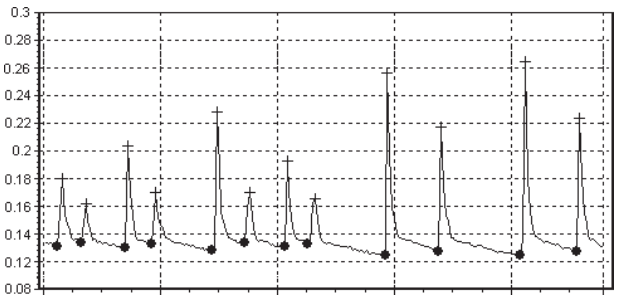

Рис. 2. Копия экрана с осциллограммой шумового сигнала и выделенными из него шумовыми импульсами

На **рис. 2** представлена осциллограмма шумового сигнала и выделенных из него (с применением разработанных алгоритмов селекции) шумовых импульсов («•» отображает момент времени появления импульсов, «+» — момент времени и амплитуду импульсов в наивысшей точке). Для указанных параметров (U, ΔT, $N(T)$) разработана библиотека подпрограмм оценки статистических и вероятностных характеристик:

— автокорреляционной функции ΔT, $N(T)$;

— взаимнокорреляционных функций $N(T)$ для разных условий эксперимента;

— описательной статистики для ΔT, $N(T)$, U;

— гистограмм относительных частот для ΔT, $N(T)$, U и суммы интервалов следования $\sum\Delta T_i$ (i=1,…,n) с возможностью оценки функции распределения;

— условных гистограмм относительных частот для ΔT, $N(T)$, U;

— фазовых траекторий для ΔT, $N(T)$;

— проверки стационарности темпа генерации шумовых импульсов.

В основе критерия отбора диодов и выбора их рабочих режимов лежит оценка стационарности темпа генерации шумовых импульсов и оценка корреляции между элементами последовательности $\{N(T)\}$. Для диодов, удовлетворяющих этому критерию, устанавливаются рабочие режимы (температура, средний ток, величина интервала счета импульсов), при которых корреляция между элементами $\{N(T)\}$ стремится к нулю. В этом случае при определенной величине T гистограмма $N(T)$ аппроксимируется нормальной функцией распределения [4, с. 427—434]. В результате становится возможным оценить энтропию, которая будет содержаться в каждом бите формируемых СЧП [5].

Для непосредственной оценки качества СЧП, формируемых при заданных режимах работы диодов и режимах селекции шумовых импульсов, предусмотрена возможность генерации файлов СЧП, а также использования простейших тестов на равномерность распределения [6]. По желанию оператор может применять алгоритмы улучшения равномерности распределения СЧП: метод Неймана или метод сложения по модулю 2 [7, с. 472—479].

Результаты эксперимента и их анализ

В физическом эксперименте исследовались кремниевые диоды — генераторы микроплазменного шума, отличающиеся напряжением пробоя $U_{пр}$: 8 и 11 В. Объем выборок диодов составлял по 11 образцов.

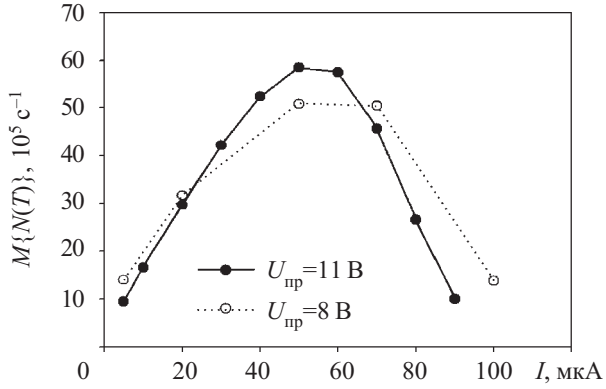

Рис. 3. Зависимость средней интенсивности шумовых импульсов от среднего тока диодов при температуре 30°С

На **рис. 3** представлены зависимости средней интенсивности шумовых импульсов от среднего тока диодов при температуре 30°С. Темп генерации шумовых импульсов определяется вероятностями включения-выключения лавинного тока в микроплазменных образованиях p–n-перехода. Данные вероятности зависят от температуры и среднего тока диодов. Видно, что наибольшая интенсивность импульсов соответствует среднему току около 50 мкА для обоих типов диодов.

