УДК 681.324 : 621.396

А. Н. Рысованый, кандидат технических наук, доцент кафедры вычислительной техники
и программирования Национального технического университета "Харьковский политехнический институт"

СПОСОБ ПОЛУЧЕНИЯ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ МАТРИЦЫ СВЯЗЕЙ В КОНЕЧНОМ ПОЛЕ GF(3)

Розглядається спосіб отримання псевдовипадкової послідовності в кінцевому полі GF(3), що грунтується на використанні матриці зв'язків як основного елементу генерації.

Рассматривается способ получения псевдослучайной последовательности в конечном поле GF(3), основанный на использовании матрицы связей в качестве основного элемента генерации.

The way of obtaining a pseudorandom sequence in a finite field GF (3), based on the use of matrix relations as a key element of generation.

Ключевые слова. Псевдослучайная последовательность, регистр сдвига.

Введение. Одной из приоритетных задач развития информационных систем таможенной службы Украины является задача создания высоконадежных защищенных систем. А в решении задач диагностирования цифровых объектов таких систем одно из значительных мест отводится генераторам псевдослучайных последовательностей (ПСП), от качества которых зависит глубина тестов. Например, при диагностировании шинных формирователей, контроллеров шин, микросхем памяти становится неэффективным псевдослучайный тест с линейного регистра сдвига с обратными связями, так как эти схемы имеют три состояния (0, 1 и R – высокий импеданс). Кроме того, для диагностирования линий передачи данных, по которым передаются двуполярные сигналы (V_+, V_-, V_0) предпочтительнее использовать устройства, предназначенные именно для решения таких задач. В этих случаях третьи состояния не диагностируются. Регистры сдвига с нелинейными обратными связями являются основой кодеров. В работе [*1,* 61] сказано, что: "… в настоящее время мы располагаем весьма скудной информацией о построении нелинейных кодеров". Перекликается с этим высказыванием и работа [*2,* 3]: "… разрыв между практикой и математической теорией недвоичного помехоустойчивого кодирования не сокращается или сокращается недостаточно быстрыми темпами".

Постановка задачи. Разработка математического описания функционирования регистров сдвига с нелинейными обратными связями в конечном поле GF(3) и способа получения ПСП на основе использования матрицы связей.

Результаты исследования. Для генерирования ПСП в поле GF(3) применяется регистр сдвига с нелинейными обратными связями, которые определяются в виде полинома:

$$P(x) = a_n x^n \oplus_3 a_{n-1} x^{n-1} \oplus_3 \ldots \oplus_3 a_0,$$

где $a_n, a_{n-1} \ldots a_0$ – коэффициенты при аргументах; $a_{i/i=1-n-1} \in \{0, 1, 2\}$; $a_0, a_n \in \{1, 2\}$.

Правила сложения и умножения в конечном поле GF(3) = {0, 1, 2} имеют следующий вид:

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Матрица связей [3–5] определяет связи между разрядами регистра сдвига и изменяется в зависимости от выбранного образующего полинома $P(x)$. В общем случае матрица связей S имеет вид:

$$S = \begin{vmatrix} a_1\ a_2\ \ldots\ a_{r-1}\ a_r \\ 1\ 0\ \ldots\ 0\ 0 \\ 0\ 1\ 0\ \ldots\ 0\ 0 \\ \ldots \\ 0\ 0\ \ldots 1\ 0 \end{vmatrix}.$$

Например, для $P(x) = x^4 \oplus_3 x^3 \oplus_3 1$ матрица связей S имеет вид:

$$S^1 = \begin{vmatrix} 0\,0\,1\,1 \\ 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \end{vmatrix}.$$

Функциональная схема классического нелинейного генератора ПСП с полиномом $P(x) = x^4 \oplus_3 x^3 \oplus_3 1$ приведена на рис. 1.

