ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 3
2012

Д. И. Шувалев (Москва, ТВП). **О некоторых вероятностных свойствах сжимающего генератора.**

Сжимающий (*shrinking* [1]) генератор вырабатывает двоичную последовательность псевдослучайных чисел, синхронно реализуя две входные двоичные последовательности $s = (s_0, s_1, \dots)$ и $a = (a_0, a_1, \dots)$: на такте с номером t при $s_t = 1$ выдается знак a_t, а при $s_t = 0$ не выдается ничего. Как правило, последовательности s и a представлены линейными рекуррентами или регистрами сдвига с переменными точками съема. Представляют практический интерес задачи восстановления конфигурации и начального заполнения a и s по отрезку выходной последовательности.

В докладе рассматривается упрощенный случай, когда последовательность $a = (1, 0, 1, 0, \dots)$ знакопеременная, а статистические свойства генератора обеспечиваются большим периодом последовательности s.

Можно показать, что если s — последовательность независимых испытаний над случайной величиной с распределением (p, q), $p + q = 1$, то выходная последовательность — цепь Маркова с матрицей переходных вероятностей

$$S = \begin{pmatrix} 1/(1+q) & q/(1+q) \\ q/(1+q) & 1/(1+q) \end{pmatrix}.$$

Указанное свойство позволяет по наблюдениям за выходной последовательностью выделять в последовательности s отрезки со значительным преобладанием единиц.

Теорема. *Пусть s — последовательность независимых испытаний над случайной величиной, принимающей значения 0 и 1 с равными вероятностями, а ξ — число знакоперемен в выходной последовательности длины $U > 1$. Тогда*

$$\mathbf{P}\{\xi = x\} = \frac{2^x}{3^{U-1}} \binom{U-1}{x}.$$

Если, кроме того, ζ — число нулей в последовательности s, появившихся между получением первого и получением U-го знака выходной последовательности, то

$$\mathbf{P}\{\xi = x,\ \zeta = U - x - 1 + 2z\} = \frac{2^{x-2z}}{4^{U-1}} \binom{U-1}{x} \binom{z+U-2}{z}.$$

Для усиления генератора используются прореживание (*decimation*), когда знаки выходной последовательности используются не подряд, а с заданным шагом, и прослаивание (*interleaving*), когда несколько отрезков выходной последовательности составляются в одну последовательность чередованием [2]. Очевидно, что статистические свойства усиленной выходной последовательности описываются подходящей степенью матрицы S.

В докладе приводятся теоретические и экспериментальные оценки длины выходной последовательности, обеспечивающей заданную вероятность появления и заданную надежность выделения отрезков s со значительным преобладанием единиц. Для выделения также может быть использована выходная последовательность с искажениями. Отмечается, что совместное распределение двоичных весов у нескольких соседних отрезков максимальной линейной рекуррентной последовательности порядка n зависит не только от n, но и от коэффициентов характеристического многочлена (здесь суммарная длина отрезков превышает n).

СПИСОК ЛИТЕРАТУРЫ

1. *Coppersmith D.*, *Krawczyk H.*, *Mansour Y.* The shrinking generator. — In: Advances in Cryptology — Crypto'93./ Ed. by D. R. Stinson. New York: Springer-Verlag, 1994, p. 22–39.
2. *Robshaw M. J. B.* Stream Ciphers. Technical Report TR–401, RSA Laboratories, revised July 1995.