УДК 681.322

**В.Д. Кротов, В.В. Мартинюк, В.В. Малих**

# ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ЛІНІЙНИХ РЕКУРЕНТНИХ РЕГІСТРІВ. МЕТОДИКА ЗНАХОДЖЕННЯ КОЕФІЦІЄНТІВ ПРИМІТИВНОГО ПОЛІНОМУ ЗА 2n СУМІЖНИМИ ЕЛЕМЕНТАМИ ЙОГО ВИХІДНОЇ ПОСЛІДОВНОСТІ

У даній статті запропонована методика знаходження коефіцієнтів примітивного поліному n за будь-якими 2n суміжними елементами його вихідної послідовності. Ця методика дозволить розширити знання студентів, зробить можливим моделювання ними процесів шифрування, дасть можливість в навчальних цілях використовувати отримані знання у розробці електронних шифроутворюючих пристроїв та проведенні аналізу стійкості систем шифрування побудованих на ЛРР. Матеріал на цю тему в якійсь мірі описаний в сучасній російській та зарубіжній літературі, але того обсягу, систематизації, яка необхідна для доступного викладення студентам, ще немає. Причиною цього, на наш погляд, є відсутність доступного та достатньо повного показу властивостей лінійних рекурентних регістрів та регістрових послідовностей у відкритих публікаціях.

***Ключові слова:*** лінійні рекурентні регістри, криптоаналіз систем шифрування, регістрові послідовності.

## Вступ

Лінійні рекурентні регістри (ЛРР), які ще називають лініями затримки із зворотним зв'язком або одноканальними лініями затримки та регістрові послідовності (ще їх називають псевдовипадкові послідовності, псевдошумові послідовності, *m*-послідовності) вже достатньо давно відомі та використовуються для виміру дальності в радіолокації, для кодування мови, пошуку помилок, моделювання процесів, модуляції, синхронізації та іншого [1-5].

Можливості використання лінійних рекурентних регістрів та регістрових послідовностей в криптології відомі широко, проте їх властивості не висвітлені так, як вони того заслуговують.

Актуальність даної статті – це можливість використання в навчальних цілях викладеного матеріалу при проведенні первинного криптоаналізу систем шифрування, які побудовані на ЛРР.

Мета статті полягає в систематизації властивостей лінійних рекурентних регістрів, за якими їх можна відновити, використовуючи 2n суміжні елементи вихідної послідовності, та показі цієї методики на простих прикладах.

Це дасть можливість застосувати підготовлений матеріал при проведенні занять з теоретичних основ криптології, що, в свою чергу, допоможе студентам (курсантам) швидше і якісніше засвоїти поданий матеріал.

## Постановка задачі

ЛРР – це перемикаюча схема, яка призначена для утворення псевдовипадкових послідовностей (рис. 1) і складається із чарунок пам'яті та суматорів по модулю два, об`єднаних зворотніми зв`язками.

Якщо $h_i = 1$ – зворотний зв'язок є, а якщо $h_i = 0$ – зворотнього зв'язку немає.

Довжиною ЛРР називають число, яке дорівнює кількості елементів пам'яті, що входять до нього.

В момент, коли почнуть поступати імпульси тактової частоти від ГТЧ, вихідний символ кожного розряду ЛРР приймає те значення, яке перед цим знаходилось у попередній чарунці пам'яті**.**

Через розімкнений зворотній зв'язок в чарунки пам'яті ЛРР попередньо подається двійкова послідовність початкового заповнення $a_{0,}\ a_{1,\ldots,}\ a_{n-1.,}$ після чого зворотній зв'язок перемикається. При надходженні першого імпульсу тактової частоти вміст усіх чарунок пам'яті зсовується на один крок праворуч, а з самої крайньої чарунки зчитується перший елемент вихідної послідовності $b_0=a_0$.

