ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной физики и метаматериалов
на базе Саратовского филиала
Института радиотехники и электроники
имени В.А. Котельникова РАН

ВОЗМОЖНОСТЬ СОЗДАНИЯ ГЕНЕРАТОРА ИСТИННО-СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ ПОЛУПРОВОДНИКОВЫХ СВЕРХРЕШЕТОК

АВТОРЕФЕРАТ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ
(БАКАЛАВРСКОЙ) РАБОТЫ
студента 4 курса 432 группы
направления 03.03.02 «Физика» физического факультета
Ермолаева Антона Александровича

Научный руководитель
к.ф.-м.н. доцент А.С. Ремизов

Заведующий кафедрой
д.ф.-м.н. профессор В.М. Аникин

Саратов
2018

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуализация проблемы. Генераторы случайных чисел (или случайных бит) имеют решающее значение для обеспечения безопасности коммуникаций, передачи и хранения данных, осуществления электронных транзакций, для проведения симуляций стохастических (случайных процессов) и многих других приложений. Поскольку программные генерируемые случайные последовательности не являются действительно случайными, быстрые энтропийные источники, такие как квантовые системы или классически хаотические системы, могут быть жизнеспособными альтернативами, если они генерируют качественные случайные последовательности достаточно быстро.

Целью данной работы ставится изучение проблематики создания генераторов истинно-случайных последовательностей и исследование модели построения такого генератора на основе полупроводниковых сверхрешеток. В работе рассматриваются: математическая модель для описания спонтанного хаоса в полупроводниковых сверхрешетках при комнатной температуре, предлагаемую авторами статьи [1], численные решения модели (выявляющие происхождение и характеристики хаотических колебаний) и ее ограничения; схема извлечения случайных биты из аналогового хаотического сигнала, создаваемого сверхрешеткой.

В **задачи** работы входит:

1) описание проблематики построение генераторов случайных последовательностей, обсуждение современных идей построения аппаратных генераторов;

2) изучение и анализ одной из существующих моделей построения генератора случайных чисел на основе полупроводниковых сверхрешеток [1].

Структура и объем работы. Выпускная квалификационная работа изложена на 38 страницах, состоит из введения, 4 глав, двух приложений и заключения. Библиографический список включает 51 наименование.

СОДЕРЖАНИЕ РАБОТЫ

В работе комментируется возможное использование спонтанно хаотических полупроводниковых сверхрешеток (SL) как истинных генераторов случайных чисел, следуя статье [1]. В главе 1 обсуждаются проблемы генерации случайных чисел и варианты генераторов истинно-случайных чисел. В главе 2 обсуждается математическую модель для одного SL под напряжением. Модель состоит из ряда связанных стохастических дифференциальных уравнений вместе с алгебраическими условиями смещения границы и напряжения. В главе 3 на основании численных решений модельных уравнений показано, что тепловые и шумовые шумы, существующие в SL, усиливают стабильный спонтанный хаос в интервалах напряжения, где соответствующая детерминированная модель проявляет хаос. Шумы также индуцируют хаос в соседних интервалах напряжения, где детерминированная система имела периодические колебания. Проводится также сравнение теоретических результатов с экспериментом и даются предложения об изменении параметров модели с целью оптимизации хаотических колебаний. В главе 3 также поясняется в соответствии с [2] поясняется, как получить высокоскоростной генератор случайных битов, обрабатывая хаотические колебания тока, предоставляемые устройством. В главе 4 рассматриваются перспективы для быстрых генераторов случайных битов на основе полупроводниковых сверхрешеток. В двух Приложениях даны подробные сведения о выводе модельных уравнений.

Графическая демонстрация результатов представлена на рисунках.

