МЕТОДИЧЕСКАЯ РАЗРАБОТКА
для проведения лекции

Занятие № 2: «Линейные регистры сдвига»

Учебные вопросы занятия:
1. Принципы построения линейных регистров сдвига
2. Свойства выходных последовательностей линейных регистров сдвига
Заключительная часть

Введение

Широкое применение для передачи, приема и хранения информации в настоящее время имеют цифровые методы обработки сигналов. Их реализация осуществляется с помощью различных технических устройств: универсальных или многофункциональных. На базе регистров сдвига можно реализовать множество функциональных зависимостей, в той или иной степени используемых при цифровой обработке сигналов.

Регистром сдвига (англ. *Shift Register*) длины n над множеством X с функцией обратной связи f называется конечный автономный автомат с множеством состояний X^n. Находясь в состоянии $(x_1,...,x_n)$ регистр сдвига вырабатывает выходной символ x_1 и переходит в состояние $(x_2,...,x_n, f(x_1,...,x_n))$.

Если функция обратной связи $f(x_1,...,x_n)$ линейна, то регистр сдвига называется *линейным*, иначе – *нелинейным*.

Роль регистров сдвига возрастает при реализации различных компонентов криптографических систем (например, комбинирующих и фильтрующих криптогенераторов).

В данной лекции будут рассмотрены принципы построения линейных регистров сдвига (ЛРС), математический аппарат их анализа и синтеза, а также наиболее важные их криптографические свойства.

Учебные вопросы:

Вопрос 1. Принципы построения линейных регистров сдвига.

Линейным регистром сдвига (ЛРС) называется регистр сдвига с линейной обратной связью, т. е. у которого входной бит является линейной булевой функцией от значений остальных битов регистра до сдвига. В качестве линейной булевой функции в таких регистрах применяется сложение

по модулю 2. Другие названия ЛРС, встречаемые в литературе, – рекуррентная линия задержки (РЛЗ), одноканальная линия задержки (ОЛЗ) с обратной связью, саморазвертка, англ. *Linear Feedback Shift Register* (*LFSR*).

В общем виде ЛРС может быть представлен в виде схемы Фибоначчи, представленной на рисунке 1.1. Согласно данной схеме, $a_i \in \{0,1\}$ – элемент памяти регистра сдвига, $h_i \in \{0,1\}$ – обратная связь с *i*-й ячейки (если обратная связь с *i*-й ячейки присутствует, то $h_i = 1$, в противном случае $h_i = 0$).

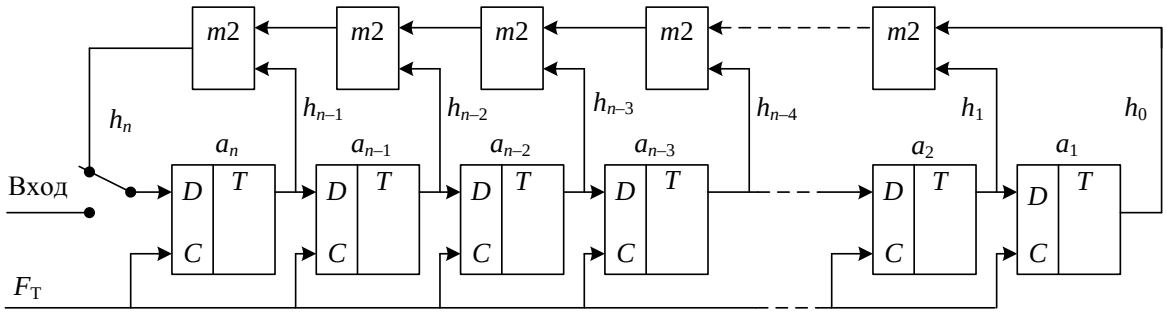


Рис. 1.1. Общая схема линейного регистра сдвига

Число элементов памяти ЛРС определяет его длину *n*. Первоначально в ячейки памяти вводится двоичная последовательность, определяющая начальное заполнение $A_1, A_2, ..., A_n$. После этого замыкается обратная связь. При поступлении тактовых импульсов содержимое ячеек памяти сдвигается вправо, а в первую ячейку записывается результат сложения по модулю 2 содержимого ячеек, имеющих отводы. Одновременно с этим с крайней правой ячейки считывается первый элемент входной последовательности.

