АНАЛИЗ ХАРАКТЕРИСТИК СХЕМЫ ПОСТОБРАБОТКИ ПОСЛЕДОВАТЕЛЬНОСТИ СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ МНОГОКАНАЛЬНОГО СИГНАТУРНОГО АНАЛИЗАТОРА

Петровский Д. А., Иванюк А. А.
Кафедра электронных вычислительных средств, кафедра информатики,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: petrovsky.dmitr@gmail.com, ivaniuk@bsuir.by

В данной работе рассматривается схема постобработки случайных чисел. Основное внимание уделяется анализу характеристик многоканального сигнатурного анализатора (МСА) при различных конфигурациях. Проведено тестирование с использованием стандарта NIST SP 800-22.

Введение

Случайные числа имеют широкую сферу применения. Они используются в криптографии, статистике, игровой индустрии, моделировании и т.д. Они делятся на два класса: псевдослучайные числа (ПСЧ) и истинно случайные числа (ИСЧ). ПСЧ генерируются в результате математических вычислений по заданному алгоритму. Генерирование ИСЧ основано на измерении характеристик неуправляемых физических процессов, происходящих внутри источников энтропии (ИЭ).

Для каждой области существует множество стандартов, описывающих необходимые характеристики случайных чисел и тесты для их источников. В качестве примера можно привести стандарты SP 800–90A–D и ряд из 15 тестов Национального института стандартов и технологий США (анг. National Institute of Standards and Technology (NIST), USA) [1].

I. Схемы постобработки случайных чисел

Структура генератора истинно случайных чисел (ГИСЧ)(рис. 1) подразумевает наличие схемы постобработки, которая улучшает статистические свойства выходной последовательности от ИЭ, для соответствия требованиям, предъявляемым к ГИСЧ.

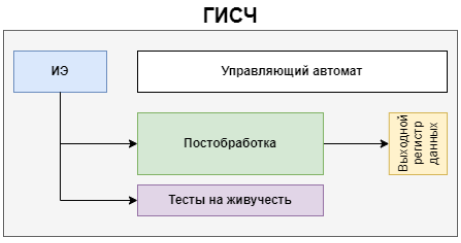

Рис. 1 – Структура ГИСЧ

Схемы постобработки, предлагаемые NIST, основаны на криптографических хеш-функциях или алгоритмах шифрования [1]. Они обеспечивают высокие статистические показатели выходной последовательности, но их схемотехническая реализация требует больших аппаратных затрат. Актуальной задачей является разработка и исследование алгоритма постобработки, имеющего меньшие аппаратные затраты, но сравнимые статистические показатели.

В работе [2] рассматривается схемотехническая реализация схемы постобработки случайных чисел на базе многоканального сигнатурного анализатора (МСА). Характеристики схемы зависят от следующих параметров: количества входных каналов G, количества выходных каналов (разрядности) N, коэффициента сжатия во времени J и порождающего полинома. Поведение схемы можно описать с помощью уравнения:

$$d_i(k+J) = \sum_{g=0}^{G-1} B_i(r-g)y_g(k) + \sum_{n=0}^{N-1} c_n(r-i)d_n(k). \quad (1)$$

где $d_i(k) \in \{0,1\}$ – содержимое i-го элемента памяти (разряда) МСА в k-й такт работы, $y_g(k) \in \{0,1\}$ – двоичное значение g-го канала в k-й такт работы, $c_n(r-i) \in \{0,1\}$ – коэффициент ,определяющий участие d_n в цепи обратной связи для d_i, рассчитывается на основе порождающего полинома и коэффициента J, $B_i(r-g) \in \{0,1\}$ – коэффициент, определяющий участие y_g в формировании d_i, рассчитывается на основе порождающего полинома и коэффициента J, r – вспомогательный коэффициент, $r = J \cdot G$.

II. Анализ характеристик

Для анализа характеристик МСА применяется набор тестов, предлагаемый NIST в SP 800 - 22 [3]. Анализируемые конфигурации МСА имеют разрядность $N = \{2^5,2^4,2^3\}$, так как схемы разрядностей степени 2 широко применяются в вычислительной технике и могут быть легко в неё интегрированы. Схемы с разрядностью $N = \{2^5,2^4\}$ имею количество входных каналов $G = 4$, для $N = 2^3$ количество входных кана-

Работа выполнена в совместной учебной лаборатории БГУИР-YADRO
https://www.bsuir.by/ru/kaf-informatiki/yadro

лов $G = 2$. Согласно рекомендациям NIST G и N должны удовлетворять следующему условию, $N\ mod\ (G) = 0$. В качестве исходной последовательности используется набор данных, сгенерированных со схемотехнической реализации физически неклонируемой функции (ФНФ) [4]. Основываясь на данных из работы [2], коэффициент J будет изменяться в диапазоне $(N,\ 2^N - 1)$ для всех схем случайным образом.