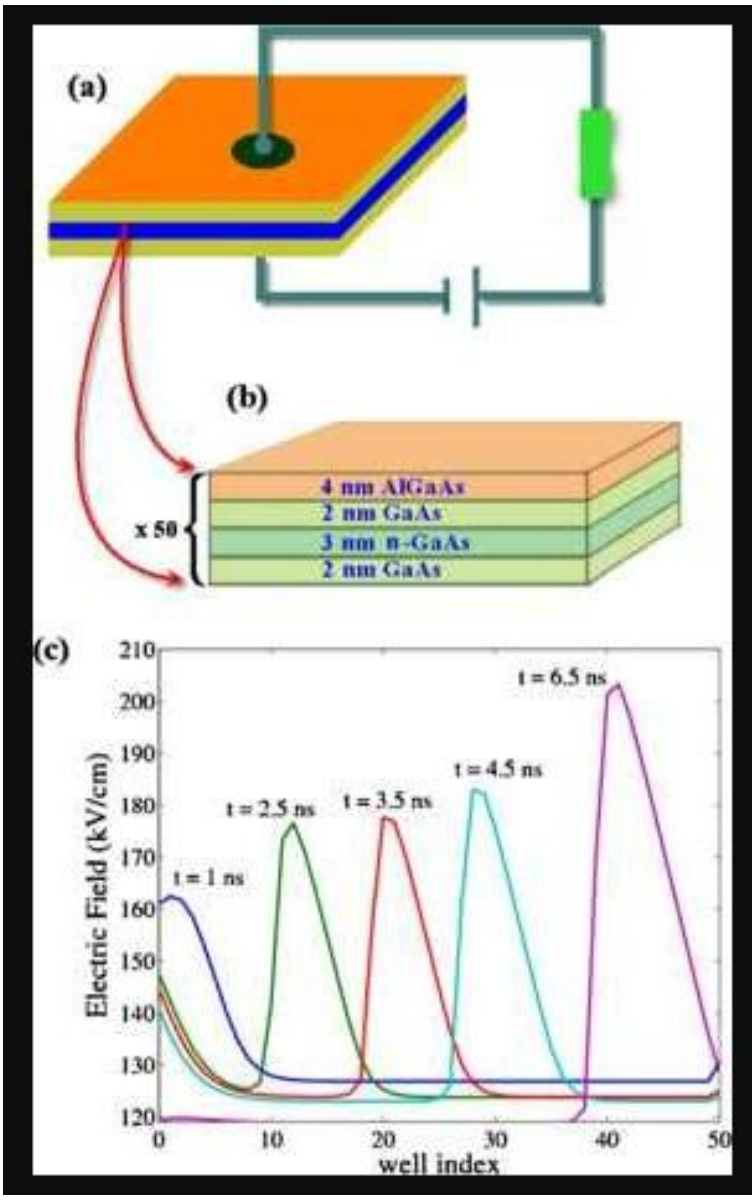

Рисунок 1. Схема мезоподобного полупроводникового сверхрешетчатого устройства из двух контактных областей шириной около 0,5 мкм и 50 периодов, образованных двумя полупроводниковыми слоями с различными запрещенными зонами и картина напряженности электрического поля во время колебаний. Показана картина напряженности электрического поля в разное время одного периода колебаний для смещения 7,532 В.

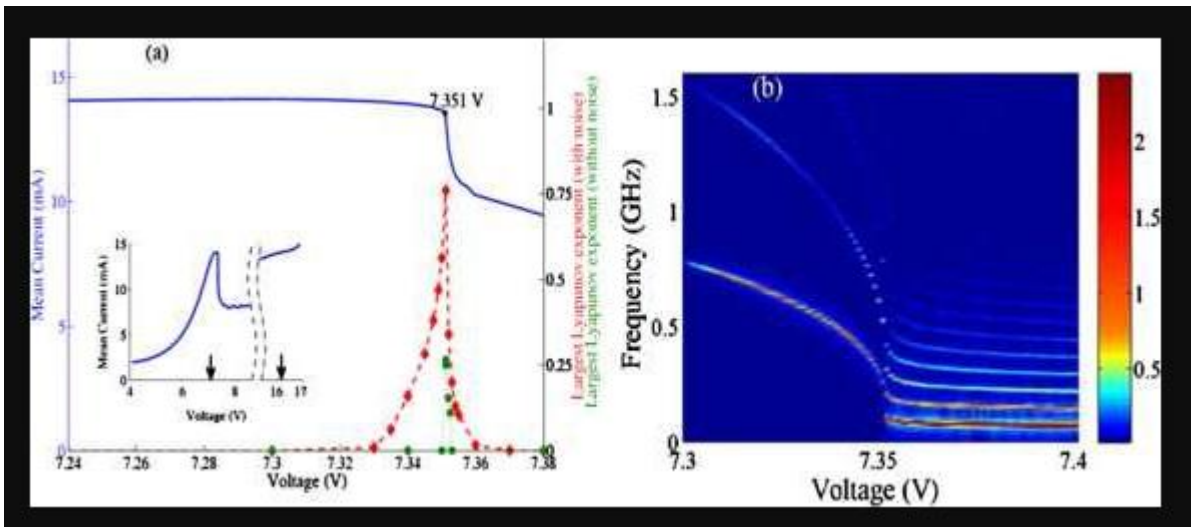

Рисунок 2. Средний ток, наибольший показатель Ляпунова и спектр Фурье по напряжению. (а) средний ток и наибольший показатель Ляпунова по напряжению и (б) спектр Фурье от напряжения для второго осциллирующего интервала. Вставка на панели (а) показывает средний ток для большего интервала напряжения, а вертикальные стрелки обозначают сверхкритические точки бифуркации Хопфа, ограничивающие второй интервал колебательного напряжения. Без шума интервал напряжения спонтанного хаоса очень узкий (ширина 3 мВ), а LLE составляет всего 0,25. Внутренний шум увеличивает LLE до 0,76 и расширяет до 30 мВ диапазона напряжений для спонтанного хаоса