При поступлении следующих тактовых импульсов работа ЛРС происходит аналогичным образом. ЛРС формирует неограниченную двоичную последовательность, которая может быть описана следующими соотношениями:

$$B_i = A_i, \text{ где } i = 1, 2, ..., n; \qquad (1.1)$$

$$B_i = \sum_{k=1}^{n} h_{n-k} \cdot B_{i-k}, \text{ где } i = n + 1, n + 2.$$

Анализ соотношений показывает, что символы выходной последовательности B_i, начиная с *n*-го такта, полностью определяются своими предыдущими значениями, поэтому соотношение (1.1) называется *рекуррентным.*

Выходная последовательность ЛРС может сниматься с любого разряда регистра. В последовательности состояний ЛРС отсутствует комбинация, состоящая из всех нулей («000…0»). Такая комбинация является запрещенной, так как при ее записи в качестве начального заполнения регистр будет генерировать одни нули.

При анализе и синтезе ЛРС используют описание их с помощью многочленов. Каждому ЛРС длины *n* можно сопоставить полином обратных связей вида $h(x) = h_n \cdot x^n + h_{n-1} \cdot x^{n-1} + h_{n-2} \cdot x^{n-2} + ... + h_1 \cdot x^1 + h_0 \cdot x^0 = \sum_{i=0}^{n} h_i \cdot x^i$,

причем всегда $h_n = h_0 = 1$.

На рисунке 1.2 приведены примеры схем ЛРС и таблицы изменения состояния их ячеек для многочленов вида:

$$h_3(x) = x^3 + x + 1; \qquad h_4(x) = x^4 + x + 1.$$

Свойства характеристического многочлена во многом определяют свойства выходных последовательностей ЛРС. Они изучаются в алгебре, теории чисел и теории конечных полей Галуа.

Полином $h(x)$ имеет двойственный многочлен $h'(x)$. Взаимосвязь с двойственным полиномом выражается соотношением

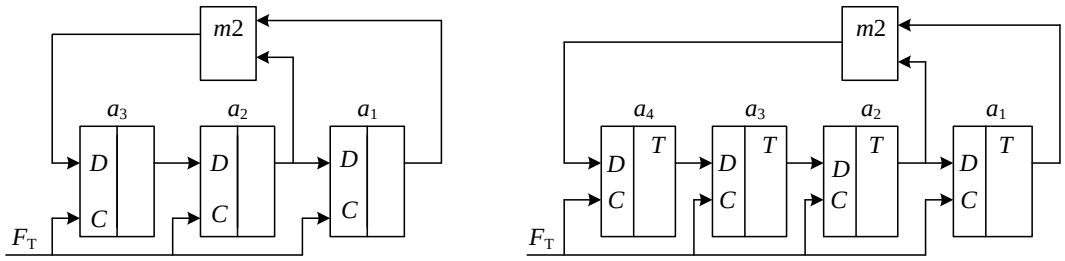
$$h'(x) = x^n \cdot h\left(\frac{1}{x}\right).$$

Например,

$h_3(x) = x^3 + x + 1 \quad \rightarrow \qquad h'_3(x) = x^3 + x^2 + 1;$

$h_4(x) = x^4 + x + 1 \quad \rightarrow \qquad h'_4(x) = x^4(1/x^4 + 1/x + 1) = x^4 + x^3 + 1.$

Полиномы $h(x)$ и $h'(x)$ обладают идентичными свойствами. Однако у двойственного полинома нумерация разрядов ведется слева направо.



а

Номер такта	Состояние ячеек		
	a_3	a_2	a_1
1	0	0	1
2	1	0	0
3	0	1	0
4	1	0	1
5	1	1	0
6	1	1	1
7	0	1	1

б

Номер такта	Состояние ячеек			
	a_4	a_3	a_2	a_1
1	0	0	0	1
2	1	0	0	0
3	0	1	0	0
4	0	0	1	0
5	1	0	0	1
6	1	1	0	0
7	0	1	1	0
8	1	0	1	1
9	0	1	0	1
10	1	0	1	0
11	1	1	0	1
12	1	1	1	0
13	1	1	1	1
14	0	1	1	1
15	0	0	1	1

Рис. 1.2. Примеры схем ЛРС (*а*) и таблицы изменения состояния их ячеек (*б*)

Например, двойственному полиному $h'_4(x) = x^4 + x^3 + 1$ соответствует схема, приведенная на рисунке 1.3.

