Бабаш АВ
Профессор НИУ ВШЭ

О периодичности функционирования генераторов псевдослучайных чисел RC4, IA, IBAA

RC4 (см.[1]). $V_N = Z_N \times Z_N \times S_N$ - множество внутренних состояний, где Z_N – кольцо вычетов по модулю N, S_N – симметрическая группа степени N и $N = 2^n$ (n=8 на практике).

$v_0 = (i_0, j_0, s_0) = (0,0,s)$ - начальное состояние RC4. Внутреннее состояние RC4 в момент времени t есть $v_t = (i_t, j_t, s_t)$, где $v_t \in V_N$.

Для $t \in [1;\infty)$:

$i_t = i_{t-1} \oplus 1$

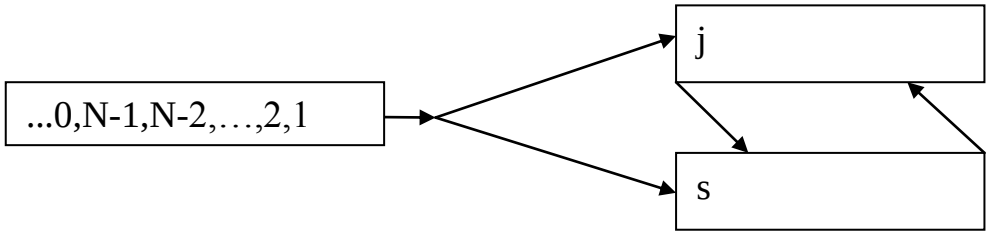
$j_t = j_{t-1} \oplus s_{t-1}(i_t)$

$s_t = s_{t-1} \circ (s_{t-1}(i_t), s_{t-1}(j_t))$

$\gamma_t = s_t(s(i_t) \oplus s_t(j_t))$ (выходной элемент),

где $\oplus$ – операция сложения по модулю N, $s_t(z)$– образ элемента z подстановки s_t, $\circ$ – операция композиции подстановок в симметрической группе S_N, а (x,y) – подстановка из S_N, являющаяся транспозицией различных элементов x и y.

Теоретико-автоматная модель процедуры RC4:



Теорема1. При входной последовательности Q=1,2,…N-1,0,1,2… период последовательности подстановок $s_t, t \in \{1,2,...\}$ кратен 2^{n-1} для любой начальной подстановки s_0. Если для подстановки s_0 выполняется неравенство $s_0(1) \neq 1 + 2^{n-1}$, то период последовательности подстановок $s_t, t \in \{1,2,...\}$ кратен величине $N = 2^n$.

IA (см.[2]). Состояниями IA являются тройки (i,q,S), где $S: Z_m \to Z_{2^K}$ - произвольное отображение кольца вычетов по модулю m=2^n в кольцо вычетов по модулю 2^K, q - произвольный элемент кольца вычетов Z_{2^K}, $K = 2n + \Delta$, $\Delta \geq 0$, $i \in Z_m$. Начальные состояния IA имеет вид $(i_0 = 0, q_0 = 0, S_0)$.

В каждый момент времени $t \in [1;\infty)$ в IA происходит переход из состояния $(S_{t-1}, q_{t-1}, i_{t-1})$ в новое состояние (S_t, q_t, i_t) и выработка нового элемента q_t выходной последовательности. При этом выполняются следующие действия:

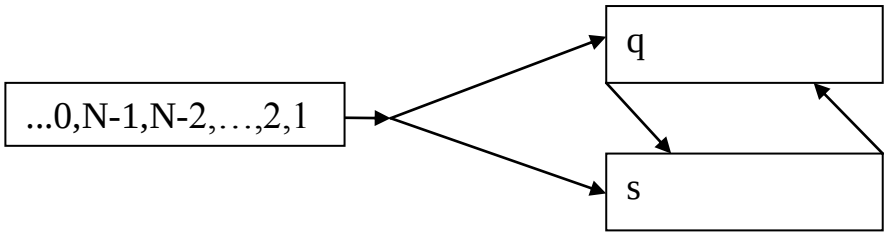
$i_t = i_{t-1} + 1 \mod(m)$,

$s_t[i_t] = s_{t-1}[s_{t-1}[i_t](\mathrm{mod}\, m)] + q_{t-1}$,

$q_t = s_t[(s_t[i_t] >> n)(\mathrm{mod}\, m)] + s_{t-1}[i_t]$,

где $s_t[j]$ - образ элемента j для отображения S_t, + - операция сложения по модулю 2^K, $(s[i_t] >> n)$- представление $s[i_t]$ в двоичном виде с последующим сдвигом вправо на n разрядов (первые n разрядов полученного бинарного вектора являются нулями), а затем перевод этого двоичного вектора в элемент Z_m.

Теоретико-автоматная модель IA:



Теорема 2. При входной последовательности Q=1,2,…m-1,0,1,2… и любом начальном состоянии вида $\sigma_0 = (q_0 = 0, S_0)$ период последовательности отображений S_t, $t \in \{1,2,...\}$ либо кратен величине m=2^n, либо равен 1, в последнем случае период выходной последовательности q_t, $t \in \{1,2,...\}$ делит m.

