ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК МЕТОДА ПОСТОБРАБОТКИ СЛУЧАЙНЫХ ДАННЫХ НА БАЗЕ МНОГОВХОДОВОГО СИГНАТУРНОГО АНАЛИЗАТОРА

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

В работе исследуются характеристики метода постобработки случайных данных на базе многовходового сигнатурного анализатора. Целью работы является оценка эффективности предложенной модификации метода. В результате эксперимента получено, что внесённые изменения позволяют избавиться от дублирования символов в выходной последовательности без увеличения числа источников энтропии. Это позволило повысить значение энтропии по Шеннону выходной последовательности случайных бит на 5 %.

Введение

Случайные числа играют ключевую роль в криптографии, статистическом моделировании, игровой индустрии и в других областях. Они делятся на псевдослучайные числа (ПСЧ), получаемые с помощью детерминированных алгоритмов, и истинно случайные числа (ИСЧ), в основе генерации которых лежит измерение характеристик неконтролируемых физических процессов, происходящих внутри источника энтропии (ИЭ).

Существует множество стандартов и рекомендаций, регулирующих проектирование генераторов истинно случайных чисел (ГИСЧ). В качестве примера можно привести документы, разработанные Национальным институтом стандартов и технологий США (*NIST*) [1]. Согласно рекомендациям независимый однобитный ИЭ должен удовлетворять условию «полной энтропии»[2] и иметь блок тестирования (БТ) для обнаружения критических сбоев.

ИЭ, применяемые в ГИСЧ, зачастую обладаю недостаточными статическими характеристиками выходной последовательности бит для их применения. *NIST* рекомендует использовать функции постобработки на базе криптографических примитивов, удовлетворяющих условию «полной энтропии». Однако широкое применение получили методы постобработки на основе регистра сдвига с линейной обратной связью (от англ. *Linear Feedback Shift Register*, *LFSR*). В качестве примера можно привести одновходовой сигнатурный анализатор и моговходовой сигнатурный анализатор (от англ. *Multi-input Signature Analyzer*, *MISA*).

I. Описание метода постобработки

Метод постобработки, использующий *MISA* (рис.1), для синтеза схемы и математического описания опирается на примитивные и неприводимые характеристические полиномы $\phi(x)$ над полем GF(2), где $\mathbf{D}(k)$ – n-разрядный двоичный вектор, являющийся состоянием *MISA* в k-й момент времени, $n = deg(\phi(x))$.

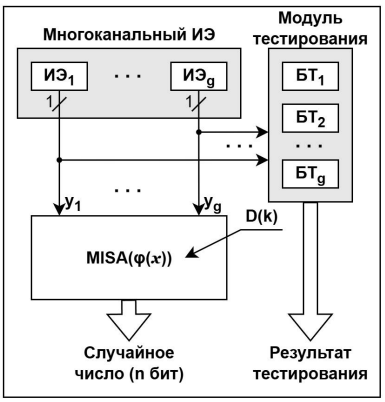

Рис. 1 – Обобщенная схема постобработки на базе *MISA*

В данной работе рассматривается модификация метода, заключающаяся в использовании принципа перехода схемы *MISA* из состояния $\mathbf{D}(k)$ в $\mathbf{D}(k+j)$ за один такт синхронизации, где $j > 1$ – коэффициент сжатия во времени. Схемотехническая реализация данной модификации представлена в работе [2]. Дальше будем обозначать модифицированную схему как *MISA**.

$$\mathbf{B}_i(C,j,g) = \sum_{s=1}^{j} \mathbf{C}^{s\cdot g-i} \times e_1, \quad \mathbf{A}(\mathbf{C},j,g) = \mathbf{C}^{j\cdot g}$$
$$\mathbf{D}(k+1) = A(\mathbf{C},j,g) \times \mathbf{D}(k) \oplus \sum_{i=0}^{g} \mathbf{B}_i(\mathbf{C},j,g) \times y_i(k). \tag{1}$$

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

[2] Discussion on the Full Entropy Assumption of the SP 800-90 Series
https://csrc.nist.gov/pubs/ir/8427/final

Математическая модель *MISA** описывается выражениями (1), где $\mathbf{C}$ — матрица сдвига и обратных связей *LFSR*, основанная на коэффициентах порождающего полинома $\phi(x)$, $\mathbf{A}(\mathbf{C}, j, g)$ — матрица обратной связи *MISA** с разрядностью входного слова g бит, основанная на матрице $\mathbf{C}$, возведенной в степень $j \cdot g$, что позволяет получить коэффициенты сдвига и обратной связи для коэффициента сжатия j, e_1 – вектор стандартного базиса, $\mathbf{B}_i(\mathbf{C}, j, g)$ — вектор-столбец коэффициентов, определяющий воздействия i-го бита входного слова $y(k)$ на $\mathbf{D}(k)$, получаемый в результате умножения матрицы $\mathbf{C}$, возведенной в степень, на вектор e_1, для получения первой строки матрицы $\mathbf{C}$ в качестве вектора коэффициентов.