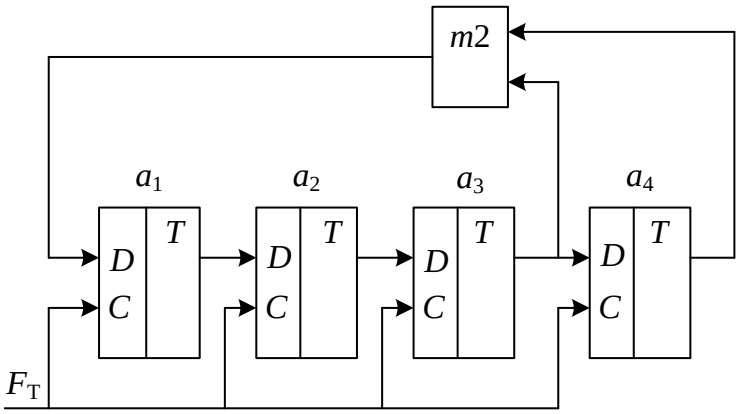


Рис. 1.3. Схема ЛРС, соответствующая полиному $h'(x) = x^4 + x^3 + 1$

Полиному же $h'_5(x) = x^5 + x^3 + x^2 + x + 1$ соответствует схема, приведенная на рисунке 1.4.

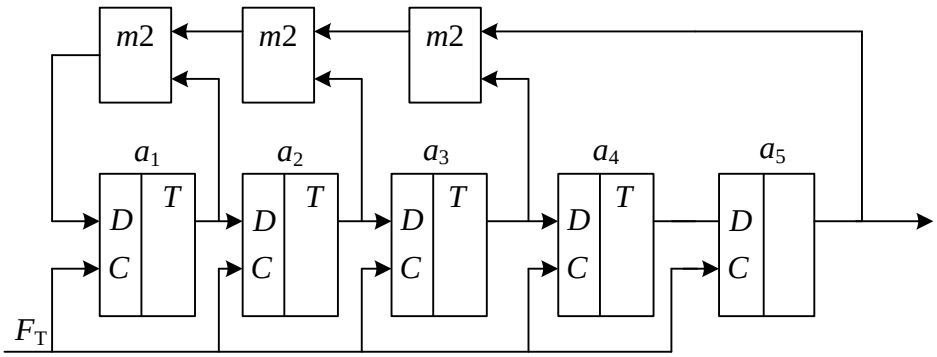


Рис. 1.4. Схема ЛРС, соответствующая полиному $h'(x) = x^5 + x^3 + x^2 + x + 1$

На основании свойства коммутативности функции неравнозначности следует, что соединение схем сложения по модулю 2 в цепи обратной связи ЛРС может быть любым. Поэтому схема, изображенная на рисунке 1.5, будет эквивалентна приведенной выше схеме на рисунке 1.4, т. е. обе эти схемы будут формировать одинаковые последовательности.

