2) при $(n, m) = 1$, $2 \leqslant m \leqslant n-2$ верна оценка $\exp\Gamma(\varphi) \leqslant n^2 + (3-m)n + 2m$ (взяты длины циклов $n - m$ и n);

3) при $m = n - 1$ выполняется $\exp\Gamma(\varphi) \leqslant 2n - 2$.

Вывод: выбор параметров модифицированного аддитивного генератора позволяет достичь полного перемешивания за число тактов работы, которое существенно меньше размера (в битах) состояний генератора.

ЛИТЕРАТУРА

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.
2. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4 (18). С. 5–13.
3. *Коренева А. М., Фомичев В. М.* Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3 (17). С. 34–40.
4. *Дорохова А. М., Фомичев В. М.* Уточнённые оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов // Прикладная дискретная математика. 2014. № 1 (23). С. 77–83.
5. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
6. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2 (12). С. 101–112.
7. *Фомичев В. М.* Свойства путей в графах и в мультиграфах // Прикладная дискретная математика. 2010. № 1 (7). С. 118–124.

УДК 512.62

АЛГОРИТМ ПОСТРОЕНИЯ СИСТЕМЫ ПРЕДСТАВИТЕЛЕЙ ЦИКЛОВ МАКСИМАЛЬНОЙ ДЛИНЫ ПОЛИНОМИАЛЬНЫХ ПОДСТАНОВОК НАД КОЛЬЦОМ ГАЛУА

Д. М. Ермилов

В отличие от полей и колец вычетов, над кольцами Галуа не существует транзитивных полиномов, то есть биективных полиномов, которые реализуют полноцикловую подстановку. Максимальная длина цикла полиномиального преобразования над кольцом Галуа равна $q(q-1)p^{n-2}$, где q^n — мощность кольца, а p^n — его характеристика. Предлагается алгоритм построения системы представителей всех циклов полиномиальных преобразований колец Галуа, имеющих максимальную длину. Сложность построенного алгоритма, выраженная в количестве операций умножения в кольце Галуа, равна $\mathrm{O}(lq^{n-1})$ при n, стремящемся к бесконечности, где l — степень многочлена полиномиального преобразования.

Ключевые слова: *кольца Галуа, нелинейные рекуррентные последовательности.*

Рассмотрим кольцо Галуа $R = \mathrm{GR}(q^n, p^n)$ мощности q^n и характеристики p^n, где $q = p^m$. Пусть $f(x) \in R[x]$ — биективный полином над кольцом Галуа R. Граф преобразования, задаваемого полиномом $f(x)$ над кольцом R, обозначим через $G_{f,R}$. Напомним, что цикловая структура графа — это таблица $[l_1^{k_1}, \ldots, l_t^{k_t}]$, указывающая, что граф состоит из k_1 циклов длины l_1, …, k_t циклов длины l_t. В работе [1] показано, что граф $G_{f,R}$ не может содержать цикл, длина которого больше $q(q-1)p^{n-2}$.

В данной работе рассматривается класс полиномов над кольцом Галуа R, граф которых содержит цикл максимальной длины $q(q-1)p^{n-2}$. Назовём такие полиномы полиномами с максимальной длиной цикла (МДЦ-полиномами).

Пусть $f(x) \in R[x]$ — МДЦ-полином. В работе решается задача построения множества $W_{f,R} \subset R$ — системы представителей всех циклов максимальной длины $(q-1)qp^{n-2}$ графа $G_{f,R}$. Мощность множества $W_{f,R}$ равна $(q/p)^{n-2}$, так как в графе $G_{f,R}$ содержится $(q/p)^{n-2}$ циклов длины $(q-1)qp^{n-2}$ [2]. Введём необходимые обозначения.

Положим $J = pR$ и $R_k = R/J^k$, $k \in \{1, \ldots, n\}$. Рассмотрим эпиморфизмы

$$\varphi_i : R \to R_i$$

для $i \in \{1, \ldots, n\}$, которые естественным образом продолжаются до эпиморфизмов колец многочленов

$$\widehat{\varphi}_i : R[x] \to R_i[x].$$

Положим $f_i(x) = \widehat{\varphi}_i(f(x))$. Строить набор $W_{f,R}$ будем итеративно, последовательно находя элементы в цепочке множеств

$$W_{f_1,R_1}, W_{f_2,R_2}, \ldots, W_{f_n,R_n},$$

и тогда $W_{f,R} = W_{f_n,R_n}$

Множество W_{f_1,R_1} состоит из одного элемента, так как граф G_{f_1,R_1} состоит из единственного цикла длины q. Поэтому в качестве множества W_{f_1,R_1} подойдёт любое одноэлементное множество $\{a\}$, $a \in R_1$.

Множество W_{f_2,R_2} также состоит из одного элемента, поскольку граф G_{f_2,R_2} состоит из двух циклов длины $q(q-1)$ и q. Следовательно, в качестве элемента множества W_{f_2,R_2} подойдёт любой элемент на цикле длины $q(q-1)$ графа G_{f_2,R_2}.

Теперь покажем, как по известному множеству W_{f_k,R_k} построить множество $W_{f_{k+1},R_{k+1}}$, $k \geqslant 2$. Рассмотрим эпиморфизмы

$$\varphi_i : R_{i+1} \to R_i$$

для $i \in \{1, \ldots, n-1\}$. Для каждого $a \in W_{f_k,R_k}$ обозначим через C_a цикл графа G_{f_k,R_k}, на котором лежит элемент a.

