УДК 004.932 **doi: 10.26906/SUNZ.2018.5.111**

А. Н. Рысованый

Национальный технический университет «ХПИ», Харьков, Украина

МЕТОД СИНТЕЗА ПРОВЕРОЧНОЙ МАТРИЦЫ ГЕНЕРАТОРОВ В КОНЕЧНОМ ПОЛЕ GF(3) В ЗАВИСИМОСТИ ОТ ВИДА МАТРИЦЫ СВЯЗЕЙ

Предметом исследования в данной статье является процесс синтеза генераторов нелинейной псевдослучайной последовательности в конечном поле GF(3) в зависимости от вида матрицы связей. **Цель –** разработать метод синтеза генераторов нелинейной псевдослучайной последовательности в конечном поле GF(3), основанный на использовании матрицы связей в качестве основного элемента генерации. **Задача**: на основе анализа известных подходов к генерированию последовательностей разработать метод, который по сравнению с двоичным регистром сдвига позволяет увеличить длину последовательности с учетом матриц связей различных степеней. Используемыми **подходами** являются: применение различных степеней матрицы связей для определения матрицы состояний. Получены следующие **результаты**: метод синтеза генераторов в конечном поле GF(3), основанный на использовании матрицы связей в качестве основного элемента генерации. Приведен математический аппарат описания функционирования регистра сдвига с нелинейными обратными связями и его классическая схема. В работе показаны примеры формирования различных степеней матрицы связей, показана роль свободного члена полинома в формировании проверочной матрицы. **Выводы**. Предложен метод синтеза проверочной матрицы нелинейного регистра сдвига псевдослучайной последовательности в конечном поле GF(3), показаны примеры построения матриц связей в конечном поле тройки.

Ключевые слова: генератор двоичной последовательности, псевдослучайная последовательность, регистр сдвига.

Введение

При реализации криптографических преобразований используют последовательности достаточно большой максимальной длины и различные первичные состояния генератора. При наиболее простом случае начальное состояние определяется свободным членом полинома. В этом случае последовательность разворачивается с учетом этого начального состояния. Стойкость криптографических преобразований напрямую зависит от применяемого алгоритма формирования случайных последовательностей. Но говорить о полностью случайной последовательности возможно только при определенных ограничениях. Как правило – это ограничение на период генерации: чем больше период генерации, тем более вероятно можно судить и о случайной последовательности в рамках этого периода. Наиболее просто случайную последовательность можно получить как часть цикла псевдослучайной последовательности [1-3, 5-7]. Но период такой последовательности должен быть таким, чтобы конечная последовательность разумной длины не была периодической. Относительно небольшие части последовательности должны быть как можно более неотличимы от различных случайных последовательностей. В этом случае, как минимум, необходимо использовать очень длинные последовательности. Но увеличение длины генерируемой последовательности попрежнему является не решенной задачей.

При одной и той же максимальной степени образующего полинома $P(X)$ намного предпочтительнее использовать полиномы, которые применяются в конечных или расширенных полях. Конкретное поле Галуа состоит из конечного диапазона чисел. Порядок поля (или количество его элементов) является натуральной степенью его характеристики p^m. При $m = 1$ такое поле является простым. Наибольший интерес представляет конечное поле Галуа $GF(3)$. Применение полиномов, которые реализуют свои состояния в этом поле позволяет существенно увеличить период генерации последовательности [4, 8].

Получение псевдослучайной последовательности в конечном поле GF(3), основанный на использовании матрицы связей в качестве основного элемента генерации и является **целью статьи**.

Основные проблемы и решения

Основная проблема генераторов псевдослучайных последовательностей – это их короткий период генерации. Увеличить этот период генерации наиболее просто, если применить полиномы в конечном поле. Рассмотрим процесс генерирования псевдослучайной последовательности в конечном поле GF(3). В качестве примера выберем полином, у которого в записи присутствуют коэффициенты 2, например,

$$P(x) = 2x^5 \oplus_3 2x^4 \oplus_3 2x^3 \oplus_3 2x^2 \oplus_3 x \oplus_3 2 .$$

Схема такого регистра сдвига приведена на рис. 1. На схеме не приведены сигналы синхронизации триггеров регистра сдвига. Каждый регистр состоит из двух триггеров, в которых хранится троичный сигнал: 0 кодируется как 00, 1 – как 01, а 2 – как 10. Выходные значения всех аргументов, кроме первого, умножаются на коэффициент 2 в блоках умножения на 2 по mod3. Свободный член полинома на схеме нигде не задействован – он принимает участие в формировании первого (исходного) состояния этого регистра [3, 4, 8].