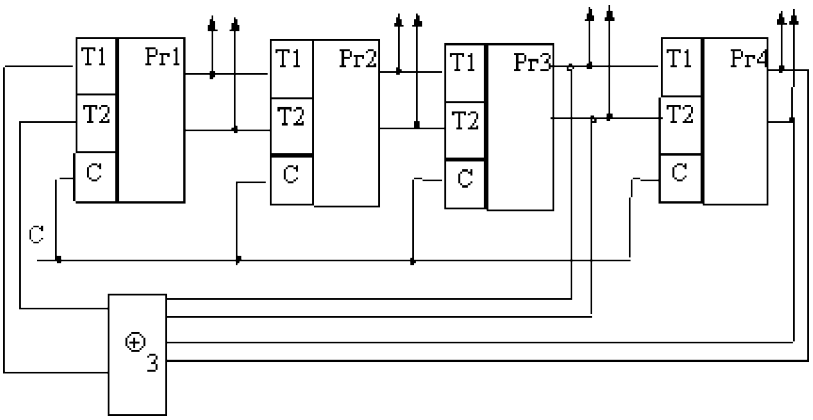

Рис. 1. Функциональная схема НСА с $P(x) = x^4 \oplus_3 x^3 \oplus_3 1$

При подаче на вход регистра с образующим полиномом $P(x) = x^4 \oplus_3 x^3 \oplus_3 1$ логической 1 и последующих сдвигах получится матрица состояний *H:*

1	0	0	1	1	0	1	2	1	1	0	0	2	1	0	2	0	1	2	2
0	1	0	0	1	1	0	1	2	1	1	0	0	2	1	0	2	0	1	2
0	0	1	0	0	1	1	0	1	2	1	1	0	0	2	1	0	2	0	1
0	0	0	1	0	0	1	1	0	1	2	1	1	0	0	2	1	0	2	0
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

1	0	1	0	1	1	1	1	2	2	2	0	1	1	2	1	2	0	0	0
2	1	0	1	0	1	1	1	1	2	2	2	0	1	1	2	1	2	0	0
2	2	1	0	1	0	1	1	1	1	2	2	2	0	1	1	2	1	2	0
1	2	2	1	0	1	0	1	1	1	1	2	2	2	0	1	1	2	1	2
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40

2	0	2	0	2	2	2	2	1	1	1	0	2	2	1	2	1	0	0	0
1	2	0	2	0	2	2	2	2	1	1	1	0	2	2	1	2	1	0	0
1	1	2	0	2	0	2	2	2	2	1	1	1	0	2	2	1	2	1	0
2	1	1	2	0	2	0	2	2	2	2	1	1	1	0	2	2	1	2	1
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80

2	0	0	2	2	0	2	1	2	2	0	0	1	2	0	1	0	2	1	1
0	2	0	0	2	2	0	2	1	2	2	0	0	1	2	0	1	0	2	1
0	0	2	0	0	2	2	0	2	1	2	2	0	0	1	2	0	1	0	2
0	0	0	2	0	0	2	2	0	2	1	2	2	0	0	1	2	0	1	0
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60

Свободный член a_0 образующего характеристического полинома $P(x) = a_r x^r \oplus_3 a_{r-1} x^{r-1} \oplus_3 \ldots \oplus_3 ax \oplus_3 a_0$ однозначно описывает первое состояние h_1 матрицы состояний H [6] и равняется: $h_1 = \|a_0 0 \ldots 0\|$. Например, для $P_1(x) = 2x^4 \oplus_3 2x^3 \oplus_3 1$ первое состояние $h_1 = = \|1000\|$, а для $P_2(x) = x^4 \oplus_3 x^3 \oplus_3 2$ первое состояние $h_1 = \|2000\|$.

Каждый столбец матрицы связей S представляет собой один из столбцов матрицы состояний H регистра ПСП.