Так как прообраз $\varphi_i^{-1}(C_a)$ состоит из q/p циклов максимальной длины $q(q-1)p^{k-1}$ графа $G_{f_{k+1},R_{k+1}}$, то для построения множества $W_{f_{k+1},R_{k+1}}$ достаточно для каждого элемента $a \in W_{f_k,R_k}$ найти множество элементов

$$\{a_1, a_2, \ldots, a_{\frac{q}{p}}\},$$

лежащих на этих циклах, причём разные элементы должны лежать на разных циклах.

Пусть элемент $a \in W_{f_k,R_k}$. Установим связь между элементами кольца R_{k+1}, которые лежат на одном цикле максимальной длины и образ которых под действием эпиморфизма φ_k совпадает с a.

Утверждение 1. Пусть элемент $a \in W_{f_k,R_k}$ является представителем цикла C максимальной длины графа G_{f_k,R_k}, тогда на любом цикле C' максимальной длины графа $G_{f_{k+1},R_{k+1}}$, таком, что $\varphi_i(C') = C$, лежат ровно p элементов, образ которых под действием эпиморфизма φ_i совпадает с a.

Теорема 1. Пусть $a_1 = a + p^k a_1^{'}, \ldots, a_p = a + p^k a_p^{'}$ — элементы на некотором цикле максимальной длины $q(q-1)p^{k-1}$ графа $G_{f_{k+1},R_{k+1}}$, образ которых под действием эпиморфизма φ_k совпадает с $a \in W_{f_k,R_k}$. Тогда выполняется соотношение

$$a_{i+1}^{'} = a_i^{'} + r, \quad i = 1, 2, \ldots, p,$$

где r — некоторый элемент поля R_1.

Следствие 1. Пусть $a \in W_{f_k,R_k}$. Два элемента $a + p^k a^{'}$ и $a + p^k a^{''}$ кольца R_{k+1} лежат на одном и том же цикле максимальной длины графа $G_{f_{k+1},R_{k+1}}$ в том и только в том случае, если элементы $a^{'}, a^{''} \in R_1$ лежат на одном цикле графа G_{x+r,R_1} полиномиального преобразования $x + r$, где элемент $r \in R_1$ находится из сравнения

$$F(a) \equiv a + p^k r \pmod{J^{k+1}}.$$

Граф G_{x+r,R_1} состоит из q/p циклов длины p. Элементы каждого цикла образуют смежный класс аддитивной группы поля $R_1 = \mathrm{GF}(q)$ по подгруппе $\langle r \rangle$. Это означает, что для нахождения q/p элементов поля $\mathrm{GF}(q)$, которые лежат на разных циклах графа $G_{x+r,\mathrm{GF}(q)}$, достаточно найти представителей смежных классов поля $\mathrm{GF}(q)$ по подгруппе $\langle r \rangle$.

Аддитивная группа поля $(\mathrm{GF}(q), +)$ изоморфна группе $(\mathbb{Z}_p^m, +)$. Если на группе $(\mathbb{Z}_p^m, +)$ ввести внешнюю операцию умножения на элементы поля $\mathbb{Z}_p$, то получим векторное пространство размерности m. Дополним до базиса пространства элемент r, получим базис $r, r_2, \ldots, r_m$ и рассмотрим представление пространства в виде прямой суммы подпространств

$$\mathbb{Z}_p^m = \langle r \rangle \dotplus \langle r_2 \rangle \dotplus \cdots \dotplus \langle r_m \rangle.$$

Представителями смежных классов группы $(\mathrm{GF}(q), +)$ по подгруппе $(\langle r \rangle, +)$ являются все элементы множества

$$\{\langle r_2 \rangle \dotplus \cdots \dotplus \langle r_m \rangle\}.$$

Изложим алгоритм построения системы представителей $W_{f,R}$ циклов максимальной длины графа $G_{f,R}$.

В качестве W_{f_1,R_1} можно взять любое одноэлементное множество $\{a\}$, $a \in R_1$, а в качестве W_{f_2,R_2} — одноэлементное множества $\{a^{'}\}$, где $a^{'}$ — элемент на цикле длины $q(q-1)$ графа G_{f_2,R_2}.

Далее покажем, как по имеющемуся элементу $a \in W_{f_k,R_k}$ построить множество из q/p элементов $A_a \subset W_{f_{k+1},R_{k+1}}$, $k \geqslant 2$. При этом, по построению, для различных $a_1, a_2 \in W_{f_k,R_k}$ множества A_{a_1} и A_{a_2} не пересекаются. Поскольку

$$\frac{q}{p}|W_{f_k,R_k}| = |W_{f_{k+1},R_{k+1}}|,$$

то $\bigcup\limits_{a \in W_{f_k,R_k}} A_a = W_{f_{k+1},R_{k+1}}$.

Алгоритм 1. Построение множества A_a

Вход: $f(x) \in R[x]$, $a \in W_{f_k,R_k}$
Выход: множество $A_a \subset W_{f_{k+1},R_{k+1}}$

1: Находим элемент $r \in R_1$, такой, что $f^{[q(q-1)p^{k-2}]}(a) \equiv a + p^k r \pmod{J^{k+1}}$.
2: Дополняем до базиса пространства $\mathbb{Z}_p^m$ элемент r, получим базис $r, r_2, \ldots, r_m$.
3: $A_a := \{c_1 r_2 + \ldots + c_m r_m : c_i \in \{0, \ldots, p-1\}, i = 1, \ldots, m\}$.

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

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