ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 24 МАТЕМАТИКИ Выпуск 5
2017

С. Ю. Мельников (Москва, ООО «Линфо»). **Регистры сдвига с последовательным суммированием не сохраняют статистические свойства входной последовательности.**

При построении генераторов случайных последовательностей часто используется каскадный метод, который заключается в выработке результирующих последовательностей из исходных с помощью автоматных преобразований, реализуемых в так называемых узлах усложнения. К таким узлам можно предъявить требование увеличения линейной сложности и другие требования ([1]). Естественным требованием является и то, чтобы равновероятная (по знакам) входная последовательность преобразовывалась бы в равновероятную.

В [2] рассматривались автоматы, которые гарантируют, что частоты знаков во входной и выходной последовательности будут не сильно различаться между собой. Пусть $A = (X, Y, Q, h, f)$ — конечный автомат с двоичными входным и выходным алфавитами $X = Y = \{0, 1\}$, множеством состояний Q, функцией переходов $h : Q \times X \to Q$, функцией выходов $f : Q \times X \to Y$. Начальное состояние, входную и выходную последовательности автомата обозначим $q^{(0)} \in Q$, $(x^{(1)}, x^{(2)}, \ldots)$, $(y^{(1)}, y^{(2)}, \ldots)$. Автомат сохраняет значковые статистические свойства входной последовательности, если равенство

$$\lim_{t\to\infty} \frac{1}{t} \sum_{j=1}^{t} x^{(j)} = \lim_{t\to\infty} \frac{1}{t} \sum_{j=1}^{t} y^{(j)}$$

выполняется для всех $q^{(0)} \in Q$ и всех бесконечных двоичных периодических (возможно, с подходом) последовательностей $(x^{(1)}, x^{(2)}, \ldots)$.

В [2] исследовался класс регистров сдвига и их функций выходов, которые обладают указанным свойством. Получена дважды экспоненциальная по размеру накопителя оценка для их количества.

Регистром сдвига с последовательным суммированием называется (см. [3]) автомат Мура с двоичными входным и выходным алфавитами, множеством состояний $\{0, 1\}^n$, $n \geqslant 1$, булевой функцией выходов $f(x_1, x_2, \ldots, x_n)$, который под действием входного символа $a_0 \in \{0, 1\}$ из состояния $(a_1, a_2, \ldots, a_n)$ переходит в состояние $(a_0 \oplus a_1, a_1 \oplus a_2, \ldots, a_{n-1} \oplus a_n)$, где $\oplus$ — суммирование по модулю 2. Такой автомат будем обозначать $A_f^{\oplus}$. Теоретико-автоматные свойства регистров, аналогичных $A_f^{\oplus}$, в автономном случае рассматривались, в частности, в [4], а вопросы их аппаратной реализации — в [5] и [6].

Утверждение. *Автомат $A_f^{\oplus}$ не сохраняет значковые свойства входной последовательности ни для какой функции выходов $f(x_1, x_2, \ldots, x_n)$.*

СПИСОК ЛИТЕРАТУРЫ

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. Учебное пособие. М.: Гелиос АРВ, 2002, 480 с.

2. *Мельников С. Ю.* Неавтономные двоичные регистры сдвига, сохраняющие значковые статистические свойства входной последовательности. — Докл. Томского гос. ун-та систем управления и радиоэлектроники (ТУСУР), 2015, № 2(36), с. 86–99.
3. *Мельников С. Ю.* О статистических характеристиках обработки двоичных последовательностей регистром сдвига с последовательным суммированием. — Обозрение прикл. и промышл. матем., 2009, т. 16, в. 4, с. 682–683,
4. *Golomb S. W.* Shift Register Sequences. Laguna Hills, CA: Aegean Park Press, 1981, 247 p.
5. *Гришкин А. С.* Генераторы псевдослучайных символов на регистрах сдвига с внутренними сумматорами по модулю два при использовании инверсных выходов. Дисс. на соискание уч. ст. канд. техн. наук, КГТУ: Казань, 2006, 142 с.
6. *Chen W.-K.* The VLSI Handbook. 2nd ed. Chicago: CRC Press, 2006, 2320 p.