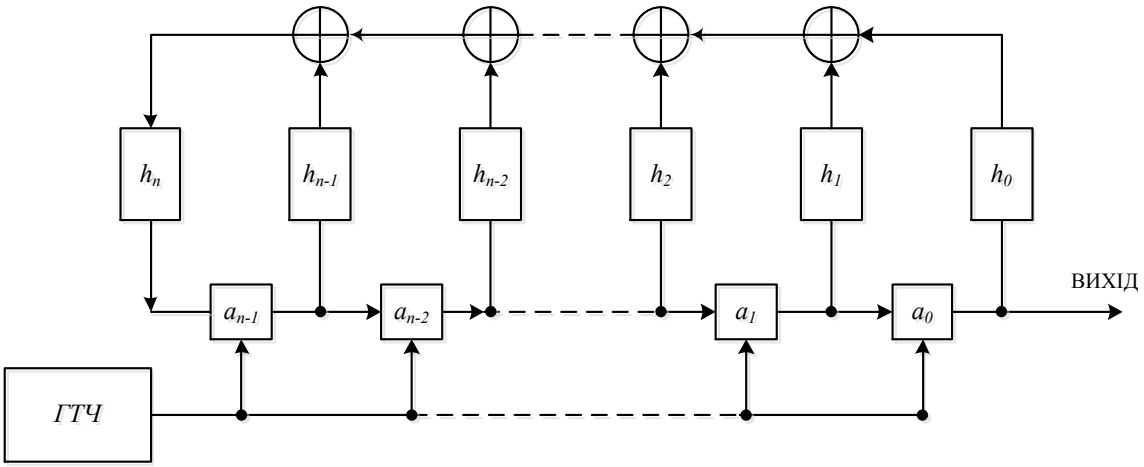


Рис.1. Структурна схема ЛРР.

$a_i$ – чарунки пам`яті;
$h_i$ – зворотні зв'язки;
$\oplus$ – суматори за mod 2;
ГТЧ – генератор тактової частоти (в усіх наступних схемах існування ГТЧ береться до уваги, але не зображується).

Одночасно відбувається додавання вихідних елементів, які знаходяться в тих чарунках пам'яті, котрі з'єднані зворотнім зв'язком з суматорами та результат суми записується в (n-1) чарунку пам'яті. При надходженні наступних імпульсів тактової частоти робота ЛРР проходить аналогічним чином, причому генерується неосяжна вихідна послідовність $b_i$, яку можливо описати наступним рекурентним співвідношенням [6]:

$$b_i = \begin{cases} a_i, & i = 0,1,...,n-1; \\ \sum_{k=1}^{n} b_{i-k} h_{n-k} \pmod 2 & i = n, n+1 \end{cases} \quad (1)$$

З даного співвідношення видно, що вихідна послідовність ЛРР повністю визначається початковим заповненням $a_0, a_{1,...,} a_{n-1}$ та відводами зворотніх зв'язків $h_i$ (i=1,2,…,n),

$h_i$ =(0,1), причому для ЛРР довжини n завжди $h_0$ =1та $h_n$=1.

Кожному ЛРР довжини n можна співставити поліном зворотніх зв'язків h(x) з двійковими коефіцієнтами та навпаки.

Для відтворення псевдовипадкової послідовності довжини, яка має період $T = 2^n - 1$, потрібен примітивний багаточлен h(x) ступеня n. Як приклад, розглянемо багаточлен у якого $n = 4$:

$$h(x) = x^4 + x + 1 \quad (2)$$

Цьому багаточлену відповідає регістр зсуву з зворотним зв'язком, показаний на рис.2.

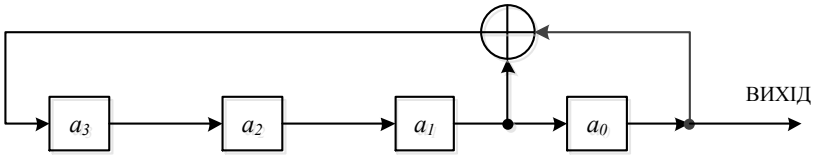


Рис.2. Регістр зсуву з зворотнім зв'язком, який відповідає багаточлену $h(x) = x^4 + x + 1$.

У загальному випадку регістр зсуву складається з n чарунок (запам'ятовуючих елементів або тригерів), кожна з яких може містити двійкові 0 або 1. В момент часу

визначеного тактовою частотою, вміст усіх запам'ятовуючих чарунок зсовується на один крок вправо, причому вміст запам'ятовуючих чарунок, котрі з`єднані зворотнім зв`язком із суматорами, сумується і поступає в крайню ліву чарунку. Сума розраховується за mod 2, так що знак ⊕ на рис. 2 відповідає суматору за mod 2, вихід якого визначається умовами 0⊕0=0, 1⊕1=0 та 0⊕1=1, 0⊕1=1.