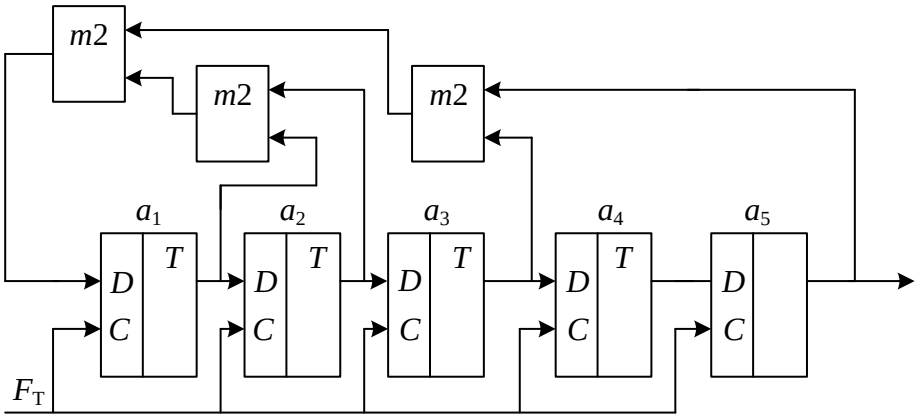
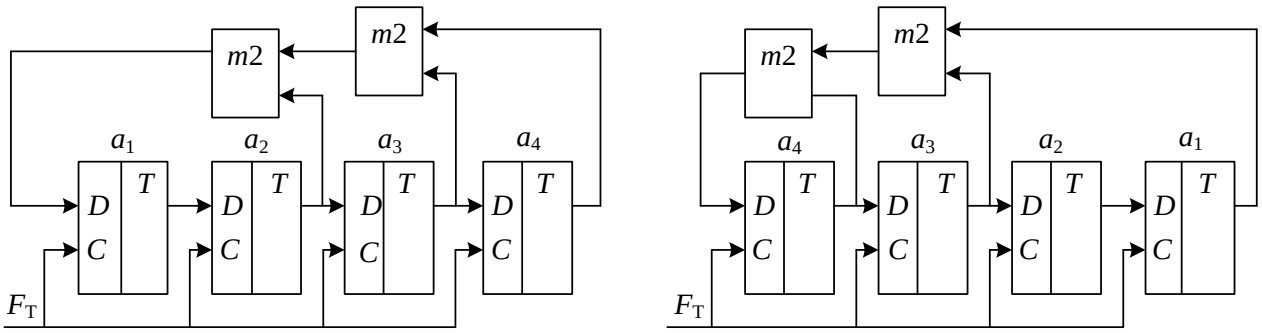


Рис. 1.5. Эквивалентная схема ЛРС для полинома $h'(x) = x^5 + x^4 + x^3 + x^2 + 1$

При построении схем ЛРС по характеристическому полиному $h(x)$ иногда пользуются тем же правилом, что и для $h'(x)$. Некорректность данного приема проявляется лишь тогда, когда важна конфигурация выходной последовательности, например при помехоустойчивом кодировании. Поэтому, когда задан полином:

$$h(x) = x^4 + x^3 + x^2 + 1,$$

описывающий кодер помехоустойчивого циклического кода $(7, 4)$, схема на рисунке 1.6, *а* не будет корректной. Правильный вид схемы показан на рисунке 1.6, *б*.



а *б*

Рис. 1.6. Схемы ЛРС для полинома $h(x) = x^4 + x^3 + x^2 + 1$ в некорректном (*а*) и правильном (*б*) видах

ЛРС может быть построен и в случае, если в цепи обратной связи вместо схем неравнозначности включить схемы равнозначности. В этом случае запрещенной комбинацией будет комбинация, состоящая из одних единиц («111…1»).

Другая разновидность построения ЛРС – схема Галуа, когда сумматоры по модулю 2 включены между ячейками памяти (рис. 1.7).

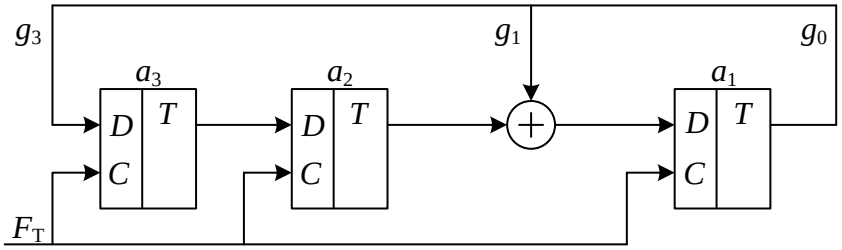


Рис. 1.7. Пример схемы ЛРС с сумматором по модулю 2 между ячейками памяти

В отличие от схемы Фибоначчи результат сложения записывается в следующую за сумматором по модулю 2 ячейку, а новый выходной бит записывается старшую ячейку. Нумерация отводов и ячеек памяти производится справа налево, а характеристический полином имеет вид:

$$g(x) = g_3 \cdot x^3 + g_1 \cdot x^1 + g_0 \cdot x^0 = x^3 + x + 1.$$

Таким образом, если генерируемый бит равен нулю, то все биты в ячейках сдвигаются вправо без изменений; если генерируемый бит равен единице, то биты отвода меняют свое значение на противоположное и все биты сдвигаются вправо.