Выходные состояния такого генератора приведены на рис. 2.

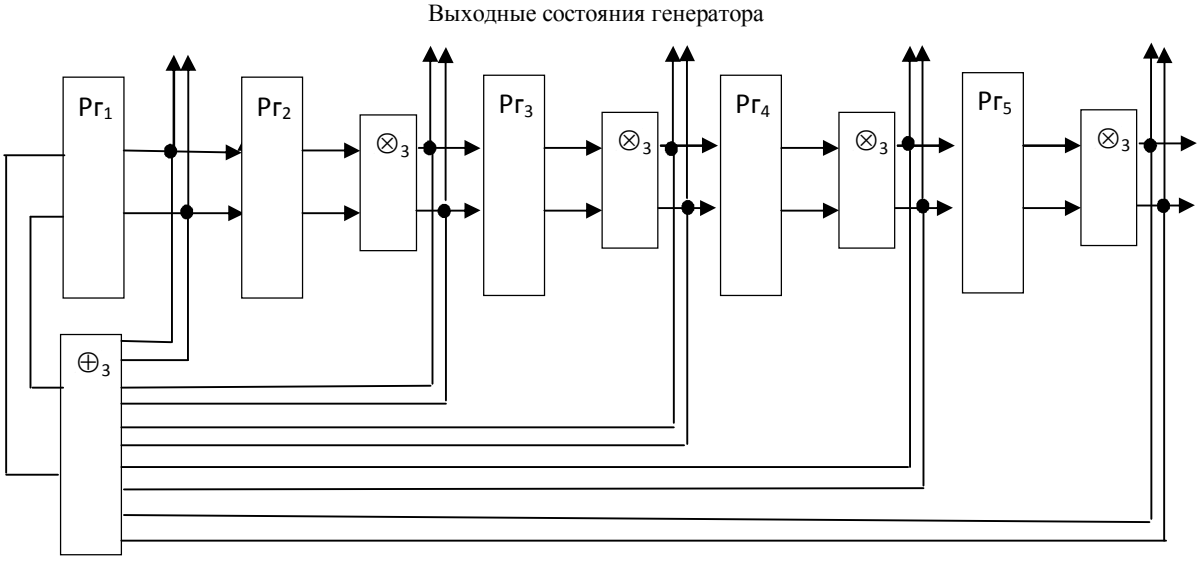

Рис. 1. Функциональная схема генератора псевдослучайных последовательностей с использованием блока сложения по mod3 с $P(x) = 2x^5 \oplus_3 2x^4 \oplus_3 2x^3 \oplus_3 2x^2 \oplus_3 x \oplus_3 2$