II. Описание эксперимента

В эксперименте оценивалась зависимость изменения энтропии по Шеннону выходного потока бит от выбранного порождающего полинома $\phi(x)$, разрядности входного слова g и коэффициента сжатия j. В качестве входного набора данных был использован CIFAR-10 [3]. Схема эксперимента представлена на рис. 3.

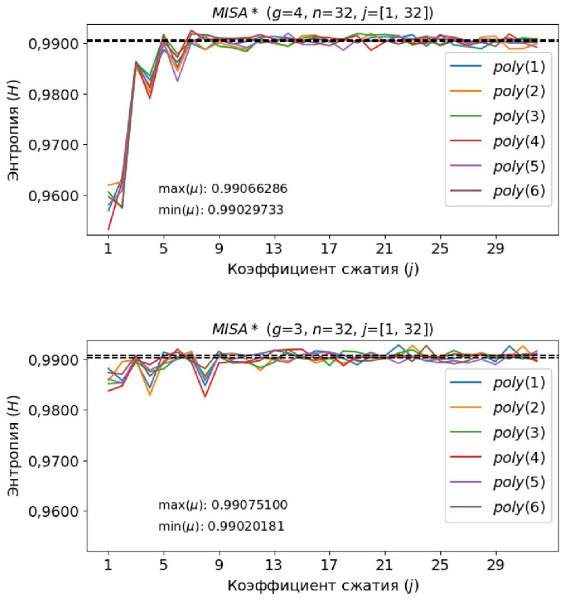

Рис. 2 – Графики зависимости энтропии по Шеннону от порождающего полинома и коэффициента сжатия

На рис. 2 представлены графики зависимости энтропии по Шеннону от порождающего полинома $\phi(x)$, разрядности входного слова и коэффициента сжатия. При этом использовались различные полиномы $\phi(x)$, заданные шестнадцатеричными значениями: {0x80000057, 0x80000062, 0x9D7826E1, 0xBD9D339, 0xFB3CFCDF, 0x80003474}, $g \in \{3, 4\}$ и $j = \overline{1, 32}$.

Из рис. 2 видно, что численное значение энтропии по Шеннону возрастает при увеличении коэффициента сжатия j. Для значений $j > 8$ при $g = 4$, а также $j > 10$ при $g = 3$, энтропии по Шеннону достигает придела, на котором наблюдается девиация матожиданий энтропии в диапазоне $[min(\mu), max(\mu)]$. Резкие провалы энтропии на графиках связаны с дублирование символов в выходной последовательности бит при малых значениях j, что видно при $HOK \neq 1$ для окна анализа, внутренней разрядности n и внутреннего сдвига $j \cdot g$. Вследствие чего можно заметить, что при достижении значения внутреннего сдвига $j \cdot g > n$, дублирование пропадет. Таким образом увеличение коэффициента сжатия j позволило получить прирост энтропии по Шеннону на 5 %, в сравнении с реализацией для $j = 1$.

III. Заключение

В ходе исследования характеристик метода постобработки на базе *MISA** модификация позволила избавиться от дублирования символов выходной последовательности, для значений $j \cdot g > n$, без увеличения количества ИЭ. Это позволило получить прирост выходной энтропии по Шеннону на 5 %, по сравнению с реализацией схемы при $j = 1$.

IV. Список литературы

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:24.10.2025.
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. The CIFAR-10 dataset [Электронный ресурс] – режим доступа https://www.cs.toronto.edu/ kriz/cifar.html. Дата доступа:24.10.2025.

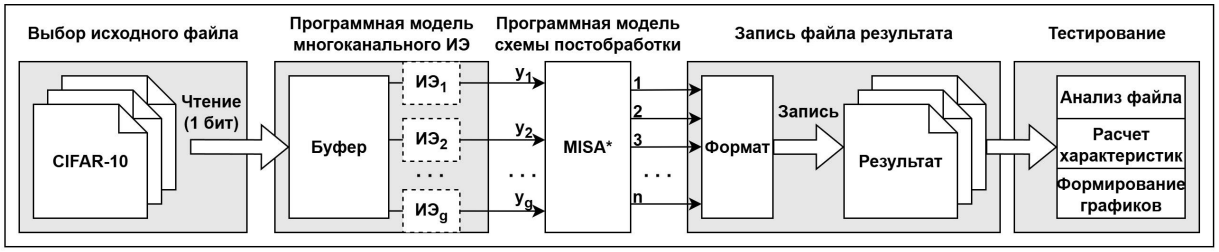

Рис. 3 – Схема эксперимента