Таблиця 1

Вміст чарунок пам'яті ЛРР при різних тактах і значеннях вихідних елементів та початковому двійковому заповненні 0001

| № такту | Стан регістра | | | | Вихід |
|---|---|---|---|---|---|
| | $a_3$ | $a_2$ | $a_1$ | $a_0$ | $b_i$ |
| 0 | 0 | 0 | 0 | 1 | – |
| 1 | 1 | 0 | 0 | 0 | 1 |
| 2 | 0 | 1 | 0 | 0 | 0 |
| 3 | 0 | 0 | 1 | 0 | 0 |
| 4 | 1 | 0 | 0 | 1 | 0 |
| 5 | 1 | 1 | 0 | 0 | 1 |
| 6 | 0 | 1 | 1 | 0 | 0 |
| 7 | 1 | 0 | 1 | 1 | 0 |
| 8 | 0 | 1 | 0 | 1 | 1 |
| 9 | 1 | 0 | 1 | 0 | 1 |
| 10 | 1 | 1 | 0 | 1 | 0 |
| 11 | 1 | 1 | 1 | 0 | 1 |
| 12 | 1 | 1 | 1 | 1 | 0 |
| 13 | 0 | 1 | 1 | 1 | 1 |
| 14 | 0 | 0 | 1 | 1 | 1 |
| 15 | 0 | 0 | 0 | 1 | 1 |
| 16 | 1 | 0 | 0 | 0 | 1 |

**Обмеження**

Взагалі ЛРР володіють багатою кількістю різних властивостей, та в цій статті буде розглянуто лише ті, які будуть необхідні для визначення коефіцієнтів примітивного поліному та побудування ЛРР.

**Основна частина**

**Загальні властивості регістрів зсуву та регістрових послідовностей**

*Властивість 1.* Якщо поліном зворотних зв'язків має ступінь *n* і є *примітивним*, то при будь-якому початковому заповненні ЛРР, відмінному від нульового, період вихідної послідовності буде дорівнювати $2^n - 1$.

Як доказ, візьмемо примітивний багаточлен $h(x) = x^4 + x + 1$. Йому відповідає лінійний рекурентний регістр, зображений на рис. 2 та таблиця істинності (табл. 1) [4, 6]. Період вихідної послідовності $T=2^n - 1=2^4 - 1=15$ де, n - це максимальна ступінь поліному. Таким чином, з таблиці 1 видно, що через 15 тактів генератора тактової частоти вміст ЛРР повторюється, отже, і вихідна послідовність буде повторюватися. Якщо змінити початковий стан ЛРР, то період від цього аж ніяк не зміниться. Таким чином ми бачимо, що при будь-якому початковому заповненні, окрім нульового, період вихідної послідовності буде дорівнювати $2^n - 1$.

При нульовому початковому заповненні період вихідної послідовності може дорівнювати і $2^n$, але регістри з таким початковим заповненням не знайшли використання в системах зв'язку, оскільки ЛРР з таким початковим заповненням буде генерувати послідовність з самих нулів.

Ця властивість правильна для примітивних поліномів та ненульових початкових станів ЛРР.

*Властивість 2.* Поелементна сума періодів 2-х вихідних послідовностей одного й того ж самого ЛРР отриманих з різних початкових заповнень також є вихідною послідовністю цього ЛРР, отриманою за його початковим заповненням, що дорівнює сумі початкових заповнень.

Перевіримо цю властивість на лінійному рекурентному регістрі, побудованому на основі поліному $h(x) = x^3 + x + 1$.

Таблиця 2

Вміст чарунок пам'яті ЛРР при різних тактах і значення вихідних елементів при початкових двійкових заповненнях 111

| № такту | Стан регістра | | | Вихід | |
|---|---|---|---|---|---|
| | $a_2$ | $a_1$ | $a_0$ | $в_i$ | |
| 0 | 1 | 1 | 1 | – | |
| 1 | 0 | 1 | 1 | 1 | $в_0$ |
| 2 | 0 | 0 | 1 | 1 | $в_1$ |
| 3 | 1 | 0 | 0 | 1 | $в_2$ |
| 4 | 0 | 1 | 0 | 0 | $в_3 = B$ |
| 5 | 1 | 0 | 1 | 0 | $в_4$ |
| 6 | 1 | 1 | 0 | 1 | $в_5$ |
| 7 | 1 | 1 | 1 | 0 | $в_6$ |
| 8 | 0 | 1 | 1 | 1 | |
| 9 | 0 | 0 | 1 | 1 | |
| 10 | 1 | 0 | 0 | 1 | |