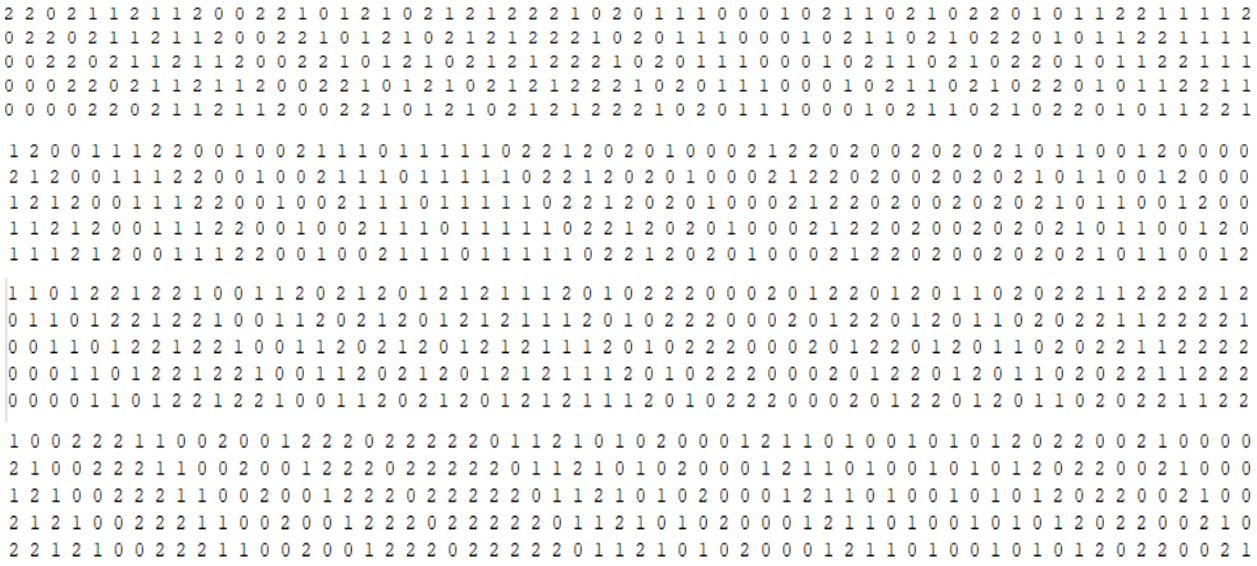

Рис. 2. Матрица состояний для $P(x) = 2x^5 \oplus_3 2x^4 \oplus_3 2x^3 \oplus_3 2x^2 \oplus_3 x \oplus_3 2$

Все классические генераторы псевдослучайных последовательностей в своей основе имеют регистр сдвига с обратными связями. В этом случае на сложность технической реализации не оказывает никакого влияние наличие коэффициентов в записи полиномов.

Значение имеют только количество и вид (в случае нелинейных преобразований) обратных связей. В таком случае изменяется сложность сумматора по модулю поля. Рассматриваемый полином генерирует максимальный период. Это обозначает, что длина генерируемой этим полиномом $P(X)$ последовательности равняется 242. Но не все $P(X)$ с $degP(X) = 5$ генерируют такую длину. Это зависит от свойств полинома: такие $P(X)$ должны быть примитивными и неприводимыми.

При рассмотрении рис. 2 видно:

первое состояние генератора с такого регистра $h_1 = \| a_0 0000 \| = \| 20000 \|$,

второе – $h_2 = \| 22000 \|$,

третье – $h_3 = \| 02200 \|$ и т.д.

Каждое новое состояние определяется по правилу выбранного образующего полинома, в соответствии с которыми и построена схема нелинейного генератора псевдослучайной последовательности. Для случая, когда анализируется максимальная последовательность, в периоде генерирования присутствуют все состояния, кроме нулевого (иначе не будет генерации).

Нелинейными такие генераторы называются потому, что в цепях обратных связей происходят нелинейные преобразования. Явно выраженной нелинейностью являются генераторы с образующим полиномом, у которого присутствует хотя бы один коэффициент 2.

Связи между регистрами описываются изначально образующим полиномом $P(X)$. Однако нагляднее использовать эти связи в виде матрицы:

$$S = \begin{Vmatrix} a_1 & a_2 & a_3 & \dots & a_{r-1} & a_r \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{Vmatrix}$$

где a_i – коэффициенты $P(X)$, $r = degP(X)$ – максимальная степень регистра сдвига.

Рассмотрим связи регистра на примере такой матрицы. Номера строк матрицы S описывают входы регистра, а номера столбцов – выходы такого регистра.

Например, коэффициент a^r располагается в 4-м столбце и первой строке, что свидетельствует о том, что выходы 4-го регистра соединены со входами 1-го регистра через сумматор по *mod*3.

Вторая строка равняется $\|10000\|$. Это свидетельствует о том, что выходы 1-го регистра соединены со входами 2-го и т.д.

Например, матрица связей S для

$$P(x) = 2x^5 \oplus_3 2x^4 \oplus_3 2x^3 \oplus_3 2x^2 \oplus_3 x \oplus_3 2$$

будет иметь вид:

$$\mathrm{S} = \begin{Vmatrix} 1 & 2 & 2 & 2 & 2 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{Vmatrix}.$$

В приведенной матрице отсутствует значение a_0. Но свободный член a_0 описывает первое состояние h_1 уже другой матрицы – матрицы состояний H [3] и всегда равняется:

$$h_1 = \|a_0 0 \dots 0\|,$$

в котором всегда учитывается это значение.

В конечном поле тройки GF(3) умножение на коэффициент 2 можно существенно упростить, если применить перекрестные линии выходов триггеров, что не противоречит последовательному кодированию состояний.

Утверждение. В матрице связей регистра сдвига с обратными связями для любого полинома *P(x)* существует своя закономерность размещения столбцов и на основании этой закономерности могут быть получены все остальные выходные состояния.

