ЛИТЕРАТУРА

1. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.
2. *Фомичев В. М., Кяжин С. Н.* Локальная примитивность матриц и графов // Дискрет. анализ и исслед. операций. 2017. Т. 24. № 1. С. 97–119.
3. *Фомичев В. М., Задорожный Д. И., Коренева А. М., Лолич Д. М., Юзбашев А. В.* Об алгоритмической реализации s-боксов // Проблемы информационной безопасности. Компьютерные системы. 2017 (в печати).

УДК 519.1 DOI 10.17223/2226308X/10/40

О СВОЙСТВАХ ТРЁХКАСКАДНОГО ГЕНЕРАТОРА С ПЕРЕМЕЖАЮЩИМСЯ ШАГОМ, ПОСТРОЕННОГО НА ОСНОВЕ СХЕМЫ ДВИЖЕНИЯ «СТОП-ВПЕРЁД»[1]

В. М. Фомичев, Д. М. Колесова

Посчитан ряд характеристик трёхкаскадного генератора гаммы с перемежающимся шагом (схема движения «стоп-вперед»), где первый управляющий каскад построен на основе регистра сдвига с линейной обратной связью (ЛРС) длины n, второй управляющий каскад — на основе двух ЛРС длин m и μ, третий генерирующий каскад — на основе двух ЛРС длин r и ρ. Если все ЛРС имеют примитивные характеристические многочлены и числа n, m, μ, r, ρ попарно взаимно простые, то длина периода t гаммы генератора равна $(2^n-1)(2^m-1)(2^\mu-1)(2^r-1)(2^\rho-1)$. Циклическая группа генератора порядка t порождается подстановкой множества состояний, реализуемой за один такт, и содержит линейную подгруппу порядка $(2^r-1)(2^\rho-1)$. Получены значения локальных $i,(p+1)$-экспонентов перемешивающего орграфа генератора, $i=1,\dots,p$, где $p=n+m+\mu+r+\rho$, из которых следует, что длину «холостого хода» генератора целесообразно определить не меньше, чем $\max\{n+2, \max(m,\mu)+1, \max(r,\rho)\}$.

Ключевые слова: *генератор гаммы, регистр сдвига с линейной обратной связью, длина периода гаммы, перемешивающие свойства, локальная примитивность орграфа.*

Введение

Генераторы гаммы с неравномерным движением, активно исследуемые как в России, так и за рубежом [1, гл. 18], относительно просто реализуются и обладают рядом положительных криптографических свойств: большая длина периода, высокая линейная сложность и др. К этому классу относятся двухкаскадные генераторы с перемежающимся шагом, построенные на основе двух генераторов «стоп-вперед». Для их обобщения — трёхкаскадных генераторов с перемежающимся шагом — получен ряд свойств.

1. Функционирование трёхкаскадного генератора с перемежающимся шагом

Первый управляющий каскад есть фильтрующий генератор на базе ЛРС-x длины n и фильтрующей функции $f(x_1,\dots,x_n)$, генерирующий управляющую гамму $\{\gamma_{i,x} : i=1,2,\dots\}$. Второй управляющий каскад состоит из ЛРС-y и ЛРС-z соответственно длины m (номера ячеек $n+1,\dots,n+m$) и μ (номера ячеек $n+m+1,\dots,$

[1]Работа первого автора выполнена в соответствии с грантом РФФИ № 16-01-00226.

$n+m+\mu$), которые управляются гаммой $\{\gamma_{i,x} : i = 1, 2, \dots\}$ и управляют третьим каскадом с помощью последовательности сумм знаков $\gamma_{i,y} \oplus \gamma_{i,z}$, снимаемых с ячеек $n+m$ ЛРС-y и $n+m+\mu$ ЛРС-z соответственно. Третий генерирующий каскад состоит из ЛРС-u и ЛРС-v длин r (номера ячеек $n+m+\mu+1, \dots, n+m+\mu+r$) и ρ (номера ячеек $n+m+\mu+r+1, \dots, n+m+\mu+r+\rho$) соответственно, которые управляются последовательностью сумм знаков $\{\gamma_{i,y} \oplus \gamma_{i,z}\}$ и вырабатывают знаки $\gamma_{i,u}$ и $\gamma_{i,v}$, снимаемые с ячейки $n+m+\mu+r$ ЛРС-u и с ячейки $n+m+\mu+r+\rho$ ЛРС-v. Сумма этих знаков образует гамму генератора. Все ЛРС имеют примитивные характеристические многочлены. Гамма генератора есть сумма $\gamma_i{=}\gamma_{i,u} \oplus \gamma_{i,v}$, $i = 1, 2, \dots$