Таблиця 3

Вміст чарунок пам'яті ЛРР при різних тактах і значення вихідних елементів при початкових двійкових заповненнях 100

| № такту | Стан регістра | | | Вихід | |
|---|---|---|---|---|---|
| | $a_2$ | $a_1$ | $a_0$ | $в_i$ | |
| 0 | 1 | 0 | 0 | – | |
| 1 | 0 | 1 | 0 | 0 | $в_0$ |
| 2 | 1 | 0 | 1 | | $в_1$ |
| 3 | 1 | 1 | 0 | 1 | $в_2$ |
| 4 | 1 | 1 | 1 | 0 | $в_3 = B'$ |
| 5 | 0 | 1 | 1 | 1 | $в_4$ |
| 6 | 0 | 0 | 1 | 1 | $в_5$ |
| 7 | 1 | 0 | 0 | 1 | $в_6$ |
| 8 | 0 | 1 | 0 | 0 | |
| 9 | 1 | 0 | 1 | 0 | |
| 10 | 1 | 1 | 0 | 1 | |

Для порівняння візьмемо вихідні послідовності з $b_0$ по $b_6$ (використаємо дані табл. 2 і табл. 3) [4, 6].

Перевіримо, чи буде лінійний рекурентний регістр, побудований на основі поліному $h(x) = x^3 + x + 1$ при початковому заповненні A″, давати вихідну послідовність B″.

Початкове заповнення

| | | | | | |
|---|---|---|---|---|---|
| 1 1 1 | | A | 1 1 1 0 0 1 0 | | B |
| $\oplus$ | | | $\oplus$ | | |
| 1 0 0 | | A′ | 0 0 1 0 1 1 1 | | B′ |
| 0 1 1 | $\rightarrow$ | A″ | 1 1 0 0 1 0 1 | $\rightarrow$ | B″ |

Отже $B \oplus B' = B''$.

Таким чином, ми отримали повну відповідність теорії та довели її на практиці, що показано в табл. 4.

Таблиця 4

Вміст чарунок пам'яті ЛРР при різних тактах і значення вихідних елементів при початкових двійкових заповненнях 011

| № такту | Стан регістра | | | Вихід | |
|---|---|---|---|---|---|
| | $a_2$ | $a_1$ | $a_0$ | $в_i$ | |
| 0 | 0 | 1 | 1 | – | |
| 1 | 0 | 0 | 1 | 1 | |
| 2 | 1 | 0 | 0 | 1 | |
| 3 | 0 | 1 | 0 | 0 | |
| 4 | 1 | 0 | 1 | 0 | $= B''$ |
| 5 | 1 | 1 | 0 | 1 | |
| 6 | 1 | 1 | 1 | 0 | |
| 7 | 0 | 1 | 1 | 1 | |

**Властивості послідовностей, які дають можливість визначити коефіцієнти примітивного поліному та побудувати ЛРР**

*Властивість 3.* Якщо відомий ступінь примітивного поліному n, але не відомі його коефіцієнти, то їх можливо однозначно визначити за будь-якими 2n суміжними елементами його вихідної послідовності.

Дійсно, якщо $b_{i-n}, b_{i-n-1}, \ldots, b_i, b_{i+1}, \ldots, b_{i+n-2}, b_{i+n-1}$ - будь-які 2n суміжні елементи вихідної послідовності ЛРР, то із співвідношення (1) отримуємо систему із n лінійних однорідних рівнянь з n невідомими:

$$\begin{cases} b_i = b_{i-1}h_{n-1} \oplus b_{i-2}h_{n-2} \oplus \ldots \oplus b_{i-n+1}h_1 \oplus b_{i-n}h_0; \\ b_{i+1} = b_i h_{n-1} \oplus b_{i-1}h_{n-2} \oplus \ldots \oplus b_{i-n}h_1 \oplus b_{i-n+1}h_0; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{i+n-2} = b_{i+n-3}h_{n-1} \oplus b_{i-1}h_{n-2} \oplus \ldots \oplus b_{i-n+2}h_1 \oplus b_{i-n+1}h_0; \\ b_{i+n-1} = b_{i+n-2}h_{n-1} \oplus b_{i+n-3}h_{n-2} \oplus \ldots \oplus b_i h_1 \oplus b_{i-1}h_0; \end{cases} \quad (3)$$

Рішення цієї системи відносно невідомих $h_0, h_1, \ldots, h_{n-1}$ дає поліном зворотних зв'язків $h$ (x), тобто саме структуру ЛРР.