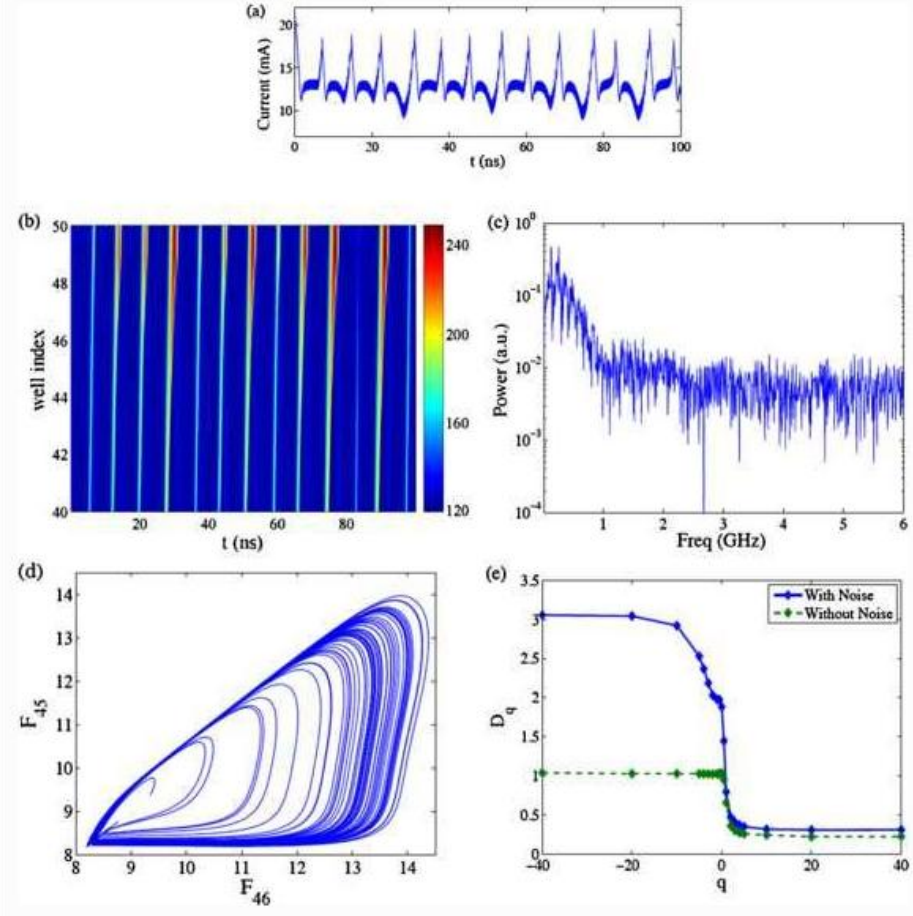

Рисунок 3. Характеристики хаотических колебаний. Зависимость тока (а) и (b) напряженности электрического поля от времени, (c) Фурье-спектр тока; (d) фазовая диаграмма электрического поля (в кВ / см) (e) мультифрактальный размер. Применяемое напряжение: 7.3513V ..

ЗАКЛЮЧЕНИЕ

Открытие быстрых спонтанных хаотических колебаний тока через полупроводниковые сверхрешетки при комнатной температуре выявляет их возможное применение как истинных генераторов случайных битов [15]. Быстрые генераторы истинных случайных битов, поступающие из крошечных субмикронных электронно-электронных устройств, могут быть бесценны в защищенных связях и хранении данных.

В работе рассмотрена математическая модель для описания спонтанного хаоса в идеальных сверхрешетках с одинаковыми лунками и барьерами. Численное моделирование, проведенное сотрудниками Мадридского университета, показывает, что спонтанный хаос, возможно, может возникнуть непосредственно из двухчастотного квазипериодического аттрактора.

При этом, неизбежные тепловые шумы, существующие в наноструктуре, усиливают существующий детерминированный хаос (увеличивая его фрактальную размерность и наибольший показатель Ляпунова) и вызывают хаос в соседних интервалах напряжения.

Также обсуждается схема генерации случайных бит из хаотического сигнала путем оцифровки и извлечения наименее значимых бит из числовых производных высокого порядка или путем объединения нескольких хаотических сигналов, поступающих либо через несколько сверхрешеток, либо из далеких друг от друга сегментов одного и того же длинного хаотического сигнала.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Luis L. Bonilla, Mariano Alvaro, Manuel Carretero. Chaos-based true random number generators // Journal of Mathematics in Industry.2016. No **7**:1. https://doi.org/10.1186/s13362-016-0026-4

2. Reidler I, Aviad Y, Rosenbluh M, Kanter I. Ultrahigh-speed random number generation based on a chaotic semiconductor laser. Phys Rev Lett. 2009;103:024102.