Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Исследование многочленов специального вида для использования фильтрующих генераторов

Фонарева Алиса,
Национальный исследовательский университет «Высшая школа экономики»

Используемые понятия и обозначения

$\delta_L: (x_1, x_2, \dots, x_n) \to \big(x_2, x_3, \dots, x_n, L(x)\big)$ – преобразование двоичного регистра сдвига с ***линейной функций обратной связи***

$$L(x) = x_1 + a_2 x_2 + \cdots + a_n x_n, \qquad x = (x_1, \dots, x_n).$$

Функция $L(x)$ однозначно соответствует ***характеристическому многочлену***

$$M_L(x) = 1 + x + \cdots + a_n x^{n-1} + x^n.$$

Используемые понятия и обозначения

Фильтрующий генератор задается парой (L, f) функций, где L – линейная функция обратной связи регистра сдвига, f – нелинейная функция выхода (фильтр).

При начальном состоянии $x = (x_1, \dots, x_n)$ выходная последовательность $y_1, y_2 \dots$ вырабатывается по закону

$$y_1 = f(x), y_2 = f\left(\delta_L(x)\right), \dots, y_j = f\left({\delta_L}^{j-1}(x)\right),$$

где $f = f(x_1, x_2, \dots, x_k)$ – функция от k аргументов (фильтрующая функция с соответствующего регистра сдвига).

Ограничения

Требования к фильтрующему генератору:

- максимальность периода ($\omega = 2^n - 1$);
- равновероятность выходных n-грамм (при случайном выборе начального состояния)*.

* – см. следующие работы:

- Рожков М. И. Биективные отображения, порождаемые фильтрующим генератором //Прикладная дискретная математика. – 2014. – №. 1 (23).
- Саранцев А. В. Построение регулярных систем однотипных двоичных функций с использованием регистра сдвига // ВЕСТНИК МОСКОВСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА ЛЕСА. – 2002. – С. 164.

Особенности решения задачи

- Достаточное условие максимальности периода: $M_L(x)$ – примитивный;
- $x^n + \alpha_n x^{n-1} + \cdots + \alpha_2 x + 1$ – примитивный $\Leftrightarrow x^n + \alpha_2 x^{n-1} + \cdots + \alpha_n x + 1$ – примитивный

Случай $k = 3$ для f_1

- Ограничения

$$f_1 = x_1x_2 + x_2 + x_3$$
$$L = x_1 + x_{n-1}$$
$$n \geq 7$$

- Поиск M_L

$$L = x_1 + x_{n-1} \Rightarrow M_L = x^n + x^{n-2} + 1 \text{ (n n-2 0)}$$
$$L_s = x_1 + x_3 \Rightarrow M_{L_s} = x^n + x^2 + 1 \text{ (n 2 0)}$$

- Результаты

$$x^{11} + x^2 + 1,$$
$$x^{21} + x^2 + 1,$$
$$x^{29} + x^2 + 1,$$
$$x^{35} + x^2 + 1,$$
$$x^{93} + x^2 + 1$$

⇨

$$x^{11} + x^9 + 1\ (L = x_1 + x_{10}),$$
$$x^{21} + x^{19} + 1(L = x_1 + x_{20}),$$
$$x^{29} + x^{27} + 1(L = x_1 + x_{28}),$$
$$x^{35} + x^{33} + 1(L = x_1 + x_{34}),$$
$$x^{93} + x^{91} + 1(L = x_1 + x_{92})$$

Случай $k = 4$ для f_2

- Ограничения

$$f_2 = x_3 + x_4 + x_1x_3 + x_2x_3 + x_1x_2x_3$$
$$L = x_1 + x_{n-2}$$
$$n \equiv 1 \pmod 3, n \geq 10$$

- Поиск M_L

$$L = x_1 + x_{n-2} \Rightarrow M_L = x^n + x^{n-3} + 1 \text{ (n n-3 0)}$$
$$L_s = x_1 + x_4 \Rightarrow M_{L_s} = x^n + x^3 + 1 \text{ (n 3 0)}$$