Наприклад:

Нехай дано n=5, та маємо 2n елементів вихідної послідовності:

$b_0 b_1 \ldots \quad b_{30}$

0 0 0 0 1 1 0 0 1 0

Знайдемо поліном зворотних зв'язків на основі якого збудований ЛРР, для цього складаємо систему з n рівнянь з n невідомими та вирішуємо її методом підстановки за допомогою співвідношення (3):

$$\begin{cases} b_5 = b_4h_4 \oplus b_3h_3 \oplus b_2h_2 \oplus b_1h_1 \oplus b_0h_0; \\ b_6 = b_5h_4 \oplus b_4h_3 \oplus b_3h_2 \oplus b_2h_1 \oplus b_1h_0; \\ b_7 = b_6h_4 \oplus b_5h_3 \oplus b_4h_2 \oplus b_3h_1 \oplus b_2h_0; \\ b_8 = b_7h_4 \oplus b_6h_3 \oplus b_5h_2 \oplus b_4h_1 \oplus b_3h_0; \\ b_9 = b_8h_4 \oplus b_7h_3 \oplus b_6h_2 \oplus b_5h_1 \oplus b_4h_0; \end{cases} \Rightarrow \begin{cases} 1 = h_4; \\ 0 = h_4 \oplus h_3; \\ 0 = h_3 \oplus h_2; \\ 1 = h_2 \oplus h_1; \\ 0 = h_4 \oplus h_1 \oplus h_0; \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} h_4 = 1; \\ h_4 = h_3 = 1; \\ h_3 = h_2 = 1; \\ h_1 = h_2 \oplus 1 = 0; \\ h_0 = h_4 \oplus h_1 = 1; \end{cases} \Rightarrow \begin{cases} h_0 = 1 \to 1; \\ h_1 = 0 \to x\ ; \\ h_2 = 1 \to x^2; \\ h_3 = 1 \to x^3; \\ h_4 = 1 \to x^4; \end{cases}$$

Таким чином поліном зворотних зв'язків має вигляд: $h(x) = x^5 + x^4 + x^3 + x^2 + 1$.

Якщо ступінь примітивного поліному n та, відповідно, довжина ЛРР невелика, коефіцієнти поліному зворотних зв'язків $h$ (x) знаходяться легко, бо ми маємо справу з невеликою кількістю невідомих у співвідношенні (3). Також на спрощення рішення системи з n рівнянь з n невідомими впливає кількість нулів у 2n суміжних елементах вихідної послідовності. Якщо нулів більше, система рівнянь спрощується, якщо більшість одиниць у вихідній послідовності, то система рівнянь ускладнюється.

Так повстала проблема, яким чином вирішувати систему рівнянь при великих значеннях ступеню примітивного поліному n, та при великій кількості одиниць у вихідній послідовності. Вирішити цю проблему допоможе методика представлена нижче.

**Алгоритм реалізації**

Наприклад :

Нехай дано n=9, та маємо 2n елементів вихідної послідовності:

$b_0 b_1 \ldots \quad b_{17}$

1 1 1 1 0 0 0 0 1 1 1 1 1 0 1 0 0 0 1

Знайдемо поліном зворотніх зв`язків на основі якого збудований ЛРР, для цього складаємо систему з n рівнянь з n невідомими за допомогою співвідношення (3):