Схема управления движением: ЛРС-x сдвигается равномерно, на один шаг в каждом такте. Если $\gamma_{i,x} = 1$, то ЛРС-y продвигается на один шаг, а ЛРС-z простаивает. Если $\gamma_{i,x} = 0$, то ЛРС-y простаивает, а ЛРС-z продвигается на один шаг. Если $\gamma_{i,y} \oplus \gamma_{i,z}{=}1$, то ЛРС-$u$ продвигается на один шаг, а ЛРС-v простаивает. Если $\gamma_{i,y} \oplus \gamma_{i,z} = 0$, то ЛРС-$u$ простаивает, а ЛРС-v продвигается на один шаг. Считаем, что все регистры левого сдвига.

В криптографических приложениях ключом генератора является, как правило, начальное состояние всех ЛРС.

2. Криптографические свойства трёхкаскадного генератора

Длина периода гаммы. Обозначим g_x, g_y, g_z, g_u, g_v линейные подстановки множеств состояний соответствующих регистров, $(\bar{x}, \bar{y}, \bar{z}, \bar{u}, \bar{v})$ — начальное состояние генератора. Тогда состояние регистра ЛРС-x в j-м такте есть $g_x^{j-1}(\bar{x})$, $j = 1, 2, \dots$, $g_x^0(\bar{x}) = \bar{x}$. Для определения длины периода гаммы посчитаем глубины продвижения регистров $\sigma_x(i, \bar{x})$, $\sigma_y(i, \bar{x})$, $\sigma_z(i, \bar{x})$, $\sigma_u(i, \bar{x}, \bar{y}, \bar{z})$, $\sigma_v(i, \bar{x}, \bar{y}, \bar{z})$ за i тактов при начальном состоянии. ЛРС-x движется равномерно, значит, $\sigma_x(i, \bar{x}) = i$, для регистров ЛРС-y и ЛРС-z верно

$$\sigma_y(i, \bar{x}) = f(\bar{x}) + \dots + f(g_x^{i-1}(\bar{x})), \quad \sigma_z(i, \bar{x}) = i - \sigma_y(i, \bar{x}), \quad i = 1, 2, \dots$$

Обозначим в j-м такте через y_j бит, записанный в ячейке $n+m$ ЛРС-y, и через z_j — бит, записанный в ячейке $n+m+\mu$ ЛРС-z. Тогда для регистров ЛРС-u и ЛРС-v верно

$$\sigma_u(i, \bar{x}, \bar{y}, \bar{z}) = (y_1 \oplus z_1) + \dots + (y_i \oplus z_i), \quad \sigma_v(i, \bar{x}, \bar{y}, \bar{z}) = i - \sigma_u(i, \bar{x}, \bar{y}, \bar{z}).$$

Пусть для определённости $f(0, \dots, 0) = 0$ и f уравновешена. Тогда при любом $\bar{x}$

$$\sigma_y(2^n - 1, \bar{x}) = 2^{n-1}, \quad \sigma_z(2^n - 1, \bar{x}) = 2^{n-1} - 1.$$

Если $(2^m - 1, 2^\mu - 1) = 1$, то при $i = (2^n - 1)(2^m - 1)(2^\mu - 1)$ и любых $\bar{y}, \bar{z}$ имеем

$$\sigma_u((2^n - 1)(2^m - 1)(2^\mu - 1), \bar{x}, \bar{y}, \bar{z}) = (2^n - 1)(2^{m+\mu-1} - 2^{m-1} - 2^{\mu-1}),$$
$$\sigma_v((2^n - 1)(2^m - 1)(2^\mu - 1), \bar{x}, \bar{y}, \bar{z}) = (2^n - 1)(2^m - 1)(2^\mu - 1) -$$
$$-(2^n - 1)(2^{m+\mu-1} - 2^{m-1} - 2^{\mu-1}).$$

Длина периода управляющей гаммы первого каскада равна $2^n - 1$, второго — $(2^n - 1)(2^m - 1)(2^\mu - 1)$.

