О ПЕРИОДИЧНОСТИ ФУНКЦИОНИРОВАНИЯ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ RC4

Бабаш А.В., Кудияров Д.С.

ИСТОРИЯ RC4

- Разработан в 1987 году Роном Райвестом из компании RSA Data Security.
- Аббревиатура означает Ron’s Code 4.
- RSA не официально не опубликовал RC4, но в 1994 году код алгоритма RC4 было размещено на странице интернет-конференции Cypherpunks, чуть позже в переписке sci.crypt.
- Требуется малое количество операций для перехода в новое состояние и выработки псевдослучайного значения, что позволяет генерировать большое количество данных за короткое время.
- Используется в алгоритмах WEP, WPA, TLS

ШИФР RC4

Внутренне состояние RC4:

Множество внутренних состояний RC4:

$$V_N = Z_N \times Z_N \times S_N$$

Где:

Z_N – кольцо вычетов по модулю *N*,

S_N – симметрическая группа степени *N*,

$N=2^n$ – параметр, от которого зависит множество внутренних состояний RC4 (промышленно используется *N=256*)

В момент времени *t* внутреннее состояние RC4:

$$v_t = (i_t, j_t, s_t)$$

$$v_t \in V_N$$

Выработка гаммы (PRGA)

В каждый момент времени $t = 1,2, \ldots$ вычисляется новое внутреннее состояние

$v_t = (i_t, j_t, s_t)$:

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

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

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

$$\gamma_t = s_t(s(i_t) \oplus s_t(j_t))$$

$\oplus$ - операция сложения по модулю *N*

$s_t(z)$ - Образ элемента z в подстановке s_t

$\circ$ - операция композиции подстановок

(x, y) - транспозиция элементов x и y

ТЕОРЕТИКО-АВТОМАТНАЯ МОДЕЛЬ RC4

Автономный автомат *A* → Неавтономный автомат *B*

Z_N Множество внутренних состояний автомата *A* (начальное состояние -1)

Z_N Выходной алфавит

$\delta : Z_N \to Z_N$, $\delta(i) = i \oplus 1$ Функция перехода

$\lambda : Z_N \to Z_N$, $\lambda(i) = i \oplus 1$ Функция выхода

$\Sigma = Z_N \times S_N$ Множество внутренних состояний

$X = Z_N$ Входной алфавит

$Y = Z_N$ Выходной алфавит

$(f_x)_{x \in X} : \Sigma \to Y$, $f_x(j, s) = s(s(x) \oplus s(j))$ Частичная функция выхода

$(h_x)_{x \in X} : \Sigma \to \Sigma$, $h_x(j, s) = (j \oplus s(x), s \circ (s(x), s(j \oplus s(x))))$ Частичная функция перехода

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И ОПРЕДЕЛЕНИЯ

$c \mid u$ — c делит u

Чисто периодическая последовательность $b_1, b_2, \ldots, b_t, \ldots$

Всегда найдется натуральное число d, при котором $b_t = b_{t+kd}$ для любых натуральных чисел t, k. Минимальное число d с указанным свойством называется периодом последовательности.

ПОСЛЕДОВАТЕЛЬНОСТИ

$v_0 = (i_0, j_0, s_0) = (0,0, s_0)$ Начальное состояние процедуры PRGA

$Q = 0,1,2,\ldots,N\text{-}1,0,1,2\ldots$ Чисто периодическая выходная последовательность автомата *A* периода *N*

$s_t, t \in \{1,2,\ldots\}$ Последовательность подстановок s_t

$(j_t, s_t), t \in \{1,2,\ldots\}$ Последовательность внутренних состояний генератора *B*

$\gamma_t = s_t(s(i_t) \oplus s_t(j_t)), t \in \{1,2,\ldots\}$ Выходная последовательность автомата *B*, выработанная с состояния $(0,s_0)$ при входной последовательности *Q*

ПЕРИОДЫ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

$\tau(\gamma)$ Период выходной последовательности автомата B

$\tau(s)$ Период последовательности подстановок $s_t, t=1,2...$

$\tau(j_t, s_t), t \in \{1,2,...\}$ Период последовательности внутренних состояний автомата *B* с начальным состоянием s_0 при входной последовательности *Q*

Заметим, что: $\tau(\gamma) \mid \tau(s)$

$$\tau(s) \mid \tau(j_t, s_t), t \in \{1,2,...\}$$

УТВЕРЖДЕНИЕ

- Последовательности $s_t, t \in \{1,2,\ldots\}$ и $\gamma_t, t \in \{1,2,\ldots\}$ являются чисто периодическими.

ДОКАЗАТЕЛЬСТВО

- Достаточно доказать, что последовательность состояний автомата $B(j_t, s_t), t \in \{1,2,\ldots\}$ начинающаяся с состояния s_0, является чисто периодической.
- Для этого достаточно доказать, что автомат B перестановочный, т.е. его частичные функции перехода $(h_x)_{x \in X}$ осуществляют биекции.
- Предположим обратное: для некоторого входного символа $x \in Z_N$ и некоторых состояний *(j,s), (j*,s*)* из $Z_N \times S_N$ выполняется равенство $h_x(j,s) = h_x(j^*, s^*)$,т.е.

  $(j \oplus s(x), s \circ (s(x), s(j \oplus s(x)))) = (j^* \oplus s^*(x), s^* \circ (s^*(x), s^*(j^* \oplus s^*(x))))$
- Следовательно $j \oplus s(x) = j^* \oplus s^*(x)$ и $s \circ (s(x), s(j \oplus s(x))) = s^* \circ (s^*(x), s^*(j^* \oplus s^*(x)))$
- Положим $j'' = j \oplus s(x) = j^* \oplus s^*(x)$, тогда $s \circ (s(x), s(j'') = s^* \circ (s^*(x), s^*(j''))$
- Следовательно $s = s^*$ и $j = j^*$.
- Полученное противоречие завершает доказательство

ТЕОРЕМА

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

РЕЗУЛЬТАТ

- Генератор RC4 представлен последовательным соединением автономного полноциклового автомата с неавтономным автоматом. Состояниями последнего являются пары: подстановка степени 2^n и вычет из кольца вычетов по модулю 2^n. Доказано, что периоды последовательностей подстановок кратны числу 2^{n-1} и даны достаточные условия, при которых эти периоды кратны 2^n.

СПАСИБО ЗА ВНИМАНИЕ!

Бабаш А.В., Кудияров Д.С.