$$\begin{cases} b_9 = b_8h_8 \oplus b_7h_7 \oplus b_6h_6 \oplus b_5h_5 \oplus b_4h_4 \oplus b_3h_3 \oplus b_2h_2 \oplus b_1h_1 \oplus b_0h_0; \\ b_{10} = b_9h_8 \oplus b_8h_7 \oplus b_7h_6 \oplus b_6h_5 \oplus b_5h_4 \oplus b_4h_3 \oplus b_3h_2 \oplus b_2h_1 \oplus b_1h_0; \\ b_{11} = b_{10}h_8 \oplus b_9h_7 \oplus b_8h_6 \oplus b_7h_5 \oplus b_6h_4 \oplus b_5h_3 \oplus b_4h_2 \oplus b_3h_1 \oplus b_2h_0; \\ b_{12} = b_{11}h_8 \oplus b_{10}h_7 \oplus b_9h_6 \oplus b_8h_5 \oplus b_7h_4 \oplus b_6h_3 \oplus b_5h_2 \oplus b_4h_1 \oplus b_3h_0; \\ b_{13} = b_{12}h_8 \oplus b_{11}h_7 \oplus b_{10}h_7 \oplus b_9h_5 \oplus b_8h_4 \oplus b_7h_3 \oplus b_6h_2 \oplus b_5h_1 \oplus b_4h_0; \\ b_{14} = b_{13}h_8 \oplus b_{12}h_7 \oplus b_{11}h_6 \oplus b_{10}h_5 \oplus b_9h_4 \oplus b_8h_3 \oplus b_7h_2 \oplus b_6h_1 \oplus b_5h_0; \\ b_{15} = b_{14}h_8 \oplus b_{13}h_7 \oplus b_{12}h_6 \oplus b_{11}h_5 \oplus b_{10}h_4 \oplus b_9h_3 \oplus b_8h_2 \oplus b_7h_1 \oplus b_6h_0; \\ b_{16} = b_{15}h_8 \oplus b_{14}h_7 \oplus b_{13}h_6 \oplus b_{12}h_5 \oplus b_{11}h_4 \oplus b_{10}h_3 \oplus b_9h_2 \oplus b_8h_1 \oplus b_7h_0; \\ b_{17} = b_{16}h_8 \oplus b_{15}h_7 \oplus b_{14}h_6 \oplus b_{13}h_5 \oplus b_{12}h_4 \oplus b_{11}h_3 \oplus b_{10}h_2 \oplus b_9h_1 \oplus b_8h_0; \end{cases} \quad (4)$$

Спростимо систему рівнянь підставивши замість $b_0, b, \ldots b_{17}$ відповідні двійкові елементи вихідної послідовності у співвідношення (4).

$$\begin{cases} 1 = h_8 \oplus h_3 \oplus h_2 \oplus h_1 \oplus h_0; \\ 1 = h_8 \oplus h_7 \oplus h_2 \oplus h_1 \oplus h_0; \\ 1 = h_8 \oplus h_7 \oplus h_6 \oplus h_1 \oplus h_0; \\ 1 = h_8 \oplus h_7 \oplus h_6 \oplus h_5 \oplus h_0; \\ 0 = h_8 \oplus h_7 \oplus h_6 \oplus h_5 \oplus h_4; \\ 1 = h_7 \oplus h_6 \oplus h_5 \oplus h_4 \oplus h_3; \\ 0 = h_8 \oplus h_6 \oplus h_5 \oplus h_4 \oplus h_3 \oplus h_2; \\ 0 = h_7 \oplus h_5 \oplus h_4 \oplus h_3 \oplus h_2 \oplus h_1; \\ 0 = h_6 \oplus h_4 \oplus h_3 \oplus h_2 \oplus h_1 \oplus h_0; \end{cases} \quad (5)$$

Отримавши спрощену систему рівнянь, перед нами повстає проблема, яким чином вирішувати цю систему рівнянь при великій кількості невідомих $h_0, h_1, \ldots, h_{n-1}$. Вирішити цю проблему допоможе методика, яка базується на властивості 2 ЛРР. Тобто, спробуємо складати за mod 2 по два рівняння з співвідношення (5) таким чином, щоб спростити рівняння і зменшити кількість невідомих, беручи до уваги те, що завжди, $h_0 = 1$ та $h_n = 1$.

При складанні за mod 2 двох рівнянь однакові коефіцієнти знищуються, а залишаються лише ті, які не повторюються.

Складаємо 4 та 5 рівняння з співвідношення (5) та отримуємо:

$$\begin{matrix} h_8 \oplus h_7 \oplus h_6 \oplus h_5 \oplus h_0 = 1 \\ \oplus \\ h_8 \oplus h_7 \oplus h_6 \oplus h_5 \oplus h_4 = 0 \end{matrix} \Rightarrow h_4 \oplus h_0 = 1 \Rightarrow h_4 = 0, \text{ бо } h_0 = 1 \text{ - завжди.}$$

Ці дії призвели до того, що ми отримали коефіцієнт $h_4 = 0$.

