За элементарную операцию возьмём операцию умножения в кольце Галуа R. Сложность построения множества W_{f_n,R_n} составляет $\mathrm{O}(lq^{n-1})$ элементарных операций при n, стремящемся к бесконечности, где l — степень многочлена $f(x)$ на входе алгоритма.

ЛИТЕРАТУРА

1. *Ермилов Д. М., Козлитин О. А.* Цикловая структура полиномиального генератора над кольцом Галуа // Математические вопросы криптографии. 2013. Т. 4. Вып. 1. С. 27–57.
2. *Ермилов Д. М.* О цикловой структуре полиномиальных преобразований колец Галуа максимального периода // Обозрение прикл. и промышл. матем. 2013. Т. 20. Вып. 3.

УДК 519.711.2

МОДЕЛЬ ФУНКЦИИ УСЛОЖНЕНИЯ В ГЕНЕРАТОРЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НАД ПОЛЕМ GF(2)

В. М. Захаров, Р. В. Зелинский, С. В. Шалагин

Предложена модель усложнения псевдослучайных последовательностей (ПСП) над полем GF(2), основанная на представлении функции усложнения системой линейных биективных преобразований (БП) от двух двоичных переменных. Расширены алгоритмические возможности функции усложнения за счёт сведения аффинного преобразования над полем GF(2) к линейному преобразованию, представляемому невырожденными двоичными матрицами размера 3. Представлен ряд свойств, характеризующих рассматриваемые БП. Отмечены возможности этих свойств по изменению структуры и ансамбля формируемых ПСП.

Ключевые слова: *генератор, псевдослучайная последовательность, биективное преобразование.*

Рассмотрим преобразование

$$f(X) : \mathrm{GF}(2)^n \to \mathrm{GF}(2)^n, \tag{1}$$

где n чётное; $\mathrm{GF}(2)^n$ — множество n-мерных двоичных векторов.

Пусть отображение (1) является биекцией и вектор X формируется некоторым генератором псевдослучайных последовательностей со свойствами случайной равновероятной последовательности. Преобразование (1) рассматривается как функция усложнения. Предлагается модель функции усложнения, обладающая алгоритмическими возможностями изменения структуры ПСП и увеличения ансамбля формируемых ПСП.

Рассмотрим линейное преобразование вектора X в виде

$$Z_L = A_i \cdot X, \tag{2}$$

где A_i — двоичная невырожденная матрица размера n и равенство понимается по модулю 2. Число линейных невырожденных преобразований, выполняемых по формуле (2), при $n = 2$ равно 6. Учтём, что отображению (1) при $n = 2$ соответствует максимальное число различных биекций равное 24 [1]. Разобьём вектор $X = x_1x_2 \dots x_n$ на непересекающиеся пары переменных (x_{2i-1}, x_{2i}), $i = 1, \dots, n/2$.

Введём в рассмотрение транспонированный кортеж вида

$$(q_1, q_2, \dots, q_m)^{\mathrm{T}}, \tag{3}$$

где $m = n/2$; q_i — некоторое линейное биективное преобразование над вектором (x_{2i-1}, x_{2i}) в вектор (z_{2i-1}, z_{2i}), $i = 1, \ldots, n/2$. Пусть в (3) $m = 24$ и число различных элементов q_i равно максимальному числу биекций от двух двоичных переменных, т. е. 24. Определение всех элементов множества $G = \{q_i : i = 1, \ldots, 24\}$ для системы (3) рассматривается как задача построения требуемой функции усложнения. Обозначим $A = \{A_i : i = 1, \ldots, 24\}$ некоторое множество невырожденных матриц A_i размера 3, позволяющих выполнить по формуле (2) 24 различных биекции. Введём векторы $(x_{2i-1}, x_{2i}, 1)$ и $(z_{2i-1}, z_{2i}, 1)$ как расширения соответственно векторов (x_{2i-1}, x_{2i}) и (z_{2i-1}, z_{2i}), $i = 1, \ldots, 24$.

Теорема 1. В системе (3) линейное биективное преобразование $q_i \in G$ над вектором (x_{2i-1}, x_{2i}) представимо однозначно соответствующей невырожденной матрицей $A_i \in A$, осуществляющей преобразование вектора $(x_{2i-1}, x_{2i}, 1)$ в вектор $(z_{2i-1}, z_{2i}, 1)$, $i = 1, \ldots, 24$.

Доказательство теоремы основано на результатах работы [2], показывающих возможность сведения аффинного преобразования к линейному.

Следствие 1. При $n = 48$ для отображения (1) существует 24! биективных преобразований вектора X в вектор Z_L вида (3).

Для случая $n = 48$ на модели (3) при фиксированной М-последовательности на входе путём перестановки элементов q_i можно получить ансамбль V периодических последовательностей векторов Z_L мощности $Q_1 = 24!$.

Множество матриц A можно разбить на три подмножества $M1$, $M2$, $M3$ с мощностями $|M1| = 10$, $|M2| = 8$, $|M3| = 6$; $M1 = \{E\} \cup \{A_i : \mathrm{O}(A_i) = 2\}$; $M2 = \{A_i : \mathrm{O}(A_i) = 3\}$; $M2 = \{A_i : \mathrm{O}(A_i) = 4\}$, где E — единичная матрица; $\mathrm{O}(A_i)$ — порядок матрицы A_i в группе GL(3).

Возможность сочетания в функции усложнения (3) невырожденных матриц A_i из множеств $M1$, $M2$, $M3$ позволяет менять строение выходной последовательности: создавать разнообразный порядок следования векторов Z_L, отличающийся от порядка следования входных векторов X; при этом последовательности векторов Z_L из ансамбля V сохраняют величину периода и статистические свойства входной М-последовательности. В частном случае на основе определённых матриц $A_i \in A$ можно получить тождественное преобразование вектора X.

На входе системы (3) можно использовать М-последовательности из ансамбля мощности $Q_2 = (\varphi(2^{48} - 1))/48$, где φ — функция Эйлера, при этом для $n = 48$ выполняется $Q_1 > Q_2$. Тогда на выходе системы (3) можно формировать ансамбль последовательностей векторов Z_L мощности $Q_1 \cdot Q_2$.

ЛИТЕРАТУРА

1. *Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В.* Криптография: скоростные шифры. СПб.: БХВ-Петербург, 2002. 496 с.
2. *Колпаков А. В.* Методы и алгоритмы линейных и аффинных преобразований для модели бинарных диаграмм решений: дис. ... канд. техн. наук. Казань, 2004.