Мерой, характеризующей ширину кривой распределения $N(T)$, является фактор Фано [8]

$$FF=\sigma^2\{N(T)\}/M\{N(T)\},$$

где $\sigma^2\{N(T)\}$ и $M\{N(T)\}$ — дисперсия и математическое ожидание, соответственно.

Если выходной поток шумовых импульсов является результатом прореживания одним из случайных функциональных преобразований исходного пуассоновского потока, фактор Фано может использоваться как мера близости по вероятностным свойствам

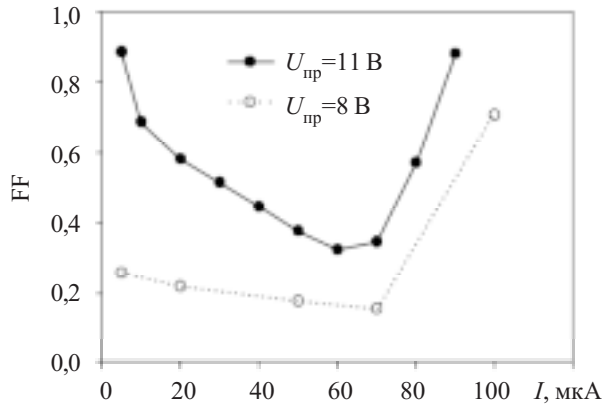

Рис. 4. Зависимость фактора Фано от среднего тока диодов при температуре 30°С

результирующего потока к пуассоновскому (для потока Пуассона FF=1).

На **рис. 4** представлены зависимости фактора Фано от среднего тока диодов при температуре 30°С. Видно, что фактор Фано меньше единицы во всем диапазоне рабочих токов диодов. Это значит, что поток шумовых импульсов не может быть описан пуассоновской статистикой. При этом потоки шумовых импульсов диодов с $U_{пр}$=11 В ближе к идеальной модели пуассоновского потока по вероятностным свойствам, чем для диодов с $U_{пр}$=8 В.

На **рис. 5** представлены гистограммы относительных частот количества зарегистрированных шумовых импульсов диодов с $U_{пр}$=8 В, характеризующихся стационарным темпом генерации импульсов, с одной и двумя микроплазмами (**МП**) в области пространственного заряда. Видно, что для диода с одной микроплазмой (1 МП) гистограмма имеет один максимум и аппроксимируется нормальной функцией распределения, для диода с двумя микроплазмами (2 МП) — два максимума. В последнем случае микроплазмы характеризуются разными интенсивностями генерации импульсов.

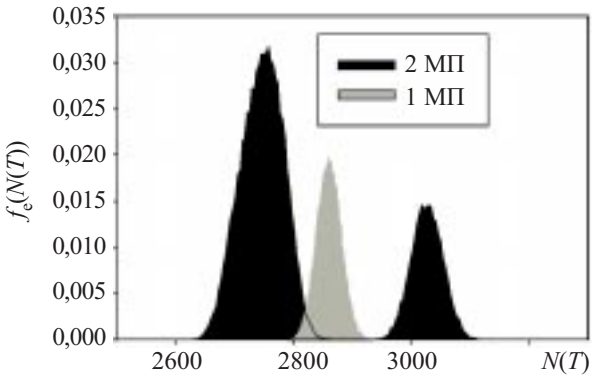

Рис. 5. Гистограмма относительных частот количества шумовых импульсов диодов с $U_{пр}$=8 В, имеющих одну и две микроплазмы, при температуре 30°С, среднем токе 50 мкА и интервале времени счета $0{,}6 \cdot 10^{-3}$ с