Складаємо 4 та 6 рівняння з співвідношення (5) та отримуємо:

$$\begin{matrix} h_8 \oplus h_7 \oplus h_6 \oplus h_5 \oplus h_0 = 1 \\ \oplus \\ h_7 \oplus h_6 \oplus h_5 \oplus h_4 \oplus h_3 = 0 \end{matrix} \Rightarrow h_8 \oplus h_4 \oplus h_3 \oplus h_0 = 0 \Rightarrow h_8 \oplus 1 \oplus h_3 \oplus 1 = 0 \Rightarrow h_8 \oplus h_3 = 1$$

Складаємо 6 та 8 рівняння з співвідношення (5) та отримуємо:

$$\begin{matrix} h_7 \oplus h_6 \oplus h_5 \oplus h_4 \oplus h_3 = 1 \\ \oplus \\ h_7 \oplus h_5 \oplus h_4 \oplus h_3 \oplus h_2 \oplus h_1 = 0 \end{matrix} \Rightarrow h_6 \oplus h_2 \oplus h_1 = 1$$

Поки що спрощення не дало нам нових коефіцієнтів.

Складаємо 1 та 2 рівняння з співвідношення (5) та отримуємо:

$$\begin{matrix} h_8 \oplus h_3 \oplus h_2 \oplus h_1 \oplus h_0 = 1 \\ \oplus \\ h_8 \oplus h_7 \oplus h_2 \oplus h_1 \oplus h_0 = 1 \end{matrix} \Rightarrow h_7 \oplus h_3 = 0$$

Складаємо 3 та 4 рівняння з співвідношення (5) та отримуємо:

$$\begin{array}{l} h_8 \oplus h_7 \oplus h_6 \oplus h_1 \oplus h_0 = 1 \\ \oplus \\ h_8 \oplus h_7 \oplus h_6 \oplus h_5 \oplus h_0 = 1 \end{array} \quad \Rightarrow \quad h_5 \oplus h_1 = 0$$

Складаємо 7 та 9 рівняння з співвідношення (5) та отримуємо:

$$\begin{array}{l} h_8 \oplus h_6 \oplus h_5 \oplus h_4 \oplus h_3 \oplus h_2 = 0 \\ \oplus \\ h_6 \oplus h_4 \oplus h_3 \oplus h_2 \oplus h_1 \oplus h_0 = 0 \end{array} \quad \Rightarrow \quad h_8 \oplus h_5 \oplus h_1 \oplus h_0 = 0$$

Складаємо отримані результати спрощення:

$$\begin{array}{l} h_5 \oplus h_1 = 0 \\ \oplus \\ h_8 \oplus h_5 \oplus h_1 \oplus h_0 = 0 \end{array} \quad \Rightarrow \quad h_8 \oplus h_0 = 0$$

Оскільки $h_0 = 1$,то також і $h_8 = 1$. Тоді з $h_8 \oplus h_3 = 1 \Rightarrow h_3 = 0$. Якщо $h_3 = 0$ то з $h_7 \oplus h_3 = 0 \Rightarrow h_7 = 0$

Складаємо 6 та 7 рівняння з співвідношення (5) та отримуємо:

$$\begin{array}{l} h_7 \oplus h_6 \oplus h_5 \oplus h_4 \oplus h_3 = 1 \\ \oplus \\ h_8 \oplus h_6 \oplus h_5 \oplus h_4 \oplus h_3 \oplus h_2 = 0 \end{array} \quad \Rightarrow \quad h_8 \oplus h_7 \oplus h_2 = 1 \Rightarrow h_2 = 0$$

виходячи з того, що $h_8 = 1$та $h_7 = 0$.

Складаємо 2 та 3 рівняння з співвідношення (5) та отримуємо:

$$\begin{array}{l} h_8 \oplus h_7 \oplus h_2 \oplus h_1 \oplus h_0 = 1 \\ \oplus \\ h_8 \oplus h_7 \oplus h_6 \oplus h_1 \oplus h_0 = 1 \end{array} \quad \Rightarrow \quad h_6 \oplus h_2 = 0 \Rightarrow \text{так як } h_2 = 0 \text{ то і } h_6 = 0$$

З рівнянь $h_6 \oplus h_2 \oplus h_1 = 1 \Rightarrow h_1 = 1$, а з $h_5 \oplus h_1 = 0 \Rightarrow h_5 = 1$

Таким чином , ми знайшли усі коефіцієнти зворотніх зв`язків ЛРР, а саме:

$$h_0 = 1, h_1 = 1,\ h_2 = 0,\ h_3 = 0,\ h_4 = 0,\ h_5 = 1,\ h_6 = 0,\ h_7 = 0, h_8 = 1, h_9 = 1.$$

Тепер побудуємо сам ЛРР використовуючи отриманий поліном зворотних зв'язків:

$$h(x) = x^9 + x^8 + x^5 + x + 1 \qquad (6)$$

Регістр зсуву для цього поліному зворотніх зв'язків показаний на рис. 3. :

