З. Р. Гарифуллина, М. А. Иванов, В. Е. Рябков, И. В. Чугунков

СПОСОБ ФОРМИРОВАНИЯ НЕЛИНЕЙНЫХ М-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Введение

Наиболее эффективными (в первую очередь из-за простоты программной и аппаратной реализации и хороших статистических свойств некриптографических генераторов ПСЧ) являются генераторы ПСЧ на регистрах с линейными обратными связями (РСЛОС) [1–8]. Используемый при их анализе математический аппарат — теория линейных последовательностных машин и теория конечных полей (полей Галуа).

Эти генераторы активно используются в качестве строительных блоков при построении поточных криптографических генераторов ПСЧ, при построении помехоустойчивых кодов БЧХ, Рида–Соломона и других циклических кодов. Они обладают очень интересными свойствами, которые позволяют решать целый ряд специфических задач, связанных с защитой информации.

В работах [3, 6] теория двоичных последовательных генераторов обобщается на случай формирования недвоичных последовательностей. Рассматриваются теоретические основы построения двоичных параллельных генераторов ПСЧ, недвоичных генераторов последовательного и параллельного типов, анализируются их свойства. Описываются принципы построения нелинейных генераторов произвольной длины, в том числе максимально возможной при заданном числе элементов памяти генератора, генераторов с предпериодом, генераторов с самоконтролем, универсальных программируемых генераторов.

1. Последовательные РСЛОС

Основными достоинствами данного типа генераторов ПСЧ являются:

- простота программной и аппаратной реализации;
- максимальное быстродействие;
- хорошие статистические свойства формируемых последовательностей;
- возможность построения генераторов, обладающих свойством самоконтроля, и др.

Последовательности, формируемые РСЛОС, к сожалению, являются предсказуемыми, поэтому эти генераторы применяются при решении задач защиты компьютерных систем от умышленных деструктивных воздействий лишь в качестве строительных блоков.

Наиболее известные примеры использования РСЛОС и математического аппарата полей Галуа:

- CRC-коды — идеальное средство контроля целостности информации при случайных искажениях информации;
- реализация концепции самотестирования СБИС;
- поточные алгоритмы A5, PANAMA, SOBER, SNOW и др.;
- блочный алгоритм RIJNDAEL, принятый в 2002 г. в качестве Американского стандарта XXI в. – AES.

Исходная информация для построения двоичного РСЛОС – так называемый образующий многочлен. Степень этого многочлена определяет разрядность регистра сдвига, а ненулевые коэффициенты — характер обратных связей.

В общем случае двоичному образующему многочлену степени N

$$\Phi(x)=\sum_{i=0}^{N} a_i x^i,\ a_N=a_0=1,\ a_j=\in\{0,1\},\ j=\overline{1,\ (N\ 1)},$$

соответствуют генераторы Фибоначчи и Галуа, уравнения работы которых имеют вид соответственно (1) и (2):

$$\begin{cases} q_1(t+1) = \sum_{i=1}^{N} a_i q_i(t) \\ q_j(t+1) = q_{j-1}(t), j = \overline{2,\ N} \end{cases}, \quad (1)$$

$$\begin{cases} q_1(t+1) = a_n q_N(t) \\ q_j(t+1) = q_{j-1}(t) \oplus a_{N-i+1} q_N(t), j = \overline{2,\ N} \end{cases}, \quad (2)$$

где $q_i(t)$ — состояние i-го разряда РСЛОС в момент времени t, $i = \overline{1,\ N}$,
или в матричной форме

$$Q(t+1) = T \cdot Q(t), \quad (3)$$

где $Q(t) = \begin{vmatrix} q_1(t) \\ q_2(t) \\ \dots \\ q_N(t) \end{vmatrix}$ — состояние РСЛОС в момент времени t, а T — квадратная матрица порядка N вида (4) для генератора Фибоначчи или (5) для генератора Галуа:

$$\begin{vmatrix} a_1 & a_2 & \dots & a_{N-1} & a_N \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \dots & & \\ 0 & 0 & \dots & 1 & 0 \end{vmatrix}, \quad (4) \qquad \begin{vmatrix} 0 & \dots & 0 & 0 & a_N \\ 1 & \dots & 0 & 0 & a_{N-1} \\ & \dots & & & \\ 0 & \dots & 1 & 0 & a_2 \\ 0 & \dots & 0 & 1 & a_1 \end{vmatrix}. \quad (5)$$

Пример РСЛОС, соответствующего $\Phi(x) = x^7 + x^4 + 1$, показан на рис. 1а.