Доказательство. В связи с тем, что матрица связей размером ($r \times r$) определяется только видом полинома *P(x)*, то любой ее *i*-й столбец соответствует какому-нибудь столбцу матрицы состояний, т.к. число состояний конечно. Причем, т.к. каждый последующий столбец получен путем сдвига предыдущего состояния по правилу выбранного полинома, то в матрице связей всегда должен быть хотя бы другой столбец, полученный от предыдущего.

Рассмотрим полиномы с $degP(X) = 4$, которые генерируют максимальный период. Будем записывать только коэффициенты при аргументах. Например, для *P(x)* с коэффициентами 11221 матрица связей S^1 имеет вид:

$$S^1 = \begin{Vmatrix} 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{Vmatrix} = \|h_2 h_{68} h_{66} h_1\|.$$

$$S^2 = S^1 \times S^1 =$$

$$= \begin{Vmatrix} 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{Vmatrix} \times \begin{Vmatrix} 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 2 & 0 & 2 \\ 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{Vmatrix} =$$

$$= \|h_3 h_{69} h_{67} h_2\|,$$

$$S^3 = S^1 \times S^2 =$$

$$= \begin{Vmatrix} 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{Vmatrix} \times \begin{Vmatrix} 0 & 2 & 0 & 2 \\ 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \\ 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{Vmatrix} =$$

$$= \|h_4 h_{70} h_{68} h_3\|,$$

$$S^4 = S^2 \times S^2 =$$

$$= \begin{Vmatrix} 0 & 2 & 0 & 2 \\ 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{Vmatrix} \times \begin{Vmatrix} 0 & 2 & 0 & 2 \\ 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 2 & 2 \\ 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \\ 2 & 2 & 1 & 1 \end{Vmatrix} =$$

$$= \|h_5 h_{71} h_{69} h_4\|,$$

$$S^5 = S^3 \times S^2 =$$

$$= \begin{Vmatrix} 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \\ 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{Vmatrix} \times \begin{Vmatrix} 0 & 2 & 0 & 2 \\ 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 2 & 1 & 0 & 1 \\ 1 & 0 & 2 & 2 \\ 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \end{Vmatrix} =$$

$$= \|h_6 h_{71} h_{69} h_5\|$$

и т.д.

Т.о. для $P(x) = 11221$ матрица связей в общем случае имеет вид:

$$S^1 = \|h_{i+1} h_{i+67} h_{i+65} h_i\|.$$

Для $P(X) \in \deg P(X) = 4$ с $T_{max} = 3^{\deg P(x)} - 1 = 80$ насчитывается всего16 полиномов, у которых матрицы связей первой степени имеют виды:

$P(X) = 10011$, $S = \|h_2 h_{79} h_{80} h_1\|$;

$P(X) = 10021$, $S = \|h_2 h_{79} h_{80} h_1\|$;

$P(X) = 11001$, $S = \|h_2 h_3 h_4 h_1\|$;

$P(X) = 11121$, $S = \|h_2 h_7 h_{15} h_1\|$;

$P(X) = 11221$, $S = \|h_2 h_{68} h_{66} h_1\|$;

$P(X) = 12001$, $S = \|h_2 h_3 h_4 h_1\|$;

$P(X) = 12111$, $S = \|h_2 h_{17} h_{55} h_1\|$;

$P(X) = 12211$, $S = \| h_2 h_{38} h_{66} h_1 \|$;
$P(X) = 10012$, $S = \| h_{42} h_{39} h_{40} h_{41} \|$;
$P(X) = 10022$, $S = \| h_{42} h_{39} h_{40} h_{41} \|$;
$P(X) = 11002$, $S = \| h_{42} h_{43} h_{44} h_{41} \|$;
$P(X) = 11122$, $S = \| h_{42} h_{57} h_{55} h_{41} \|$;
$P(X) = 11222$, $S = \| h_{42} h_{38} h_{36} h_{41} \|$;
$P(X) = 12002$, $S = \| h_{42} h_{43} h_{44} h_{41} \|$;
$P(X) = 12112$, $S = \| h_{42} h_{57} h_{15} h_{41} \|$;
$P(X) = 12212$, $S = \| h_{42} h_{68} h_{26} h_{41} \|$.

Выводы

Предложен метод определения проверочной матрицы в зависимости от вида матрицы связей, которая, в свою очередь, формируется в зависимости от вида используемого образующего полинома из выбранного конечного поля Галуа GF(3).

Для каждого полинома существует своя закономерность формирования матрицы связей из столбцов матрицы состояний, что позволяет определить все матрицы связей различных степеней без предварительных расчетов.