Теорема 3. Период $\tau(S)$ последовательности S_t, $t \in \{1,2,...\}$ равен 1, тогда и только тогда, когда выполнены равенства P:

$S_0[1] = S_0[S_0[1](\mathrm{mod}\, m)]$

$S_0[2] = S_0[S_0[2](\mathrm{mod}\, m)] + q_1 = S_0[S_0[2](\mathrm{mod}\, m)] + S_0[(S_0[1] >> n)(\mathrm{mod}\, m)] + S_0[1]$

$S_0[3] = S_0[S_0[3](\mathrm{mod}\, m)] + q_2 = S_0[S_0[3](\mathrm{mod}\, m)] + S_0[(S_0[2] >> n)(\mathrm{mod}\, m)] + S_0[2]$

$S_0[4] = S_0[S_0[4](\mathrm{mod}\, m)] + q_3 = S_0[S_0[4](\mathrm{mod}\, m)] + S_0[(S_0[3] >> n)(\mathrm{mod}\, m)] + S_0[3]$

……

$S_0[0] = S_0[S_0[m-1](\mathrm{mod}\, m)] + q_{m-1} = S_0[S_0[0](\mathrm{mod}\, m)] + S_0[(S_0[m-1] >> n)(\mathrm{mod}\, m)] + S_0[m-1]$

Разработан алгоритм получения всех состояний вида $\sigma_0 = (q_0 = 0, S_0)$, при которых период последовательности отображений S_t, $t \in \{1,2,...\}$ равен 1.

IBAA. Положим $m = 2^n$, $K \geq 2n$, для практических приложений m=256 (т. е. n=8), K=32. Определим натуральные числа p и q с условием p+q=K. Введем обозначения:

$\oplus$ - операция xor (сложение двоичных векторов по модулю 2);

+ -сложение по модулю 2^K;

$\otimes$- сложение по модулю m;

$\ll p$ - сдвиг влево двоичного вектора на p шагов (p правых разрядов вектора становятся нулями);

$\gg q$ сдвиг вправо двоичного вектора на q шагов (q левых разрядов вектора становятся нулями). Состояниями генератора является множество четверок (i,a,S,q), где $i \in Z_m$, $a \in Z_K$, $q \in Z_K$, $S=(S[1],S[2],...,S[m])$ – отображение Z_m в Z_K, $S[i]$ - образ i при отображении S, $S[S[i] \ll n \bmod m]$ - результат последовательного выполнения сдвига $S[i] \ll n$, приведения $S[i] \ll n$ по $\bmod m$ и вычисление образа полученной величины при отображении S. Состояния генератора индексируются временем t.

Начальным состоянием генератора является четверка $(i_0=0,a_0,S_0,q_0)$. Функционирование генератора задается индуктивными равенствами

$$a_t=((a_{t-1} \ll p) \oplus (a_{t-1} \gg q)) + S_{t-1}[i_t \otimes \frac{m}{2}],$$

$$q_t = S_t[S_t[i_t] \ll n \bmod m] + S_{t-1}[i_t],$$

$$S_t[i_t] = S_{t-1}[S_{t-1}[i_t] \bmod m] + a_t + q_{t-1}.$$

Последовательность q_t, $t \in \{1,2,...\}$ является выходной последовательностью генератора.

Теорема 4. Период последовательности отображений генератора IBAA для начального состояния $(i_0=0,a_0,S_0,q_0)$ либо кратен m, либо равен единице. Если для начального состояния $(i_0=0,a_0,S_0,q_0)$ генератора IBAA не выполняется условие У(IBAA) (условие приводится ниже), то период последовательности отображений S_j, $j \in \{0,1,2,...\}$ кратен m.

Сформулируем условие У(IBAA):

1) получаемые по ниже приведенным формулам последовательности

$*q_1, *q_2, ..., *q_j, ...$; $*a_2, *a_3, ..., *a_j, ...$ являются периодическими с периодами, делящими величину m.

$$*a_t = F*a_{t-1} + S_0[i_t \otimes \frac{m}{2}], \quad (1)$$

$$*q_t = S_0[S_0[i_t] \ll n \bmod m] + S_0[i_t], \quad (2)$$

$$S_0[i_t] = S_0[S_0[i_t] \bmod m] + *a_t + *q_{t-1}, \quad (3)$$

где, в свою очередь, последовательность i_t периодическая периода m имеет вид 1,2,3,…, m-1,0,1.2.3…;

2) выполняются равенства

$$*q_1 = S_0[S_0[1] \ll n \bmod m] + S_0[1],$$

$$*q_2 = S_0[S_0[2] \ll n \bmod m] + S_0[2],$$

.....

$$*q_{m-1} = S_0[S_0[m-1] \ll n \bmod m] + S_0[m-1],$$

$$*q_m = S_0[S_0[0] \ll n \bmod m] + S_0[0],$$

$$*a_1 = Fa_0 + S_0[1 \otimes \frac{m}{2}],$$

$$*a_2 = F * a_1 + S_0[2 \otimes \frac{m}{2}],$$

$$*a_3 = F * a_2 + S_0[3 \otimes \frac{m}{2}],$$

……..

$$*a_j = F * a_{j-1} + S_0[j \otimes \frac{m}{2}],$$

……

$$*a_{m-1} = F * a_{m-2} + S_0[m-1 \otimes \frac{m}{2}],$$

$$*a_m = F * a_{m-1} + S_0[0 \otimes \frac{m}{2}],$$

$$*a_{m+1} = F * a_m + S_0[1 \otimes \frac{m}{2}]$$

и одновременно:

$$*a_1 = S_0[1] - S_0[S_0[1] \bmod m] - q_0,$$

$$*a_2 = S_0[2] - S_0[S_0[2] \bmod m] - *q_1,$$

……

$$*a_m = S_0[0] - S_0[S_0[0] \bmod m] - *q_{m-1},$$

$$*a_{m+1} = S_0[1] - S_0[S_0[1] \bmod m] - *q_m.$$

Литература

1. Бабаш А.В., Кудияров Д.А. Период функционирования генератора псевдослучайных чисел RC-4. Системы высокой доступности №2 т.8, 2012.
2. Бабаш А.В., Кудияров Д.А. О периоде функционирования генератора псевдослучайных чисел IA. Проблемы информационной безопасности. Компьютерные системы. № 3 2013.