2. Линейные двоичные параллельные РСЛОС

Рассмотренные последовательные РСЛОС могут использоваться только для генерации битовых последовательностей. Если необходима n-разрядная последовательность, можно предложить два возможных метода решения.

В первом случае выбираем образующий многочлен степени $N > n$ (еще лучше $N >> n$), выбираем схему Фибоначчи или Галуа и считываем очередной n-разрядный элемент псевдослучайной последовательности (ПСП) с соседних разрядов регистра сдвига каждые n тактов работы генератора. Недостатком такого решения является низкое быстродействие. Второй метод предполагает синтез схемы генератора, работающего в n раз быстрее исходного РСЛОС (иначе говоря, выполняющего за один такт своей работы преобразования, которые в исходном РСЛОС выполняются за n тактов). Второй вариант решения более эффективен с точки зрения затрат памяти и быстродействия при программной реализации в случае использования разреженного многочлена (многочлена с относительно небольшим числом ненулевых коэффициентов) $\Phi(x)$, в особенности когда образующий многочлен генератора Фибоначчи имеет вид $\Phi(x) = x^N + x^j + 1$, а i кратно n.

В общем случае уравнение РСЛОС, работающего в n раз быстрее последовательного генератора, логика работы которого описывается уравнением (3), имеет вид:

$Q(t+1) = T^n Q(t)$.

Так как нулевое состояние всех элементов памяти РСЛОС является запрещенным, максимально возможное число состояний устройства, а значит, и максимально возможная длина формируемой двоичной последовательности, снимаемой с выхода любого разряда, равны $2^N - 1$. В этом случае диаграмма состояний генератора состоит из одного тривиального цикла и цикла максимальной длины $2^N - 1$.

Многочлен $\Phi(x)$ степени N называется *примитивным*, если он не делит нацело ни один многочлен вида $x^S - 1$, где $S < 2^N - 1$. Примитивные многочлены существуют для любого N. Показателем многочлена $\Phi(x)$ называется наименьшее натуральное число e, при котором $x^e - 1$ делится на $\Phi(x)$ без остатка.

Пусть $\Phi(x)$ — примитивный многочлен степени N, тогда справедливо следующее утверждение.

Формируемая последовательность имеет максимальный период $S = 2^N - 1$ тогда и только тогда, когда наибольший общий делитель чисел S и n равен 1 (т. е. S и n взаимно просты). При $n = 1$ примитивность $\Phi(x)$ является необходимым и достаточным условием получения последовательности максимальной длины.

Последовательность максимальной длины принято называть М-последователь-ностью, а формирующий ее генератор — генератором М-последовательности. Именно генераторы М-последовательностей обычно используются для формирования ПСП. На рис. 1б показан пример параллельного РСЛОС, соответствующего $\Phi(x) = x^7 + x^4 + 1$, $n = 3$, формирующего 3-разрядную ПСП длиной 127.