Реализация ЛРС по схеме Галуа дает выигрыш в производительности, так как все операции сложения по модулю 2 посредством распараллеливания можно выполнить за одно действие, а не последовательно одна за другой, как в схеме Фибоначчи.

И схема Фибоначчи, и схема Галуа ЛРС, описываемого с помощью какого-либо характеристического полинома, генерируют одинаковые, но смещенные по времени одна относительно другой последовательности.

При рассмотрении свойств ЛРС особое внимание уделяют следующим двум основным свойствам полиномов обратных связей.

1. Полином $h(x)$ называется *неприводимым*, если его нельзя представить в виде произведения двух или более полиномов ненулевой степени.

Перемножение или сложение коэффициентов полиномов должно осуществляться по модулю 2.

Например, полином $h(x) = x^2 + 1$ приводим, так как

$$(x+1) \cdot (x+1) = x^2 + x + x + 1 = x^2 + 1,$$

а полином $h(x) = x^3 + x + 1$ является неприводимым.

В натуральном ряду чисел имеются аналоги неприводимых полиномов – простые числа (3, 5, 7, 11, 13 и т. д.).

2. Неприводимый полином называется *примитивным*, если он делит без остатка многочлен вида $x^k + 1$, где $k = 2^n - 1$, и не делит ни один многочлен вида $x^z + 1$, где $z < 2^n - 1$.

Для каждой степени n имеется один или более примитивных полиномов. В настоящее время построены таблицы неприводимых примитивных полиномов.

Если $h(x)$ примитивный, то примитивным является и двойственный ему полином $h'(x)$.

Таким образом, любой ЛРС можно математически описать с помощью характеристических полиномов $h(x)$.

Вопрос 2. Свойства выходных последовательностей линейных регистров сдвига

В настоящее время известно множество свойств выходных последовательностей ЛРС, однако важнейшими из них при построении функциональных узлов средств криптографической защиты информации, техники связи и других устройств являются следующие.

1. *Свойство детерминированности*.

Символы выходной последовательности ЛРС, начиная с n-го такта, полностью определяются своими предыдущими значениями. Это вытекает из рекуррентного соотношения

$$B_i = \sum_{k=1}^{n} h_{n-k} \times B_{i-k};\ i = n, n+1, n+2, \ldots .$$

2. *Свойство периодичности*.

Период ЛРС – минимальная длина получаемой рекуррентной последовательности до начала ее повторения. Период ЛРС зависит от полинома, на основе которого он строится.

Если число разрядов ЛРС n, то максимально возможное число состояний ЛРС составляет 2^n. Учитывая, что одно состояние ЛРС является запрещенным, максимальный период линейной рекуррентной последовательности ЛРС равен:

$$T = 2^n - 1.$$

Линейная рекуррентная последовательность максимального периода может быть сформирована ЛРС, характеристический полином которого является неприводимым.

3. *Свойство группового сложения*.

Результат суммирования по модулю 2 любых двух выходных последовательностей одного ЛРС, получаемых при разных начальных заполнениях, является выходной последовательностью этого же ЛРС с другим начальным заполнением, которое равно сумме исходных. Например, для ЛРС, построенного на основе характеристического многочлена $h(x) = x^3 + x + 1$ (рис. 1.2), выходные последовательности при разных начальных заполнениях приведены в таблице 2.1.

Таблица 2.1

Начальные заполнения ЛРС	Выходные последовательности
0 0 1	1 0 0 1 0 1 1
1 1 0	0 1 1 1 0 0 1
1 1 1	1 1 1 0 0 1 0

4. *Свойство сдвига*.

Циклический сдвиг выходной последовательности ЛРС есть его же выходная последовательность при другом начальном заполнении (табл. 2.1):

$$1\,0\,0\,1\,0\,1\,1 \;\rightarrow\; 1\,1\,1\,0\,0\,1\,0.$$

5. *Свойство баланса*.

Любая последовательность максимального периода, формируемая ЛРС, содержит 2^{n-1} единиц и $2^{n-1}-1$ нулей (табл. 1.1).

6. *Свойство «окна»*.