- Результаты

$$x^{10} + x^3 + 1,$$
$$x^{25} + x^3 + 1,$$
$$x^{28} + x^3 + 1,$$
$$x^{31} + x^3 + 1, x^{31} + x^{28} + 1,$$
$$x^{151} + x^2 + 1$$

⇨

$$x^{10} + x^7 + 1 (L = x_1 + x_8),$$
$$x^{25} + x^{22} + 1 (L = x_1 + x_{23}),$$
$$x^{28} + x^{25} + 1 (L = x_1 + x_{26}),$$
$$x^{31} + x^{28} + 1 (L = x_1 + x_{29}),$$
$$x^{151} + x^{148} + 1 (L = x_1 + x_{149})$$

Случай $k = 4$ для f_3

- Ограничения

$$f_3 = x_4 + x_1x_2 + x_1x_3 + x_2x_3$$
$$L = x_1 + x_{n-1}$$
$$n \equiv 1 \pmod 2, n \geq 11$$

- Поиск M_L

$$L = x_1 + x_{n-1} \Rightarrow M_L = x^n + x^{n-2} + 1 \text{ (n n-2 0)}$$
$$L_s = x_1 + x_3 \Rightarrow M_{L_s} = x^n + x^2 + 1 \text{ (n 2 0)}$$

- Результаты

$$x^{11} + x^2 + 1,$$
$$x^{21} + x^2 + 1,$$
$$x^{29} + x^2 + 1,$$
$$x^{35} + x^2 + 1,$$
$$x^{93} + x^2 + 1$$

⇨

$$x^{11} + x^9 + 1\ (L = x_1 + x_{10}),$$
$$x^{21} + x^{19} + 1(L = x_1 + x_{20}),$$
$$x^{29} + x^{27} + 1(L = x_1 + x_{28}),$$
$$x^{35} + x^{33} + 1(L = x_1 + x_{34}),$$
$$x^{93} + x^{91} + 1(L = x_1 + x_{92})$$

Случай $k = 4$ для f_4

- Ограничения

$$f_4 = x_2 + x_3 + x_1x_3 + x_3x_4 + x_1x_3x_4$$

$$L = x_1 + x_{n-2}, n \geq 8$$

- Поиск M_L

$$L = x_1 + x_{n-2} \Rightarrow M_L = x^n + x^{n-3} + 1 \text{ (n n-3 0)}$$

$$L_s = x_1 + x_4 \Rightarrow M_{L_s} = x^n + x^3 + 1 \text{ (n 3 0)}$$

- Результаты

$$x^{10} + x^3 + 1,$$
$$x^{17} + x^3 + 1, x^{17} + x^{14} + 1,$$
$$x^{20} + x^3 + 1,$$
$$x^{25} + x^3 + 1,$$
$$x^{28} + x^3 + 1,$$
$$x^{31} + x^3 + 1, x^{31} + x^{28} + 1,$$
$$x^{41} + x^3 + 1,$$
$$x^{52} + x^3 + 1,$$
$$x^{151} + x^2 + 1$$

⇨

$$x^{10} + x^7 + 1(L = x_1 + x_8),$$
$$x^{17} + x^{14} + 1(L = x_1 + x_{15}),$$
$$x^{20} + x^{17} + 1(L = x_1 + x_{18}),$$
$$x^{25} + x^{22} + 1(L = x_1 + x_{23}),$$
$$x^{28} + x^{25} + 1(L = x_1 + x_{26}),$$
$$x^{31} + x^{28} + 1(L = x_1 + x_{29}),$$
$$x^{41} + x^{38} + 1(L = x_1 + x_{39}),$$
$$x^{52} + x^{49} + 1(L = x_1 + x_{50}),$$
$$x^{151} + x^{148} + 1(L = x_1 + x_{149})$$

В планах

- Рассмотрение случаев при $k = 5, 6$;
- поиск примитивных многочленов более высоких степеней.

Литература

- Рожков М.И. Биективные отображения, порождаемые фильтрующим генератором. // Прикладная дискретная математика. – 2014. № 1(23). – С. 27–39.
- Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. – М.: Юрайт, 2016. – 473 с.
- Лидл Р., Нидеррайтер Г. Конечные поля. Т. 2 – М.: Мир, 1988. – 818 с.
- Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.