Для каждого полинома с максимальным периодом генерации [7] есть своя закономерность кольцевого расположения столбцов матриц связи. Например, для $P(x) = x^4 \oplus_3 x^3 \oplus_3 1$ расположение элементов будет таким:

$$S^1 = \begin{vmatrix} 0\,0\,1\,1 \\ 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \end{vmatrix} = ?\ h_2 h_3 h_4 h_1 ?\ ;$$

$$S^2 = \begin{vmatrix} 0\,1\,1\,0 \\ 0\,0\,1\,1 \\ 1\,0\,0\,0 \\ 0\,1\,0\,0 \end{vmatrix} = ?\ h_3 h_4 h_5 h_2 ?\ ;$$

$$S^3 = \begin{vmatrix} 1\,1\,0\,0 \\ 0\,1\,1\,0 \\ 0\,0\,1\,1 \\ 1\,0\,0\,0 \end{vmatrix} = ?\ h_4 h_5 h_6 h_3 ?\ \text{и т. д.}$$

Следовательно, обобщенная формула расчетов степеней матрицы связей для $P(x) = x^4 \oplus_3 x^3 \oplus_3 1$ имеет вид:

$$S^i = \| h_{i+1}\ \ h_{i+2}\ \ h_{i+3}\ \ h_i \|.$$

Для полинома $P(x) = x^4 \oplus_3 x \oplus_3 1$ усеченная матрица состояний H(1-16) имеет вид:

$Рг_1$	1	1	1	1	2	0	1	2	1	1	2	1	2	0	2	0
$Рг_2$	0	1	1	1	1	2	0	1	2	1	1	2	1	2	0	2
$Рг_3$	0	0	1	1	1	1	2	0	1	2	1	1	2	1	2	0
$Рг_4$	0	0	0	1	1	1	1	2	0	1	2	1	1	2	1	2
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Для этого полинома расположения элементов будет таким:

$$S^1 = \begin{vmatrix} 1\,0\,0\,1 \\ 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \end{vmatrix} = ?\ h_2 h_{79} h_{80} h_1 ?\ ;$$

$$S^2 = \begin{vmatrix} 1\,0\,1\,1 \\ 1\,0\,0\,1 \\ 1\,0\,0\,0 \\ 0\,1\,0\,0 \end{vmatrix} = ?\ h_3 h_{80} h_1 h_2 ?\ ;$$

$$S^3 = \begin{vmatrix} 1\,1\,1\,1 \\ 1\,0\,1\,1 \\ 1\,0\,1\,1 \\ 1\,0\,0\,0 \end{vmatrix} = ?\ h_4 h_1 h_2 h_3 ?\ \text{и т. д.}$$

Следовательно, обобщенная формула расчетов степеней матрицы связей для $P(x) = x^4 \oplus_3 x \oplus_3 1$ имеет вид:

$$S^i = \| h_{i+1} \;\; h_{i-2} \;\; h_{i-1} \;\; h_i \|$$

Таким образом, для каждого полинома есть своя закономерность размещения столбцов проверочной матрицы H в матрице связей S^i, которые можно использовать для генерирования ПСП. Причем для приведенных примеров все столбцы матрицы состояний получаются из столбца, который располагается последним. То есть эти столбцы получаются путем соответствующего сдвига последнего столбца в регистре сдвига с обратными связями.

Полученные обобщенные формулы позволяют найти все другие столбцы на основе известного одного путем его сдвига.