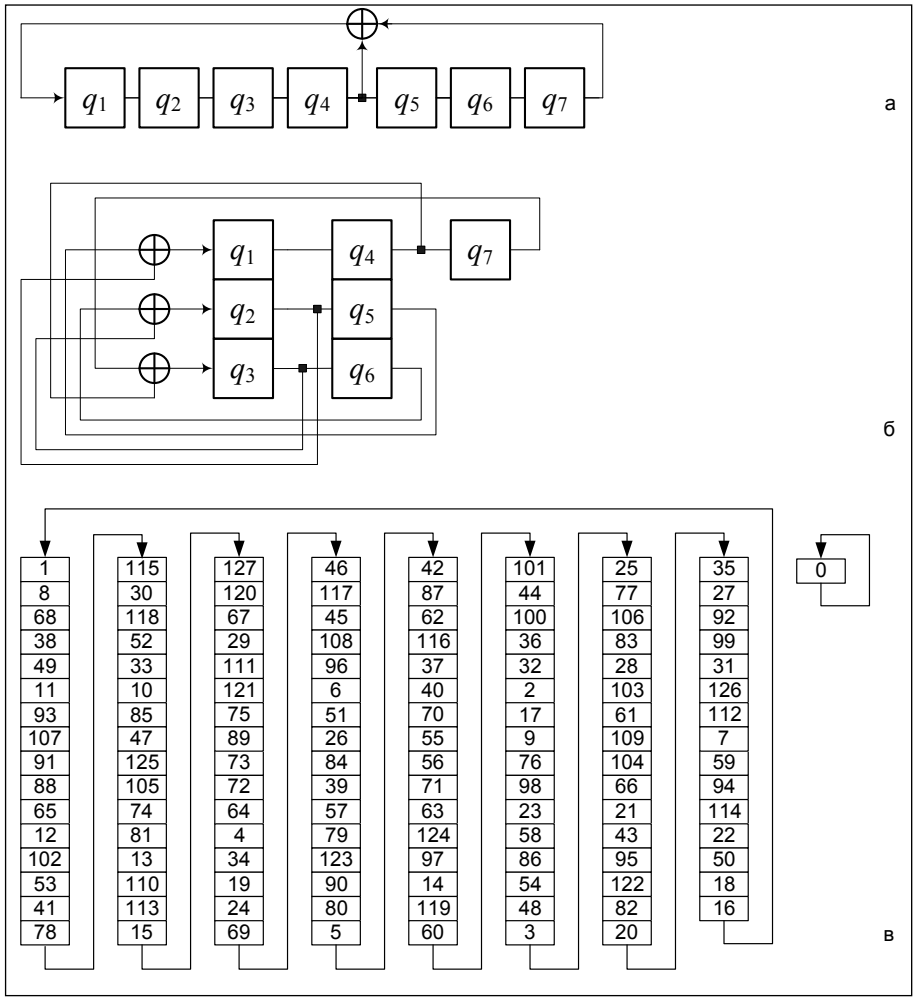

Рис. 1. Линейные генераторы М-последовательностей, соответствующие $\Phi(x) = x^7 + x^4 + 1$: а — последовательный РСЛОС, $n = 1$; б — параллельный РСЛОС, $n = 3$; в — диаграмма переключений для случая $n = 3$

3. Нелинейный генератор М-последовательности

Предлагается в двоичном параллельном РСЛОС заменить n-разрядный элемент XOR на n-разрядный R-блок, в результате при соответствующем выборе таблицы H стохастического преобразования удается получить нелинейный генератор М-последовательности, по своим статистическим свойствам превосходящей линейные М-последовательности, генерируемые РСЛОС.

На рис. 2 показан пример нелинейного генератора М-последовательности длиной 127.