Если по выходной последовательности максимальной длины перемещать «окно» шириной n элементов, то на периоде ЛРС каждая из возможных комбинаций длины n будет зафиксирована только один раз.

7. *Свойство серий*.

Серией называется последовательность одинаковых элементов. Любая выходная последовательность максимальной длины имеет:

– половину всех серий длины в один знак;

– четверть всех серий длины в два знака;

– одну восьмую всех серий длины в три знака и так далее, пока доли дают целое число.

Например, для последовательности, формируемой ЛРС на основе полинома $h(x) = x^4 + x + 1$ (рис. 1.2), {1 0 0 0 1 0 0 1 1 0 1 0 1 1 1} количество серий длиной в один знак («1») – 8, длиной в два знака («10», «01») – 4, длиной в три знака («001», «010», «011», «100») – 2, длиной в четыре знака – 1.

Следует отметить, что одна из первых формулировок основополагающих статистических свойств периодических псевдослучайных последовательностей была представлена Соломоном Голомбом и получила известность как три постулата Голомба, первые два из которых соответствуют описанию свойств 5 и 7, а третий постулат раскрывается с помощью автокорреляционной функции от значения сдвига относительно друг друга двух копий одной и той же последовательности, результат вычисления которой должен принимать лишь два значения.

8. *Свойство однозначной определяемости многочлена обратной связи по выходной последовательности ЛРС*.

Если известна степень n примитивного полинома, но не известны его коэффициенты, то они могут быть однозначно определены по любым $2n$ соседним элементам его выходной последовательности. Поиск коэффициентов h_i, $i = 1,..., n-1$ характеристического полинома сводится к решению системы n однородных линейных уравнений с n неизвестными. Ее решение потребует около n^3 операций типа сложение, умножение. Существуют алгоритмы

проверки любой двоичной последовательности на рекуррентность, которые позволяют найти коэффициенты полинома $h(x)$ при неизвестной длине ЛРС (например, алгоритм Берлекэмпа–Мэсси).

Свойство 1 используется при построении систем синхронизации (например, при реализации анализаторов).

Свойство 2 используется в системах связи с циклическими корректирующими кодами для построения кодеров и декодеров.

С целью улучшения криптографических свойств получаемых псевдослучайных последовательностей и для уменьшения преобладаний «1» или «0» используется свойство 3.

Свойство 4 используется для построения на основе ЛРС логических сумматоров многоразрядных двоичных чисел.

Свойства 5–7 выходной последовательности ЛРС весьма близки к аналогичным свойствам случайной двоичной последовательности, поэтому такие последовательности обычно называются псевдослучайными, а ЛРС используются для построения датчиков псевдослучайных чисел.

Свойство 8, которое является следствием линейности ЛРС, не позволяет использовать его непосредственно в качестве генератора гаммы, поскольку оно противоречит третьему требованию, предъявляемому к системам гарантированной стойкости. Поэтому при формировании гаммы необходимо сохранить полезные свойства ЛРС, но исключить предсказуемость элементов его выходной последовательности. На практике для увеличения аналитической сложности выходной последовательности ЛРС используется *функция усложнения*, реализуемая нелинейными узлами усложнения (НУУ), или нелинейными криптографическими узлами.

Заключительная часть

– напомнить изученные вопросы и цели занятия;

– подвести итоги занятия, определить полноту достижения целей занятия.

Контрольные вопросы

1. Определение линейного регистра сдвига.
2. Схема линейного регистра сдвига.
3. Описание линейного регистра сдвига с помощью многочлена.
4. Построение линейного регистра сдвига по прямому и двойственному многочлену.
5. Неприводимые и примитивные многочлены.
6. Свойство детерминированности.
7. Свойство периодичности.
8. Свойство группового сложения.
9. Свойство сдвига.
10. Свойство баланса.
11. Свойство «окна».
12. Свойство серий.
13. Свойство взаимоопределяемости коэффициентов.

Рекомендуемая литература:

1. Алферов, А. П. Основы криптографии : учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – Москва : Гелиос АРВ, 2002. – 480 с.

2. Васильева, И. Н. Криптографические методы защиты информации. Учебник и практикум для академического бакалавриата / И. Н. Васильева. – Москва : Юрайт, 2016. – 349 с.