

О КРИПТОГРАФИЧЕСКИХ СВОЙСТВАХ ГЕНЕРАТОРА МАКЛАРЕНА – МАРСАЛЬИ

И.Б. Бережной, Ю.С. Харин

Белгосуниверситет, факультет прикладной математики и информатики,
пр. Независимости 4, 220030 Минск, Беларусь

bereznoy@tut.by

Доклад посвящен изучению некоторых криптографических свойств генератора псевдо-случайных последовательностей Макларена – Марсальи [1, 2]. Генератор Макларена – Марсальи состоит из таблицы T размера N и двух простейших генераторов псевдослучайных

последовательностей: G_1 и G_2 . Генератор G_1 порождает "заполняющую" ("исходную") последовательность u над множеством $\{0, \dots, p-1\}$, генератор G_2 — "управляющую" последовательность v над $\{0, \dots, N-1\}$, результирующая последовательность — z над $\{0, \dots, p-1\}$.

Если $T_j(i)$ — заполнение j -й ячейки памяти перед началом i -го такта, то преобразование информации на i -м такте описывается следующим образом:

$$z(i) = T_{v(i)}(i), \quad T_j(i+1) = \begin{cases} T_j(i), & \text{если } j \neq v(i), \\ u(i), & \text{если } j = v(i), \end{cases} \quad j \in \{0, \dots, N-1\}, \quad i = 1, 2, \dots$$

Таким образом, последовательность v определяет адреса, по которым считываются в z и записываются в память элементы последовательности u .

Введем специальную характеристику для элементов выходной последовательности генератора — расстояние сдвига $L(i) = \min\{l \in N : v(i) = v(i-l)\}$. Смысл данной характеристики — расстояние между местом элемента в последовательности z и местом его же в исходной последовательности u : $z(i) = u(i - L(i))$.

Найдены вероятностные свойства $L(i)$ при условии случайной и равномерно распределенной последовательности v :

$$E\{L(i)\} = N - \frac{iC^i}{1-C^i} \xrightarrow{i \rightarrow \infty} N, \quad D\{L(i)\} = N^2 - N - \frac{i^2 C^i}{(1-C^i)^2} \xrightarrow{i \rightarrow \infty} N^2 - N,$$

где $C = 1 - 1/N$.

Получено выражение для периода выходной последовательности $T(z)$, уточняющее формулу из [1]; в случае применения в качестве G_2 LFSR генератора с примитивным характеристическим многочленом найден период последовательности расстояний сдвигов $T(\{L(i)\})$, и в случае использования в качестве G_1 и G_2 LFSR генераторов с различными примитивными характеристическими многочленами выдвинута гипотеза относительно значения линейной сложности $\Lambda(z)$, справедливость которой подтверждается компьютерными экспериментами:

$$T(z) \stackrel{\text{п.н.}}{=} HOK\{T(u), T(\{L(i)\})\}, \quad T(\{L(i)\}) = \frac{T(v)}{N-1}, \quad \Lambda(z) = \Lambda(u) \cdot \frac{N^{\Lambda(v)} - 1}{N-1}.$$

Кроме того, для малых значений был проведен анализ марковости последовательности z , который показывает высокое качество "запутывания" исходной структуры генератора G_1 .

Литература

- Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005
- Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. Минск: Новое знание, 2003.