Литература

1. *Ровбуть А. Ю.* Стабильность фазового состава тонкопленочных систем Ti-Zr-Al-N под воздействием ионов ксенона // Сб. работ 69-ой научн. конф. студентов и аспирантов БГУ. Минск, 2012. С. 149–152.

ФОРМИРОВАНИЕ СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГАРАНТИРОВАННОГО КАЧЕСТВА НА ФИЗИЧЕСКОМ ИСТОЧНИКЕ ШУМА

А. Д. Ширяева

В настоящее время ни одна криптографическая система не обходится без генераторов случайных числовых последовательностей. Получение СЧП гарантированного качества особенно важно для процедур генерации ключей, формирования параметров для криптографических алгоритмов и протоколов. СЧП также используется во многих цифровых схемах. Во всех этих приложениях, безопасность во многом зависит от качества источника СЧП.

Целью моей работы являются: изучение принципов получения СЧП гарантированного качества на физических источниках шума, а также изучение и реализация некоторых методов тестирования для контроля качества СЧП.

Для получения качественных СЧП используют источник шума, обычно реализованный на электронных схемах (например, с использованием шумовых диодов, свободно осциллирующих генераторов или построенных на иных физических явлениях – радиоактивный распад, квантовые эффекты полупроводников и т.п.) [1].

Принцип действия генераторов шума основан на свойствах лавинного пробоя перехода диода. В начальной стадии лавинного пробоя процесс ударной ионизации оказывается неустойчивым: ударная ионизация возникает, срывается, возникает вновь в тех местах перехода, где оказывается в данный момент достаточная напряженность электрического поля. Результатом случайной неравномерности генерации новых носителей заряда при ударной ионизации являются шумы, которые характерны для определенного диапазона токов. Таким образом, в качестве генераторов шума можно использовать обратносмещенные диоды в диапазоне обратных токов от минимального до максимального пробивного тока, где наблюдается наибольшая интенсивность электрических флуктуаций [1].

В данной работе для получения СЧП использовалось аппаратно-программное устройство «КЛЮЧ-ВС», разработанный НИИ Прикладных Физических Проблем им. А.Н. Севченко, в котором в качестве ис-

точника шума используется шумовой диод ND103L. Данный диод представляют собой кремниевые планарные диоды – генераторы шума.

Для криптографических задач необходимо, чтобы СЧП были непредсказуемыми. Однако некоторые физические источники весьма предсказуемы. Это может быть минимизировано использованием комбинаций СЧП, получаемых с различных типов источников. Однако результирующая СЧП может быть несовершенной, что выявляется при статистическом тестировании.

В данной работе рассмотрен пакет статистических тестов, разработанных Лабораторией информационных технологий (англ. Information Technology Laboratory), являющейся главной исследовательской организацией Национального института стандартов и технологий (NIST). В его состав входят 15 статистических тестов, целью которых является определение меры случайности двоичных последовательностей, порождённых либо аппаратными, либо программными генераторами случайных чисел. Эти тесты основаны на различных статистических свойствах, присущих только случайным последовательностям [2].

Отличие этих тестов от других современных открытость алгоритмов. Также среди достоинств однозначная интерпретация результатов тестирования.

В ходе работы была написана программа на языке C++ реализации основных тестов из пакета NIST Pub 800-22, а именно частотный побитовый тест, частотный блочный тест, тест на последовательность одинаковых битов.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЯ

Для тестирования использовались СЧП, полученные с АПУ «Ключ-ВС». Тестировалось 1000 последовательностей, каждая по 10^3 бит.

Каждую последовательность подвергали тестированию с использованием пакета NIST Pub 800-22. В результате формируется статистический портрет генератора:

Таблица

Статистический портрет АПУ «Ключ-ВС»

S_i №	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	..
1	0.838	0.451	0.871	0.740	0.052	0.258	0.359	0.155	0.985	0.458	..
2	0.859	0.496	0.954	0.895	0.054	0.384	0.541	0.175	0.941	0.468	..
3	0.214	0.549	0.354	0.945	0.589	0.125	0.859	0.475	0.478	0.985	..