Зависимости корреляции между количеством шумовых импульсов в соседних интервалах времени счета $C_{N(T)}(1)$ от ширины интервалов для диодов с $U_{пр}$=8 В, имеющих соответственно одну и две микроплазмы, представлены на **рис. 6** (интервалы времени счета нормированы на средний интервал времени следования шумовых импульсов $M\{\Delta T\}$). Видно, что для диода с одной микроплазмой корреляция стремится к нулю с увеличением времени счета импульсов. Для диода с двумя микроплазмами начиная с некоторой величины интервала T>10$M\{\Delta T\}$ наблюдается возрастание положительной корреляции, которая достигает максимума при интервалах счета импульсов, приблизительно равных среднему интервалу времени между переключениями лавинного умножения из одной микроплазмы в другую.

Таким образом, в рамках экспериментального исследования проведены отбор диодов со стационарным темпом генерации импульсов в микроплазменном образовании p–n-перехода, выбор их рабочих режимов и режимов селекции импульсов, при которых средняя интенсивность шумовых импульсов

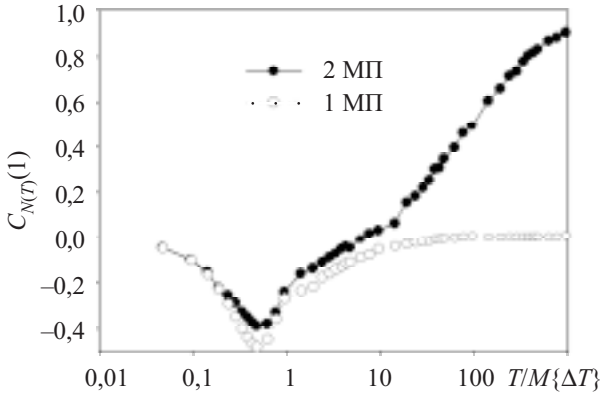

Рис. 6. Зависимость корреляции между количеством шумовых импульсов в соседних интервалах времени счета от ширины интервалов для диодов с $U_{пр}$=8 В при температуре 30°С и среднем токе 50 мкА

$M\{N(T)\}$, фактор Фано FF, корреляция между количеством зарегистрированных импульсов в соседних интервалах пересчета $C_{N(T)}(1)$ и длительность этого интервала T удовлетворяют заданным значениям. Результаты эксперимента подтвердили возможность применения этих диодов в генераторах случайных числовых последовательностей.

Заключение

Разработана автоматизированная компьютерная система, позволяющая решать задачи измерения характеристик шумовых импульсов диодов, анализа статистических и вероятностных свойств случайных потоков импульсов со средней интенсивностью до 10 МГц. Система использована в методике формирования случайных потоков шумовых импульсов с заданными статистическими свойствами, включающей отбраковку диодов — генераторов микроплазменного шума и выбор их рабочих режимов. Показано, что для генерации случайных числовых последовательностей гарантированного качества необходимо отбирать диоды с одной микроплазмой в области пространственного заряда, что обеспечивает уменьшение корреляции между количеством зарегистрированных импульсов в соседних интервалах времени счета при увеличении их длительности.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Грехов И. В., Сережкин Ю. Н. Лавинный пробой p–n-перехода в полупроводниках.— Л.: Энергия, 1980.

2. Бобнев М. П. Генерирование случайных сигналов.— М.: Энергия, 1971.

3. Vincent C. The generation of truly random binary numbers // Journal of Physics E.— 1970.— Vol. 3, N 8.— P. 594—598.

4. Тихонов В. И., Миронов Н. А. Марковские процессы.— М.: Сов. радио, 1977.

5. Барановский О. К., Кучинский П. В., Чернявский А. Ф. Оценка энтропии случайных числовых последовательностей, формируемых с использованием физического источника шума // Вести НАН Беларуси. Сер. Физ.-мат. наук.— 2004.— № 4.— С. 105—110.

6. Иванов М. А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей.— М.: КУДИЦ-ОБРАЗ, 2003.

7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.— М.: Триумф, 2002.

8. Fano U. Ionization yield of radiations. II. The fluctuations of the number of ions // Phys. Rev.— 1947.— Vol. 72, N 1.— P. 26—29.