NIST тестирование проводилось на последовательностях длинной 10^6 бит. В таблице 1 представлены результаты одного из тестирований для каждой конфигурации, отражающие общую картину.

Для конфигураций использовались примитивные и неприводимые порождающие полиномы, изменение которых на всех конфигурациях не оказало значительного влияния на прохождения тестирования. Если полином не является примитивным и неприводимым, наблюдается значительное снижение характеристик схемы.

Изменение разрядности MCA влияло на прохождение тестирования. Конфигурации с разрядностью 32-бита показали высокие статистические показатели в NIST тестировании. Конфигурации с разрядностью 16-бит, при тестировании показали хорошие характеристики в 14 из 15 тестов, но тест Rank на всех запусках тестирования был не пройден. Непрохождение данного теста свидетельствует о наличии линейной зависимости в выходных последовательностях данных. Для конфигураций с разрядностью 8-бит 9 из 15 тестов не проходили, что указывает на зависимости в выходных последовательностях данных и наличие повторяющихся последовательностей.

III. Заключение

Выбор разрядности схемы и порождающего полинома оказывает основное влияние на статистические характеристики. Таким образом, схема постобработки случайных чисел на базе MCA показала хорошие результаты при NIST тестировании для конфигураций с разрядностью 32 бита. Схемы с разрядностью меньше 32 бит показали низкие характеристики, в результате NIST тестирование не было пройдено, но данные конфигурации могут быть использованы для дальнейшего изучения зависимостей выходных характеристик схемы от количества входных каналов и коэффициента J.

1. NIST Special Publication (SP) 800 –90B, Recommendation for the Entropy Sources Used for Random Bit Generation[Электронный ресурс] – режим доступа `https://doi.org/10.6028/NIST.SP.800-90B`. – Дата доступа: 20.10.2024.
2. Петровский Д. А Схема постобработки цифровой последовательности случайных чисел / Д. А. Петровский // Компьютерные системы и сети : сборник статей 60-й научной конференции аспирантов, магистрантов и студентов, Минск, 22 –26 апреля 2024 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2024. – С. 729 –730
3. NIST Special Publication (SP) 800 –22, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Электронный ресурс]. – Режим доступа: `https://doi.org/10.6028/NIST.SP.800-22r1a`. – Дата доступа: 20.10.2024.
4. Шамына А. Ю., Иванюк А. А. Исследование временных параметров физически неклонируемой функции типа арбитр с использованием кольцевого осциллятора. Цифровая трансформация. 2022. – С.27 –38.

Таблица 1 – Результаты NIST тестов

Название теста	Разрядность MCA					
	32		16		8	
	p-value	propotion	p-value	propotion	p-value	propotion
Frequency	0.350485	10/10	0.122325	10/10	0.534146	10/10
BlockFrequency	0.122325	10/10	0.534146	9/10	0.739918	10/10
CumulativeSums(Forvard)	0.534146	10/10	0.739918	10/10	0.534146	10/10
CumulativeSums(Revers)	0.350485	10/10	0.739918	10/10	0.534146	10/10
Runs	0.350485	9/10	0.035174	10/10	0.350485	10/10
LongestRun	0.534146	9/10	0.066882	10/10	0.000000*	0/10*
Rank	0.534146	10/10	0.000000*	0/10*	0.000000*	0/10*
FFT	0.350485	10/10	0.350485	10/10	0.991468	10/10
NonOverlappingTemplate	0.350485	10/10	0.739918	10/10	0.000000*	0/10*
OverlappingTemplate	0.876132	10/10	0.911413	10/10	0.000000*	0/10*
Universal	0.122325	10/10	0.739918	10/10	0.000000*	2/10*
ApproximateEntropy	0.122325	10/10	0.739918	10/10	0.000000*	0/10*
RandomExcursions	0.342678	7/7	0.271566	7/7	0.000000*	2/6 *
RandomExcursionsVariant	0.212553	7/7	0.429302	7/7	0.420789	5/6
Serial1	0.534146	10/10	0.350485	10/10	0.000000*	0/10*
Serial2	0.350485	10/10	0.213309	10/10	0.000000*	0/10*
LinearComplexity	0.213309	10/10	0.122325	10/10	0.122325	10/10
∗ - результат интерпретируемый как не случайные данные						