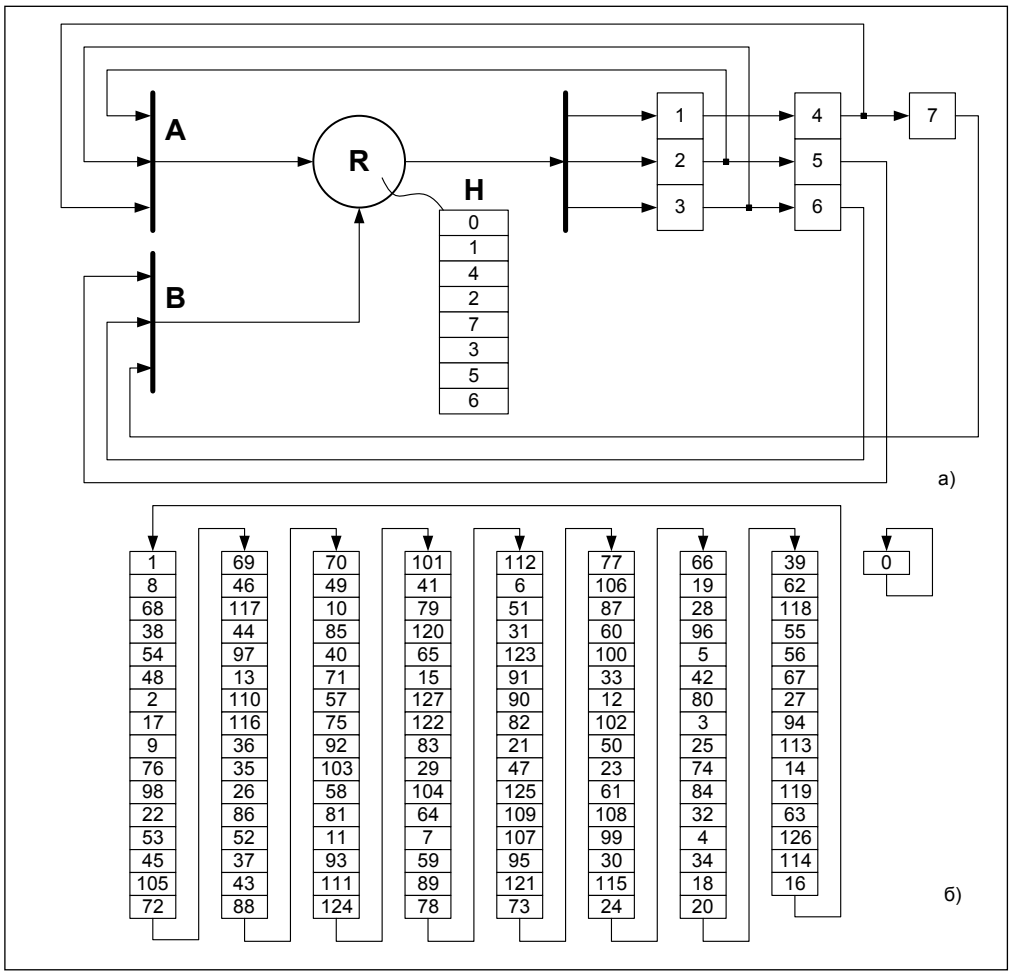

Рис. 2. Нелинейный генератор М-последовательности, соответствующий $\Phi(x) = x^7 + x^4 + 1$ при $n = 3$: а — схема генератора и таблица H стохастического преобразования; б — диаграмма переключений генератора

На рис. 3 изображена схема генератора ПСЧ для случая $\Phi(x) = x^5 + x^3 + 1$ при $n = 2$, а также его диаграммы переключений для всех возможных вариантов заполнения таблицы H стохастического преобразования.