По полученному статистическому портрету определяем долю последовательностей прошедших каждый статистический тест. Для этого, при

заданном уровне значимости α=0,01 и осуществляем подсчет значений вероятности *P*, превышающих заданный уровень α для каждого из *q* тестов, т.е. определяют коэффициент:

$$r_j = \frac{\#\left\{P_{ij} \geq \alpha \middle| i = 1,2,\ldots,m\right\}}{m}, \quad (1)$$

где *m* – количество последовательностей.

В результате формируется вектор коэффициентов $R = \{r_1, r_2, \ldots, r_q\}$, элементы которого характеризуют, в процентном соотношении, прохождение последовательности S_i всех статистических тестов.

Считается, что генератор G прошел тестирование по *j*-му тесту, если значение коэффициента r_j находится внутри доверительного интервала $[r_{max}, r_{min}]$. Границы доверительного интервала определяются согласно выражению [2]:

$$r_{\max(\min)} = p \pm t\sqrt{\frac{p(1-p)}{m}}, \quad (2)$$
$$p = 1 - \alpha$$

где *t* – нормированное отклонение: отношение ошибки конкретной выборки к средней квадратичной ошибке. В данном случае *t* = 3. При таком значении диапазона *t* вероятность приближается к единице.

Рассчитываем границы доверительного интервала:

$$0.981 < r_{ij} < 0.999$$

Коэффициенты r_{ij} рассчитывались программно.

1. Частотный побитовый тест

$$r_{ij} = \frac{997}{1000} = 0.997$$

2. Частотный блочный тест

$$r_{ij} = \frac{995}{1000} = 0.995$$

3. Тест на последовательность одинаковых битов

$$r_{ij} = \frac{989}{1000} = 0.989$$

Все эти коэффициенты входят в доверительный интервал. Поэтому можно сказать, что АПУ «Ключ-ВС» прошел тестирование по трем тестам из пакета NIST Pub 800-22, а именно частотный побитовый тест, частотный блочный тест и тест на последовательность одинаковых битов. Также в рамках настоящей работы планируется реализация набора всех 15 тестов, согласно NIST Pub 800-22. Результаты работы будут вне-

сены в существующий проект аппаратно-программного устройства «Ключ-ВС», что позволит пользователям осуществить контроль качества СЧП.

Литература

1. *Букингем М.* Шумы в электронных приборах. М.: Изд. ин. лит., 1986.
2. *Andrey Pykhin, Juan Soto, James Nechavatal*. A statistical test suite for random and pseudorandom number generators for cryptographic application // NIST Special Publication 800-22. 2010.

ИССЛЕДОВАНИЕ МЕЖХРОМОФОРНЫХ ВЗАИМОДЕЙСТВИЙ *м*-ТГФХ И *м*-ТГФБХ В МИЦЕЛЛЯРНЫХ СИСТЕМАХ

И. В. Яковец

ВВЕДЕНИЕ

Структурные и фотофизические характеристики комплексов фотосенсибилизаторов (ФС) с мицеллами представляют интерес для различных областей науки, включая медицину, наноэлектронику, фармакологию и др. Особый интерес к ним в последние годы связан с разработкой наноразмерных фармакологических форм ФС для фотодинамической терапии (ФДТ). В настоящее время в клинической практике используют несколько типов липосомальных форм порфириновых ФС (Fospeg, Foslip, Verteporfin, TUKAD и др.). Введение ФС в состав липосомальных форм позволяют значительно улучшить их фармакокинетические свойства. Одной из характерных особенностей липосомальных форм является высокая локальная концентрация ФС, что может обуславливать сильные межхромофорные взаимодействия их молекул.

В данной работе проведено исследование процессов переноса энергии возбуждения между двумя структурноподобными ФС (мезо-тетра(гидроксифенил)хлорином (м-ТГФХ) и мезо-тетра(гидроксифенил)бактериохлорином (м-ТГФБХ), находящимися в составе мицеллярных структур.

МАТЕРИАЛЫ И МЕТОДЫ

В работе использовали м-ТГФХ) и (м-ТГФБХ) предоставленные Biolitec (Йена, Германия). Соединения растворяли в 99,6 %-ном этиловом спирте. Концентрация красителей в растворе оценивалась спектрофотометрически.