Теорема 1. Если числа n, m, μ, r, ρ попарно взаимно простые и все ЛРС имеют примитивные характеристические многочлены, то длина периода генератора равна

$$t_\gamma = (2^n - 1)(2^m - 1)(2^\mu - 1)(2^r - 1)(2^\rho - 1).$$

Группа генератора. Обозначим: $a = y_1$; $b = z_1$, тогда подстановка g множества состояний генератора (за один такт) имеет вид

$$g(\bar{x}, \bar{y}, \bar{z}, \bar{u}, \bar{v}) = (g_x(\bar{x}), g_y^{f(x)}(\bar{y}), g_z^{f(x)\oplus 1}(\bar{z}), g_u^{a\oplus b}(\bar{u}), g_v^{a\oplus b\oplus 1}(\bar{v})).$$

Группа генератора циклическая, порождается подстановкой $g(\bar{x}, \bar{y}, \bar{z}, \bar{u}, \bar{v})$.

Теорема 2. Подстановка g^i является линейной, если и только если число i кратно $(2^n-1)(2^m-1)(2^\mu-1)$. Отсюда порядок линейной подгруппы группы генератора равен $(2^r-1)(2^\rho-1)$.

Перемешивающие свойства трехкаскадного генератора.

Перемешивающие свойства генератора определяются перемешивающим $(p+1)$-вершинным орграфом Γ подстановки $g(\bar{x}, \bar{y}, \bar{z}, \bar{u}, \bar{v})$, где $p = n+m+\mu+r+\rho$. Орграф Γ состоит из вершины $p+1$ и компонент сильной связности K_x, K_y, K_z, K_u, K_v, соединённых дугами. Компонента K_x есть перемешивающий n-вершинный орграф подстановки g_x; K_y, K_z, K_u, K_v суть перемешивающие орграфы с числом вершин m, μ, r, ρ подстановок g_y, g_z, g_u, g_v соответственно, к которым в каждую вершину добавлена петля (следует из свойств схемы управления «стоп-вперед»). В каждую вершину из $K_y \cup K_z$ входит дуга, исходящая из каждой вершины множества $E(f)$, где $E(f)$ — множество номеров существенных переменных функции f. В каждую вершину из $K_y \cup K_z$ входит дуга, исходящая из вершины $n+m$ компоненты K_y и из вершины $n+m+\mu$ компоненты K_z (снимаемые с этих ячеек гаммы управляют третьим каскадом). В Γ также есть дуги $(p-\rho, p+1)$ и $(p, p+1)$.

Орграф Γ не является сильносвязным, но является локально примитивным. Если в Γ вершина j достижима из вершины i, то i,j-exp Γ равен длине кратчайшего пути из i в j, проходящего через любую вершину с петлей [2, с. 187]. Отсюда верна

Теорема 3. Локальные экспоненты $i, (p+1)$-exp Γ равны

$$i, (p+1)\text{-exp}\,\Gamma = \begin{cases} n+2, & i = 1, \ldots, n; \\ \max(m, \mu)+1, & i = n+1, \ldots n+m+\mu; \\ \max(r, \rho), & i = n+m+\mu+1, \ldots, p. \end{cases}$$

Из теоремы 3 следует, что длину «холостого хода» генератора целесообразно определить не меньше чем $\max\{n+2, \max(m, \mu)+1, \max(r, \rho)\}$. Для генераторов с другой схемой перемежающихся шагов результаты аналогичны.

Вывод: криптографические свойства генераторов с перемежающимся шагом усиливаются с ростом числа каскадов.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
2. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты. М.: Изд-во Юрайт, 2016. 209 с.