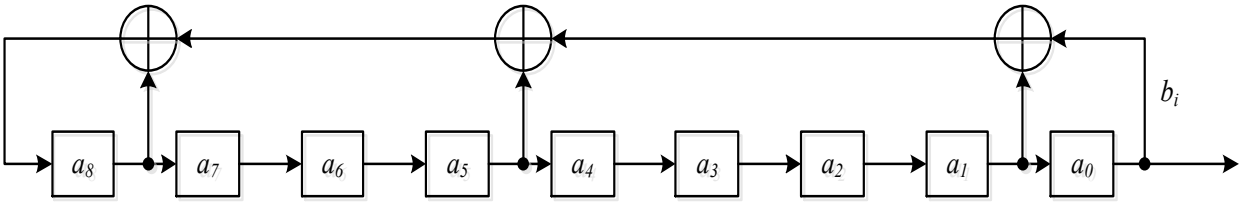


Рис.3. Регістр зсуву з зворотнім зв'язком, який відповідає багаточлену $h(x) = x^9 + x^8 + x^5 + x + 1$.

Таблиця 5

Вміст чарунок пам'яті цього ЛРР при різних тактах і значеннях вихідних елементів при початковому двійковому заповненні 100001111

| № такту | Стан регістра | | | | | | | | | Вихід |
|---|---|---|---|---|---|---|---|---|---|---|
| | $a_8$ | $a_7$ | $a_6$ | $a_5$ | $a_4$ | $a_3$ | $a_2$ | $a_1$ | $a_0$ | $b_i$ |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | - |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 2 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 3 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 4 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 5 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 6 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 7 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| 8 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 9 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 10 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 11 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 12 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 13 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 14 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 15 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| 16 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 17 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 18 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |

**Аналіз отриманих результатів**

Як видно з табл.5, вихідна послідовність повністю співпадає з тією, що була надана для пошуку коефіцієнтів поліному зворотних зв'язків. Таким чином, можна зробити висновки, що представлена в цій роботі методика для знаходження невідомих $h_0, h_1, \ldots, h_{n-1}$ примітивного поліному n за будь-якими 2n суміжними елементами його вихідної послідовності повністю працює та може бути використана студентами ( курсантами) під час лабораторної роботи при проведенні первинного криптоаналізу систем шифрування побудованих на ЛРР, в навчальних цілях.

Взагалі лабораторні роботи, які пов`язані з елементами первинного криптоаналізу найпростіших методів шифрування є дуже ефективними для розвитку здібностей абстрактного мислення при підготовці криптоаналітиків початкового рівня. Практичні знання властивостей лінійних рекурентних регістрів та регістрових послідовностей не тільки розширюють кругозір студентів (курсантів), але й роблять можливим моделювання ними процесів шифрування, дають можливість використовувати отримані знання у розробці електронних шифраторів, проведенні аналізу стійкості систем шифрування, в яких присутні ЛРР.

**Висновок**

Представлена методика на практиці доказує, що використовувати ЛРР в загальному вигляді при розробці електронних шифроутворюючих пристроїв неможливо.

ЛРР мають негативні властивості, які треба враховувати з метою їх усунення. Проте є наявними ряд позитивних характеристик, а саме:

максимально велика довжина періоду;
відсутність прихованих періодичностей;
статистична рівномірність.

**Список використаної літератури**

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайдер. – М.: Триумф, 2013. – 816 с.

2. Гайбидулин Э.М. Защита информации: учебное пособие / Э.М. Гайбидулин, А.С. Кшевецкий, А.И. Колыбельников. – М.: МФТИ, 2011. – 225 с.

3. Фомичев В.М. Дискретная математика и криптология; Курс лекций / В.М. Фомичев. – М.: Диалог, МИФИ, 2013. – 397 с.

4. Фомичев В.М. Методы дискретной математики в криптологии. / В.М. Фомичев. – М.: Диалог, МИФИ, 2010. – 424 с.

5. Баранов А.П. Математические основы информационной безопасности / А.П. Баранов, Н.П. Борисенко, П.Д. Зегжда, С.С. Корт, А.Г. Ростовцев. – О.: ВИПС, 1997.

6. Лидл Р. Конечные поля. Т. 1,2. / Р. Лидл, Г. Нидеррайтер. – М.: Мир, 1998.

Надійшла 15.04.2017 р. Рецензент: д.т.н., проф. Хорошко В.О.