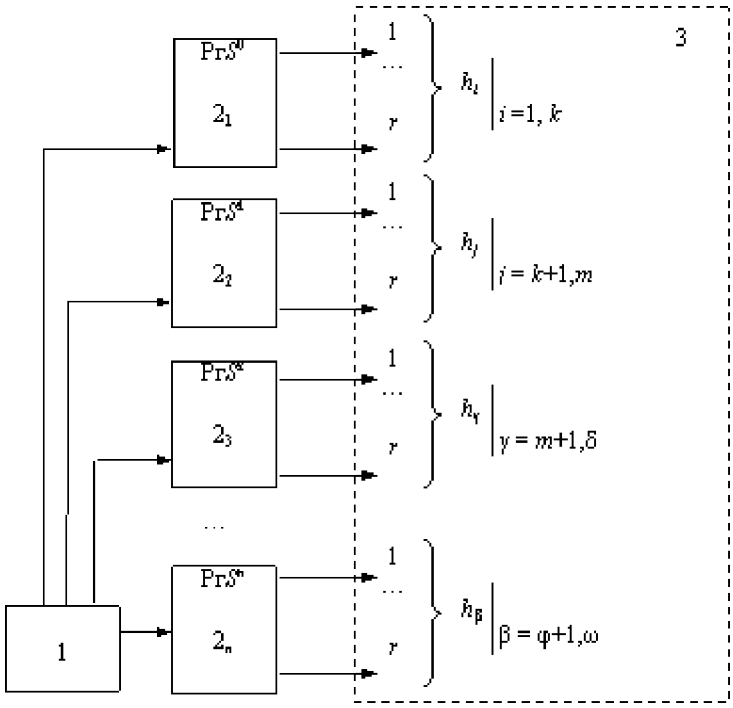

Рис. 1. Схема устройства генерирования ПСП

Способ, который предлагается [3], может быть реализован, например, с помощью устройства, структурная схема которого в общем виде приведена на рис. 2. Устройство включает: блок 1 управление выдачей ПСП; группу из n блоков регистров $2_1 - 2_n$ хранения матриц связей разных степеней и группу 3 r- разрядных выходных состояний.

Устройство работает следующим образом. В регистры блоков $2_1 - 2_n$ занесены матрицы связей соответствующих степеней, каждый столбец которой является одним из состояний матрицы H. Блок управления 1 последовательно, за избранным для каждого полинома алгоритмом подает сигналы считывания. В результате чего r-разрядные состояния через блок 3 передаются на выход схемы. Каждый блок 2_i выдает свои состояния, которые не должны быть повторены, чтобы не нарушить последовательность генерирования ПСП. Блок управления 1 обеспечивает выдачу соответствующих к избранному алгоритму данных. Причем начинать выдавать r-разрядные данные можно из какого угодно состояния.

Выводы. Предложеный способ, представленный в виде полученного выражения, позволяет определить все столбцы матрицы состояний H без выполнения подсчетов и быть применимым для определения ПСП с использованием примитивного неприведенного характеристического полинома. В предложенном способе отсутствуют обратные связи, как у классического регистра сдвига, поэтому могут генерироваться ПСП для любого выбранного полинома, который удовлетворяет условие получения максимального периода генерации.

Литература

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Блейхут Р. ; пер. с англ. – М. : Мир, 1986. – 576 с.

2. Муттер В. М. Основы помехоустойчивой телепередачи информации / Муттер В. М. – Л. : Энергоатомиздат, 1990. – 288 с.

3. Патент України на корисну модель № 67874 № u201109344 ; заяв. 26.07.2011 ; опубл. 12.03.2012. – Бюл. № 5/2012. – 4 с. (Спосіб отримання псевдовипадкової послідовності на основі використання матриці зв’язків в

кінцевому полі GF(3). G06F 7/00).

4. Патент України на корисну модель № 67039 № u201109374 ; заяв. 26.07.2011 ; опубл. 25.01.2012. – Бюл. № 2/2012. – 10 с. (Генератор двійкової псевдовипадкової послідовності на основі використання матриці зв'язків першого ступеня. G06F 7/00).

5. Патент України на корисну модель № 67880 № u201109369 ; заяв. 26.07.2011 ; опубл. 12.03.2012. – Бюл. № 5/2012. – 3 с. (Генератор псевдовипадкової послідовності на основі використання матриці зв'язків першого ступеня в кінцевому полі GF(3). G06F 7/58 (2006.01).

6. Патент України на корисну модель № 67872 № u201109342 ; заяв. 26.07.2011 ; опубл. 12.03.2012. – Бюл. № 5/2012. – 2 с. (Генератор псевдовипадкової послідовності на основі використання першого стовпця матриці станів в кінцевому полі GF(3). G06F 7/00).

7. Рысованый А. Н. Выбор полиномов для нелинейных регистров сдвига с обратными связями по критерию формирования последовательности максимальной длины / А. Н. Рысованый, В. В. Гоготов // Системи управління, навігації та зв'язку. – К. : Центральний науково-дослідний інститут навігації і управління, 2007. – Вип. 1. – С. 77–79.