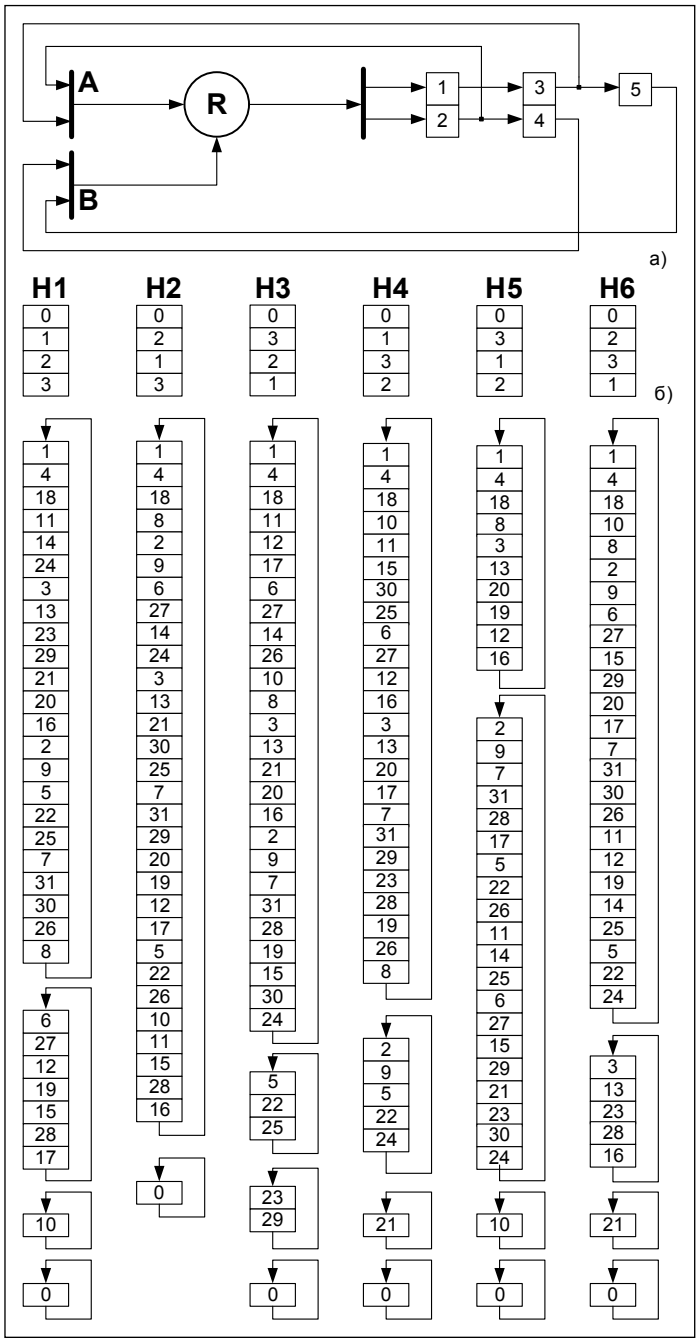

Рис. 3. Генератор ПСЧ для случая $\Phi(x) = x^5 + x^3 + 1$, $n = 2$:
а — схема генератора; б — таблицы H стохастического преобразования и соответствующие им диаграммы переключений

Выводы

В результате предлагаемой замены получается быстродействующий, допускающий эффективную программную и аппаратную реализацию генератор нелинейной последовательности максимальной длины. Достоинством предлагаемого решения является также возможность использования всех схемотехнических приемов получения ПСП длиной 2^N, получения универсальных генераторов ПСЧ с произвольными значениями периода и предпериода (длины нестационарного участка) формируемых последовательностей, работающих в случае РСЛОС [3, 6].

СПИСОК ЛИТЕРАТУРЫ:

1. *Бурдаев О. В., Иванов М. А., Тетерин И. И.* Ассемблер в задачах защиты информации. М.: КУДИЦ-ОБРАЗ, 2004.
2. *Доценко В. И., Фараджев Р. Г.* Анализ и свойства последовательностей максимальной длины // Автоматика и телемеханика. 1969. № 11. С. 119–127.
3. *Иванов М. А., Чугунков И. В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей. (Серия СКБ (специалисту по компьютерной безопасности). Книга 2). М.: КУДИЦ-ОБРАЗ, 2003.
4. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976.
5. *Асосков А. А., Иванов М. А., Тютвин А. Н. и др.* Поточные шифры. (Серия СКБ (специалисту по компьютерной безопасности). Книга 3). М.: КУДИЦ-ОБРАЗ, 2003.
6. *Иванов М. А., Мацук Н. А., Чугунков И. В. и др.* Стохастические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ПРЕСС, 2009.
7. *Алексеев А. И., Шереметьев А. Г., Тузов Г. И., Глазов В. И.* Теория и применение псевдослучайных сигналов. М.: Наука, 1969.
8. *Элспас Б.* Теория автономных линейных последовательных сетей // Кибернетический сборник. 1963. Вып. 7. С. 90–128.