СПИСОК ЛІТЕРАТУРИ

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.
2. Муттер В.М. Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат, 1990. – 288 с .
3. Рысованый А.Н., Гоготов В.В. Выбор полиномов для нелинейных регистров сдвига с обратными связями по критерию формирования последовательности максимальной длины // Системы управления, навигации и связи. – Киев : Центральный научно-исследовательский институт навигации и управления, 2007. – Вып.1.– С. 77 – 79.
4. Рысованый А.Н. Метод генерирования нелинейной псевдослучайной последовательности без использования обратных связей/ А.Н. Рысованый // Системи управління, навігації та зв'язку. – Полтава : ПНТУ, 2018. – №4(50).– С. 144-146.
5. Литиков И.П. Кольцевое тестирование цифровых устройств. – М.: Энергоатомиздат, 1990. – 160 с.: ил.
6. Горяшко А.П. Синтез диагностируемых схем вычислительных устройств. – М.: Наука. – 1987. – 288 с.
7. Ватолин Д., Ракушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ-МИФИ. – 2002. – 384 с.
8. Сорока Л.С., Рысованый А.Н., Мороз Б.И. Способ получения псевдослучайной последовательности на основе использования матрицы связей в конечном поле GF(3) // Патент Украины № u201109344. 2012. Бюл. № 5.

Рецензент: д-р техн. наук, проф. О. В. Козелков,
Державний університет телекомунікацій, Київ
Received (Надійшла) 28.08.2018
Accepted for publication (Прийнята до друку) 29.09.2018

Метод синтезу перевірочної матриці генераторів в кінцевому полі GF (3) в залежності від виду матриці зв'язків

О. М. Рисований

Предметом дослідження в даній статті є процес синтезу генераторів нелінійної псевдовипадкової послі-довності в кінцевому полі GF (3) в залежності від виду матриці зв'язків. **Мета** - розробити метод синтезу ге-нераторов нелінійної псевдовипадкової послідовності в кінцевому полі GF (3), заснований на використанні матриці зв'язків в якості основного елемента генерації. **Завдання**: на основі аналізу відомих підходів до генерування послідовностей розробити метод, який в порівнянні з двійковим регістром зсуву дозволяє збільшити довжину послідовності з урахуванням матриць зв'язків різних ступенів. Використовуваними підходами є: застосування різних ступенів матриці зв'язків для визначення матриці станів. Отримані наступні **результати**: метод синтезу генераторів в кінцевому полі GF (3), заснований на використанні матриці зв'язків в якості основ-ного елемента генерації. Наведено математичний апарат опису функціонування регістра зсуву з нелінійної зворотними зв'язками і його класична схема. У роботі показані приклади формування різних ступенів матриці зв'язків, показане місце вільного члена полінома в формуванні перевірочної матриці. **Висновки**. Запропоновано метод синтезу перевірочної матриці нелінійного регістра зсуву псевдовипадкової послідовності в кінцевому полі GF (3), показані приклади побудови матриць зв'язків в кінцевому полі трійки.

Ключові слова: генератор двійковій послідовності, псевдовипадкова послідовність, регістр зсуву.

The method of synthesis of the checking matrix of generators in a finite field GF (3) depending on the type of matrix of relations

A. Rysovaniy

The subject of research in this article is the process of synthesis of nonlinear pseudo-random sequence generators in the finite field GF (3), depending on the type of coupling matrix. The goal is to develop a method for synthesizing generators of a nonlinear pseudo-random sequence in a finite field GF (3), based on the use of a bond matrix as the main element of generation. **Task**: based on the analysis of known approaches to the generation of sequences, develop a method that, as compared with the binary shift register, allows to increase the length of a sequence taking into account coupling matrices of various degrees. The approaches used are: the use of different degrees of the bond matrix to determine the state matrix. The following results were obtained: method of synthesis of generators in the final field GF (3), based on the use of a matrix of bonds as the main element of generation. The mathematical apparatus for describing the operation of a shift register with nonlinear feedbacks and its classical scheme are given. The paper shows examples of the formation of various degrees of the matrix of relations, shows the role of the free member of a polynomial in the formation of a test matrix. **Findings**. A method for synthesizing a checking matrix of a nonlinear shift register of a pseudo-random sequence in a finite field GF (3) is proposed, examples of constructing a matrix of links in the finite field of a triple are shown.

Keywords: binary sequence generator, pseudo-random sequence, shift register.